MEMORANDUM

Special Review Report No. R-01-03

DATE: September 7, 2001

TO: William Ivey, Chairman

THRU: Daniel L. Shaw, Inspector General

FROM: Anthony S. Premici, Assistant Inspector General

SUBJECT: Evaluation of NEA's Implementation of the Government Information Security Reform Act

The Government Information Security Reform Act 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 Government Information Security Reform Act (Security Act) became effective on November 29, 2000, and focuses on the program management, implementation, and evaluation aspects of the security of unclassified and national security systems. Generally, the Act codifies existing Office of Management and Budget (OMB) security policies, Circular A-130, Appendix III, and reiterates security responsibilities outlined in the Computer Security Act of 1987, the Paperwork Reduction Act (PRA), and the Clinger-Cohen Act of 1996.

OMB Memorandum M-01-08, dated January 16, 2001, entitled "Guidance on Implementing the Government Information Security Reform Act," focuses on unclassified Federal systems and addresses those areas that introduce new or modified requirements. It defines the responsibilities of the agency head, program officials, the Chief Information Officer, and the Inspector General. It also identifies what the Security Act requires agencies to report.

OMB Memorandum M-01-24, dated June 22, 2001, entitled "Reporting Instructions for the Government Information Security Reform Act," provides instructions to Chief Information Officers and Inspectors General on reporting their information to OMB.

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 the Wang computer. These are the Automated Panel Bank System, which contains information on panelists who review grant applications; the Grants Management System, which contains information on grant applications and awards; and the Financial Management Information System, which contains financial information on grantees and NEA employees. In addition, NEA operates support systems including electronic mail and internet services. NEA is currently migrating the agency's three systems to a local area network (LAN). This effort is expected to improve the agency's ability to conduct business using the internet, improve system and data security, improve client assistance, and upgrade the IT infrastructure to improve system performance.

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. Total NEA security funding is estimated to be $93,500 for fiscal year 2001 and $82,800 for fiscal year 2002.

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.

EVALUATION RESULTS

NEA needs to take immediate action to ensure that the Office of Information and Technology Management complies with existing Federal requirements for information security. NEA has not: 1) conducted a risk assessment since 1997; 2) developed an up-to-date security plan; and 3) documented written performance measures for IT

operations. These are significant deficiencies that are required to be reported as material weaknesses under the Security Act.

In addition, NEA: 1) does not have formal documented procedures for reporting security incidents; 2) does not have a documented disaster recovery plan for its LAN system; 3) implemented access controls to ensure that terminated employee names are deleted as users of NEA's LAN system; 4) has not conducted a complete physical inventory of computer equipment and software since 1996; and 5) has not formalized a training program to ensure that agency employees with significant IT security responsibilities are receiving specialized security training.

Risk Assessment

NEA has not had a formal risk assessment of its computer system since August 1997. The Security Act requires that appropriate senior agency officials are "responsible for assessing the information security risks associated with the operations and assets for programs and systems over which such officials have control." It requires "periodic risk assessments that consider internal and external threats to" both 1) "the integrity, confidentiality, and availability of systems" and 2) "data supporting critical operations and assets." The assessment should consider major factors in risk management including the value of the system or application, threats, vulnerabilities, and the effectiveness of current or proposed safeguards.

The August 1997 assessment identified 38 areas of vulnerability. These included access controls (6), procedures (5), evaluation (4), policy (3), construction (3), fire (3), labeling (2), maintenance (2), Privacy Act (2), compliance (2), reliability (2), administration (1), organization (1), emergency response (1), and contingency (1).

NEA needs to conduct a current risk assessment. This deficiency is a material weakness and until such an assessment is completed, NEA cannot be assured that all the risks associated with its computer system are identified and that appropriate actions are taken to mitigate these risks.

Security Plan

NEA has not prepared a formal security plan that addresses the requirements of the Security Act. The Security Act requires that "each agency shall develop and implement an agency-wide information security program to provide information security for the operations and assets of the agency . . . ." 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.

NEA needs to prepare a formal security plan that meets the Security Act guidelines and needs to ensure that the plan is communicated to the system users and administrators.

This deficiency is a material weakness and until such actions are taken, NEA cannot be assured that it has adequately addressed its security needs and that security policies and procedures have become an integral part of the agency's operations.

Performance Measures

NEA does not have written performance measures for ITM operations as they relate to program officials, the Chief Information Officer, and the Chairman. This deficiency is a material weakness. Specific details are presented below.

