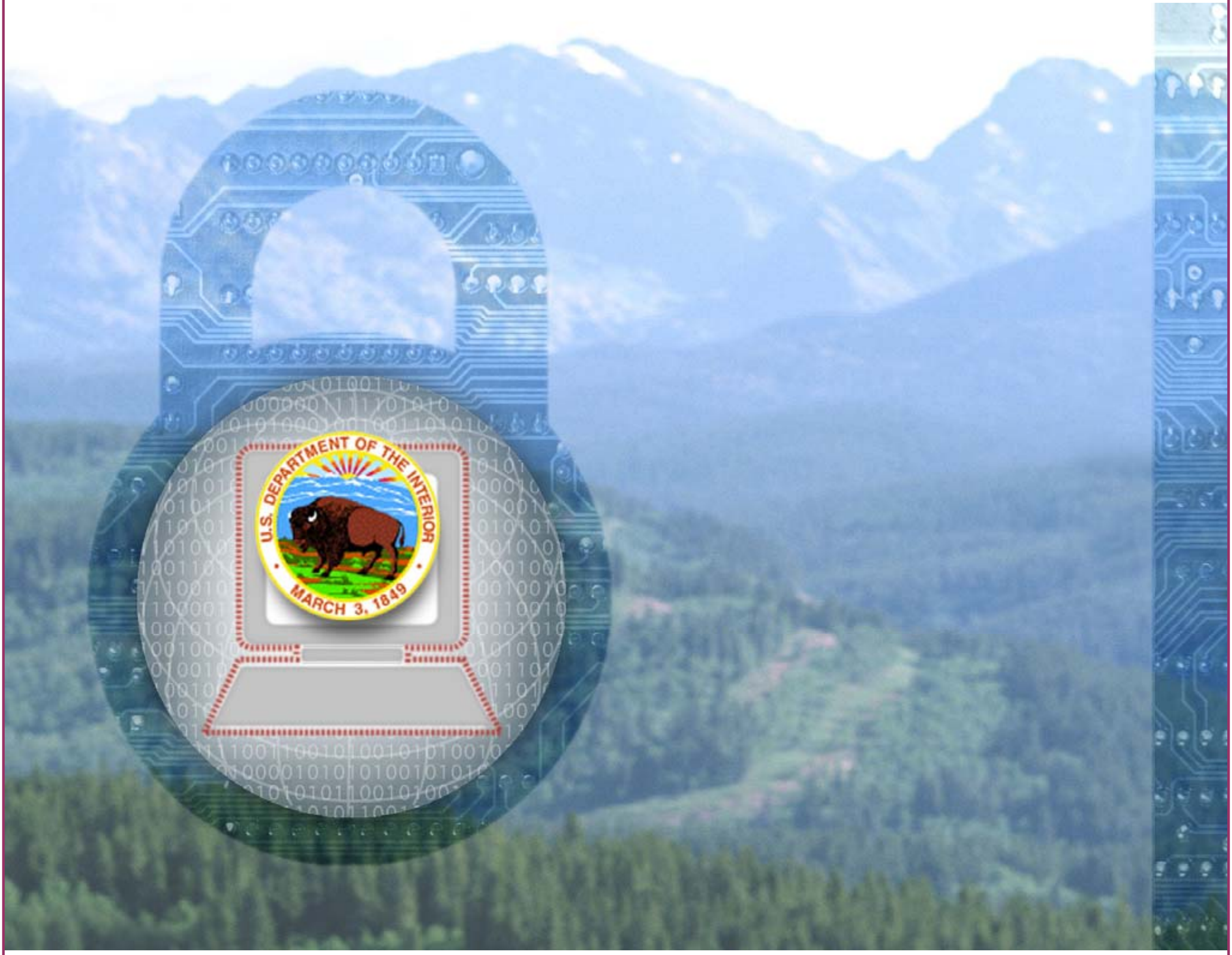
U.S. DEPARTMENT OF THE INTERIOR
OFFICE OF INSPECTOR GENERAL

AUDIT REPORT

IMPROVEMENTS NEEDED IN MANAGING INFORMATION TECHNOLOGY SYSTEM SECURITY NATIONAL PARK SERVICE



Graphic Courtesy of the U.S. Department of the Interior Office of the Chief Information Officer

REPORT NO. A-IN-NPS-0074-2003 **MARCH 2004**

United States Department of the Interior

Office of Inspector General

National Information Systems Office
134 Union Boulevard, Suite 510
Lakewood, Colorado 80228

March 29, 2004

To: Director, National Park Service

From: Diann Sandy Diann Sandy
Manager, National Information Systems Office

Subject: Final Report, Improvements Needed in Managing Information Technology System Security, National Park Service (No. A-IN-NPS-0074-2003)

The subject report presents the results of our audit of security over National Park Service's (NPS) information technology (IT) systems. The purpose of the audit was to determine whether controls effectively safeguarded the systems' integrity, confidentiality, and availability. Although NPS has recently improved the security of its IT systems, much remains to be accomplished before an effective IT security management program is implemented.

In the February 6, 2004 response to the draft report, the Director of NPS concurred with the report's 18 recommendations. Based on the actions described in the response and subsequent information provided by the Chief Information Officer for NPS, we classified 2 recommendations as resolved, 2 recommendations as resolved but not implemented, 10 recommendations as management concurs but additional information needed, and 4 recommendations as unresolved. The status of all the recommendations and the additional information requested is presented in Appendix 4.

The legislation, as amended, creating the Office of Inspector General requires that we report to the Congress semiannually on all audit reports issued, actions taken to implement our audit recommendations, and recommendations that have not been implemented.

Please provide a written response to this report by May 14, 2004. The response should supply the information requested in Appendix 4. We appreciate the cooperation provided by NPS staff during our audit. If you have any questions regarding this report, please call me at (303) 236-9243.

This Page Intentionally Left Blank

EXECUTIVE SUMMARY

BACKGROUND AND OBJECTIVE

To support its mission, the National Park Service (NPS) implemented local area networks in most of its approximate 400 offices, program centers, regions and support offices, and park units throughout the United States and its territories. These local area networks connect to 13 regional networks and one NPS-wide network. During our review, NPS reported to the Department of the Interior that NPS' major IT systems comprised 14 general support systems (networks) and 6 major applications. NPS established a senior executive service level chief information officer (CIO) position to provide standardized IT system security policy and management and to head the Office of the Chief Information Officer (OCIO). This office contains approximately 75 federal and contractor employees whose responsibilities included management of IT security and operation of three primary data centers located in Washington, D.C., and Denver, CO. NPS had also established information officers and IT security managers in program centers and regional offices to promote information and IT system security.

The objective of the audit was to evaluate the effectiveness of the management and controls over NPS' IT resources for ensuring integrity, confidentiality, and availability of information and IT systems. During our audit, we visited NPS locations as identified in Appendix 1.

RESULTS IN BRIEF

Despite recent organizational changes, we concluded that NPS lacked the basic foundation for an effective IT security program to ensure that issued IT security directives were consistently practiced. Specifically, NPS had not made sure that:

- Personnel were empowered to fulfill their assigned IT responsibilities or were effectively evaluated; IT duties were separated; IT security duties and responsibilities were included in position descriptions; risks of performing IT functions were mitigated through appropriate assignment of position sensitivity levels and subsequent background clearances; and IT personnel were adequately trained to fulfill their duties and responsibilities.

