



**NATIONAL ENDOWMENT FOR THE ARTS  
OFFICE OF INSPECTOR GENERAL**

---

## **EVALUATION REPORT**

### **FISCAL YEAR 2008 EVALUATION OF NEA'S COMPLIANCE WITH THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT OF 2002**

**REPORT NO. R-09-02  
OCTOBER 9, 2008**

---

#### **REPORT RELEASE RESTRICTION**

**This report may not be released to anyone outside of the National Endowment for the Arts (NEA) without the approval of the NEA Office of Inspector General.**

**Information contained in this report may be confidential. The restrictions of 18 USC 1905 should be considered before this information is released to the public.**

**Furthermore, information contained in this report should not be used for purposes other than those intended without prior consultation with the NEA Office of Inspector General regarding its applicability.**

## INTRODUCTION

The Federal Information Security Management Act of 2002 requires an annual evaluation by the Inspector General on its agency's information security programs and practices. This report presents the results of our evaluation of NEA's information 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 replaced 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.

Office of Management and Budget (OMB) Memorandum M-08-21, dated July 14, 2008, entitled "FY 2008 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management," updates instructions to Senior Agency Officials for Privacy, Chief Information Officers and Inspectors General for reporting their 2008 information to OMB.

The National Institute of Standards and Technology (NIST), which has the responsibility for developing technical standards and related guidance, has issued numerous publications including An Introduction to Computer Security: The NIST Handbook. This publication explains important concepts, cost considerations, and interrelationships of security controls as well as the benefits of such controls. NIST also has published a Guide for Developing Security Plans for Information Technology Systems. In addition,

guidance is found in the Government Accountability Office publication, Federal Information System Controls Audit Manual (FISCAM). NIST has also issued Special Publication 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems; Special Publication 800-53, Recommended Security Controls for Federal Information Systems; and FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems.

NEA's Office of Information and Technology Management (ITM) maintains and operates two of the Agency's three core systems on a local area network (LAN). These are the Grants Management System (GMS), which contains information on grant applications and the Automated Panel Bank System (APBS), which contains information on panelists who review grant applications. NEA has contracted with the Department of Transportation Enterprise Service Center to host NEA's Financial Management System (FMS) through its Delphi Financial Management System. In addition, NEA operates support systems including electronic mail, and internet and intranet services.

The Chief Information Officer (CIO) is responsible for developing policies and procedures to ensure that security is provided over NEA's networks.

## **OBJECTIVE AND SCOPE**

The objective of the evaluation was to determine the adequacy of NEA's information technology (IT) security program and practices. In the past, 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. This year the FISMA guidance included additional questions on privacy.

## **PRIOR EVALUATION**

The NEA Office of Inspector General issued a report entitled "Fiscal Year 2007 Evaluation of NEA's Compliance with the Federal Information Security Act of 2002" (Report No. R-08-01) dated October 18, 2007. The report had two recommendations, both of which were resolved; however, only Recommendation 2 was implemented. During our review, we found that ITM is not reporting weaknesses identified in its self-assessment (POA&Ms) in its quarterly FISMA reports as required by OMB.

## **EVALUATION RESULTS**

Our current evaluation determined that there are several issues that need to be addressed by NEA's Office of Information and Technology Management. These issues are related to the risk assessment, updating the Continuity of Operations (COOP) and Security Plan, implementing procedures related to change management, IT Security Awareness training,

IT policies and procedures, and reporting of POA&Ms on the quarterly FISMA reports. Details are presented in the following narrative.

