NATIONAL ENDOWMENT FOR THE ARTS
OFFICE OF INSPECTOR GENERAL

EVALUATION REPORT

FISCAL YEAR 2007 EVALUATION

NEA'S COMPLIANCE WITH THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT OF 2002

REPORT NO. R-08-01
OCTOBER 22, 2007

INTRODUCTION

The Federal Information Security Management Act of 2002 requires an annual evaluation by the Inspector General on its agency's information security programs and practices. This report is an evaluation of NEA's information security program and practices for protecting its information
technology (IT) infrastructure.

BACKGROUND

The Federal Information Security Management Act (FISMA) of 2002 was signed into law on November 27, 2002. It replaced the Government Information Security Reform Act (GISRA), which expired in November 2002. The Act requires each federal agency to develop, document, and implement an agency-wide information security program to provide information security over the operations and assets of the agency. This includes:

- Periodic risk assessments;
- Policies and procedures that are based on risk assessments;
- Subordinate plans for providing adequate information security for networks, facilities, information systems, or groups of information systems, as appropriate;
- Security awareness training to inform employees (including contractors) of the security risks associated with their activities and their responsibilities to comply with those agency policies and procedures designed to reduce those risks;
- Periodic testing and evaluation of the effectiveness of information security policies;
- A process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices, of the agency;
- Procedures for detecting, reporting, and responding to security incidents; and
- Plans and procedures to ensure continuity of operations of the agency's information systems.

Office of Management and Budget (OMB) Memorandum M-07-19, dated July 25, 2007, entitled "FY 2007 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management," updates instructions to Senior Agency Officials for Privacy, Chief Information Officers and Inspectors General for reporting their 2007 information to OMB.

The National Institute of Standards and Technology (NIST), which has the responsibility for developing technical standards and related guidance, has issued numerous publications including An Introduction to Computer Security: The NIST Handbook. This publication explains important concepts, cost considerations, and interrelationships of security controls as well as the benefits of such controls. NIST also has published a

Guide for Developing Security Plans for Information Technology Systems. In addition, guidance is found in the Government Accountability Office publication, Federal Information System Controls Audit Manual (FISCAM). NIST has also issued Special Publication 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems; Special Publication 800-53, Recommended Security Controls for Federal Information Systems; and FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems.

NEA's Office of Information and Technology Management (ITM) maintains and operates two of three core systems on a local area network (LAN). These are the Grants Management System (GMS), which contains information on grant applications and the Automated Panel Bank System (APBS), which contains information on panelists who review grant applications. NEA has contracted with the Department of Transportation Enterprise Service Center to host NEA's Financial Management System (FMS) through its Delphi Financial Management System. In addition, NEA operates support systems including electronic mail, and internet and intranet services.

The Chief Information Officer (CIO) is responsible for developing policies and procedures to ensure that security is provided over NEA's computer and data networks.

OBJECTIVE AND SCOPE

The objective of the evaluation was to determine the adequacy of NEA's information technology (IT) security program and practices. This included a review of NEA's IT security policies and procedures, interviews with responsible agency officials managing the IT systems, and tests on the effectiveness of security controls.

PRIOR EVALUATION

The NEA Office of Inspector General issued a report entitled "Fiscal Year 2006 Evaluation of NEA's Compliance with the Federal Information Security Act of 2002" (Report No. R-06-02) dated September 21, 2006. The report had eight recommendations, all of which have been resolved. It is noted that there was a recommendation that NEA IT conduct an e-authentication risk assessment as required by OMB. It was subsequently determined that NEA systems did not meet the necessary requirements for an e-authentication risk assessment to be conducted. Therefore, the recommendation was considered to be resolved.

EVALUATION RESULTS

Our current evaluation determined that there are several issues that need to be addressed by NEA's Information and Technology Management Division. These include issues

related to e-authentication risk assessment, updating the Security and Disaster Recovery Plans, and implementing procedures related to security awareness training, inventory, and change management. Details are presented in the following narrative.

Risk Assessment

SeNet International Corporation performed the last risk assessment, the results of which were issued on August 26, 2005. The review concluded, "The implementation and management of the security architecture supporting the National Endowment for the Arts enterprise network appears to require strengthening in order to more effectively restrict unauthorized internal access to information resources."

The review cited the following weaknesses at the time of their review:

- Systems were discovered that did not have the latest security patches,
- Systems were discovered running unnecessary or potentially vulnerable services,
- Weak passwords were identified, and
- Open shares were discovered where potentially sensitive information could be discovered.

