



**NATIONAL
ENDOWMENT
FOR THE ARTS**

OFFICE OF INSPECTOR GENERAL

EVALUATION REPORT

**FISCAL YEAR 2010 EVALUATION OF
NEA'S COMPLIANCE WITH THE
FEDERAL INFORMATION SECURITY
MANAGEMENT ACT OF 2002**

REPORT NO. R-11-01

November 15, 2010

REPORT RELEASE RESTRICTION

In accordance with Public Law 110-409, The Inspector General Act of 2008, this report shall be posted on the National Endowment for the Arts (NEA) website not later than three (3) days after it is made publicly available with 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 December 17, 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-10-15, dated April 21, 2010, entitled *FY 2010 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 2010 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 NIST Publication 800-12, *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*; Special Publication 800-37 Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*; *A Security Life Cycle Approach*; 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*. In addition, guidance is found in the Government Accountability Office publication, *Federal Information System Controls Audit Manual* (FISCAM).

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 (DOT) Enterprise Service Center to host its Financial Management System (FMS) through DOT's Delphi Financial Management System and the U.S. Department of Agriculture (USDA) National Finance Center for payroll services. NEA has also contracted with other providers for email, grant application process and its personal identity verification program (PIV). ITM operates support systems for 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. This included a review of NEA's IT security policies and procedures and privacy management program. It also included 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 (OIG) issued a report entitled *Fiscal Year 2009 Evaluation of NEA's Compliance with the Federal Information Security Act of 2002* (Report No. R-10-02) dated January 22, 2010 (rev. 2/26/10). The report had seven (7) recommendations. Corrective actions have been implemented for six (6) of the recommendations. The remaining recommendation addresses unimplemented corrective actions in NEA's Change Management program.

EVALUATION RESULTS

The FY 2010 FISMA evaluation concluded that NEA's Office of Information and Technology Management (ITM) have established a security program for protecting its information technology (IT) infrastructure. However, we identified several issues that need to be addressed by ITM to strengthen its security program and increase its compliance with FISMA and NIST requirements. The issues are related to contractor systems oversight, IT security and privacy awareness training, security incident reporting, plans of action and milestones (POA&Ms) and change management program. Details of our evaluation are presented in the following narrative.

Privacy Reporting and Privacy Impact Assessment

The FY 2010 FISMA guidance included additional questions on security and privacy policies, which requires agencies to submit information on privacy issue allegations, policies and the types of privacy reviews ITM conducted. OMB directed agencies to submit their most current documentation related to OMB Memorandum M-07-16, of May 22, 2007, "*Safeguarding Against and Responding to the Breach of Personally Identifiable Information*," (PII). OMB Memorandum M-07-16 requires agencies to review their use of Social Security Numbers (SSN), 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 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 (1) NEA collects only PII that is relevant and necessary for administrative purposes and (2) 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. ITM also indicated that there were no changes to the policy since the 2008 FISMA status report on PII and SSNs which was issued September 18, 2008.

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 Financial 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, which is used by multiple Federal agencies; and the Consolidated Automation System for Time and Labor Entry (CASTLE), which is used to support DOT operations only.

The audit concluded that management's description of controls presents fairly, in all material respects, the controls that have been placed in operation as of June 30, 2010. In addition, controls are suitably designed and were operating effectively except in the areas of configuration management and access controls. Specifically, the Delphi system operated on a database for which the vendor stopped providing security updates in February 2009. Furthermore, ESC did not apply in a timely manner critical security updates that the vendor had provided, and did not assess the system for vulnerabilities and risks associated with the vulnerabilities. The DOT Deputy Chief Financial Officer has committed to implementing corrective actions.

Payroll System

NEA uses the U.S. Department of Agriculture (USDA) National Finance Center (NFC) as its payroll provider. In September 2010, the USDA OIG issued its Statement on Auditing Standards Number 70 Report, *Review of the Department of Agriculture Office of the Chief Financial Officer/National Finance Center (OCFO/NFC)*. The 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 in the description were suitably designed and operating with sufficient effectiveness to provide reasonable assurance that associated control objectives would be achieved if customer agencies and subservice organizations applied the controls contemplated in the design of NFC's controls." There were no recommendations in the report.

Contractor Systems Oversight Program

OMB's FY 2010 FISMA instructions, states that "each agency must ensure their contractors are abiding by FISMA requirements." Section 3544(a)(1)(A)(ii) describes Federal agency security responsibilities as including "information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. Therefore, Federal

security requirements continue to apply and the agency is responsible for ensuring appropriate security controls (see OMB Circular A-130, Appendix III). Agencies must develop policies for information security oversight of contractors and other users with privileged access to Federal data. Agencies must also review the security of other users with privileged access to Federal data and systems.”

We obtained and reviewed agreements, including Interconnection Security Agreements and Memorandums of Understanding (MOU) with service providers. We found that ITM does not properly document, authorize or maintain interface agreements as required by FISMA and OMB. Details of our review are below.