- Information and IT system risks were effectively managed by: conducting asset valuations to properly categorize systems as mission critical, conducting adequate assessments of risks, and developing system security plans and Plans of Actions and Milestones.

- Technical and physical access controls were effectively managed and safeguarded personnel and IT resources.

- Changes to operating systems and applications were authorized, tested, and approved.

- IT services could be continued in the event of a system failure or disaster.

- IT security controls were integrated throughout NPS including incident response capability and a standardized network security infrastructure.

As a result, NPS information and IT systems are vulnerable to unauthorized access, misuse, and disruption of service and its IT resources are at risk of being unreliable.

RECOMMENDATIONS

We made 18 recommendations to improve the NPS information security program.

AGENCY RESPONSE AND OFFICE OF INSPECTOR GENERAL REPLY

In the February 6, 2004 response to the draft report, the NPS Director concurred with the 18 recommendations. Based on the response and subsequent information provided, we considered 2 recommendations resolved and implemented, and classified 2 as resolved but not implemented, 10 as management concurs with additional information required, and 4 as unresolved. We requested that NPS provide us additional information on the unresolved recommendations.

TABLE OF CONTENTS

APPENDICES

This Page Intentionally Left Blank

RESULTS OF AUDIT

NPS' organization does not support an effective information security management program.

Until the National Park Service (NPS) implements a sound and consistently practiced information security program, it will have little assurance that its information technology (IT) systems provide reliable, confidential, and available information. An effective information security program should provide for assigning responsibilities, establishing and enforcing security policies and procedures, managing risk, and monitoring the adequacy of IT security controls. NPS has not, however, established the basic framework for a good program. As a first step, NPS needs to make IT security an overall top priority and ensure that all levels of management understand their roles and responsibilities and are held accountable for safeguarding information and IT systems. The discussions that follow highlight areas where we believe improvements are needed for NPS to have effective information security management program.

CIO lacked authority to be fully effective.

The NPS chief information officer (CIO) does not have the authority to manage all NPS information resources. Although the CIO position reports to a NPS Deputy Director, the CIO position has not been empowered to fulfill the responsibilities of a chief information officer. For example, the CIO is not an active member of the NPS National Leadership Council, as required by the Secretary of the Interior.[1] As such, the CIO was not able to effectively aid senior management in identifying IT security requirements and in developing sound IT security strategies. We also found that although the CIO may develop IT security policies, procedures, standards, and guidelines, the CIO lacked the authority to issue and to enforce compliance with these IT security directives by office, program center, region, and park unit management. Figure 1 presents our understanding of NPS' IT management structure and shows that the CIO does not have authority over office, program center, region, and park unit IT staffs.

[1] The NPS National Leadership Council is the NPS' executive-level decision-making team. Secretarial Order, 3244, requires each bureau to have its CIO be a fully participating member of each bureau's executive leadership/management team.

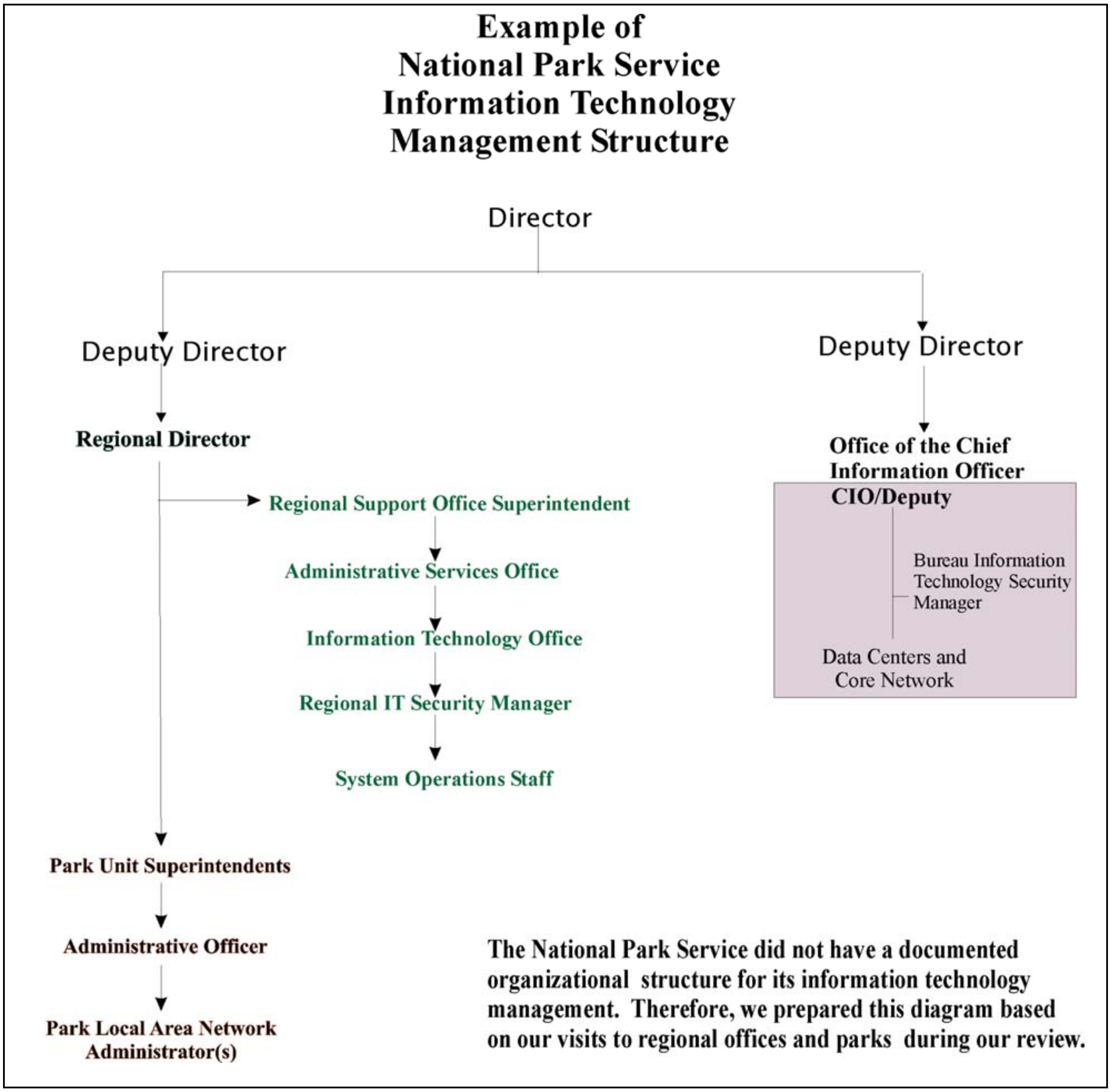

Example of
National Park Service
Information Technology
Management Structure
Director
Deputy Director
Deputy Director
Regional Director
Regional Support Office Superintendent
Administrative Services Office
Information Technology Office
Regional IT Security Manager
System Operations Staff
Office of the Chief Information Officer
CIO/Deputy
Bureau Information Technology Security Manager
Data Centers and Core Network
Park Unit Superintendents
Administrative Officer
Park Local Area Network Administrator(s)
The National Park Service did not have a documented organizational structure for its information technology management. Therefore, we prepared this diagram based on our visits to regional offices and parks during our review.