Program Officials. There are no specific performance measures to ensure that agency program officials, such as the Deputy Chairman for Guidelines, Panel and Council Operations; the Deputy Chairman for Grants and Awards; the Deputy Chairman for Management and Budget; the Grants and Contracts Officer; and the Accounting Officer: 1) assess the risks to operations and assets under their control; 2) determine the level of security appropriate to protect such operations and assets; 3) maintain an up-to-date security plan (that is practiced throughout the life cycle) for each system supporting the operations and assets under their control; and 4) test and evaluate security controls and techniques.

OMB Memorandum M-01-08 states:

> Program officials must assess the risks to the operations and assets over which they have control. This includes determining the appropriate levels of security and periodically testing and evaluating security controls and techniques to ensure that they are cost effective and they enable, but do not necessarily impede, business operations.

The memorandum further states that "agency program officials, not security officers or CIOs, are ultimately responsible for the security of programs under their control."

Chief Information Officer. There are no specific performance measures to ensure that the CIO: 1) adequately maintains an agency-wide security program; 2) ensures the effective implementation of the program and evaluates the performance of major agency components; and 3) ensures the training of agency employees with significant security responsibilities.

OMB Memorandum M-01-08 states:

> The CIO must administer the agency functions under the Security Act. Consistent with the PRA and the Clinger-Cohen Act, this reconfirms the role of the CIO in providing a strategic view of the agency's architecture and crosscutting security needs.

The Memorandum further states:

> The CIO must participate in developing agency performance plans. These plans must include descriptions of the time periods required to implement the agency-wide security program required under section 3534(d)(1), and the budget, staffing, and training resources necessary to implement the program.

Chairman. There are no specific performance measures used by the Chairman to ensure that the agency's information security plan is practiced throughout the life cycle of each agency system.

OMB Memorandum M-01-08 states:

> Each agency must develop and implement information security policies, procedures, and control techniques sufficient to afford security protections commensurate with the risk and magnitude of harm. The head of each agency must also ensure that the agency practices its security program throughout the life cycle of each agency system.

Disaster Recovery Plan

There is no documented disaster recovery plan for NEA's LAN system. Backup tapes are securely maintained on-site, but these tapes would be susceptible to loss in the event a catastrophe occurred at the site. According to FISCAM, the backup location "should be protected from unauthorized access and from environmental hazards, such as fires and power outages." FISCAM also recommends that the location be far enough away so that the backup will not be impacted by the same events, i.e., fires, storms, etc.

NEA contracts for disaster recovery for its Wang minicomputer that houses the agency's Automated Panel Bank System, Grants Management System, and Financial Management Information System. In the event of a disaster at NEA, a technical team of Wang professionals would be available to respond with replacement equipment and software. This contractor will be terminated when the new LAN based system replaces the Wang system, which is targeted to be in operation by October 1, 2001.

Security Training

NEA provides every new employee with a computer security awareness indoctrination and provides agency-wide information technology training throughout the year. However, NEA does not have documented procedures to ensure that employees and contractor personnel involved with the management, use, or operation of NEA's computer systems are provided periodic training in computer security awareness and accepted computer security practices. According to ITM personnel, the courses provided throughout the year include some security issues, but the courses are not intended to be security oriented.

The Computer Security Act of 1987 requires Federal agencies to:

> Provide for the mandatory periodic training in computer security awareness and accepted computer practices of all employees who are involved with the management, use, or operation of each federal computer system within or under the supervision of that agency.

The NIST Handbook and the NIST Guide for Developing Security Plans for Information Technology Systems (Guide) provides guidance for implementing an effective computer security awareness and training program. The Guide says that plans should be developed that include the type and frequency of application-specific training provided to employees and contractor personnel, the type and frequency of general support system training provided to employees and contractor personnel, and the procedures for assuring that employees and contractor personnel have been provided adequate training. In addition, the Guide states "OMB Circular A-130, Appendix III, issued in 1996, enforces such mandatory training by requiring its completion prior to granting access to the system and through periodic refresher training for continued access."

The NIST Handbook notes that different levels of security training are needed for different groups and states "many groups need more advanced or more specialized training than just basic security practices." The Handbook states "computer technology is an ever-changing field" and "efforts should be made to keep abreast of changes in computer technology and security requirements." It cites the importance of managers to understand security consequences and costs so that they can factor security into their decisions. It also notes that more advanced training is necessary for system administrators involved with organizing, directing and evaluating security measures and programs.

NEA needs to implement procedures to ensure that employees and contractor personnel with significant IT security responsibilities are provided periodic training in computer security awareness and accepted computer security practices.

.

Security Incidents

NEA does not have formal documented procedures for reporting security incidents and sharing information regarding common vulnerabilities. There have been related e-mails which have been sent to NEA employees regarding security, but there is no agency directive addressing this issue. According to ITM officials, the policy is for NEA to report any security incidents to the General Services Administration's FedCIRC (Federal Computer Incident Response Center). In cases of theft, NEA's Administrative Services Division and the Federal Protective Service or another appropriate law enforcement agency are notified.