1. GSA – HSPD-12 Shared Services Solution to provide Federal employees and contractors with HSPD-12 compliant Personal Identity Verification credentials. The Interconnection Security Agreement was executed in July 2008 for one year. The agreement provided by ITM had only one signature, the NEA-CIO.
2. Grants.gov - provide federal grant applicants with a system through which they can search for federal funding opportunities, download grant packages and submit completed applications. The agreement was executed April 20, 2010 and is valid for three years.
3. DOT – Memorandum of Understanding to provide financial management services. The agreement was dated November 3, 2005 and was valid for three years which expired in 2008. The MOU provided by ITM was not signed by either organization.
4. USDA – NFC MOU to provide payroll services. The agreement was dated July 9, 2007 and was valid for three years from the date of the last signature. The MOU was not signed by either organization.
5. New World Apps – email services provider. There is no agreement in place with this contract provider.

We recommend that ITM immediately execute memorandums of understanding or interagency agreements with all contracted services providers utilizing interconnections with NEA IT systems that require assessments under FISMA. ITM should also develop and implement procedures to adequately monitor contractors and ensure that contractor systems are compliant with FISMA and OMB requirements.

Subsequent to our review, ITM provided a copy of an executed agreement with DOT dated November 3, 2010 and is valid for three years. The ISSO also informed us that they are in the process of executing agreements with GSA, USDA-NFC and New World Apps. The expected date of completion for agreements with GSA and USDA-NFC is November 19, 2010. The expected date of completion with New World Apps is January 15, 2011.

IT Security and Privacy Awareness Training

NIST Special Publications 800-50, *Building an Information Technology Security Awareness and Training Program* and 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model* provide the standards for security awareness and training. ITM combined *IT Security and Privacy Awareness Training* in the FY 2008 Annual Refresher Training and included computer incident reporting in FY 2009.

We obtained and reviewed the FY 2010 *IT Security and Privacy Awareness Refresher* training materials and notification sent to employees by email. We found that although the email included instructions and information on the requirement for refresher training; it did not include a required date of completion. A required due date provides a standard to evaluate timely completion. We also found that the FY 2010 security awareness training did not include information on computer incidents and reporting.

We obtained and reviewed the list of employees who had completed the FY 2010 security awareness training and determined that 97% of the staff completed the required *Annual IT Security and Privacy Awareness Refresher* training on security awareness and privacy (179 completed, 7 did not complete).

Subsequent to our review, 100% of the NEA staff had completed the training.

We recommend that ITM includes a required date of completion when administering its security awareness refresher training. We also recommend that ITM includes computer incident and reporting in its annual security awareness training.

Computer Security Incidents Reporting Program

NEA has formalized a “Computer Security Incident Policy” (revised January 2010), 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.

During our review of the Computer Security Incident Policy and ITM’s security webpage, we noted that although the policy directs staff to report incidents to the ITM Help Desk, the security webpage directs staff to report incidents to the ISSO. For timely and effective response, incidents should be reported to the helpdesk as directed by ITM security policy.

We recommended that ITM ensure that the Computer Security Incident Policy and website instructions for reporting computer incidents are consistent. We suggest that ITM consider adding a link for reporting computer incidents to the front webpage for easier access by users.

Subsequent to our review, ITM revised the intranet website instructions to report computer incidents to the helpdesk in accordance with the Computer Security Incident Policy.

We obtained and reviewed incident reports submitted during FY 2010. There were three computer security incidents reported. Two have been resolved and closed. The remaining incident involves computer-related theft, a potential breach of personally identifiable information. NEA Administrative Services Division was notified of the incident; however, according to the ITM Computer Incident Policy, both “NEA’s Administrative Services Division and the Federal Protective Service will be notified of all computer-related thefts.” There is no indication on the report that the Federal Protective Service was notified. In addition, the ITM policy states that computer incident reports should be submitted to the Inspector General quarterly. Quarterly reports have not been submitted to the OIG.

Subsequent to our review, the OIG was notified by the ITM ISSO that the incident regarding the computer theft was reported to the Federal Protective Service by the NEA Administrative Services Division.

OMB Memorandum, M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, states, in part, that agencies should notify law enforcement agencies and Inspectors General of actual or suspected breaches involving personally identifiable information. The OIG did not receive notification of this incident. We recommend that ITM complies with its policy on reporting computer security incidents involving potential breach of PII information and FISMA requirements. We also recommend that ITM revises its computer incident policy to include notification to the OIG of actual or suspected breaches involving personally identifiable information.

Subsequent to our review, ITM revised its policy to include the notification of the OIG of all computer theft related incidents.

Inventory Controls

NEA has an inventory of its hardware that was updated as of October 14, 2010. 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 Program

ITM issued its revised *Change Management Policy/Procedure* in February 2010. 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 also states that the “Change Management Process is designed to also provide an orderly method in which changes to the IT environment are requested and approved prior to the installation or implementation.” 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 a 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 requires that an approved change request form be submitted to the Information System Security Officer (ISSO). In our FY 2006 through 2009 evaluations, we noted that changes we made to the system, without approved change requests. In FY 2008 and 2009, we found that no change requests had been submitted to the ISSO.