NEA ITM has addressed these weaknesses in its "The Security Audit Action Plan" in response to the risk assessment. The only vulnerability remaining for corrective action related to systems that were discovered running unnecessary or potentially vulnerable services. The solution was to replace the Windows 2000 Servers with Windows 2003 Servers. These new Windows 2003 Servers were installed by December 31, 2005.

E-Authentication Risk Assessment. OMB Memorandum 04-04 issued December 16, 2003, directed "agencies to conduct 'e-authentication risk assessments' on electronic transactions to ensure that there is a consistent approach across government." The guidance applies to "remote authentication of human users of Federal agency IT systems for the purposes of conducting government business electronically (or e-government)."

The 2007 FISMA guidance issued by OMB asks Inspectors General to determine whether such an assessment was conducted. No such assessment was conducted. NEA IT determined that NEA systems did not meet the necessary requirements to conduct an e-authentication risk assessment. Since NEA systems are not internet-based, are not available to users outside of the agencies firewall, and do not require authentication from users on the outside. As such, we agreed that NEA ITM was not required to perform the e-authentication risk assessment.

NIST Self-Assessment

ITM conducted its 2007 self-assessment using the controls found in the National Institute of Standards and Technology (NIST) Special Publication 800-53, "Recommended Security Controls for Federal Information Systems." The primary issues identified in this assessment included the lack of written policies regarding remote access monitoring, portable and mobile devices, media protection, risk assessment, and system and service acquisition. Weaknesses identified in this self-assessment should be included in NEA's *Plans of Action and Milestones* (POA&Ms), which is updated quarterly and submitted to the Office of Management and Budget.

Security Plan

NEA issued its security plan for each of its in-house GMS and APBS systems that address FISMA and OMB requirements in September 2004. The development of security plans are an important activity in an agency's information security system that directly supports the security accreditation process required under FISMA and OMB Circular A-130. Security plans should ensure that adequate security is provided for all agency information collected, processed, stored, or disseminated in NEA's general support systems and major applications. It is noted that there has been changes to the NEA Network. The last update for the NEA Network that is included in the Security Plan is dated June 2007.

Security Certification and Accreditation. As noted previously, NEA hosts both the GMS and APBS, both of which were certified and accredited on September 26, 2004. The FMS is contracted to the Department of Transportation Enterprise Service Center. The 2005 SeNet Report noted that three major systems were identified and granted the Authority to Operate in November 2004. In their review of the Certification and Accreditation (C & A) documentation, they stated, "it appears that the process that was used to perform the C & A does not meet established best practices or federal guidelines.

As a result, ITM took appropriate action and in March 2006, ITM recertified that that the Local Area Network (LAN), and all Information Systems (GMS - Grants Management System, Delphi – Financial Management System, and APBS – Automated Panel Bank System) have the appropriate safeguards in place and the data processed is secure. NEA implemented a single site certification program and accreditation program using the Federal Information Security Act of 2002, Public Law 107-347, OMB Circular A-130, and NIST 800-37 as the implementation guidance for its development. This accreditation is valid until March 2009.

Disaster Recovery Plan

NEA has documented its disaster recovery plan (July 2002). The recovery plan provides that:

- NEA will maintain an alternate e-mail address resident on a server outside of the NEA facilities to support emergency communications.

- An Emergency Recovery Server will be maintained within the building, but in a physical location distant from ITM to facilitate Level One and Level Two recoveries. It shall contain current software, updated nightly, that duplicates that which is in use by NEA.

- Standby network equipment will be maintained in a location outside of ITM to restore operations.

- At the end of every business day, two backup copies of all systems data will be taken. One will be stored outside of the building and one will be stored within the building, but outside of the Computer Center.

Our prior evaluation included a recommendation that IT update the Disaster Recovery Plan to include changes in the handling of backup copies of systems data. A supplement to the Disaster Recovery Plan has been issued to include those changes.

Security Training

ITM had previously documented a security-training plan (August 2002) for ITM staff and contractors. The purpose of the plan was to ensure that NEA employees with significant security responsibilities (1) have the most current computer security information and (2) have an adequate understanding of computer/IT security laws and requirements.

NIST Special Publication 800-50, Building an Information Technology Security Awareness and Training Program and NIST Special Publication 800-16, Information Technology Security Training Requirements: A Role- and Performance-Based Model, provide the standards for security awareness and training. We recommended in our 2005 evaluation that ITM implement security awareness training to all NEA employees as soon as possible. This training was implemented in December 2005. However, it was noted in our previous 2006 evaluation that ITM did not develop a system to readily identify those who have taken or have not taken the training. ITM has since implemented procedures to document who has taken the training.