## **Risk Assessment**

SeNet International Corporation (SeNet) performed the latest risk assessment, the results of which were issued on August 28, 2008. The review concluded the following:

**The implementation and management of the security architecture supporting the National Endowment for the Arts enterprise network appears to require strengthening in order to more effectively restrict unauthorized internal access to information resources.**

The review cited the following weaknesses:

- Web applications were discovered that are vulnerable to SQL Injection;
- Web applications were discovered that are vulnerable to Cross-Site Scripting

The report also stated that the NEA Continuity of Operations Plan (COOP) was weak. The COOP was reviewed against the guidance provided in the Federal Emergency Management Agency (FEMA) Federal Preparedness Circular (FPC-65), the NIST 800-34, "Contingency Planning Guide for Information Technology Systems" and the NIST 800-53, "Recommended Security Controls for Federal Information Systems." The report noted the following deficiencies:

- The plan does not contain contact information for key personnel;
- The plan does not identify any Vital Records and Databases;
- The current section on Mission Essential Functions does not clearly identify the critical NEA functions which must be continued under all circumstances as required by the PFC-65;
- The plan mentions "Procuring needed services and/or equipment" but does not provide a list of vendors and their contact information;
- The plan does not list contact information for customers or other agencies (NEA Panel and National Council of Arts) that NEA may be required to contact and inform regarding the emergency and COOP activation;
- The plan does not define in detail where the work will be performed in the 30 days during the COOP period using an alternate site;
- The COOP does not clarify steps that will be taken to ensure strategy for critical personnel to continue operating at an alternate facility or remotely; and
- The plan does not reference the existence of any contingency/disaster recovery/business continuity plans which may exist.

ITM included revision of the COOP in the 2007-2008 POA&M Summary. We recommend that ITM revise the COOP and implement corrective actions to address the deficiencies noted in the SeNet report.

## **E-Authentication Risk Assessment**

OMB Memorandum 04-04 issued December 16, 2003, directed “agencies to conduct ‘e-authentication risk assessments’ on electronic transactions to ensure that there is a consistent approach across government.” The guidance applies to “remote authentication of human users of Federal agency IT systems for the purposes of conducting government business electronically (or e-government).”

The 2008 FISMA guidance issued by OMB asks Inspectors General to determine whether the agency has identified all e-authentication applications and validated that the applications have operationally achieved the required assurance level in accordance with the NIST Special Publication 800-63, “Electronic Authentication Guidelines.” NEA ITM determined that an e-authentication risk assessment of NEA systems was not required since its systems are not internet-based, are not available to users outside of the Agency’s firewall, and do not require authentication from users on the outside. Based on our review, we agree that NEA ITM is not required to perform the e-authentication risk assessment.

## **NIST Self-Assessment**

ITM conducted its 2007 self-assessment using the controls found in the National Institute of Standards and Technology (NIST) Special Publication 800-53, “Recommended Security Controls for Federal Information Systems.” The primary issues identified in this assessment included the lack or revision of written policies regarding the Security Plan, Continuity of Operation Plan (COOP), media protection, and system and service acquisition. In our prior review, we recommended that weaknesses identified in the self-assessment be included in NEA’s *Plans of Action and Milestones* (POA&Ms), which is updated quarterly and submitted to the Office of Management and Budget. Our review found that this had not been implemented. Therefore, we will repeat the previous recommendation.

## **Security Plan**

NEA issued its security plan for each of its in-house GMS and APBS systems that addressed 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. We noted changes to the NEA Network. However, the last update for the NEA Security Plan was June 2007. ITM has advised us that the plan is currently being updated.

## **Privacy Reporting and Privacy Impact Assessment**

The 2008 FISMA guidance included additional questions on security and privacy policies, which requires agencies to submit information on the types of privacy reviews conducted, policies, and privacy issue allegations. This guidance specifically relates to OMB Memorandum M-08-09, dated January 18, 2008, “New FISMA Privacy Reporting Requirements for FY 2008.” OMB also directed agencies to submit their most current documentation related to OMB Memorandum M-07-16, “Safeguarding *Against and Responding to the Breach of Personally Identifiable Information*,” (PII). OMB Memorandum M-07-16 requires agencies to review their use of SSNs, in agency systems and programs, in order to identify instances in which collection or use is superfluous.