Figure 1. Office of Inspector General's representation of NPS' IT management structure.

Regional IT security managers lacked authority to be effective.

Regional IT Security Managers (RITSM) were not delegated sufficient authority to exercise their responsibilities and were not at organizational levels commensurate with their IT security responsibilities. (See Figure 1 above.) In the two regions we visited, one RITSM was organizationally three levels below the regional director and the other RITSM was one level below the regional director. Also, one of the RITSMs stated he/she did not have the authority to enforce information security policies and procedures at the park units. We believe that the regional IT security function should be part of the regional directorate to be at an organizational level to exercise their responsibilities and authority.

Adequate separation of IT duties was not implemented throughout NPS.

NPS did not assign IT duties and responsibilities to provide for adequate separation of duties to prevent overriding critical processes by a single individual. For example:

- The Bureau IT Security Manager (BITSM) was responsible for overall NPS information security and was also designated the system security manager for the NPS primary wide area network, NPSNet. Therefore, the BITSM was responsible for reviewing his own activities. Additionally, the BITSM was performing as both the BITSM and as the OCIO Project Manager.

- RITSMs were responsible for IT security and performed daily regional IT operations. Therefore, they could not independently perform their security responsibilities.

- Individuals responsible for system security management were also responsible for administering systems and networks. For example, at the Network Management Office, Intermountain Region support office, Natural Resources Program Center, Rocky Mountain National Park, Point Reyes National Seashore, and Bandelier National Monument, system administrators were also performing IT security functions.

- At three data centers, application programmers had access to the data centers, which may provide programmers the opportunity to modify or change production data, operating system configuration, and database management systems. Generally accepted information security practices recommend that application programmers should not have access to production data, operating systems, and database management systems because of the risk that inappropriate or malicious code could be installed and result in a compromise of the information and IT systems.

We realize that separation of duties may not be feasible at each park unit, but controls could be implemented such that regional IT staff help support the park units by performing some of the park unit's security functions, such as reviewing system generated logs. At locations where adequate separation of duties cannot be achieved, NPS should ensure that risk assessments identify the lack of adequate separation of duties so that management understands this risk and can make a cost-effective decision to either mitigate or accept the risk.

Position descriptions and performance standards did not address IT security.

Position descriptions for personnel with significant information security responsibilities, such as system owners, system and network administrators, and RITSMs, did not specify IT security responsibilities and duties. In addition, the CIO's performance standards did not include information security as a rating factor. Consequently, NPS management and personnel that should be responsible for ensuring IT resources are adequately safeguarded could not be evaluated based on how they performed their security responsibilities.

Level of risk associated with IT positions was not established.

NPS had not established an overall sensitivity level for IT positions in relation to the duties to be performed. The Departmental Manual (441 DM 3) requires that positions be reviewed to determine the risk of an individual performing the duties of the position and for assigning the appropriate sensitivity level for those positions. Specifically, NPS had not designated the appropriate sensitivity level of public trust[2] IT positions, such as system security manager, system administrator, and telecommunications specialist, commensurate with the risks associated with the duties. For example:

- Position sensitivity designations were different for personnel performing the same IT duties. One RITSM was designated a sensitivity level of "non-sensitive" (low risk), while the other was designated a sensitivity level of "noncritical-sensitive" (moderate risk). This resulted in NPS management accepting different levels of risk for positions with similar duties and functions. In addition, different types of background investigations would be required.

- IT positions and functions being performed by contractors were not assigned sensitivity levels. For instance, we reviewed three contracts that provided for contractor personnel to perform IT functions at NPS' data centers. We found that the contracts had no requirement for designating sensitivity of the contractor positions, such as application programmer, network administration, and telecommunications support, or for background investigations and resultant security clearances. One of these contracts required contract employees to be fingerprinted and for background checks to be performed. However, NPS was not able to substantiate that background investigations were completed and that the appropriate security clearances were obtained.

[2] According to the Departmental Manual (441 DM 3), public trust positions are those that are not related to national security duties.

- Management at one region stated that background reinvestigations had not been performed of its employees.

To determine position sensitivity, NPS could develop a matrix of all positions related to IT responsibilities and identify the associated risks to information and IT systems and the sensitivity level of those positions. Appendix 2 presents an example of this matrix concept.

IT training required to safeguard IT resources was not mandated.

During our site visits throughout NPS, we observed that overall the IT staffs at these sites were resourceful and effective in providing IT services and customer support. However, while NPS provided basic computer security awareness training and other IT-related training, it did not ensure that IT specialists in regions and park units were encouraged or required to receive training specific to information security and IT security management. For example, an IT specialist at a park unit had to determine on his/her own how to implement a new system. In addition, at most locations we visited, personnel had not been provided training specific to their duties and fulfilling their responsibilities in managing and operating NPS networks and servers. For instance, one IT specialist did not receive training on implementing a planned new NPS operating system. In that regard, NPS had not developed an IT career management program that included training requirements for all levels of IT positions. Without a structured training program for employees with IT responsibilities, NPS lacks assurance that networks, systems, and data were adequately safeguarded.

IT systems were not properly categorized.

NPS did not properly categorize its general support systems and applications as mission critical. The Department of the Interior's "Asset Valuation Guide" requires bureaus to categorize an IT system that processes, stores, or transports (1) Privacy Act or proprietary information as Mission Critical and (2) financial-related information as Financial Systems, which is above mission critical. The guideline also states that IT systems that are critical to the support of the Department's core missions and goals and not assigned a higher category are to be categorized as mission critical. Almost all NPS networks transport these types of information; however, NPS categorized its networks at a lower level—business essential. Further, NPS' Facilities Maintenance Support System, a major application, was categorized as business essential, even though the information in this system was used and maintained to support a DOI mission goal. Without performing asset valuations to properly categorize its systems, NPS has little assurance that all system resources have appropriate levels of protection.

IT risk assessments were not performed.

NPS had not performed risk assessments for 17 of its 20 general support systems and major applications. NPS reported to the Department that risk assessments had been performed for the 3 remaining systems—a general support system (NPSNet) and 2 major applications (Lotus Notes/Domino and ParkNet). However, we reviewed two of these risk assessments (NPSNet and Lotus Notes/Domino) and found that the assessments were incomplete, as follows:

- The NPSNet risk assessment was an initial assessment, which is less detailed and less extensive than a full risk assessment.

- The Lotus Notes/Domino risk assessment focused only on three major data centers, which would not likely represent the NPS-wide risk environment. Also, the assessment did not identify and assess all possible risks such as those introduced by the supporting general support systems. Further, the assessment was based on the loss of operations only, and did not consider the value of the data maintained in the major application.

- Neither of the risk assessments included:

    - Input from all data owners, such as program center managers, regional directors, or park unit superintendents, in the determination of the risks.

    - Evidence that management agreed to mitigate the identified risks or to accept the residual risks.

Therefore, the level of risk may not be at an acceptable level to ensure that all information processed, stored, and transported was adequately safeguarded and that residual risk was understood and accepted by management.

System security plans were not adequate.

