NATIONAL ENDOWMENT FOR THE ARTS
OFFICE OF INSPECTOR GENERAL

EVALUATION REPORT

Fiscal Year 2004 Evaluation of NEA's Compliance with the Federal Information Security Management Act of 2002

REPORT NO. R-05-01
OCTOBER 5, 2004

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-04-25, dated August 23, 2004, entitled "FY 2004 Reporting Instructions for the Federal Information Security Management," updates instructions to Chief Information Officers and Inspectors General for reporting their 2004 information to OMB. This guidance requires that:

- The agency must respond to performance measures and provide narrative responses.
- Agencies must follow NIST standards and guidance or non-national security programs and systems.
- Senior agency program officials and CIOs review all programs and systems at least annually.
- Agencies should use the NIST "Security Self-Assessment Guide for Information Technology Systems."
- Requires each agency to test and evaluate security controls annually.
- Agencies' corrective action plans must be shared with the agency Inspector General to ensure independent verification and guidance.

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 General Accounting Office publication, Federal Information System Controls Audit Manual (FISCAM). During the past year, NIST has issued Special Publication 800-37, Guide for the Security Certification and Accreditation of 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 three core systems on a local area network (LAN). These are the Grants Management System (GMS), which contains information on grant applications and awards; the Financial Management Information System (FMIS), which contains financial information on payroll, purchase orders, contracts, etc.; and the Automated Panel Bank System (APBS), which contains information on panelists who review grant applications. 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 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 2003 Evaluation of NEA's Compliance with the Federal Information Security Act of 2002" (Report No. R-03-03) on September 17, 2003. The report recommended that NEA ITM (1) develop written policies and procedures related to security certification and accreditation of NEA's systems; (2) develop written policies and procedures related to change management and control for the development and modification of systems; (3) install the procured intrusion detection software as soon as possible; (4) adhere to its security-training plan to provide specialized training for NEA employees with significant security responsibilities on an annual basis; (5) revise its computer incident security policy to reflect FedCIRC timeframe requirements for security incident reporting; and (6) ITM not initiate computer or e-mail access for interns, temporary contractors, or volunteers unless NEA's Human Resources Division provides a departure date for those individuals.

Of the six recommendations in the prior evaluation, five were resolved and implemented. (See Appendix) The recommendation to develop written policies and procedures related to change management and control for the development and modification of systems is being repeated in the current evaluation.

EVALUATION RESULTS

Our current evaluation determined that NEA's Information and Technology Management Division has made substantial improvements for compliance with existing Federal requirements for information security. Details are presented in the following narrative.

Risk Assessment

As noted in our prior FISMA review, SeNet International Corporation was contracted to perform a risk assessment, the results of which were issued on July 5, 2002. The overall assessment stated, "NEA should concentrate on documenting and implementing its security program plan, contingency planning, and operating procedures." ITM has taken corrective action on all deficiencies noted in the report. NEA contracted with the Federal

Aviation Administration to host its financial management system beginning in fiscal year 2005. NEA also plans to contract for another risk assessment during fiscal year 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 August 2004. Again, it was noted that ITM must develop written change management control policy and procedures for the development and modification of its systems. This was noted in the prior 2003 self-assessment, which also concluded that (1) ITM must develop policies and procedures related to security certification and accreditation of NEA’s systems and (2) install intrusion detection software.

Security Certification and Accreditation. The 2003 self-assessment concluded that ITM must develop policies and procedures related to security certification and accreditation of NEA’s systems. This conclusion was based on criteria established by NIST in its draft Special Publication 800-37 “Guide for the Security Certification and Accreditation of Federal Information Systems.” As stated in the draft guide, “*Security accreditation* is the official management decision to authorize operation of an information system.” The guide further states, “Security accreditation, which is required under OMB Circular A-130, provides a form of quality control and challenges managers and technical staff at all levels to implement the most effective security controls and techniques, given technical constraints, operation constraints, cost and schedule constraints, and mission requirements.”

NEA IT management policy now requires that all systems that access NEA data be certified and accredited. For new application systems, the certification process must begin during the design and development stage. All systems must be recertified at least once every three years or if the systems undergo a significant modification or is violated.

The NEA’s certification and accreditation process appears to be in compliance with NIST Special Publication 800-37 and the FIPS 199. All three NEA systems were certified and accredited on September 26, 2004.

Change Management Control Policy and Procedures. The 2003 self-assessment also concluded that ITM must develop policies and procedures related to change management and control for the development and modification of systems. Such policy and procedures are important because any system changes can have security implications that may introduce or remove vulnerabilities. Furthermore, such changes may require an update of the contingency plan, risk analysis, or accreditation. We agreed that ITM must develop policies and procedures related to change management and control for the development and modification of systems. However, our current evaluation determined that these policies and procedures have not been completed. This is due primarily to the unexpected departure of the prior security officer and subsequent delays in assigning a new permanent security officer. ITM now expects to complete these policies and procedures early in fiscal year 2005. We are again recommending that ITM develop written policies and procedures related to change management and control for the development and modification of its systems.

