U.S. Department of the Interior

Office of Inspector General

Evaluation Report

Information System Security over Systems and Applications Used by the National Business Center to Provide Services to Non-Department of the Interior Clients

No. A-EV-0SS-0094-2004

August 2004

United States Department of the Interior

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

August 23, 2004

Memorandum

To: Director, National Business Center

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

Subject: Review of Information System Security over Systems and Applications Used by the National Business Center to Provide Services to Non-Department of the Interior Clients (Report No. A-EV-OSS-0094-2004)

We performed the subject review based on inquiries from other Inspector General offices about the security over systems and applications used by the National Business Center (NBC) to provide services, such as payroll processing, to their respective agencies.[1] The purpose of our review was to assess NBC's information security management program and practices over these client-oriented systems and applications.

We discussed the results of our review with representatives of NBC. The officials generally agreed with our report and commented on certain report findings. We modified the report as appropriate based on the comments.

BACKGROUND

Information on NBC and the Department of the Interior's (DOI) security program are described below.

NATIONAL BUSINESS CENTER

In 2000, under the Assistant Secretary for Policy, Management and Budget, NBC was created to centralize the operations and maintenance of DOI-wide administrative systems. NBC serves as the systems manager and general purpose computing host (using servers at its Denver, Colorado, and Reston, Virginia, data centers) for systems supporting budget, procurement and contracts, personnel management, financial and accounting, E-government, and other general administrative systems. In this

[1] The Federal Information Security Management Act of 2002 (FISMA) requires Inspectors General to evaluate their agency security program "including information systems operated by a contractor of an agency or other organization on behalf of an agency."

capacity, NBC provides services related to such automated systems as the Federal Personnel and Payroll System (FPPS); Federal Financial System (FFS); Fixed Assets and Inventory Subsystems; Interior Department Electronic Acquisition System (IDEAS); electronic commerce; electronic time and attendance system (Quicktime); mainframe time-sharing; and Internet publishing. NBC also provides specialized services such as quarters' management and employee drug testing. NBC provides its systems and services to DOI and other Federal organizations on a full cost-recovery basis.

NBC's services are provided through negotiated Inter-Agency Agreements (IAA). Regarding IT system operations, overall agreements are supposed to include:

- Service Level Agreements – defines specific tasks to be performed and roles and responsibilities of the respective parties.
- Security Service Agreements – defines security roles and responsibilities of the respective parties.
- Interconnect Security Agreements – defines the roles and responsibilities for client network management in connecting to NBC systems and applications.

DOI SECURITY PROGRAM

The Chief Information Officer (CIO) for DOI is responsible for providing policy, guidance, advice, and oversight for information technology (IT) security. DOI's information security program is based on Office of Management and Budget policies, National Institute of Standards and Technology (NIST) standards and guidelines, and DOI policy established in the Departmental directives.

The DOI CIO reviewed the information security programs of DOI components and established an automated DOI Computer Incident Reporting Center (DOI CIRC) for internally reporting and tracking computer incidents and for externally reporting incidents to the Federal information security incident center.[2] Additionally, DOI implemented a Command Center to track and monitor certification and accreditation of DOI components'

[2] FISMA requires agencies to notify and consult with the Federal information security center of computer security incidents. At the issuance of FISMA the reporting agency was the Federal Computer Incident Response Center. Effective March 2004, under the Department of Homeland Security, the reporting agency is the U.S. Computer Emergency Readiness Team (US-CERT).

general support systems and major applications (herein after referred to as system or systems).

To further aid in improving DOI's information security management program, the Chief Information Security Officer established an Information Technology Security Team comprised of information technology security managers from all the DOI components. Components also report monthly to the DOI CIO on security improvements and on the status of the certifications and accreditations completed for each system under their control.

SCOPE AND METHODOLOGY

To complete our review we: reviewed documentation supporting certifications and accreditations completed in fiscal year 2004 (as of July 30, 2004) for 8 systems; tested selected controls at the data centers; interviewed NBC management and staff; judgmentally selected and examined 15 of about 200 agreements between NBC and external clients. The 15 agreements selected were those of clients that used more than 1 NBC system. In addition, we analyzed information on system certification and accreditation which NBC reported monthly to the DOI CIO and DOI senior management.