NPS began drafting system security plans for local area and wide area networks, such as NPSNet, Intermountain Region,[3] Pacific West Region, and Natural Resources Program Center networks. This is good; however, the requirement for system security plans was established in 1987.[4] The purpose of a system security plan is to provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements. System security plans should include the elements identified in the National Institute of Standards and Technology

[3] Intermountain Regionwide area network security plan included appendices for 67 of the park units within the region.

[4] Computer Security Act of 1987 required that for each system a plan for the security and privacy of each Federal computer system be developed one year after the enactment of the Act.

Special Publication 800-18 “Guide for Developing Security Plans for Information Technology Systems,” and DOI policies. However, the NPS security plans did not always include the following required features:

- Appropriate assignment of responsibilities.
- Appropriate classification of data sensitivity and criticality that was processed, stored, and transported.
- Descriptions of components of general support systems and the applications they support.
- Identification of general support systems that support the major applications.
- Identification of all of the interconnection points (including Internet service providers and dial-in access) and agreements for connecting to other NPS internal and external networks.
- Physical and environmental controls.
- All milestone dates for implementing planned controls.

In a related matter, the CIO was in the process of consolidating individual park unit local area networks and regional wide area networks for the purpose of performing only one certification and accreditation. Office of Management and Budget (OMB) Circular A-130, Appendix III, “Security of Federal Automated Information Resources” stipulates that any interconnected system, such as a local area network, under the same direct management control is considered a general support system requiring a system security plan. Local area networks at the park units and the regions are under the management control of the park superintendents and the regional directors, respectively. Therefore, we believe that unless the consolidated system is under the direct management control of the CIO, each network will require a separate security plan that should be included as part of the one general support system security plan.

Plans of Actions and Milestones were not adequate.

OMB requires that agencies develop Plans of Actions and Milestones (POA&M) for every program and system for which weaknesses are identified through internal and external reviews. The POA&M process is to aid management in identifying, prioritizing, and monitoring the progress towards correcting the security weaknesses. Although NPS’ POA&Ms have improved, they were not adequate for the following reasons:

- All of the weaknesses identified by the Office of Inspector General (OIG), NPS internal control reviews, and DOI program reviews were not included. For example, all financial statement findings related to IT that had been reported by the OIG for fiscal years 2001 and 2002 were not included in the POA&M.

- There was no prioritization or strategy for correcting the weaknesses. For example, a security plan was to be developed for a general support system by July 1, 2003, whereas prerequisite reviews and documents, such as an asset valuation, a technical vulnerability assessment, and a management control review, were not planned to be completed until October 1, 2004.

- Dates reported for corrective actions were not consistent with the supporting documentation. For example, in the June 2003 POA&M submitted to the Department, NPS reported that the system security plan for NPSNet was completed in December 2002; however, only a draft system security plan dated June 2003 had been done.

- All of the weaknesses in systems' components were not identified by NPS and therefore were not included in the POA&M. For example, NPS did not recognize that storing backup media at employees' homes was a security weakness.

- Incremental steps needed to mitigate identified weaknesses were not reported. For example, in the June 2003 POA&M, NPS identified a weakness related to Internet connections. The planned corrective action involved two options and one milestone completion date of December 30, 2004. However, the POA&M did not include steps and completion dates for determining which option to select and the incremental steps for implementing the selected option. Consequently, NPS reported the status of this particular item action as "ongoing" and did not indicate the progress in correcting the weakness.

During the course of our audit, NPS began to identify the resources needed to correct the reported IT weaknesses. However, these resource costs had not been integrated with the NPS IT capital planning and control process.

System users' accounts were mismanaged throughout NPS.

Because system users' accounts were managed by each NPS organizational unit (offices, program centers, regions, and park units) and inconsistent methodologies were practiced in managing system user accounts, NPS had little assurance that users' access levels were based on the users' day-to-day activities or that the user accounts were authorized. For example:

- User accounts were not always disabled or deleted when individuals left NPS or changed positions within NPS.

- Users were issued multiple system user identifications, which may allow them to circumvent system access controls and bypass separation of duties.

- Users at one park unit were automatically provided dial-in access when their user accounts were established by the park unit's IT staff even though we found no evidence that the users were authorized this type of access.

- There appeared to be no periodic review of user accounts by system owners or supervisors to ensure that the level of access granted was appropriate for each system user.

Password management was inconsistent.

NPS had not consistently applied standard password procedures and practices for its servers to ensure adequate password management. For example, at one location the setting for lockout duration was "Forever" and at another location the setting was for 90 minutes. If the setting for "password lockout duration" is not set on "Forever" an intruder has the opportunity to obtain the password because it allows unlimited guesses. Additionally, we found that password settings in servers at some locations allowed users to circumvent the requirement for changing their passwords periodically. Consequently, the users could continually change their passwords until their original password could be used again. As a result, NPS systems may be operating with less stringent controls than expected by management.

Physical access to IT resources was not sufficiently controlled and monitored.

We found that access to data centers was not always adequately controlled. For example:

- Although the Information Technology Center (ITC) used access cards and video monitoring as physical access controls to the data center, individuals who had key cards and accessed the data center were not always approved for access. We also noted that there were an excessive number of personnel with access to the data center, such as application programmers who were not part of the ITC or the OCIO. Due to potential blind spots in video monitoring, best practices suggests that methods be used to monitor personnel exiting data centers.

- At the National Information Systems Center (NISC) data center, access was through the use of a cipher door lock. Although there were sign in/sign out logs, only non-NISC personnel were required to sign the logs. Consequently, there was no record of NISC personnel activities and specific NISC personnel could not be held accountable for any misuse of computer resources.

At the park units we found that:

- Access to telecommunications closets was not limited. That is, they were located in general working areas, such as where a copy machine was located, a loading/receiving dock, a break room, and an amphitheater.

- One server room was located in a general work area and was accessible by personnel other than IT personnel.

Environmental controls were not adequate to protect personnel and IT equipment.

At many park units visited, we noted that the server rooms did not adequately protect personnel and IT equipment. Specifically, some server rooms did not have adequate air conditioning units and proper fire suppression capabilities. For example, at Bandelier National Monument:

- The air conditioner in the server room had a water leak. Although a bucket was placed below the air conditioner to catch the water, we observed water stains on the floor.

- Access to the server room was from the outside of the building and the access door was not sealed, thus the room was susceptible to dust, sand, and rain.

The room was too small to house all of the equipment along with personnel and to provide for proper wire management. See Figure 2.

