NATIONAL ENDOWMENT FOR THE ARTS
OFFICE OF INSPECTOR GENERAL

EVALUATION REPORT

Fiscal Year 2002 Evaluation of NEA's Compliance with the Government Information Security Reform Act

REPORT NO. R-02-04
SEPTEMBER 2002

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-02-09, dated July 2, 2002, entitled "Reporting Instructions for the Government Information Security Reform Act and Updated Guidance on Security Plans of Action and Milestones," updates instructions to Chief Information Officers and Inspectors General for reporting their 2002 information to OMB. This guidance requires that:

- The agency must respond to performance measures and provide narrative responses.
- Agencies must 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; and 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 "Evaluation of NEA's Implementation of the Government Information Security Reform Act" (Special Review Report No. R-01-03) on September 7, 2001. The report noted that NEA had 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 were

determined to be significant deficiencies reported as material weaknesses under the Security Act.

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

The prior evaluation contained 11 recommendations, 10 of which were resolved and implemented and 1 of which was resolved and partially implemented. (See Appendix 1.)

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. Our review determined that corrective actions taken since our prior evaluation were sufficient to eliminate the material weaknesses disclosed in that review. However, we did make recommendations related to the disaster recovery plan, security training, and access controls. 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 July 5, 2002. (See Appendix 2.) The overall assessment stated, "NEA should concentrate on documenting and implementing its security program plan, contingency planning, and operating procedures." The major findings included:

Management Issues

- No formal security program.
- No written performance measures.
- ITM missed scheduled dates for publication of some security documents per the CIO's Plan of Action and Milestones for deficiencies addressed by the IG GISRA report for 2001.
- Security roles and responsibilities not defined in writing.

Operational

- New access control policy implemented, but additional fine tuning required.
- No formal software change and maintenance control.
- Incident control procedures are not fully implemented.

Technical

- Potentially dangerous but easily mitigated vulnerabilities found during the external penetration test.
- Multiple vulnerabilities at the Operating System level were found during the internal tests (no vulnerabilities at the SQL level).
- Several network configuration issues identified from provided documents and discussions with ITM personnel.

ITM has taken or has begun corrective action on all of the above noted deficiencies. NEA no longer needs to report this as a material weakness since a risk assessment has been performed.

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 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 agree that ITM needs to formalize all such practices in writing.

Security Plan

NEA has prepared formal security plans (dated July 31, 2002) for each its three major systems (GMS, FMIS, APBS) that address the Security Act requirements. 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's preparation of the security plans addresses the prior year's recommendation that cited the lack of a security plan as a material weakness. NEA no longer needs to report this as a material weakness since a security plan has been developed.

Performance Measures

NEA has established written performance measures for ITM operations as they relate to program officials, the Chief Information Officer, and the Chairman. NEA no longer needs to report this as a material weakness since NEA has established specific performance measures. Specific details are presented below.

Program Officials. NEA established performance measures for the managers of the GMS, FMIS, and APBS with the goal of ensuring that "any threats or vulnerabilities to the security of the systems for which they have control are identified, evaluated, and eradicated (or mitigated at an acceptable level) throughout the system's life cycle." The measures include (1) reviewing and approving all modifications to their respective systems prior to implementation to ensure that security is not compromised; (2) testing security control modifications made to their systems; and (3) certifying and accrediting their systems every three years, or if there is a significant security-relevant change, in accordance with NIST guidelines.

Chief Information Officer. NEA established performance measures for the CIO to ensure that a security program is implemented to protect all IT resources from unauthorized disclosure, destruction or modification. The measures include that the CIO ensure that (1) security plans are developed; (2) NEA staff receives IT security awareness and training; (3) IT staff with significant security responsibilities receive annual security training; (4) a computer security incident policy is in place and reporting requirements meet the General Services Administration's Federal Security Response Center (FedCIRC) requirements; (5) IT risk assessments are performed annually; and (6) NEA maintains and periodically tests an IT disaster recovery/contingency plan.

Chairman. NEA established a performance measure for the NEA Chairman to ensure that security policies and plans are established and implemented and that NEA's mission critical systems are protected from unauthorized disclosure, destruction, or modification. The measure provides that the Chairman will approve the IT security program that includes security awareness and training, computer security incident tracking and reporting, and disaster recovery.