To comply with the requirements above, NEA’s ITM has:

- Implemented PII policies regarding breach notification and rules of behavior;
- Completed technical security assessments to evaluate the level of security protecting NEA IT assets;
- Reviewed PII holdings and updated the system of records notice (SCORNs) to include OMB recommended “routine uses” of PII language; and
- Modified security orientation and privacy training for all NEA staff to include responsibility to protect Agency information and technology assets.

ITM’s review of PII holdings determined that NEA collects only PII that is relevant and necessary for administrative purposes and determined that there are adequate administrative, technical and physical safeguards in place for the PII collected. NEA does not use SSNs, truncated SSNs, or any part of SSNs as tracking numbers for its applications, grants, cooperative agreements or contracts. NEA does not share PII with outside agencies other than for processing payments. ITM indicated there have been no reported breaches or security incidents involving PII collected or maintained by the Agency.

Section 208 of the E-Government Act (2002) requires that “agencies ensure sufficient protections for the privacy of personal information as agencies implement citizen-centered electronic Government.” It further requires agencies to conduct a privacy impact assessment (PIA) and make that assessment available to the public on the agency website.

NEA has reviewed the PIA requirements and identified four external systems where PIAs are required (Personal Identity Verification Card system, Electronic Official Personnel File System, NFC Payroll System, and Delphi Financial Management System). NEA’s internal systems do not require PIAs since they were in place prior to the law.

## Security Incidents

NEA has formalized a “Computer Security Incident Policy” (revised November 2007), 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. 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.**

Any NEA computer security incidents are handled by ITM’s Computer Security Incident Team (CSIT), which consists of four ITM employees. One employee, who is designated as the CSIT coordinator, serves as the team’s central resource for monitoring computer security incidents.

NEA’s policy states, “The CSIT will be comprised of the following staff from the Office of Information and Technology Management:

- two representatives from the Customer Services Division (the Director and one additional staff member)
- two representatives from the Plans, Policy and Programs Division (the Director and one additional staff member)”

Currently, NEA ITM does not have a Customer Services Division or a Plans, Policy and Programs Division; therefore, we recommend that the policy be revised to reflect the appropriate CSIT staff.

## IT Security and Privacy Awareness Training

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. ITM implemented agency-wide training in 2005. ITM combined *IT Security and Privacy Awareness Training* in the FY 2008 Annual Refresher Training.

The August 2008 SeNet report noted that the Security Awareness and Training Policy was a sound basic document. However, to make the policy “more explicit, robust, and compliant with Federal guidance,” SeNet made several recommendations and suggestions to improve the policy. We recommend that ITM revise the Security Awareness and Training Policy to include the recommended changes and implement the suggested

changes in developing *all* of its policies. In addition, we recommend that ITM implement the following:

- Add an “Authority” section that includes Federal agency requirements which mandate the establishment of the policy;
- A numbering system to track policies and indicate if it is a revision;
- Develop a formal policy manual;
- Notify employees of new policies and place all official policies on the *IT Policy* webpage on the NEA Intranet; and
- Include reporting of security incidents procedures in the IT Security Awareness Training.

## **Inventory Controls**

NEA has an inventory of its hardware and has updated its listing as of July 17, 2008. The perpetual inventory listing is maintained and updated as equipment is added or deleted. The inventory lists each item by office, barcode number, serial number, manufacturer, model number and description, as well as the user. It also indicates the date the inventory was taken and the initials of the person who took the inventory.