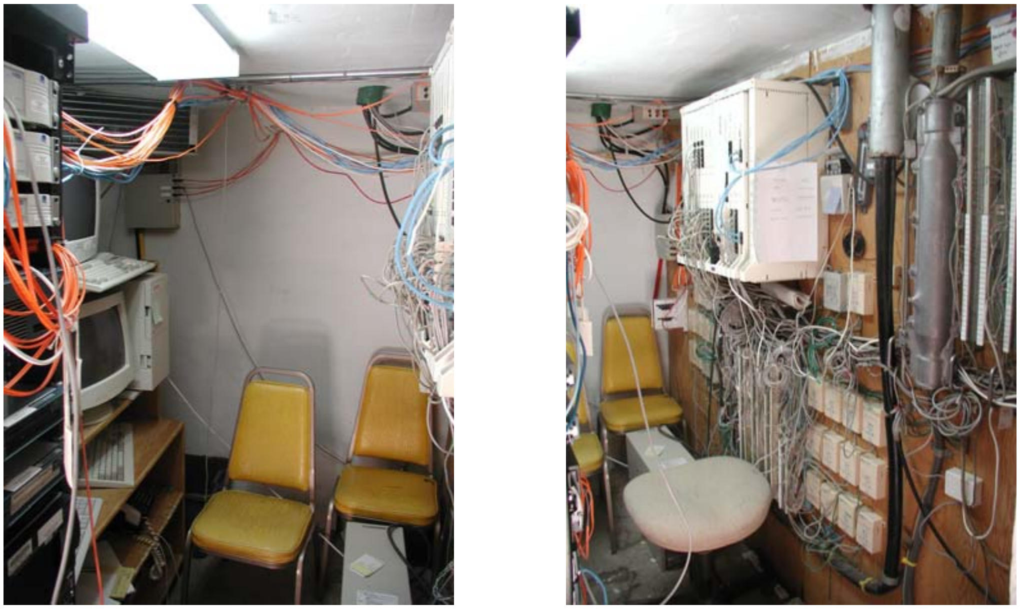


Figure 2. Photographs of the Bandelier National Monument Server Room

Although many park units use historical buildings as facilities for housing local area network server rooms, locating servers in historical buildings should not preclude NPS from implementing adequate environmental controls. Some examples of improvement that would not require changes to the historical structure or the building of new facilities may include:

- Installing air conditioning units.
- Installing rack and shelf systems to better use small spaces.
- Installing weather seals around doors.
- Supplying fire extinguishers.

Change management controls were not effective.

NPS has an Information System Life Cycle Manual which contains instructions on managing changes to systems. However, NPS did not have adequate controls over changes to computer hardware, such as computers, servers, and routers; operating systems; and application software. We found no evidence that changes made by IT personnel in program centers, regions, and park units to operating systems and application programs were authorized, tested, and approved prior to installation. We also found no evidence that the program centers, regions, and park units were required to develop test plans for changes and enhancements to operating systems and application software.

Continuity of services planning needs improvement.

NPS has not instituted adequate continuity of services planning. Continuity of services planning helps management identify and prioritize those daily processes or critical business functions that need to be restored first after emergencies, such as power interruptions or system failure. Weaknesses we observed in NPS' preparation for continuity of services included:

- Inadequate backup practices and offsite storage facilities to keep backup media and system and application documentation. For example, NPS practices did not include full back up of data and systems on any scheduled cycle.

- Using employee homes as the off-site storage location for application software and network operating system back-up media rather than a location that could be easily accessed by all required personnel.

- Not storing at an off-site location security documents, such as system security plans and continuity of operations plans.

- Not testing those contingency or continuity of operations plans that did exist.

Incident response capability was not fully developed.

While some guidance had been issued, NPS had not distributed specific procedures for incident detection, reporting to FedCIRC, and responding to incidents. Additionally, we believe NPS' policy for computer incident response was insufficient because it did not: (1) include all types of incidents, such as the misuse of government computers; (2) provide the protocol for communicating an incident; and (3) specify the procedures for mitigating an incident. For example, one regional network manager reported to the NPS wide area network management that an Internet scan had occurred of the regional network, which was trafficked through the NPS wide area network firewall. However, the regional network manager did not receive feedback or a response from NPS management, thus the regional network manager had little assurance that the potential incident had been mitigated. In addition, NPS had not ensured that all individuals responsible for IT security management were adequately trained in their incident handling responsibilities.

Capability for detecting, identifying, and reporting IT misuse was limited.

NPS was not routinely creating, reviewing, and maintaining system logs for network operating systems and routers. System logs are used to detect and identify system misuse or inappropriate actions of authorized and unauthorized users. At several locations the logs were set to overwrite at a very low threshold; thus the logs were overwritten frequently and historical information was lost. At some locations we visited, the logs were not created, and logs that did exist were not being periodically reviewed. NPS had no policy for creating, reviewing, and maintaining system logs. Without appropriate logging of system activities, NPS may not be aware of potential incidents and be able to timely identify individuals who were misusing IT resources.

Standardized configuration of network security infrastructure was lacking.

There was no standard configuration of NPS' network security infrastructure, such as the use and placement of firewalls and intrusion detection systems. At one park, IT security personnel incorrectly assumed that the NPS wide area network, NPSNet, was providing security to protect their specific network, systems, and data. We also found that regions and park units had not always implemented significant protection for their networks such as firewalls. At two locations that had implemented firewalls, IT system administrators detected scanning of their networks from the Internet, which could be considered a threat that was not blocked at the NPSNet level. Without a standard security configuration, NPS was not able to effectively protect its IT resources and ultimately implement security best practices.

This Page Intentionally Left Blank

RECOMMENDATIONS FOR IMPROVING NPS' INFORMATION SECURITY MANAGEMENT PROGRAM

We recommend that the Director, NPS:

1. Assign to the CIO the duties and responsibilities as defined by the Secretary and authorize the CIO to issue information security directives to NPS personnel with IT security responsibilities.

2. Implement an effective information security program. In establishing this program, NPS should consider:

   ❖ Dual reporting of information security management staff:

     - At regions, RITSMs should report to the regional directors and to the CIO and be authorized to carry out IT security management responsibilities directly to regional and park IT staff.

     - At park units, IT personnel should report to the superintendents and to the regional information security managers.

   ❖ Dedicate the BITSM and RITSMs to only security program management.

3. Provide written notification to personnel with IT security responsibilities specifying their duties and functions. Hold individuals accountable for fulfilling these responsibilities through annual performance evaluations. In meeting this requirement, NPS should:

   ❖ Identify all individuals/positions such as associate directors, program managers, regional directors and all staff who are responsible for managing and administering NPS IT systems, networks, and data.

   ❖ Review position descriptions of all positions identified as having IT security responsibilities and update the position descriptions to reflect current duties and responsibilities.

   ❖ Update individual performance evaluation plans for those positions identified as having IT security responsibilities to include information security management tasks, functions, and strategic planning.

- ❖ Designate, for each position having IT responsibilities, a sensitivity level commensurate with the risks of the duties performed and ensure the appropriate background checks or re-checks be performed based on the designated sensitivity level.

4. Separate the duties and responsibilities of IT personnel to ensure that unauthorized activities can be detected timely. To ensure duties and responsibilities are adequately separated NPS should:

- ❖ Identify personnel at all locations who have IT security management duties and responsibilities and who are also responsible for performing system and network administration duties. If possible, separate these duties or develop alternative processes to provide for separation of duties.

- ❖ Implement alternative controls, such as, moving some security management responsibilities to different organizational levels if separation of duties at some locations is not cost effective.

- ❖ Identify personnel at all major data centers who are responsible for programming software applications and for system administration functions and separate these duties or develop alternative processes to provide for separation of duties.

- ❖ Identify the lack of separation of duties in the security plans and require management to formally accept the risk associated with the lack of separation of duties if alternative controls are not feasible.

5. Modify all IT support contracts to require position sensitivity for all IT positions and require appropriate background investigations and security clearances for all contractor personnel performing IT functions.

6. Establish an IT career-training program for all NPS IT professionals. The training program should be based on NPS' implemented and planned systems, networks, and software. NPS should periodically review the training program to ensure that IT professionals are provided training on the most current security requirements and the most up-to-date technology implemented or planned by NPS.

