NATIONAL ENDOWMENT FOR THE ARTS
OFFICE OF INSPECTOR GENERAL

EVALUATION REPORT

Fiscal Year 2003 Evaluation of NEA's Compliance with the Federal Information Security Management Act of 2002

REPORT NO. R-03-03
SEPTEMBER 2003

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-03-18, dated August 1, 2003, entitled "Implementation Guidance for the E-Government Act of 2002," provides guidance on specific actions that are now required by federal agencies under the E-Government Act.

OMB Memorandum M-03-19, dated August 6, 2003, entitled "Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting," updates instructions to Chief Information Officers and Inspectors General for reporting their 2003 information to OMB. This guidance requires that:

- The agency must respond to performance measures and provide narrative responses.
- Agencies should use the NIST "Security Self-Assessment Guide for Information Technology Systems."
- Agencies' corrective action plans must be shared with the agency Inspector General to ensure independent verification and guidance.

Guidance on information security also has been developed. 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).

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 grantees and NEA employees; 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 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 2002 Evaluation of NEA's Compliance with the Government Information Security Reform Act" (Special Review Report No. R-02-04) on September 16, 2002. The report recommended that NEA ITM (1) develop written policies and procedures for all actions implemented as a result of its contracted risk assessment, (2) continue its efforts to fully implement its disaster recovery plan, (3) mandate annual security awareness updates for all NEA employees, and (4) institute procedures to ensure that ITM is notified of departing student interns so that their respective user IDs and passwords can be deleted.

The prior evaluation contained 4 recommendations, all of which were resolved and implemented. (See Appendix)

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 GISRA 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 of the deficiencies noted in the report.

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. This assessment covered the same areas covered by the SeNet Risk Assessment, which was organized in accordance with

the NIST Self-Assessment Guide criteria. However, ITM's 2002 self-assessment noted that all of the practices and procedures implemented as a result of the SeNet review had not been documented in writing. We agreed that ITM needed to formalize all such practices in writing and included it as a recommendation in the prior year's report. As a result, ITM has developed a written risk assessment policy, a system life cycle security policy, and a password policy.

The risk assessment policy defines the standards for performing information security risks at the NEA. The system life cycle security policy defines the standards to be used by NEA to address security during a system's life cycle. Lastly, the password policy outlines the standards designed to prevent unauthorized use and potential damage to NEA's Local Area Network (LAN) and/or mission-critical data.

The 2003 self-assessment concluded that ITM must (1) develop policies and procedures related to security certification and accreditation of NEA's systems, (2) develop written change management control policy and procedures for the development and modification of systems, and (3) 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." We agree with the self-assessment conclusion that ITM needs to develop written policies and procedures related to security certification and accreditation of NEA's systems.

Change Management Control Policy and Procedures. The 2003 self-assessment 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 changes to the system can have security implications because they may introduce or remove vulnerabilities and because such changes may require an update of the contingency plan, risk analysis, or accreditation. We agree that ITM must develop policies and procedures related to change management and control for the development and modification of systems.

Intrusion Detection Software. The 2003 self-assessment concluded that intrusion detection software must be installed. This software has been procured by NEA, but has not yet been installed. Real-time intrusion detection is aimed at detecting outsiders attempting to gain access to the system. We agree and recommend that this

intrusion detection software be installed as soon as possible. We do want to note that NEA does currently have two active firewalls in place to protect from intrusion.

Security Plan

NEA has formal security plans (dated July 31, 2002) for each of its three major systems (GMS, FMIS, APBS) that address FISMA and OMB requirements. 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). However, it had not yet been fully implemented at the time of our last GISRA evaluation. The recovery plan provides that:

- NEA will maintain an alternate e-mail address resident on a server outside of the Old Post Office Building (where NEA is located) 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.

During our prior review, we noted that the Disaster Recovery Plan was not fully implemented because the Emergency Recovery Server was not yet operational. The Emergency Recovery Server became operational in December 2002.

Security Training

NEA does provide every new employee with computer security awareness indoctrination and provides agency-wide computer training throughout the year. In addition, periodic

bulletins are provided to all NEA employees with updated information on computer security.

ITM had documented a security-training plan (August 2002) for ITM staff and contractors. The purpose of the plan is 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. In addition, system managers were also to be invited to attend.