## **Change Management**

ITM issued a “Change Management Policy/Procedure” in 2004. This policy “describes the responsibilities, policies, and procedures to be followed by ITM when making changes or recording events to the National Endowment for the Arts IT infrastructure.” It defines “change” and “event” as follows:

**Change: to transform, alter, or modify the operating environment or standard operating procedures; any modification that could have potential and/or significant impact on the stability and reliability of the infrastructure and impacts conducting normal business operation by our users and ITM; any interruption in building environments (i.e., electrical outages) that may cause disruption to the IT infrastructure.**

**Event: any activity outside of the normal operating procedures that could have a potential and/or significant impact on the stability and reliability of the infrastructure, i.e. a request to keep a system up during a normal shutdown period.**

The change management process includes the submission of a change request with management approval. During our prior evaluation, it was noted that when we requested a log and/or copies of such requests, none had been submitted. As a result, a recommendation was made that ITM implement procedures to ensure compliance with the NEA Change Management Policy. This year, we again requested copies of completed change management request forms and reviewed the *ITM Change Request Folder*, located on the server. Our evaluation found that there were no submissions during FY 2008. We recommend that ITM implement procedures to ensure compliance with the NEA Change Management Policy.

## **Financial Management System**

NEA has an agreement with the U.S. Department of Transportation (DOT) to utilize the Enterprise Service Center's (ESC) Oracle Federal Financials System, Delphi, as their financial management system. OMB requires that such service organizations provide client agencies with an independent report describing system controls. To comply with this requirement, DOT OIG hired an independent contractor, Clifton Gunderson, LLP, to conduct a review on the computer controls over the information technology and data processing environment, as well as the input processing, and output controls built into the Delphi system.

The independent contractor rendered an opinion on the effectiveness of those controls for the nine-month period from October 1, 2007 through June 30, 2008. The audit concluded that the "controls of ESC Services presents fairly, in all material respects, the relevant aspects of ESC's controls that had been placed in operation as of June 30, 2008. In addition, controls "are suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described controls were complied with satisfactorily and the user organizations applied the controls contemplated in the design of ESC controls." The exceptions are "logical access and segregation of duties concerning the CASTLE<sup>1</sup> system operations." CASTLE is used to support DOT operations only.

## **Payroll System**

NEA uses the Department of Agriculture (USDA) National Finance Center as its payroll provider. The latest Statement on Auditing Standards Number 70 (SAS 70) Review of the Department of Agriculture Office of the Chief Financial Officer/National Finance Center (OCFO/NFC) issued by the USDA OIG was for fiscal year 2007. This review concluded that the OCFO/NFC's "description of controls presented fairly, in all material respects, the relevant aspects of OCFO/NFC." Also, in their opinion, "the controls included and/or referenced in the description, as updated, were suitably designed to provide reasonable assurance that associated control objectives would be achieved if the described policies and procedures were complied with satisfactorily and customer agencies applied the controls specified in the OCFO/NFC description of controls."

The 2007 USDA report described "weaknesses in OCFO/NFC internal control policies and procedures that may be relevant to the internal control structure of OCFO/NFC customer agencies." The report further stated that "as of August 30, 2007, OCFO/NFC had corrected or was in the process of correcting the exceptions identified."

The 2008 USDA SAS 70 Report on the National Finance Center was not available at the time of our evaluation in September 2008. We recommend that NEA ITM provide us with a copy of the report as soon as it becomes available.

---

<sup>1</sup> Consolidated Automated System for Time and Labor Entry (CASTLE).

## **EXIT CONFERENCE**

An exit conference was held with NEA's CIO on October 7, 2008. The CIO generally concurred with our recommendations and has agreed to initiate corrective actions.

## **RECOMMENDATIONS**

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

1. Respond and implement procedures to address weaknesses found during the risk assessment.
2. Revise the COOP to address the deficiencies noted in the SeNet report.
3. Include corrective actions for weaknesses identified in NEA's *Plans of Action and Milestones* (POA&Ms), which are more than 90 days beyond the planned remediation date, in its quarterly FISMA report as required by the Office of Management and Budget.
4. Revise the *Computer Incident Policy* to reflect the appropriate CSIT staff.
5. Implement standard procedures for developing policies, which will ensure that only approved policies are issued. It should also implement procedures to ensure that policies are made available to employees.
6. Provide the Office of Inspector General with a copy of the 2008 Statement on Auditing Standards Number 70 (SAS 70) Review of the Department Agriculture National Finance Center.