7. Perform asset valuations for all general support systems and applications to properly categorize these systems based on their importance and critical loss criteria in accordance with the Department's "Asset Valuation Guide."

8. Perform risk assessments of all general support systems and major applications to identify risk, threats, and vulnerabilities that impact the accomplishment of the NPS' and the Department's missions and the

security and data integrity, confidentiality, and availability. NPS should also ensure that risk assessments include input from senior management and data owners.

9. Develop security plans for all general support systems and major applications following NIST and Departmental guidelines.

10. Establish procedures to ensure that the POA&Ms are used as a management tool. The procedures should include:

- Requirements for reporting all the weaknesses identified and reported by OIG, NPS, and other reviews performed on behalf of NPS.
- A prioritized strategy to correct all identified security problems.
- Assurance that the completion dates are supported by the applicable documentation.
- Requirements for corrective actions that exceed 6 months to have incremental steps to correct the weaknesses, milestone dates, and resources required.
- Integration of resources identified in the POA&Ms for correcting weaknesses with the capital investment planning and control process.

11. Establish a standardized process for system user accounts that includes:

- Coordinating with Human Resources, system owners, and supervisors to identify and report to the IT system security administration staff the names of employees who are no longer employed by NPS, have a change in responsibilities and duties, or have transferred from NPS locations. Upon notification, IT system security administration staff should disable user accounts or immediately terminate access from all applicable systems, applications, and data centers.
- Establishing a policy requiring each user of NPS systems to have unique user identifications. The policy should specifically state when a single user could have multiple identifications and describe the controls to ensure the use of multiple identification does not circumvent separation of duties.
- Developing procedures requiring system owners or supervisors to periodically review and validate users' access and privileges.

12. Establish standard password configuration settings to ensure that all IT system resources are protected at an acceptable level.

13. Establish policies, procedures, and practices to ensure that physical and environmental controls protect systems and data from misuse or interruption, and physical damage or destruction and that personnel have a safe working environment. In developing these policies, procedures, and practices NPS should:

- ❖ Evaluate the facilities that house the data centers, server rooms, and telecommunications closets to determine if the access controls and environmental controls are effective. If the controls are not effective, identify cost effective remediation controls and report the status in NPS' POA&Ms.

- ❖ Review the current lists of personnel with access to the all data centers and determine if the access granted is necessary and revoke access that is not required.

- ❖ Require the use of sign in/sign out logs or other entrance/exit technologies at data centers and compare physical access logs to computer logs.

14. Establish standard change management procedures to ensure that all changes are authorized, tested, and approved prior to updating operating systems and applications. To aid in standardizing its change management process, NPS should consider the use of change management software to assist in the control over modifications made to operating systems and applications.

15. Establish policies and procedures to ensure that all NPS systems and applications can be restored or recovered timely in the event of system failures or disasters. These policies and procedures should:

- ❖ Define the appropriate backup and recovery requirements of IT services that clearly define personnel roles and responsibilities and standard types of back-ups and timeframes for backing up systems and data.

- ❖ Define appropriate offsite storage locations and ensure that backup data and system documentation are stored in these offsite storage locations.

- ❖ Develop continuity of operations plans for all NPS locations and ensure that the plans are tested and updated annually.

16. Establish an incident handling organizational structure and a process for identifying, reporting, and mitigating computer-related incidents.

17. Establish policies and procedures to ensure that systems are logging relevant information, logs are maintained for an appropriate period of time to provide an adequate audit trail of systems activities, and the logs are reviewed periodically to identify inappropriate activities.

18. Establish standard network security infrastructure based on a layered security approach that includes firewalls and intrusion detection systems throughout the NPS internal networks. To accomplish this layered security approach, NPS should:

- ❖ Require networks topologies be developed for all offices, program centers, regions, and park units to determine the appropriate security infrastructure solution that complies with best practices.

- ❖ Create standard firewall rules that prevent unauthorized access from the Internet into the park unit networks.

This Page Intentionally Left Blank

AGENCY RESPONSE AND OFFICE OF INSPECTOR GENERAL REPLY

In the February 6, 2004 response to the draft report (Appendix 3) the NPS Director concurred with the 18 recommendations. The response described recent NPS IT security accomplishments, and commented on the findings and recommendations. Also, the NPS CIO provided subsequent information about the report and the response. We revised the report as we considered appropriate based on the NPS response and additional information provided.

Based upon NPS' replies, we classified Recommendations 7 and 8 as resolved; Recommendations 12 and 13 as resolved but not implemented; Recommendations 1, 2, 3, 4, 5, 6, 10, 11, 14, and 16 as management concurs but additional information required; and Recommendations 9, 15, 17, and 18 as unresolved. (See Appendix 4.) Even though NPS agreed with all the recommendations, we considered four of the recommendations as unresolved because the proposed actions did not meet the intent of the recommendations, as discussed below.

Recommendation 9. Although NPS completed all "initial" system security plans in December 2003, our recommendation was to develop system security plans for all general support systems following NIST Special Publication 800-18 and Departmental guidelines. While Departmental guidelines include the development of "initial" system security plans, these initial plans are not a finalized system security plan. That is, they do not include information from risk assessments and system testing and evaluations. As such, they do not adequately address the controls necessary to reduce risk to an acceptable level. Further, NPS disagreed that system security plans were needed for each park unit's and regional office's local area networks even though these networks are under the management control of the respective parks and regions. According to Office of Management and Budget Circular A-130, Appendix III, these networks are general support systems requiring system security plans. Furthermore, without system security plans for each of these local area networks, NPS has little assurance that these networks are operating securely and that the NPS-wide network is adequately safeguarded. NPS should prepare a plan for developing system security plans for all general support systems and major applications and for incorporating park units and regional office local area networks into its one general support system.

Recommendation 15. NPS stated that a continuity of operations plan would be completed by its IT Infrastructure team by 2005. Our understanding is that NPS is developing one continuity of operations plan for its one general support system. If that is the case, we do not believe that NPS will have sufficient procedures to ensure that major applications are restored timely and those NPS locations that input, process, transport, and store information will be able to recover from system failures or disasters expeditiously. NPS should develop policies and procedures ensuring that NPS information, systems, and applications can be restored or recovered timely; that backup and recovery is practiced by all levels of NPS management; that offsite facilities are adequate; and that continuity of operations plans are tested and updated annually.

Recommendation 17. NPS is requesting funding for acquiring software to manage system events. Our recommendation, however, dealt with preparing policies and procedures to make sure relevant information about system events was logged and reviewed. As logging capability currently exists within most NPS systems, the intent of our recommendation was for NPS to consider acquiring a software tool that would take advantage of existing logging capability and for NPS to periodically review logs to identify inappropriate activities.

Recommendation 18. The response focused on the conversion of the NPS core networks to the Department’s Enterprise Services Network. However, the recommendation was for NPS to develop a layered approach to security to include safeguarding all internal networks, such as the networks operated and maintained at regions and park units.

AUDIT OBJECTIVE, SCOPE, AND METHODOLOGY

Our objective was to evaluate the effectiveness of NPS' management and controls over IT resources to ensure integrity, confidentiality, and availability of information and IT systems. Specifically, we evaluated information security management practices and general controls over non-financial IT systems (see Appendix 1 for the systems reviewed).