Intrusion Detection Software. As stated above, the 2003 self-assessment concluded that intrusion detection software must be installed. Real-time intrusion detection is aimed at detecting outsiders attempting to gain access to the system. ITM did install intrusion detection software, entitled "SiteProtector," in December 2003.

Security Plan

NEA reissued its security plan for each of its three major systems (GMS, FMIS, APBS) 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.

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.

ITM is currently negotiating an agreement with the Federal Aviation Administration Enterprise Service Center (ESC) to provide an off-site processing site in the event of an emergency for all of NEA's in-house systems including e-mail. It is noted that the NEA is currently transitioning from an outdated financial management system to a Joint Financial Management Improvement Program (JFMIP) approved system provided through an interagency cross-servicing agreement with the ESC starting October 1, 2004.

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.

Annually, an on-site security-training seminar was to be held to update staff with significant security responsibilities on current developments regarding computer security. These sessions were to range from half-day to multiple days as necessary. In addition, staff would be encouraged to attend off-site security-related classes throughout the year and to attend security meetings and briefings sponsored by other Federal agencies.

However, our prior evaluation noted that no annual training was held during that year and we recommended that NEA adhere to its security-training plan to provide specialized training for NEA employees with significant security responsibilities on an annual basis. During the past year, all seven employees with significant IT security responsibilities received specialized security training.

According to the updated NEA Information Systems Security Plan (September 2004), ITM is currently developing a formal training and awareness program that identifies the training frequency associated with job functions (users, managers, system administrators, etc.). The program will address awareness, training, and maintenance and is expected to be in place by June 2005.

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 recommend that ITM establish a training plan that includes periodic refresher IT security awareness training to all of NEA’s employees.

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 is made of four members, two from ITM's Customer Services Division and two from ITM's Plans, Policy and Programs Division. One member is designated as the CSIT coordinator who 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 was only one successful incident referred by employees to NEA ITM officials within the context of NEA's Computer Security Incident Policy. This August 2004 incident was a virus that was eradicated. According to the "Computer Security Incident Report Log," this incident was reported as required to FedCIRC. All other attempts were successfully blocked by NEA's firewalls and intrusion detection software.

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 had 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.” Our current evaluation disclosed no problems since the access policy was revised.

NEA ITM conducts vulnerability testing using Nessus software. During our evaluation, we observed such a test. Most of the vulnerabilities disclosed involved computers that needed updated patches, which ITM planned to update immediately. NEA ITM plans to perform this testing periodically throughout the year.

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 August 20, 2004). 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. According to the CIO, 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 contractors involved with NEA systems and the help desk generally is unrestricted. However, the CIO and ITM carefully screen these contractors and require background checks.

RECOMMENDATIONS

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

1. Develop written policies and procedures related to change management and control for the development and modification of systems.

2. Establish a training plan that includes periodic refresher IT security awareness training to all NEA employees.

CONCLUSIONS

An exit conference was held with NEA's CIO on October 4, 2004. The CIO generally concurred with our recommendations and has agreed to initiate corrective action.

OMB memorandum M-04-25 requires that agencies develop a plan of action with milestones (POA&M) for all programs and systems where a security weakness has been found. Agencies must provide on a quarterly basis summary information on the POA&M

progress and an update on IT security performance measures. The quarterly updates are to be submitted together and are due on December 15, 2004, March 15, 2005, and June 15, 2005. Quarterly updates are to be sent electronically to both Kristy LaLonde at klalonde@omb.eop.gov and Dan Costello at daniel_j.costello@omb.eop.gov.

The Office of Inspector General plans to review the agency's compliance with the Security Act on an ongoing basis. Results from these reviews will be included in our annual security evaluations, which are required by the Act to be submitted to OMB.

STATUS OF PRIOR REPORT RECOMMENDATIONS
FISCAL YEAR 2003 EVALUATION OF NEA'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT OF 2002
REPORT NO. R-03-03 (SEPTEMBER 2003)

Recommendation	Status
1. Develop written policies and procedures related to security certification and accreditation of NEA's systems.	Implemented. Written policies and procedures related to security certification and accreditation of NEA's systems were finalized in September 2004.
2. Develop written policies and procedures related to change management and control for the development and modification of systems.	Not implemented. These policies have not been completed. This is due primarily to the unexpected departure of the prior security officer and subsequent delays in assigning a new permanent security officer. ITM now expects to complete these policies early in fiscal year 2005. This recommendation is repeated in the current evaluation.
3. Install the procured intrusion detection software as soon as possible.	Implemented. The intrusion detection software, entitled "SiteProtector," was installed in December 2003.
4. Adhere to its security-training plan to provide specialized training for NEA employees with significant security responsibilities on an annual basis.	Implemented. During the past year, all seven employees with significant IT security responsibilities received specialized security training.
5. Revise its computer incident security policy to reflect FedCIRC timeframe requirements for security incident reporting.	Implemented. A revised computer incident policy dated November 2003 established timeframes for reporting security incidents to FedCirc.
6. ITM should not initiate computer or e-mail access for interns, temporary contractors, or volunteers unless NEA's Human Resources Division provides a departure date for those individuals.	Implemented. 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."