Disaster Recovery Plan

NEA has documented its disaster recovery plan (July 2002). However, it has not yet been fully implemented at the time of our 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.

According to ITM officials, the Emergency Recovery Server will not be operational until November 2002. NEA has contracted for outside storage with Records Management, Inc., located in Springfield, Virginia. Also, the procedure regarding backup copies has not been fully implemented. One backup copy is currently being stored off-site on a weekly basis. We recommend that ITM continue its efforts to fully implement its disaster recovery plan.

Security Training

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.

ITM has 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 will also be invited to attend.

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

In addition, NEA provides every new employee with computer security awareness indoctrination and provides agency-wide information technology training throughout the year. However, ongoing employees do not receive updates or refreshers on matters of computer security. We recommend that annual computer security awareness training be mandated for all NEA employees.

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.

All computer security incidents will be 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 will designated as the CSIT coordinator who will serve as the team's central resource for monitoring computer security incidents.

The recent risk analysis performed by SeNet Inc., noted the following:

- The Computer Security Incident Team has yet to be officially designated.
- Stakeholders were not familiar with the details of the procedure for reporting security incidents.
- No security incidents reports (either specific or periodic) have been issued so far, and no incident log has been kept.

Subsequent to the SeNet report, ITM has officially designated an incident security team. A security incident report was prepared for the June 2002 quarter.

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.

The 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.).

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 employment with NEA 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.

One problem 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. We recommend that NEA implement procedures to address this access control weakness.

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 27, 2002). 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. According to an ITM official, the longest contract for fiscal year 2002 was 28 days.

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 for all actions implemented as a result of the contracted risk assessment.

2. Continue its efforts to fully implement its disaster recovery plan (i.e., Emergency Recovery Server, backup copies).

3. Mandate annual security awareness updates for all NEA employees.

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.

CONCLUSIONS

An exit conference was held with NEA's CIO on September 12, 2002. The NEA Chief Information Officer generally concurred with our recommendations and has agreed to initiate corrective action.

OMB memorandum M-02-09 requires that the CIO develop a plan of action with milestones for all programs and systems where a security weakness has been found. This plan is due to OMB by October 31, 2002. This plan must be shared with the Office of Inspector General to ensure independent verification and validation.

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
EVALUATION OF NEA'S IMPLEMENTATION OF THE
GOVERNMENT INFORMATION SECURITY REFORM ACT
SPECIAL REVIEW REPORT NO. R-01-03 (SEPTEMBER 2001)**

Recommendation	Status
1. Conduct a current assessment to identify all the risks associated with its computer system and develop an action plan to mitigate those risks.	Implemented. A contracted consultant performed a risk assessment and has taken or has begun corrective action on deficiencies identified in the report.
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.	Implemented. ITM issued a security plan for each of its three mission critical systems in July 2002.
3. Prepare and implement a documented disaster recovery plan for the LAN system.	Partially implemented. According to ITM officials, the Emergency Recovery Server will not be operational until November 2002. Also, procedures involving backup copies of data have not been fully implemented at the time of our review.
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.	Implemented. Specific performance measures incorporating the identified elements have been developed for the system managers (program officials).

STATUS OF PRIOR REPORT RECOMMENDATIONS (CONT.)

Recommendation	Status
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.	Implemented. Specific performance measures incorporating the identified elements have been developed for the CIO.
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.	Implemented. A specific measure incorporating the identified element has been developed for the Chairman.
7. Implement procedures for ensuring that employees and contractor personnel with significant security responsibilities are provided periodic training in computer security awareness and accepted computer security practices.	Implemented. Security training has been provided since the prior report and procedures have been implemented to ensure that periodic training is provided to those with significant security responsibilities.
8. Implement procedures to ensure that a terminating employee is removed from the LAN user list not later that the employee's final day of work at NEA.	Implemented. ITM has developed and implemented an "Access Control Policy" that establishes procedures for removing terminating employees' user IDs and passwords for LAN, e-mail, and mission critical systems. ITM has also developed and implemented office procedures that specifically note the steps required to clear applicable user IDs and passwords.

STATUS OF PRIOR REPORT RECOMMENDATIONS (CONT.)