To evaluate these controls, we reviewed NPS policies, procedures, and practices in place during April through August 2003, tested and observed security practices and IT security control techniques in operation, and held discussions with NPS staff to determine whether IT security controls were in place, adequately designed, and operating effectively. We performed on-site work at NPS headquarters in Washington, D.C. and other NPS locations listed in Appendix 1.

Our audit was conducted in accordance with the "Government Auditing Standards" as issued by the Comptroller General of the United States. Accordingly, we included tests and other auditing procedures that were considered necessary under the circumstances.

This Page Intentionally Left Blank

SITES VISITED AND SYSTEMS REVIEWED

Office of the Chief Information Officer

Network Management Office (NMO) NPS wide area network (WAN)/(NPSNet)	Denver, Colorado
National Information Systems Center (NISC) Denver General Support System (GSS)/local area network (LAN)	Denver, Colorado
Information Technology Center (ITC) ITC LAN	Washington, D.C.

Natural Resources Program

Natural Resources Program Center (NRPC) NRPC GSS/LAN	Ft. Collins, Colorado and Denver, Colorado

Intermountain Region (IMR)[5]

Santa Fe Support Office IMR GSS/WAN	Santa Fe, New Mexico
Rocky Mountain National Park Rocky Mountain LAN	Estes Park, Colorado
Bandelier National Monument Bandelier LAN	Los Alamos, New Mexico

Pacific West Region (PWR)

Regional Office and Pacific Great Basin Support Office PWR GSS/WAN	Oakland, California
Golden Gate National Recreation Area Golden Gate LAN	San Francisco, California
Point Reyes National Seashore Point Reyes LAN	Point Reyes, California

[5] The Intermountain Regional Office headquarters is located in Denver, Colorado and is supported by the National Information Systems Center. The Santa Fe Support Office provides support for regional and support personnel located in Santa Fe, New Mexico and for all the parks in the region.

This Page Intentionally Left Blank

SUGGESTED MATRIX OF POSITION SENSITIVITY DESIGNATIONS FOR A GENERAL SUPPORT SYSTEM

(The minimum level of investigation associated with Public Trust Positions)

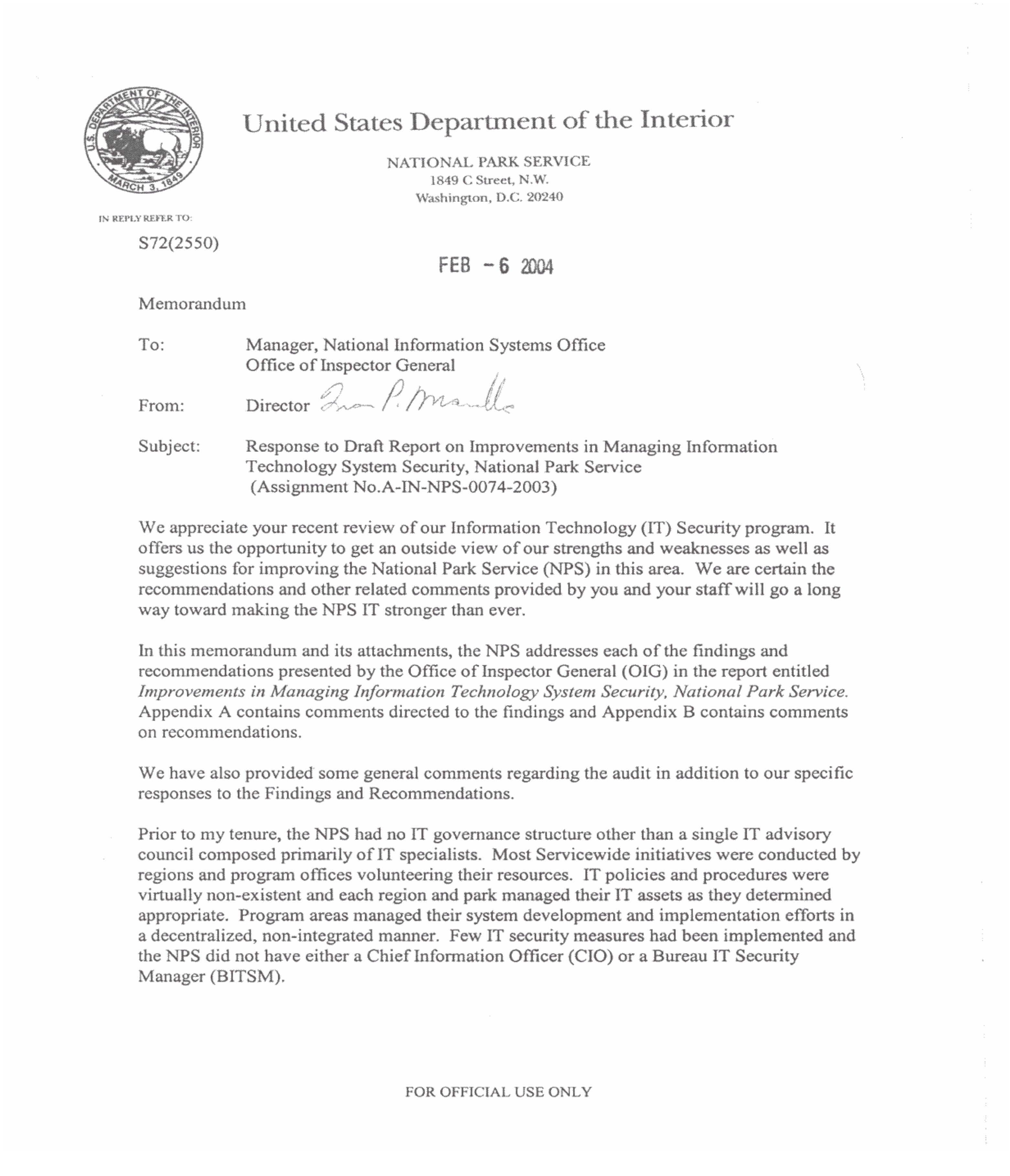
Role	Position	Designation Investigation Requirement[6]	Justification
Program Manager	Deputy Director	High Risk – BI	Senior manager for system. As program manager who has ultimate management authority for systems.
Information Owner	Program Managers, Regional Directors, Park Unit Superintendents	Moderate Risk – MBI	Senior manager for data contained in the system for their individual program, region, or park unit. System security and back-up procedures, minimize the opportunity for a regional director, superintendent or program manager to do major harm to the system. Oversight provided by headquarters.
Information System Owner	CIO	Moderate Risk – MBI	Minimal system access. Provides policy oversight for data management.
Security Manager	BITSM/RITSM	High Risk – BI	Responsible for system integrity, confidentiality, and availability. Prepares bureau policy for system security.
System Manager	Deputy CIO	High Risk – BI	Provides technical oversight to all system operations and administration from a headquarters level. Provides policy and guidance for regional and field operations.
System[7] Security Manager	Multiple employees located in headquarters, offices, program centers, regions, and park units.	Moderate Risk – MBI	Responsible for system security design, testing, and maintenance under the technical guidance of the OCIO.
System[2] Administrator	Multiple employees located in headquarters, offices, program centers, regions, and park units.	Moderate Risk – MBI	Responsible for system operation and maintenance at headquarters, offices, program centers, regions, or park units. Work is under the technical oversight of Regional Directors or Associate Directors.
Internal NPS Users[2]	Office, program center, regional, and park unit employees	Low risk – NACI	Responsible for data entry and update. Access to the system is limited to the functions performed and registration is required and managed by the system security managers or system administrators.

