ASSESSMENT OF THE CONTROLS AND SECURITY OF NARA CLASSIFIED SYSTEMS

OIG REPORT No. 04-10

March 31, 2004

Office of Inspector General

*****

National Archives and Records Administration

TABLE OF CONTENTS

AUDIT RESULTS

AUDIT RESULTS

ASSESSMENT OF THE CONTROLS AND SECURITY OF NARA CLASSIFIED SYSTEMS

BACKGROUND

As the national record keeper, NARA continues to receive more and more records that have been electronically created and maintained. NARA anticipates this trend will continue with exponential growth in the number of electronic records they will be expected to house and care for in the coming years. To deal with this inundation of electronic records, NARA has planned specific strategies for the maintenance, preservation, and accessibility of electronic records in order to continue to fulfill its mission as the nation's record keeper.

Classified information in NARA's custody is also stored and processed in electronic format on computer systems. These classified systems have specialized security needs and must be protected at a higher level than unclassified systems in order to protect against unauthorized disclosure as well as loss or modification. It is critical that NARA ensure that the appropriate security controls are applied to its classified systems or the safety of these systems and the information contained on these systems is at risk.

[redacted].

[redacted]

[redacted] we informed the Archivist that NARA had not designated a central point of management for these systems. Therefore, we were unable to obtain or identify a complete, up-to-date classified systems inventory. In addition, security responsibility for NARA classified systems was not under the purview of the Chief Information Officer (CIO). Rather, the individual system owners and the Space and Security Management Division (NAS) shared responsibility for the maintenance and security of NARA classified systems. These employees did not demonstrate to the OIG the IT expertise needed to ensure that adequate security has been implemented for each system.

OBJECTIVES, SCOPE, AND METHODOLOGY

The overall objective of the assessment was to determine whether NARA classified systems were adequately managed and secured. We incorporated audit steps designed to determine if NARA had developed and maintained a classified systems inventory. We identified the personnel responsible for these systems including their varying roles. We also determined if the classified systems were properly secured and complied with government and NARA security policies and guidelines.

AUDIT RESULTS

To accomplish our objectives, we interviewed key NARA personnel. We identified and examined applicable classified systems security regulations including those issued by NARA and those that preside government wide. We also intended to examine available pertinent systems security documentation including classified system security plans, certification and accreditation, risk assessments, security controls testing reports, contingency plans, etc. However, we did not complete this step because this documentation had not been developed or finalized for any of NARA's classified systems. While formal documentation did not exist, the auditors did selected one classified system to examine the level of security controls that had been applied to the system.

The fieldwork was performed intermittently from May 2003 through January 2004 at the Archives II facility in College Park, Maryland, in accordance with *Government Auditing Standards.*

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

- [redacted]

AUDIT RESULTS

In December 2002, NARA hired an information security officer whose position responsibilities included oversight of NARA classified computer systems operation and security. However, the information security officer who was hired lacked the technical expertise necessary to ensure that the security measures applied to NARA classified systems were adequate, appropriate, and cost effective. In addition, the information security officer was unaware of the body of security requirements governing federal classified systems.

The NARA Information Security Oversight Office (ISOO) in 32 CFR Part 2004, Classified National Security Information Directive No.1, instructs each agency to ensure that classified information electronically accessed, processed, stored, or transmitted is protected in accordance with policies[1] (see Appendix I) issued by the Committee on National Security Systems (CNSS)[2] and Director of Central Intelligence Directives (DCIDs).

One of the CNSS policies[3] requires all federal government departments and agencies to establish and implement programs that mandate the certification and accreditation (C&A) of national security systems[4] under their operational control. These C&A programs should ensure that information processed, stored, or transmitted by national security systems is adequately protected with respect to requirements for confidentiality, integrity, and availability. The C&A program is to be performed and documented by competent personnel at appropriate points throughout the total system life cycle.

The CNSS issued guidance[5] for implementing this C&A requirement referred to as the National Information Assurance Certification and Accreditation Process (NIACAP). The NIACAP establishes minimum national standards for certifying and accrediting national security systems including a standard national process, set of activities, general tasks, and a management structure. It applies to all U.S. Government Executive Branch departments, agencies, and their contractors and consultants.

The CNSS also issued a directive[6] requiring federal departments and agencies to develop and implement information systems security education, training, and awareness programs for national security systems as countermeasures that effectively reduce exposure to a variety of known risks by shaping a work force that is aware of, and educated about, the prob1ems of information security. The education, training, and awareness activities are required for all employees offered in three types:

[1] A complete list of the policies, directives, instructions, and memoranda issued by the CNSS can be found in the Index of National Security System Issues found online at http://www.nstissc.gov/Assets/pdf/index.pdf and Appendix 1 of this report

[2] Under Executive Order (E.O.) 13231 of October 16,2001, Critical Infrastructure Protection in the Information Age, the President redesignated the National Security Telecommunication and Information Systems Security Committee (NSTISSC) to the Committee on National Security Systems (CNSS).

[3] NSTISSP No. 6, National Policy on Certification and Accreditation of National Security Telecommunications and Information Systems.