The systems reviewed were:

- Denver Data Center Enclave General Support System (DDC) and supported applications:
  - Federal Financial System (FFS) – major application
  - Federal Personnel and Payroll System (FPPS)[3] – major application
  - Quarters Management Information System (QMIS) – major application
  - Oracle Federal Financials[4]

[3] FPPS includes Web FPPS, a Web-based front end for access to FPPS, and Quicktime, an electronic time and attendance system.

[4] Oracle Federal Financials and Momentum are not used by DOI; therefore, are not considered major applications. NBC has drafted system security plans for these applications.

- Reston Local Area Network General Support System (Reston-LAN) and supported applications:
    - Interior Department Electronic Acquisition System (IDEAS)[5] – major application (databases are housed within the DDC and Reston-LAN general support systems)
    - Momentum Financial and Acquisition[4]
- Interagency Aviation Services Local Area Network (IAS-LAN) General Support System and supported applications:
    - Automatic Flight Following (AFF)
    - Federal Aviation Resources System (FARS)
    - SAFECOM
    - SAFENET
    - Interagency Aviation Training (IAT)
    - Aviation Management Information Resource System (AMIRS)
- Drug Testing System – major application

Our review was conducted in accordance with the Quality Standards for Inspections issued by the President's Council on Integrity and Efficiency.

RESULTS OF REVIEW

With minor exceptions, we concluded that NBC's information security management program and practices met FISMA requirements. Our findings are described below. Also, the Appendix identifies the state of security processes which each system has undergone to meet FISMA requirements, as of July 30, 2004.

ASSESSING AND MANAGING RISK AND DETERMINING THE APPROPRIATE INFORMATION SECURITY LEVEL

Controls: DOI and NBC policies and procedures require risks be assessed every 3 years or whenever significant changes to the information system environment occurs. Further, as part of implementing FISMA, DOI has specified processes to identify risks, implement security protections commensurate with mitigating the risks to an acceptable level, and identify system security levels as part of system

[5] IDEAS comprises several applications including IDEAS-PD and IDEAS-EC. Non-DOI clients primarily use IDEAS-PD and can use IDEAS-EC, however clients must have IDEAS-PD before they can use IDEAS-EC. Clients can implement IDEAS-PD in several ways, including using DOI as a service organization that hosts the computing platform for the application and the related database or installing the application software and operating it in the clients' computing environment.

certification and accreditation. DOI’s process for identifying the system security levels is based on NIST Federal Information Processing Standards (FIPS) Publication 199, “Standards for Security Categorization of Federal Information and Information Systems.”[6] These processes for identifying risk and determining security levels include conducting:

- Assessments of privacy impact based on the information collected, stored, and processed by the systems.

- Assessments of technical vulnerabilities to test technical controls of the “as built” system.

- Evaluations of the asset and information to determine the overall importance of the system, the services the system provides, importance and sensitivity of the data, and the costs of the resources to operate and maintain the system. Based on the reviews, systems are categorized between high risk systems, such as National critical infrastructure information systems, financial systems, or wide area network systems; mission critical or business essential systems; or other sensitive but unclassified systems.

- Reviews of the 17 key control areas identified by NIST Special Publication 800-26, “Self Assessment of Information Technology Security Controls” [7] and through DOI’s 800-26 based questionnaire.

- Risk assessments based on NIST Special Publication 800-30 “Conducting Risk Assessments for Federal Information Systems.”[8]

Additionally, the Departmental Manual requires component-level IT security managers to certify and document system interconnections and information sharing arrangements to

[6] FIPS Publication 199 establishes the standards for categorizing information and information systems and establishes a common framework for Federal agencies in expressing adequate security and effectiveness of information security policy, procedures, and practices.

[7] NIST Special Publication 800-26 provides an agency with a methodology to determine the current status of its information security program and provides a target for improvement. The assessment questionnaire is based on 5 levels of security and 17 control areas. The results can produce a reliable measure of security effectiveness.

[8] NIST Special Publication 800-30 provides the foundation for developing an effective risk management program. The assessment allows management to make well-informed risk management decisions to justify IT expenditures and to determine whether an IT system should be accredited.

assure that inherited risks from other organizations are understood and managed.

Finding: NBC had identified the level of risk for the eight systems reviewed. However, some of these systems were not subject to a risk assessment or had not been re-assessed within a 3-year timeframe. For two of the systems (IAS-LAN and the Drug Testing System) no assessments of risk were conducted and for the remaining six systems, risk assessments had been completed, but the assessments were not conducted utilizing NIST Special Publication 800-30 guidance. NBC performed security tests and evaluations (ST&E)[9] of seven of the eight systems during fiscal year 2004. The ST&Es examined the risk assessments and reported them as insufficient. In addition, risk assessments of FFS and FPPS were performed over 3 years ago. NBC has reported these weaknesses in its Plan of Action and Milestone (POA&M) report.