Security Incidents

NEA has formalized a "Computer Security Incident Policy" (Revised November 2003), which (1) identifies the type of activity characterized as a computer security incident, and (2) defines the steps to be taken to report a computer security incident. The policy applies to all permanent and temporary employees, including contractors who utilize NEA's computer equipment and systems.
It is generally known that security incidents have become more frequent whether they are caused by viruses, hackers, or software bugs. Appendix III to OMB Circular A-130 states:

> **When faced with a security incident, an agency should be able to respond in a manner that both protects its own information and helps to protect the information of others who might be affected by the incident. To address this concern, agencies should establish formal incident response mechanisms. Awareness and training for individuals with access to the system should include how to use the system's incident response capability.**

Any NEA computer security incidents are handled by ITM's Computer Security Incident Team (CSIT), which consists of two employees from ITM's Customer Services Division and two employees from ITM's Plans, Policy and Programs Division. One employee, who is designated as the CSIT coordinator, serves as the team's central resource for monitoring computer security incidents.

NEA's policy states, "Any employee or contractor who has knowledge of a computer security incident should report the incident to the CSIT Coordinator via e-mail (or phone if e-mail is not available)."

Our 2003 evaluation recommended that NEA revise its computer incident security policy to reflect FedCIRC timeframe requirements for security incident reporting. A revised computer incident policy was issued in November 2003 and established timeframes for reporting security incidents to FedCirc.

Despite numerous attempts to intrude NEA systems during the past year, there were no successful incidents referred by employees to NEA ITM officials within the context of NEA's Computer Security Incident Policy.

Access Controls

ITM developed and implemented an "Access Control Policy" in December 2001 that established procedures for removing terminating employees' user IDs and passwords for the LAN, e-mail and mission critical systems. ITM also developed and implemented procedures applicable to employees terminating their NEA employment that specifically note the steps required to clear applicable user IDs and passwords.

NIST recommends periodic reviews of user account information for managing user access. NEA does have controls in place that requires LAN users to change their passwords every 60 days and ensures that intruders (those who make numerous attempts to access the LAN) are locked out of the system after four attempts to log in with an invalid password.

Our 2002 evaluation noted that ITM was not always notified when school interns leave NEA. These are students who work during the summer or break periods, but are not paid by NEA. Since NEA does not pay the interns, there was no means to ensure that exit clearance procedures were followed (such as withholding their final pay). In addition, the supervisors of these interns were not always informing ITM of their departure because there was no requirement for such. Thus, these interns could potentially continue to access and use the e-mail system from an alternate location for unauthorized purposes. As a result, NEA instituted new sign-out procedures for interns, temporary contractors and volunteers. However, our 2003 evaluation found that ITM was still not being informed timely about such individuals. Although ITM has requested departure dates from the Human Resources Division for these temporary employees, the dates were not always provided. We recommended that ITM not initiate computer or e-mail access unless a departure date is provided.

As a result, the "Access Control Policy" was revised in November 2003 to include that "before computer access can be granted to temporary employees/contractors, the Human Resources Division must inform ITM of the anticipated end dates for these individuals' assignments in order to ensure that their access rights are removed at the appropriate time." The August 2005 SeNet report noted that weak passwords were identified and, as a result, NEA ITM implemented a new stronger password policy, which was formally issued in March 2006. This password policy continues to be followed.

Physical Controls

NEA appears to have adequate physical controls to protect its IT inventories and supplies. The facilities are protected by fire alarms and sprinkler systems. Access to NEA's space in the building is controlled by guards who require proper identification for entry. During nonworking hours, sign-in and sign-out procedures are in effect. The computer data room has cipher locks to restricted areas and this entire area is always secured and locked.

If NEA contracts for IT services that requires access to its computer data room, the access code (via a cipher lock) that is used by the contractor is different from the code used by NEA ITM employees. In addition, the contractor's access code is changed whenever one of the contractor's operators is terminated.

Inventory Controls

NEA has an inventory of its hardware and has updated its listing with the last entry as of September 20, 2007. The inventory lists each item by office, barcode number, serial number, manufacturer, model number and description, as well as the user. The inventory is maintained on a perpetual basis and is updated as equipment is added or deleted. It also indicated the date the inventory was taken and the initials of the person who took the inventory.

