NATIONAL ENDOWMENT FOR THE ARTS
OFFICE OF INSPECTOR GENERAL

EVALUATION REPORT

FISCAL YEAR 2006 EVALUATION

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

REPORT NO. R-06-02
SEPTEMBER 21, 2006

INTRODUCTION

The Federal Information Security Management Act of 2002 requires an annual evaluation by the Inspector General on its agency's security programs and practices. This report is an evaluation of NEA's 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 replaces 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-06-20, dated July 17, 2006, entitled "FY 2006 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 2006 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 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 2005 Evaluation of NEA's Compliance with the Federal Information Security Act of 2002" (Report No. R-06-01) on October 4, 2005. The report recommended that NEA ITM (1) review the certification and accreditation process for deficiencies identified in an independent vulnerability analysis report and take appropriate corrective actions, (2) ensure that the Windows 2003 servers are installed in a timely manner, and (3) implement security awareness training for all NEA employees.

NEA ITM has implemented all three of the recommendations in the prior report. For Recommendation 1, NEA ITM issued a document entitled "National Endowment for the Arts Information System Network and Site Accreditation" in March 2006. Also, the Certification and Accreditation (C & A) documents for the three major systems have been combined into one. For Recommendation 2, Windows 2003 servers were installed and a monthly maintenance program began in November 2005. For Recommendation 3, ITM began periodic refresher IT security awareness training to all NEA employees in October 2005.

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 was contracted to perform a risk assessment, the results of which were issued on August 26, 2005. (See Appendix 1.) 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 systems 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 2006 FISMA guidance issued by OMB asks Inspectors General to determine whether such an assessment was conducted. It was determined that NEA ITM has not conducted an e-authentication risk assessment. We are recommending, therefore, that such an assessment be conducted.

NIST Self-Assessment

ITM conducted its 2006 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 issue identified in this assessment related to change modifications and the logging of such information, which is discussed under the "Change Management" section of this report.

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 May 2004. It is recommended that the Security Plan be updated to reflect changes to the Network.

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.

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 current review noted that there have been changes made with respect to backup copies of systems data. The Disaster Recovery Plan has not been updated 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. NEA issued a "Security Awareness and Training Policy" in April 2005. In our October 2005 Evaluation Report, we recommended that ITM implement security awareness training to all NEA employees as soon as possible. This training was implemented in December 2005. However, ITM needs to develop a system to readily identify those who have taken or have not taken the training. While employees reply to ITM through an e-mail notification that they have taken this training, there is no master list of current NEA employees to which this information is recorded. This makes it difficult to follow up with non-participating employees. ITM did have a listing of who took the training, but it was found to be inaccurate as there were employees not listed who actually did complete the required training.

New NEA employees are given general security awareness training as part of their orientation, but ITM does not have this documented nor does the employee sign an acknowledgement that such training was provided. While there is a form signed by employees acknowledging security responsibilities, it does not acknowledge security awareness training. We recommend that procedures be implemented to acknowledge when a new employee has received this 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.

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 secured and locked from 7:30 PM to 6:30 AM on weekdays and throughout the weekend.

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 August 9, 2006. The inventory lists the 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. However, although we observed the taking of a physical inventory recently by ITM in our own offices, ITM did not record the date the inventory was actually performed. We recommend that ITM implement procedures to record the date and the person actually performing 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 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 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. However, when we requested a log and/or copies of such requests, there have been none submitted since this policy was implemented.

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 was to render an opinion on the effectiveness of those controls for the eight-month period from October 1, 2005 through May 31, 2006. The final audit report was to be issued by June 30, 2006. However, per DOT OIG, this report has not yet been issued as of September 12, 2006. DOT OIG expected the report to be released by the end of September 2006.

As part of our prior 2005 evaluation, we reviewed the DOT Office of Inspector General (OIG) "Quality Control Review of the Report on Controls over the Delphi Financial Management System, DOT" (Report No. QC-2005-075 dated September 2, 2005). The audit itself was performed by performed by Clifton Gunderson, LLP, an independent auditor. The DOT OIG performed a quality control review of Gunderson's work to ensure that it complied with *Generally Accepted Government Auditing Standards* and the American Institute of Certified Public Accountants *Statement on Auditing Standards (SAS) 70*. In the opinion of the DOT OIG, the audit work complied with applicable standards.

The independent auditor's report made 12 recommendations to improve controls and submitted the recommendations to DOT management. The DOT Deputy Chief Financial Officer concurred with the recommendations and committed to implementing corrective actions in a response dated August 25, 2005.

During the 2005 Delphi review, it was reported that NEA had 32 incompatible roles related to users of the Delphi system. Per NEA, this is primarily due to the fact that NEA has only six persons to perform all the functions. NEA has been working with DOT's Enterprise Service Center to address this segregation of duties issue. The number of incompatible roles was reduced from 32 to 6 as of September 5, 2006. NEA is continuing to work with DOT to eliminate this problem.

We recommend that NEA ITM provide us with a copy of the 2006 Delphi SAS 70 Report as soon as it becomes available.

EXIT CONFERENCE

An exit conference was held with NEA's CIO on September 20, 2006. 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. Conduct the e-authentication risk assessment required by OMB.

2. Update the Security Plan to include changes in the NEA Network.

3. Update the Disaster Recovery Plan to include changes in the handling of backup copies of systems data.

4. Develop a system to readily identify NEA employees who did and did not complete annual security awareness training.

5. Implement procedures to document that a new NEA employee actually participated in security awareness training.

6. Implement procedures to record the date and the person actually performing an ITM physical inventory.

7. Implement procedures to ensure compliance with the NEA Change Management Policy.

8. Provide the Office of Inspector General with a copy of the 2006 independent audit report on DOT's Delphi Financial Management System.