The Drug Testing System is owned, managed, and operated by a contractor on behalf of DOI. Although NBC conducted some form of assessment of this system and identified the risk level as “low,” we do not agree with the risk level assigned. NBC had not conducted a privacy impact assessment or risk assessment of this system to support its decision. NBC’s self assessment of the system identified that the system contains Privacy Act information and sensitive information (results of employee drug tests); therefore, we believe the security level should be higher.

IAS-LAN is located in a contractor facility and operated by NBC staff and was evaluated during fiscal year 2004. However, we found that two agreements for acquiring IAS-LAN services did not clearly articulate the types of services provided, the applications to be used by the client, and each party’s roles and responsibilities for securing information.

The ST&E process also identified that NBC did not ensure that all inter-agency agreements included the information needed to ensure that risks were fully understood and protections were in place to reduce the risks to an acceptable level. To address this problem, NBC developed Security Service Agreements and Interconnect Security Agreements

[9] Security test and evaluation (ST&E) is a process to identify security weaknesses or vulnerabilities. DOI requires an ST&E for each system as part of the certification and accreditation process. DOI’s ST&E methodology is based on NIST Special Publication 800-37, “Guide for the Security Certification and Accreditation of Federal Information Systems.”

that are to be included as part of the overall agreements. However, only 1 of the 15 agreements we reviewed had a Security Service Agreement, and none had Interconnect Security Agreements. NBC reported in its POA&M that the Security Service and Interconnect Security Agreements will be incorporated by December 2005 as part of all applicable inter-agency agreements.

To ensure that risks are understood and security protections are established to reduce the risks to acceptable levels, we believe that an exchange of system security plans between NBC and its clients should be accomplished. This exchange will provide each party the necessary information to understand the level of importance each party assigns to the sensitivity and criticality of the systems and information as well as describing the respective control environments. Through these exchanges NBC will have a better understanding of the risks to its systems and external clients' requirements to ensure that appropriate protections are implemented.

PERIODICALLY TESTING AND EVALUATING INFORMATION SECURITY CONTROLS AND TECHNIQUES

Control: DOI's policy requires security controls and techniques to be tested and evaluated by DOI components through conducting monthly vulnerability scans of internal networks and annual self-assessments of controls based on DOI's self-assessment questionnaire. Additionally, as part of the certification and accreditation process, systems' controls are evaluated.

Finding: All eight systems reviewed had undergone DOI's self-assessment evaluation during fiscal year 2004. Also, FFS, FPPS, and Momentum are reviewed annually under Statement on Auditing Standards 70,[10] established by the American Institute of Certified Public Accountants. Controls over DOI's administrative systems (FFS, FPPS, and IDEAS) and the hosting general support systems are tested and evaluated as part of DOI's annual financial statement audits. Testing under the financial statement audits has not, at this time, identified any significant weaknesses in security of FFS, FPPS, and the supporting DDC general support system.

[10] Statement on Auditing Standard 70, "Reports on the Processing of Transactions by Service Organizations," includes EDP service centers that process transactions and data for others. The Standard provides guidance on the factors an independent auditor must consider when auditing the financial statements of an entity that uses a service organization. The review identifies control objectives, controls established to meet the objectives, and tests of the controls to determine whether they are operating effectively.

During fiscal year 2004 (as of July 30, 2004), NBC conducted limited technical vulnerability assessments of two systems, QMIS and IAS-LAN. Of the remaining six systems, all but the Drug Testing System, which had not had a technical vulnerability assessment, had limited technical vulnerability assessments performed during fiscal year 2003.

Additionally, as part of the certification and accreditation process, NBC conducted ST&Es on seven of the eight systems. We reviewed the ST&E methodology and scope for each system evaluated and concluded the ST&E process was generally comprehensive, except for the evaluation of the Reston-LAN. In this evaluation, the facility that housed Momentum was excluded. We also generally agreed with the level of risk assigned to the weaknesses. We reviewed the ST&E results of 74 weaknesses or vulnerabilities and the related residual risk reports which identified security related risks of the weaknesses or vulnerabilities that may affect NBC operations. Of the ST&E and residual risk reports reviewed, FFS and the enterprise server component of DDC had no weaknesses and the remaining six systems had 74 weaknesses of which 13 were considered high risk (IAS-LAN), 32 were considered medium risk, 22 were considered low risk, and 7 high-risk weaknesses were mitigated. NBC did include all of the other 67 weaknesses in its POA&M.