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 was also 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 review noted that no annual training was held during the past year. Only 2 of the 11 NEA employees tasked with significant IT security responsibilities received specialized training during the past fiscal year. ITM is planning additional security training for employees with significant IT security responsibilities by this calendar year-end, but this has not been finalized. We recommend that NEA adhere to its security-training plan to provide specialized training for NEA employees with significant security responsibilities on an annual basis.

Security Incidents

NEA has formalized a "Computer Security Incident Policy" (January 2002), 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 common 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)." It further notes what information is to be provided, such as the date and time of the incident, the physical location of the hardware/software involved in the incident and the nature of the incident (virus, theft, etc.).

During the past year, there were 11 potential incidents referred by employees to NEA ITM officials. However, none of these 11potential incidents were "successful virus/worm infections" and did not result in a "successful introduction of a virus/worm into a network." Therefore, there were no incidents to report to FedCIRC. However, current NEA policy on security incidents needs to reflect the current timeframes required by FedCIRC for incident reporting.

Access Controls

ITM has developed and implemented an "Access Control Policy" (December 2001) that established procedures for removing terminating employees' user IDs and passwords for the LAN, e-mail and mission critical systems. ITM has 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 prior review noted was that ITM is not always notified when school interns leave NEA. These are students who come to work during the summer or break periods, but are not paid by NEA. Since NEA does not pay the interns, there is no means to ensure that exit clearance procedures are followed (such as withholding their final pay). In addition, the supervisors of these interns are not always informing ITM of their departure because there is 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 review found that ITM is still not being informed timely about such individuals. Although ITM has requested departure dates from the Human Resources Division for these temporary employees, it is not always provided. We recommend that ITM not initiate computer or e-mail access unless a departure date is provided.

Physical Controls

NEA appears to have adequate physical controls to protect its 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 area has cipher locks to restricted areas and the entire computer area is secured and locked from 7:30 PM to 6:30 AM on weekdays and throughout the weekend.

If NEA contracts for computer services that requires access to its computer area, 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 and has updated its inventory listing (dated August 26, 2003). The inventory lists the item by office, barcode number, serial number, manufacturer, model number and description, as well as the user. The inventory is now 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. The ITM Director of Plans, Policy and Programs stated that all short-term 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. Since the contracts are short-term, users are deleted from the system upon termination of the contract.

Any computer access for a long-term contractor is restricted similar to that of the short-term contractors described above. If one of the contractor's employees is terminated, their user access is deleted from the system.

RECOMMENDATIONS

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

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.

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.

CONCLUSIONS

An exit conference was held with NEA's CIO on September 12, 2003. The NEA CIO generally concurred with our recommendations and has agreed to initiate corrective action. It is noted that Recommendations 1, 2, and 3 are a direct result of ITM's own self-assessment.

OMB memorandum M-03-19 requires that the CIO develop a plan of action with milestones (POA&M) for all programs and systems where a security weakness has been found. This plan is to be submitted twice a year to OMB on October 1, 2003 and March 15, 2004. This plan must be shared with the Office of Inspector General to ensure independent verification and validation. In addition, quarterly updates on POA&M implementation must be submitted with the first update due on October 1, 2003 (subsequent reports are due December 15, 2003; March 15, 2004; and June 15, 2004). Beginning with the December 15, 2003, quarterly update, agencies must also provide a quarterly update on their performance against a subset of performance measures in the OMB reporting instructions (M-03-19).

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 2002 EVALUATION OF NEA'S IMPLEMENTATION OF THE GOVERNMENT INFORMATION SECURITY REFORM ACT
SPECIAL REVIEW REPORT NO. R-21-04 (SEPTEMBER 2002)

Recommendation	Status
1. Develop written policies and procedures for all actions implemented as a result of the contracted risk assessment.	Implemented. ITM has implemented policies related to the cited lack of a risk assessment policy, life cycle policy and password policy. ITM has developed written policies to address each of these deficiencies.
2. Continue efforts to fully implement the disaster recovery plan (i.e., Emergency Recovery Server, backup copies).	Implemented. ITM has taken the final step to complete the implementation of the Disaster Recovery Plan related to the operation of the Emergency Recovery Server that became operational in December 2002.
3. Mandate annual security awareness for all NEA employees.	Implemented. ITM is distributing quarterly Computer Security newsletters to NEA employees to provide staff with pertinent information throughout the year regarding computer security.
4. Recommend that NEA institute procedures to ensure that ITM is notified of departing student interns so that their respective user IDs and passwords can be deleted.	Implemented. ITM worked with the Office of Human Resources to develop sign-out procedures and a clearance form for interns and other temporary employees.