[4] The current definition of national security systems according to NAD-42, para 11.e includes those telecommunications and information systems operated by the U.S. Government, its contractors, or agents that contain classified information or, as set forth in 10 U.S.C. Section 2315, that involves intelligence activities, involves cryptologic activities related to national security, involves command and control of military forces, involves equipment that is an integral part of a weapon or weapon system, or involves equipment that is critical to the direct fulfillment of military or intelligence missions.

[5] NSTISSI No. 1000, National Information Assurance Certification and Accreditation Process (NIACAP).

[6] NSTISSD No. 500, Information Systems Security (INFOSEC) Education, Training and Awareness.

1. Initial orientation
2. More advanced education and training commensurate with duties and responsibilities
3. Reinforcement activities

The CNSS directs[7] agencies to ensure additional training for national security information system security professionals, system administrators, information systems security officers, and system certifiers. The objective of this directive is to require the implementation of a training program to provide information security professionals with a common body of knowledge encompassing both communications security and computer security as these individuals, without a basic, yet broad perception of both of these disciplines, put classified systems at risk for breach of security. To assist agencies, the CNSS issued detailed, specific curriculums for each of the separate positions including: Information Systems Security Professional[8], system administrators[9], Information Systems Security Officers (ISSO)[10], and system certifiers[11].

In addition to the CNSS, the Director of Central Intelligence and the Department of Defense have issued other requirements and guidance that are applicable to government agencies. The Director of Central Intelligence issued a directive[12] that establishes the security policy and procedures for storing, processing, and communicating classified intelligence information, referred to as Sensitive Compartmented Information (SCI), in information systems. The Department of Defense issued the National Industrial Security Program Operating Manual (NISPOM) that prescribes requirements, restrictions, and other safeguards that are necessary to prevent unauthorized disclosure of classified information and to control authorized disclosure of classified information released by Federal agencies and departments to their contractors.

[redacted]

[redacted]

[redacted]

[7] NSTISSD No 501, National Training Program for Information Systems Security (INFOSEC) Professionals.
[8] NSTISSI No. 4011, National Training Standard for Information Systems Security (INFOSEC) Professionals.
[9] NSTISSI No. 4013, National Training Standard for System Administrators in Information Systems Security (INFOSEC).
[10] NSTISSI No. 4014, National Training Standard for Information Systems Security Officers (ISSO)
[11] NSTISSI No. 4015, National Training Standard for System Certifiers
[12] Director of Central Intelligence Directive (DCID)) 6/3, Protecting Sensitive Compartmented Information Within Information Systems Policy and Manual

[redacted]

[redacted]

[redacted] evolved from the original placement of responsibility for classified systems being assigned to the Space and Security Management Division (NAS). Traditionally, classified information was recorded on paper-based media. However, our culture is adopting more digital and electronic -based media for information including classified system. [redacted]

[redacted]

[redacted]

[redacted]

RECOMMENDATIONS

The Archivist of the United States (N) should ensure that:

1. NARA classified computer systems are centrally managed by technically qualified personnel by redesignating responsibility for these systems from NA to NH.

The Assistant Archivist for Human Resources and Information Services (NH) should ensure that:

2. A NARA Classified IT Systems Security Program is developed in accordance with the requirements setout by the CNSS, DCID, and DOD.
3. All existing NARA classified systems are identified and the inventory kept up-to-date.
4. An initial C&A is completed and periodically updated for each NARA classified system including a risk assessment, systems security plan, security controls testing and vulnerability analysis, and contingency.

MANAGEMENT RESPONSE

Management concurred with the recommendations and agreed to initiate corrective actions.

APPENDIX I -PARTIAL LIST OF CLASSIFIED SYSTEM SECURITY REOUIRMENTS AND GUIDANCE

Number	Title
32 CFR Part 2004	Classified National Security Directive No. 1
NSTISSP No. 5	National Policy for Incident Response and Vulnerability Reporting for National Security Systems
NSTISSP No. 6	National Policy on Certification and Accreditation of National Security Telecommunications and Information Systems
NTISSP No. 200	National Policy on Controlled Access Protection
NSTISSD No. 500	Information Systems Security (INFOSEC) Education, Training, and Awareness
NSTISSD No. 501	National Training Program for Information Systems Security (INFOSEC) Professionals
NSTISSD No. 502	National Security Telecommunications and Automated Information Systems Security
NSTISSD No. 503	Incident Response and Vulnerability Reporting for National Security System
NSTISSD No. 900	Governing Procedures of the National Security Telecommunications and Information Systems Security Committee (NSTISSC)
NSTISSD No. 901	National Telecommunications and Information Systems Security Issuance System
NSTISSI No. 1000	National Information Assurance Certification and Accreditation Process (NIACAP)
NSTISSI No. 4009	National Information Systems Security (INFOSEC) Glossary (Revision 2)
NSTISSI No. 4011	National Training Standard for INFOSEC Professionals
NSTISSI No. 4013	National Training Standard for System Administrators in Information Systems Security (INFOSEC)
NSTISSI No. 4014	National Training Standard for Information Systems Security Officers (ISSO)
NSTISSI No. 4015	National Training Standard for System Certifiers
NISPOM	National Industrial Security Program Operating Manual
DCID 6/3	Protecting Sensitive Compartmented Information Within Information Systems Policy, Manual, and Appendices