MINIMALLY ACCEPTABLE SYSTEM CONFIGURATION REQUIREMENTS

Control: DOI has established security technology implementation guidelines for configuration requirements of specific IT resources, such as UNIX operating system, and has also adopted certain NIST security configuration guidance, such as securing Windows XP.

Finding: NBC has guidance regarding baseline and security configuration requirements for its servers. Additionally, NBC reported that additional security configuration requirements are needed and this condition is reported as a weakness in its POA&M report. Within six of the seven systems that had security plans, we found some identification of system security configurations, but the configurations were not necessarily consistent.

SUBORDINATE PLANS

Control: DOI's policy requires each general support system and major application have an individual system security plan that is based on NIST Special Publication 800-18, "Guide for

Developing Security Plans for Information Technology Systems."[11]

Finding: All but one of the eight systems reviewed (Drug Testing System) had a system security plan. However, improvements are needed to most of the plans. The needed improvements include: better description of the control environment; assignment of security responsibility to appropriate personnel rather than to the NBC IT security manager or deputy or to individuals with other system management duties; descriptions of applications being supported by general support systems including external clients; clarification between current controls and planned controls; and identification of laws and regulations specific to a system rather than general information security laws and regulations such as FISMA. NBC reported these weaknesses in its POA&M.

INFORMATION SECURITY MANAGEMENT INTEGRATED WITH STRATEGIC AND OPERATIONAL PLANNING PROCESSES

Control: DOI specifies that security requirements be included in information technology budget and investment justification documents and that the DOI Office of the Chief Information Security Officer verify that the documents contain security requirements. Additionally, DOI requires that resource requirements needed to correct identified weaknesses be included in POA&Ms.

Finding: Generally, NBC included estimated funding for all planned corrective actions in the appropriate documents. Further, the DOI CIO requires that as part of the certification and accreditation process, POA&Ms be used for identifying, prioritizing, managing, and tracking actions to correct security weakness. NBC followed this process.

TRAINING PERSONNEL IN SECURITY RESPONSIBILITIES

Control: DOI requires that all employees and contractors complete annual online security awareness training. Additionally, DOI instituted a tracking system to identify and report the numbers and percentages of employees who have successfully completed the annual training. Further, NBC's policy requires that all newly hired employees and contractors successfully complete security training prior to obtaining access to NBC systems and applications.

[11] NIST Special Publication 800-18 identifies information to be included in a general support system and major application system security plan. This information includes a description of the system's security requirements, controls in place or planned for meeting those requirements, and the protection of information resources. The security plan is also the foundation for system accreditation.

Finding: As of June 2004, all NBC employees and contractors had successfully completed their annual security awareness training. In tests of systems and reviews of certification and accreditation documentation, we did not find any instances where new NBC staff and contractors were granted access to systems before completing the required training.

NBC has established a process to monitor the completion of specialized security training, including security awareness training, for employees holding key IT positions, such as program managers and system owners. However, NBC does not have a process to monitor the completion of technical or specialized training to ensure that training is regularly completed by employees and contractors with IT security responsibilities. DOI IT staff who manage the security of systems are also encouraged to attain the Certified Information System Security Professional certification. The NBC IT security manager and five other NBC staff have attained this certification. Also, NBC IT Directorate management had attended specialized training related to their information security management responsibilities.

Incident Detection and Reporting

Control: DOI's incident reporting and handling policy and handbook requires components to develop specific incident reporting and handling policies and procedures and to establish incident response teams. In addition, DOI has implemented an automated incident reporting system (DOI CIRC) and requires DOI components to report all incidents. Incidents reported to DOI CIRC are also reported to US-CERT. NBC also has policies and procedures for identifying, reporting, and handling computer security incidents and has a computer security incident response team. Further, NBC has rules of behavior that describe the process users of the systems should take in identifying and reporting incidents. Finally, all internal users are required to sign the rules of behavior prior to being granted access to NBC systems and applications.

Finding: NBC is following its handbook and is reporting incidents to DOI CIRC which are automatically reported to US-CERT.