Contractor Security

NEA appears to have imposed adequate security measures on its contractors. All short-term (data entry) contractors have limited computer access. That is, they do not get a full menu upon login and are limited on what they can input into the system, which is restricted by their user name and password. For example, they cannot access or input data into any systems management function. They also do not have internet or intranet access. Since the contracts are short-term, users are deleted from the system upon contract termination.

Computer access for a long-term contractor involved with NEA systems and the help desk generally is unrestricted. However, the CIO and ITM carefully screen these contractors and require background checks.

Change Management

Both our 2003 and 2004 evaluations concluded that ITM must develop policies and procedures related to change management and control for the development and modification of IT systems. ITM issued a "Change Management Policy/Procedure" effective December 1, 2004. This policy "describes the responsibilities, policies, and procedures to be followed by ITM when making changes or recording events to the National Endowment for the Arts IT infrastructure." It defines "change" and "event" as follows:

> **Change: to transform, alter, or modify the operating environment or standard operating procedures; any modification that could have potential and/or significant impact on the stability and reliability of the infrastructure and impacts conducting normal business operation by our users and ITM; any interruption in building environments (i.e., electrical outages) that may cause disruption to the IT infrastructure.**
>
> **Event: any activity outside of the normal operating procedures that could have a potential and/or significant impact on the stability and reliability of the infrastructure, i.e. a request to keep a system up during a normal shutdown period.**

The change management process includes the submission of a change request with management approval. During our prior evaluation, it was noted that when we requested

a log and/or copies of such requests, there have been none submitted. As a result, a recommendation was made that IT implement procedures to ensure compliance with the NEA Change Management Policy. Our current evaluation noted that IT has implemented such procedures and *ITM Change Management Request Forms* are now maintained.

Financial Management System

NEA has an agreement with the U.S. Department of Transportation (DOT) to utilize the Enterprise Service Center's Oracle Federal Financials System, Delphi, as their financial management system. OMB requires that such service organizations to provide client agencies with an independent report describing system controls. To comply with this requirement, DOT OIG hired an independent contractor, Clifton Gunderson, LLP, to conduct a review on the computer controls over the information technology and data processing environment, as well as the input processing, and output controls built into the Delphi system.

The independent contractor rendered an opinion on the effectiveness of those controls for the eight-month period from October 1, 2006 through May 31, 2007. The audit concluded that "management's description of controls presents fairly, in all material respects, the controls that have been placed in operation as of May 31, 2007. In addition, controls are suitably designed and were operating effectively on 9 of 10 control objectives during the period from October 1, 2006, through May 31, 2007. The exception is logical access controls because management has not completed the move of the Delphi servers to a more secure environment."

NEA also uses the Department of Agriculture (USDA) National Finance Center as its payroll provider. The latest Statement on Auditing Standards Number 70 (SAS 70) Review of the Department of Agriculture Office of the Chief Financial Officer/National Finance Center (OCFO/NFC) issued by the USDA OIG was for fiscal year 2006. This review concluded that the Department of Agriculture Office of the Chief Financial Officer/National Finance Center's "description of controls presented fairly, in all material respects, the relevant aspects of OCFO/NFC." Also, in their opinion, "the controls included and/or referenced in the description, as updated, were suitably designed to provide reasonable assurance that associated control objectives would be achieved if the described policies and procedures were complied with satisfactorily and customer agencies applied the controls specified in the OCFO/NFC description of controls."

The 2006 USDA report described "weaknesses in OCFO/NFC internal control policies and procedures that may be relevant to the internal control structure of OCFO/NFC customer agencies." The report further stated that "OCFO/NFC reinstituted control activities that were disrupted after Hurrican Katrina and updated its procedures to address the control weaknesses" that were identified.

The 2007 USDA SAS 70 Report on the National Finance Center was not available at the time of our evaluation in September 2007. We recommend that NEA ITM provide us with a copy of the report as soon as it becomes available.

EXIT CONFERENCE

An exit conference was held with NEA's CIO on October 22, 2007. The CIO generally concurred with our recommendations and has agreed to initiate corrective actions.

RECOMMENDATIONS

We recommend that the NEA Office of Information and Technology Management:

1. Include corrective actions for weaknesses identified in its IT self-assessment in NEA's *Plans of Action and Milestones* (POA&Ms), which is updated quarterly and submitted to the Office of Management and Budget.

2. Provide the Office of Inspector General with a copy of the 2007 Statement on Auditing Standards Number 70 (SAS 70) Review of the Department of Agriculture National Finance Center.