In our FY 2009 evaluation, we recommended that ITM revise, approve and implement the *NEA Change Management Policy/Procedure* as required by its *Standard Procedures for Developing Information Technology Policies*. We also recommended that the CIO direct staff to adhere to those procedures.

ITM submitted a revised, approved change management policy and in February 2010, the CIO directed the staff to adhere to the change management policy. However, this year, we again requested copies of approved change management request forms and found that no submissions had been made.

As part of the FY 2010 Annual FISMA reporting instructions, the IG is required to report on the status of the agency’s Certification and Accreditation program. Included in the assessment is the agency’s process for tracking changes to information systems as directed by NIST SP 800-37, Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems A Security Life Cycle Approach*, which states in part:

A disciplined and structured approach to managing, controlling, and documenting changes to an information system or its environment of operation is an essential element of an effective security control monitoring program.

We again recommend that the CIO directs the ITM staff to adhere to its change management policy and monitor the change management process to ensure compliance.

NIST Self-Assessment and Plans of Action and Milestones (POA&Ms)

OMB FY 2010 FISMA instructions direct Inspectors General to determine whether the Agency has established and is maintaining a certification and accreditation program that is generally consistent with NIST and OMB's FISMA requirements. An external risk assessment was performed in FY 2008 and is valid for three years, or until 2011. ITM also performed a certification and accreditation site assessment in July 2010. Our review found that NEA has an established certification and accreditation program in accordance with both NIST and OMB's FISMA requirements.

OMB's instructions also direct Inspectors General to review the status of the agency's POA&Ms program. The program should be consistent with NIST and OMB's FISMA requirements and include written policies for managing security weaknesses. The program should also include reports to the CIO, on a regular basis, at least quarterly, on the progress of remediation. During our review, we found that ITM had not developed written policies for its POA&Ms program.

We also reviewed the quarterly FISMA submissions for the past year to determine whether ITM was reporting all of its POA&Ms which were unresolved more than 90 to 120 days beyond the planned remediation date.

Our review of the quarterly FISMA reports submitted to OMB noted the following POA&Ms:

- March 2010 (2)
- June 2010 (0)

Therefore, as of the June 2010 FISMA quarterly report, there were no outstanding security issues which had not been resolved 90 to 120 days beyond the planned remediate date.

We recommend that ITM develop and implement written policies and procedures for its POA&Ms program consistent with NIST and OMB's FISMA requirements. The policy should include procedures for regular reporting on the progress of remediation to the CIO, at least quarterly.

Continuous Monitoring Program

OMB's FY 2010 FISMA instructions, describes continuous monitoring of security controls as a cost-effective and important part of managing enterprise risk and maintaining an accurate understanding of the security risks confronting the agency's information systems. Continuous monitoring of security controls is required as part of the security authorization process to ensure controls remain effective over time in the face of changing threats, missions, environments of operation, and technologies. A robust and effective continuous monitoring program will ensure important procedures included in an agency's security authorization package (e.g., as described in system security plans, security assessment reports, and POA&Ms) are updated as appropriate and contain the necessary information for authorizing officials to make credible risk-based decisions regarding the security state of the information system on an ongoing basis.

During our review, we found that ITM has established a continuous monitoring program. However, we found that ITM has not developed written policies and procedures for its program. In addition, by implementing the above recommendations in its Change Management, POA&Ms and Contract Oversight Programs, the continuous monitoring program will be further strengthened.

We recommend that ITM develop and implement written policies and procedures for its continuous monitoring program consistent with NIST and OMB's FISMA requirements. The policy should include ITM's strategy and plans for continuous monitoring, such as vulnerability scanning, log monitoring and notification of unauthorized devices. OMB directs agencies to review NIST Special Publications 800-37 Rev.1, 800-53, and 800-53A for guidance on continuous monitoring programs.

EXIT CONFERENCE

An exit conference was held with ITM officials on November 15, 2010. The officials generally concurred with our findings and recommendations and agreed to initiate corrective actions.

RECOMMENDATIONS

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

1. Execute memorandums of understanding or interagency agreements with all contracted services providers utilizing interconnections with NEA IT systems that require assessments under FISMA.
2. Develop and implement procedures to adequately monitor contractors and ensure that contractor systems are compliant with FISMA and OMB requirements.

3. Include a required date of completion and information on computer security incidents and reports in its security awareness refresher training.
4. Complies with its policy on reporting computer security incidents involving potential breach of PII information and FISMA requirements.
5. The CIO directs the ITM staff to adhere to its change management policy and monitor the change management process to ensure compliance.
6. Develop and implement written policies and procedures for its POA&Ms program consistent with NIST and OMB's FISMA requirements. The policy should include procedures for regular reporting on the progress of remediation to the CIO, at least quarterly.
7. Develop and implement written policies and procedures for its continuous monitoring program consistent with NIST and OMB's FISMA requirements. The policy should include ITM's strategy and plans for continuous monitoring, such as vulnerability scanning, log monitoring and notification of unauthorized devices.