Security incidents are becoming 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.

NEA needs to prepare documented procedures for reporting security incidents described above including those involving theft.

Access Controls

NEA needs to strengthen its controls for deleting terminated employee names from the NEA's LAN system users' list. We conducted a review of ten employees that left NEA during the past year and found that four (40 percent) of those former employees had not been deleted as users on the LAN system. All four of these former employees had "Employment Clearance Statements" on file indicating that they were "cleared" for LAN IDs.

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.

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.

NEA ITM personnel and the contractor for the Wang System have access to the computer room. However, the access code (via a cipher lock) that is used by NEA employees is different from the code used by the contractor. In addition, the contractor's access code is changed whenever one of the contractor's operators is terminated.

Inventory Controls

NEA needs to improve its computer equipment inventory system to provide greater assurance that NEA's computer assets are identified and accounted for on an agency-wide basis. NEA has not conducted a complete physical inventory of its computer equipment since 1996. According to the ITM Director of Plans, Policy and Programs,

inventory records are updated as new purchases are made and obsolete items are discarded or identified as surplus.

Since the last physical inventory, there has been a large turnover of employees and many offices have relocated to different space within the building. Until a complete physical inventory has been conducted, NEA cannot be assured that its equipment inventory is valid, accounted for, and properly protected from theft or loss.

Contractor Security

NEA appears to have imposed adequate security measures on its contractors. In a discussion with the ITM Director of Plans, Policy and Programs, all short-term contractors (all contractors other than those involved with the Wang System) have limited computer access. That is, they do not get a full menu upon login and are restricted on what they can input into the system, which is monitored 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. According to an ITM official, the longest contract for fiscal year 2001 was 28 days.

As noted previously, controls appear adequate regarding the Wang contractor's access to the computer room. Computer access for this 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.

There have been no audits or inspections of the Wang contractor who provides two onsite persons to maintain services for the Wang system which houses the Automated Panel Bank System, the Grants Management and the Financial Management Information System. As noted, our evaluation did examine access controls for contractor personnel and found such controls to be adequate. This contractor will be terminated when the new LAN based system replaces the Wang system, which is targeted for replacement by October 1, 2001.

RECOMMENDATIONS

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

1. Conduct a current assessment to identify all the risks associated with its computer system and develop an action plan to mitigate those risks.

2. Prepare a security plan to ensure that adequate security is provided for all agency information collected, processed, stored, or disseminated in NEA's general support systems and major applications.

3. Prepare and implement a documented disaster recovery plan for the LAN system.

4. Develop specific measures of performance to ensure that agency officials, such as the Deputy Chairman for Guidelines, Panel and Council Operations; the Deputy Chairman for Grants and Awards; the Deputy Chairman for Management and Budget; the Grants and Contracts Officer; and the Accounting Officer:

    a. Assess the risk to operations and assets under their control.

    b. Determine the level of security appropriate to protect such operations and assets.

    c. Maintain an up-to-date security plan for each system supporting the operations and assets under their control.

    d. Test and evaluate security controls and techniques.

5. Develop specific measures of performance to ensure that the CIO:

    a. Adequately maintains an agency-wide security program.

    b. Ensures the effective implementation of the program and evaluates the performance of major agency components.

    c. Ensures the training of agency employees with significant security responsibilities.

6. Develop specific measures of performance used by the Chairman to ensure that the agency's information security plan is practiced throughout the life cycle of each agency system.

7. Implement procedures for ensuring that employees and contractor personnel with significant IT security responsibilities are provided periodic training in computer security awareness and accepted computer security practices.

8. Implement procedures to ensure that a terminating employee is removed from the LAN user list not later than the employee's final day of work at NEA.

9. Conduct periodic reviews of LAN users to ensure that terminated employees or invalid users are deleted and denied access to the system.

10. Prepare documented procedures for reporting security incidents involving viruses, hackers, or software bugs as well as those involving theft.

11. Conduct a physical inventory of all computer equipment within NEA. This inventory should identify the equipment item, the individual and location to which the equipment is assigned.

CONCLUSIONS

An exit conference was held with NEA's CIO on August 30, 2001. Although the NEA Chief Information Officer expressed concerns about our recommendation regarding security training procedures, he generally concurred with our other recommendations and has agreed to initiate corrective action.

OMB memorandum M-01-24 requires that the CIO develop a plan of action with milestones to correct any security weaknesses identified by annual program reviews and independent evaluations. This plan is due to OMB by October 31, 2001.

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.