Recommendation	Status
9. Conduct periodic reviews of LAN users to ensure that terminated employees or invalid users are deleted and denied access to the system.	Implemented. ITM has established a policy whereby the ITM Customer Services Division and Plans, Policy and Programs Division will review the access logs for the LAN, e-mail and the mission critical systems every 60 days to ensure that invalid user IDs and passwords are not resident.
10. Prepare documented procedures for reporting security incidents involving viruses, hackers, or software bugs as well as those involving theft.	Implemented. ITM has established a "Computer Security Incident Policy" that identifies the type of activity characterized as a computer security incident and defines the steps to be taken to report a security incident. It has also established procedures to "ensure that all computer security incidents are investigated and contained or eradicated in a timely fashion."
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.	Implemented. ITM has conducted a physical inventory that identifies the equipment item, the individual and location to which the equipment is assigned. The latest inventory listing was dated August 27, 2002.

NATIONAL ENDOWMENT FOR THE ARTS

RISK ANALYSIS AND ASSESSMENT OF THE INFORMATION PROCESSING AND COMPUTING ENVIRONMENT

July 5, 2002

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

Prepared by:

SeNet International Corporation

e-Security – we make it practical.

3040 Williams Drive, Suite 510
Fairfax, Virginia 22031-4618
FAX: (703) 206-9666
TEL: (703) 206-9383
www.senet-int.com

1. Introduction and Executive Summary

This document summarizes finding and recommendations for a vulnerability and risk assessment study of the NEA mission critical applications and IT environment. This study was conducted under GSA Schedule Contract GS-35-0092L, task order CO2-44, dated April 17, 2002.

The NEA has recently completed the first phase of transitioning its critical applications from a legacy WANG VS environment to a modern SQL Server system. One of the main objectives was to move the applications while preserving the same functionality and "look and feel" as on the old system. The next phase, termed the "Refactoring Phase", in which the applications' architecture and functionality continue to evolve, is in progress.

The major applications are accessed exclusively from within NEA's security perimeter (with the exception of dial-in users) by NEA staff. The staff access privileges are assigned based on their job function.

Overall we have found that the NEA mission critical applications are exposed to a ***moderate*** level of risk. This risk can manifest itself primarily in the following areas:

- Short to mid-term unavailability due unfinished Disaster Recovery Plan and not completely implemented Incident Response procedures
- Unauthorized access, modification or destruction of data from within the NEA security perimeter due to improper system configurations and technical vulnerabilities within systems and applications
- An externally accessible server infected with a remote Trojan horse virus sidestepping the firewall perimeter defense.

SeNet International findings are included in the following sections and are organized in accordance with the NIST and CIO Council Self Assessment Guide criteria. The main findings are presented below:

Management Issues:

- No formal Security Program
- No written performance measures
- Missed schedule for publication of some security documents
- Security roles and responsibilities not defined in writing.

Operational Issues:

- New access control policy implemented, but additional fine tuning required
- There are no Disaster Recovery Plan and Procedures
- Incident Response Procedure exists but have not yet been fully implemented.

Technical Issues:

- Potentially dangerous but easily mitigated vulnerabilities found during the external penetration test
- Multiple vulnerabilities at the Operating System level were found during the internal tests (no vulnerabilities at the SQL application level)
- Several network configuration issues identified from provided documents and discussions with ITM personnel
- The new firewall was not installed in time for SeNet to verify the effectiveness of its rules.

SeNet International Corporation wishes to express our thanks to all NEA staff members for their assistance and extraordinary cooperation in conducting this study.

7. Recommendations

The following sections provide SeNet's recommendations based on the findings listed in Sections 3, 4 and 5 of this report.

7.1 Management Recommendations

7.1.1 Security Policy and Planning. SeNet concurs with the IG findings and recommends that NEA should develop a Security Program Implementation Plan, and formulate written security-related performance measures for IT operations. In addition, System Security Plans for NEA mission critical applications must be developed and maintained.

7.1.2 Security Roles and Responsibilities. NEA should formally appoint an IT Security Officer. Since NEA is a small agency, it is not necessary to have a separate FTE for this role. The Director of Policy Planning and Programs that is currently acting in this role, can successfully continue as an official NEA ISSO. It is also necessary to appoint system owners in writing, and to clarify the system owners' role in ensuring the security of their respective systems. End-user responsibilities should be formalized in an agency-wide "Acceptable IT Usage Policy" or "Rules Of Behavior" to be acknowledged by the employee's signature prior to granting access to systems/applications.