This matrix was developed by the Office of Inspector General for use by the National Park Service as a guide to develop position sensitivity designations consistently for its personnel with IT responsibilities. The matrix was based on a U.S. Geological Survey review of roles and positions identified with IT responsibilities for one of its major applications. For each role and position, a level of risk/sensitivity and the related type of background investigation was defined along with the justification for the sensitivity level and type of background investigation.

[6] BI – Background Investigation; MBI – Minimum Background Investigation; NACI – National Agency Checks and Inquiries.

[7] The duties and background investigation requirements are applicable to federal employees, contractor employees, and volunteers.

This Page Intentionally Left Blank



United States Department of the Interior

NATIONAL PARK SERVICE
1849 C Street, N.W.
Washington, D.C. 20240

IN REPLY REFER TO:

S72(2550)

FEB - 6 2004

Memorandum

To: Manager, National Information Systems Office
Office of Inspector General

From: Director Fran P. Mainella

Subject: Response to Draft Report on Improvements in Managing Information Technology System Security, National Park Service (Assignment No.A-IN-NPS-0074-2003)

We appreciate your recent review of our Information Technology (IT) Security program. It offers us the opportunity to get an outside view of our strengths and weaknesses as well as suggestions for improving the National Park Service (NPS) in this area. We are certain the recommendations and other related comments provided by you and your staff will go a long way toward making the NPS IT stronger than ever.

In this memorandum and its attachments, the NPS addresses each of the findings and recommendations presented by the Office of Inspector General (OIG) in the report entitled *Improvements in Managing Information Technology System Security, National Park Service.* Appendix A contains comments directed to the findings and Appendix B contains comments on recommendations.

We have also provided some general comments regarding the audit in addition to our specific responses to the Findings and Recommendations.

Prior to my tenure, the NPS had no IT governance structure other than a single IT advisory council composed primarily of IT specialists. Most Servicewide initiatives were conducted by regions and program offices volunteering their resources. IT policies and procedures were virtually non-existent and each region and park managed their IT assets as they determined appropriate. Program areas managed their system development and implementation efforts in a decentralized, non-integrated manner. Few IT security measures had been implemented and the NPS did not have either a Chief Information Officer (CIO) or a Bureau IT Security Manager (BITSM).

Many of the governing statutes and requirements have been in place for a number of years. Since July 2001, however, NPS has moved forward on a rapid pace to ensure its IT assets were properly managed and secured. We have highlighted, for the OIG's consideration, some of the significant improvements the NPS has made during the current administration as an indicator of the NPS' resolve to continue improving:

- The establishment of the CIO and BITSM positions
- The creation of NPS's first IT Investment Council
- Combined two separate NPS IT organizations into one under the direct control of the CIO.
- Successfully responding to DOI requirements for securing our network perimeter, including the installation of firewalls and intrusion detection software
- Movement of over 50 NPS web servers into a centrally managed DMZ
- The implementation of an IT asset management system that tracks every desktop in the NPS
- Authorization of the CIO to shut-down any system or IT infrastructure component failing to meet NPS security directives
- The development of an internal application to track systems, IT personnel, network components, recently expanded to include radio equipment
- The standardization of 13 general support systems (GSS) into one enclave
- The creation of configuration management boards for our wide-area-network (WAN), desktop and local-area-network (LAN) infrastructure, Active Directory (AD) and our voice systems; who are now constructing the standard Servicewide policies and procedures upon which sound operations can be based and will form the foundation of a strong IT security posture.
- The establishment of a formal NPS Computer Incident Response Team using the Regional IT Security Managers (RITSMs)
- The purchase of 500 computer-based on-line training licenses for its IT specialists in FY 2002 – 2003.
- NPS has purchased a policy and procedures template that may be used as both a model and a taxonomy for classifying policies.
- The creation of information officers, technology officers, regional IT security managers at each region and program office
- The issuance of a formal software development lifecycle handbook
- NPS is leading Departmental initiatives for applications in law enforcement and records management
- Playing a major role in the reservation module of the RecOneStop
- Taking a lead role in the Enterprise Services Network (ESN)
- Management of the NPS Active Directory implementation which is on schedule to meet the Department's December deadline
- Completing Interim approval to operate on all major applications

- Meeting all FY 2003 Government Paperwork Elimination Act requirements
- Taking the lead in negotiating the Microsoft Enterprise Agreement which established the model for the Departmental agreement
- Using FY 2003 funding for new positions to add a second IT security staff member as an Associate BITSM and reassigning a third employee as a second Associate BITSM.
- Encouraging security credentials for our IT managers with NPS having the only CIO in DOI with not one, but two IT security certifications (Certified Information Systems Security Professional - CISSP and Global Information Assurance Certification Security Leadership Certificate – GLSC). In addition, our BITSM, Associate BITSM, Chief Technology Officer and a number of RITSMs have earned the CISSP credential. Our Deputy CIO for Systems has earned the Certified Information Systems Security Management Professional (CISSM).

We fully understand there is much work to be accomplished and NPS is far from satisfied. However, the process of developing an acceptable IT security framework rests on: 1) a strong IT governance platform with standard policies and procedures; 2) an organization that values a common approach to the management of its IT assets through compliance; and, 3) an organization that works internally as a team. We feel we are well on the way to establishing this solid base.

Most of the recommendations have significant budgetary implications and the result of implementing these recommendations will have a major impact on the operations of the NPS. We will actively work with the DOI and the Office of Budget and Management in an effort to identify funds for reprogramming in order to fully implement all the recommendations. The NPS will, with guidance from the Department, also continue to assess the value of our assets against the potential risks. There may be cases where we find that certain risk mitigation efforts are too costly when weighed against the risk probability, and, in these instances, we may decide to accept the risk.

For additional information, please contact the CIO, Dom Nessi at 202 354-2093.

Attachments

A Comments on Findings
B Comments on Recommendations

cc: Assistant Secretary for Fish and Wildlife and Parks
Audit Liaison Officer, Assistant Secretary for Fish and Wildlife and Parks
Audit Liaison Officer, National Park Service
Focus Leader, Management Accountability and Audit Follow-up

Attachments withheld by the Office of Inspector General.

This Page Intentionally Left Blank

STATUS OF AUDIT REPORT RECOMMENDATIONS

RECOMMENDATION REFERENCE	STATUS	ACTION REQUIRED
7 and 8	Resolved	No further response is required.
12 and 13	Resolved, not implemented	No further response to the Office of Inspector General is required. The recommendations will be forwarded to the Assistant Secretary for Policy, Management and Budget for tracking of implementation.
2, 3, 4, 6, 10, 11, and 16	Management concurs, additional information required.	Provide the title of the official responsible for implementation.
1, 5, and 14	Management concurs, additional information required.	Determine how the recommendation will be implemented and provide plans describing implementing actions, target dates, and responsible officials
9, 15, 17, and 18	Unresolved.	Reconsider the proposed corrective actions and provide an updated reply.

This Page Intentionally Left Blank