Remedial Actions to Address Deficiencies

Control: DOI policy requires that weakness identified during any review be reported in POA&Ms. As part of the POA&M process, DOI requires components provide the DOI CIO with quarterly updates on progress in completing and managing corrective actions for each weakness.

Finding: NBC generally included weaknesses identified through Office of Inspector General audits and through NBC's system tests, evaluations, and self assessments in its POA&M.

Continuity of Operations

Control: DOI requires that continuity of operations plans be developed for every system and that the plans be tested at least annually.

Finding: NBC had business resumption plans and continuity of operations plans for six of the eight systems reviewed. However, contingency plans were not always updated based on tests of the plans and improvements were needed in documenting test results and applying lessons learned. We also noted that NBC's ST&E and self-assessment processes evaluated backup and recovery procedures and practices and identified only low-risk weaknesses.

Security Practiced throughout Life Cycle of Each Information System

Control: DOI's policy requires that every system include security as part of its life cycle management process. In addition, systems are required to be certified and accredited and are re-certified and re-accredited every 3 years or whenever significant changes occur.

Finding: NBC generally followed DOI's certification and accreditation process. That is, NBC generally described the security life cycle management for each of the seven system security plans we reviewed. Further, through the various reviews and assessments, NBC demonstrated that security was being practiced for six of the systems and that needed security improvements were reported, tracked, and monitored through NBC's POA&M process.

Suggestion for Improvement

To improve its security program, we suggest that NBC obtain from its clients' the system security plans for general support systems and major applications attributable to the application services being provided. In addition, we suggest that NBC provide to its clients the system security plans of the applications and general support systems used.

APPENDIX

Department of the Interior
National Business Center General Support Systems and Major Applications
Used by non-DOI Clients

										System Test and Evaluation				
System Name	**Operated By**	**Asset Valuation**	**Privacy Impact Assessment**	**System Security Plan**	**Self Assessment (800-26)**	**Limited or Technical Vulnerability Assessment**	**Risk Assessment**	**Contingency Plan**	**Testing of Contingency Plan**	**Report**	**Residual Risk Report**	**Weaknesses in Plans of Actions and Milestones**	**Certification**	**Accreditation**
Denver Data Center Enclave General Support System	DOI	Sept. 03	Yes	Sept. 03	March 04	Sept. 03	June 01	April 04	March 04	June 04	June 04	Yes	June 04	June 04
Applications Housed by Denver Data Center														
Federal Financial System	DOI	Sept. 03	Yes	Feb. 04	April 04	Sept. 03	July 00	April 04	March 04	June 04	July 04	Yes	July 04	July 04
Federal Personnel and Payroll System	DOI	July 04	Yes	July 04	March 04	Sept. 03	June 00[1]	April 04	Aug. 04	June 04	July 04	Yes	July 04	July 04
Quarters Management Information System	DOI	June 04	Yes	April 04	April 04	May 04	July 01	April 04	March 04	June04	July 04	Yes	July 04	July 04
Oracle Federal Financial[2]	This application is not considered as a DOI major application, therefore, it was included as part of the Denver Data Center Enclave General Support System													
Reston Local Area Network General Support System	DOI	May 04	Yes	May 04	April 04	Oct. 03	Sept. 03	Aug 03	Aug 03	June 04	June 04	Yes	June 04	June 04
Applications Housed by Reston Local Area Network General Support System														
Momentum[2]	This application is not considered as a DOI major application, therefore, it was included as part of the Reston Local Area Network General Support System													
Interior Department Electronic Acquisition System	DOI	July 03	Yes	Mar. 04	March 04	July 03	Oct. 01	Aug. 03	Aug. 03	May 04	June 04	Yes	June 04	July 04
Drug Testing System	Contractor				May 04							Yes		
Interagency Aviation Services Local Area Network General Support System	DOI/ Contractor	May 04	Yes	April 04	April 04	April 04				June 04	June 04	Yes	June 04	June 04
Applications Housed by Interagency Aviation Services Local Area Network														
Automatic Flight Following System	These applications are not considered by DOI as major applications, therefore, they were included as part of the Interagency Aviation Services Local Area Network													
Federal Aviation Resources System														
SAFECOM														
SAFENET														
Interagency Aviation Training System														

[1] An asset valuation, technical vulnerability assessment, and a self-assessment were completed in June 2003 of the Federal Personnel and Payroll System based on the Department's definition of an "initial" risk assessment.

[2] Oracle Federal Financial System and Momentum are used by non-DOI clients.