7.1.3 Security Awareness and Training Program. We recommend that NEA develop a security training that goes beyond new employees' orientation and include refresher sessions and technical training to IT staff (LAN/system administrators and the Web administrators)

7.1.4 Service Level Agreements. We recommend that NEA negotiates IT security clauses into contracts with outsourcing vendors, such as the National Finance Center.

7.2 Operational Recommendations

7.2.1 Contingency Planning. NEA should give a high priority to the development of an IT Disaster Recovery Plan. The draft we reviewed is an important first step in this direction, but much work is left to be done in identifying systems' priorities, resources (including budgets), action plans, testing etc.

7.2.2 Data Integrity/Validation Controls. We recommend that all security features in new applications or revisions to current applications be formally documented and tested according to a formal Systems Development and Life Cycle Management (SDLCM) methodology.
7.2.3 Network/application do
cumentation. We recommend that all IT assets configurations be thoroughly documented and tracked according to a standard change control procedure.

7.2.4 Logical Access Controls. We recommend that the Access Control Procedures be extended to encompass volunteers and contractors. Systems should also be re-configured to enforce the "lock-out" for unsuccessful login attempts, and to enforce uniform password requirements (yet to be defined).

7.2.5 Security Incident Response Procedures. SeNet recommends to continue implementing these developed procedures. IT staff should issue incident and summary reports as called for, and practice the resolution of incidents in accordance with the procedures. SeNet also suggests these minor changes:

7.2.5.1 Designate the "help desk" as the first contact point for reporting incidents. The help-desk is universally known and possesses the capabilities to make an initial assessment, record the incident and report it the CSIT.

7.2.5.2 Modify/remove requirement for completeness of data as precondition to action by CSIT Coordinator. In many incidents the end-user may have only partial or inaccurate information.

7.3 Technical Recommendations

7.3.1 General Recommendations

7.3.1.1 LAN and firewall configuration
SeNet recommends to implement the new firewall with a DMZ segment, where all externally accessible systems be placed including the NEA web server, DNS and E-mail servers. This will further secure the NEA network in the event of a breach into one of these systems.

7.3.1.2 Intrusion Detection Capabilities
SeNet recommends that NEA adds an Intrusion Detection System to its network. This system will augment the firewall in detecting and alerting security events, such as hacking attempts, Trojan viruses etc.

7.3.1.3 Content Filtering
SeNet recommends to add content filtering capabilities to web, ftp and e-mail traffic in order to limit exposure to Internet-born viruses and undesirable content (porn, hate-mail, SPAM etc.). NEA should also consider implementing URL blocking mechanism to prevent access to web-site containing objectionable material.

7.3.1.4 Password Policy
NEA should unify password requirements to all systems to include minimum length, composition, frequency of change etc. Ensure that servers and network component each have different password and that these passwords also get changed periodically. Prevent or minimize the use of "fixed" password in applications or scripts.

7.3.1.5 Logging and Audit Trails
Formalize review of logs and audit trails for all systems and applications. Some systems' logs are not reviewed at all while others are not reviewed on a regular basis.

7.3.2 System Specific Recommendations

The following recommendations address the most serious vulnerabilities found in the internal and external tests. NEA's IT staff should refer the corresponding systems' entries in the "Findings, Implications and Recommendations" sections above for complete lists of vulnerabilities.

7.3.2.1 Remote e-mail WEB server
This system needs to be re-built from scratch because it was found to be infected with a Trojan virus (code-red) and it is easier to re-build it rather then verify that it does not contain additional viruses.

7.3.2.2 FileMaker Web Server
Reconsider the need for this server to be open to the public and if so modify its access rights so that the public cannot erase or modify its content.

7.3.2.3 SQL Server
Review with the application developer the need to have the shared sequential files and set up an acceptable time table for their removal and discontinuing the shared access to system files and directories. No-end users should have access to the system other then via the SQL application in accordance with his/her functional role. Also, remove unneeded services running on this system such as FTP and Web.

7.3.2.4 GroupWise E-mail Server
Consider disabling the web management interface or restrict its access to IT staff only.

7.3.2.5 Cisco Switches/Routers
Implement security patches to eliminate vulnerabilities found.

7.3.2.6 HR PCs
Consider implementing additional security measures to protect access to/from HR PCs via Access Control Lists or an internal firewall.