NATIONAL ENDOWMENT FOR THE ARTS
OFFICE OF INSPECTOR GENERAL

EVALUATION REPORT

Fiscal Year 2005 Evaluation of NEA's Compliance with the Federal Information Security Management Act of 2002

REPORT NO. R-06-01
OCTOBER 4, 2005

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.

OMB Memorandum M-05-15, dated June 13, 2005, entitled "FY 2005 Reporting Instructions for the Federal Information Security Management and Agency Privacy Management," updates instructions to Senior Agency Officials for Privacy, Chief Information Officers and Inspectors General for reporting their 2005 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 recently 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 2004 Evaluation of NEA's Compliance with the Federal Information Security Act of 2002" (Report No. R-05-01) on October 5, 2004. The report recommended that NEA ITM (1) develop written policies and procedures related to change management and control for the development and modification of systems, and (2) establish a training plan that includes periodic refresher IT security awareness training to all NEA employees.

Of the two recommendations in the prior evaluation, NEA has implemented the recommendation related to change management. NEA has also established a training plan that includes periodic refresher IT security awareness training to all NEA employees, but had not provided any such training to NEA employees as of the time of our evaluation in September 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 security certification and accreditation, the replacement of Windows 2002 servers, and the implementation of periodic security training for all NEA employees. 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 "The Security Audit Action Plan," which is included as Appendix 2. The only vulnerability remaining for corrective action relates to systems that were discovered running unnecessary or potentially vulnerable services. The solution is to replace the Windows 2000 systems with Windows 2003 Servers.

According to NEA ITM officials, the new servers will be installed by December 31, 2005.

NIST Self-Assessment

ITM used the National Institute of Standards and Technology (NIST) self-assessment guide (Special Publication 800-26, "Security Self-Assessment Guide for Information Technology Systems") to review NEA's systems in September 2005. The prior year's assessment noted that ITM must develop a written change management control policy and procedures for the development and modification of its systems. Such policy and procedures are important because any system changes can have security implications that may introduce or remove vulnerabilities. Such a policy and procedures were developed and implemented in December 2004.

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.

Security Certification and Accreditation. NEA hosts both 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. The two NEA-hosted systems were certified and accredited on September 26, 2004.

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. For example, the LAN is not even considered and a GSS (General Support System) was not identified." The SeNet report recommended that NEA create four separate C & A packages.

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.

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. It is noted that although new NEA employees are given general security awareness training as part of their orientation, NEA does not provide refresher IT security training to its employees on a regular basis. ITM does send out periodic IT security awareness flyers and e-mails to its employees, but NIST Pub 800-16 states that "awareness is not training." We recommended in our 2004 evaluation that ITM establish a training plan that includes periodic refresher IT security awareness training to all of NEA's employees.

NEA ITM established a training policy in November 2004 that included a security education plan. One of the subject areas of that plan was refresher training, which was defined as "programs and products designed to provide continuing education to the Agency community on relevant security topics. Such programs include annual briefings through the Government Online Learning Center." As of September 29, 2005, no such refresher training has been offered to NEA employees. We recommend that NEA ITM implement security awareness training to all NEA employees as soon as possible.

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.

Security incidents have generally 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.

All 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 SeNet report noted that weak passwords were identified and NEA ITM immediately implemented a stronger password policy.

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 conducted a physical inventory of its hardware and has updated its inventory listing (dated September 12, 2005). 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.

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.

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. As part of our 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 Gunderseron, 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.

EXIT CONFERENCE

An exit conference was held with NEA's CIO on October 4, 2005. 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. Review the certification and accreditation process for deficiencies identified in the SeNet Vulnerability Analysis Report and take appropriate corrective actions.

2. Ensure that the Windows 2003 servers are installed in a timely manner.

3. Implement security awareness training for all NEA employees.

National Endowment for the Arts
A Great Nation Deserves Great Art

Vulnerability Assessment

August 26, 2005

Prepared by:

SeNet International Corporation
e-Security—we make it practical.

***Note*: The Office of Inspector General has included only the "Executive Summary" of this report for this Appendix.**

1. Executive Summary

The implementation and management of the security architecture supporting the National Endowment for the Arts (NEA) enterprise network appears to require strengthening in order to more effectively restrict unauthorized internal access to information resources. Through the performance of the network security assessment, SeNet discovered that NEA has implemented some effective controls for protecting information resources. However, several areas were identified where NEA can improve upon its security architecture to further enhance its overall security posture. Implementing strong computer security is extremely important for organizations of all sizes.

SeNet last performed a vulnerability assessment for NEA in 2002. Since that time NEA has made some marked improvements in its protection of information resources, especially in the areas of documentation and external perimeter security. When SeNet last performed the review, documentation was severely lacking. Currently NEA has compiled documentation covering the primary security topics. While this is a step in the right direction there is still more work to do in this area. For example, the C&A package that was reviewed does not follow all of the standards and format that NIST recommends. Likewise, when SeNet last performed vulnerability testing from an external perspective some serious findings were noted. During this round of external testing no critical findings were noted.

When SeNet began the internal testing some serious findings were discovered. Through a combination of vulnerabilities the SeNet team was able to compromise several systems and even gain control of the firewall. The majority of these vulnerabilities were related to un-patched systems, unnecessary services, and weak passwords. The vulnerabilities SeNet did find and exploit can all be fixed with minimal financial outlay, but do require time and trained personnel.

The areas of concern noted during the network security assessment contain several high-risk vulnerabilities as well as several medium to low risk vulnerabilities. The more serious vulnerabilities are discussed below; all other vulnerabilities appear in the *"Detailed Findings and Recommendations"* section and in *Appendix A* of this report:

Vulnerabilities

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

It is suggested that NEA follows these recommendations:

- Apply the latest security patches
- Review all services that are enabled and disable those that are not needed
- Enforce the use of strong passwords on all accounts
- Review all shares and require authentication

For a complete listing of all recommendations please see Appendix A. Also see the discussion in Section 3 of this report.

NEA management should be aware that due to the potential risk associated with connectivity to the Internet, and the regularity in which new vulnerabilities are identified with information technology, results of test procedures performed may not have revealed all potential vulnerabilities.

The Security Audit Action Plan

Some of the vulnerabilities SeNet found were corrected with minimal financial outlay.

Vulnerabilities

Vulnerability: Systems were discovered that did not have the latest patches.

Completed Solution: The latest service patches were applied, and it is resolved that once a month the latest patches will be applied to each networked system.

Vulnerability: Systems were discovered running unnecessary or potentially vulnerable services.

Solution: The systems discovered were Windows 2000 systems that will be replaced with Windows 2003 Servers. This replacement will eliminate the potentially vulnerable services.

Vulnerability: Weak passwords were identified.

Completed Solution: Enforced the use of strong passwords on all accounts thru Directory Services and the password policy.

Vulnerability: Open shares were discovered where potentially sensitive information could be discovered.

Completed Solution: This open share happens to be the Unix Xerox machine connected to our network. Disconnecting the copier eliminated this problem.

<u>Note</u>: The above Security Audit Action Plan was prepared by NEA ITM.