



OFFICE OF INSPECTOR GENERAL

**FISCAL YEAR 2013 EVALUATION OF
NEA'S COMPLIANCE WITH THE
FEDERAL INFORMATION SECURITY
MANAGEMENT ACT OF 2002**

REPORT NO. R-14-01

February 4, 2014

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.

Office of Management and Budget (OMB) Memorandum M-14-04, dated November 18, 2013, entitled *Fiscal Year 2013 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 2013 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 and a *Contingency Planning Guide for Federal Information Systems*, Special Publication 800-34.

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. ITM also operates support systems for internet and intranet services.

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). The Chief Information Officer (CIO) is responsible for developing policies and procedures to ensure that security is provided over all 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 AND OTHER REPORTS

According to the Office of Management and Budget (OMB) Memorandum 14-04, *Fiscal Year 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, Cybersecurity has been identified as one of 14 Cross Agency Priority (CAP) Goals for FY 2013 and FY 2014. (See http://goals.performance.gov/goals_2013.) To accomplish these goals the Administration is prioritizing: (1) measuring agency implementation of Trusted Internet Connections; (2) focusing on strong authentication through the use of multifactor authentication in accordance with Homeland Security Presidential Directive-12 (HSPD-12); and (3) performing monitoring of security controls in federal information systems and environments in which those systems operate on a continuous basis.

NEA OIG has issued prior reports which address weaknesses found in its information systems security program, including its continuous monitoring, HSPD-12, patch management and perimeter security programs. Below are the details of the reports which have open recommendations as of September 30, 2013.

Fiscal Year 2011 Evaluation of NEA's Compliance with the Federal Information Security Act of 2002 (Report No. R-12-01) dated November 15, 2011. The report had eleven recommendations. NEA has implemented corrective actions for nine of the eleven recommendations. The following recommendations remain open:

Recommendation No. 8 Develop and implement written policies and procedures to ensure that it establishes an Information System Contingency Plan in compliance with NIST SP 800-34.

Recommendation No. 10 Establish and maintain a security capital planning and investment control process program for information security.

Fiscal Year 2012 Evaluation of NEA's Compliance with the Federal Information Security Act of 2002 (Report. R-12-01), dated December 17, 2012. The report had four recommendations. NEA has implemented corrective actions for one recommendation. The following recommendations remain open.

Recommendation No. 1 Develop an implementation policy to require the use of PIV smartcard credentials for logical access to its networks as directed by HSPD-12.

Recommendation No. 2 Implement the use of the PIV smartcard credentials for access to its network and information systems.

Recommendation No. 3 Implement an automatic encryption method which includes all data on all mobile computers/devices that carry agency information to ensure PII and sensitive information are not compromised.

Although corrective actions have not been completed for the above recommendations, NEA has made progress on implementing corrective actions.

TECHNICAL ASSISTANCE

As part of our FY 2013 evaluation process, we obtained technical assistance from the United States International Trade Commission Office of Inspector General (US/ITC OIG). An US/ITC OIG staff member with technical expertise was assigned to conduct a high-level, independent review of NEA's computer information security program. Specifically, the staff member performed penetration and patch testing. Two reports were issued: *Evaluation of NEA's Patching Program*, Report No. R-13-02 and *Evaluations of NEA's Perimeter Security*, Report No. R-13-03, dated February 15, 2013. There were a total of thirteen recommendations, all of which remained open at the end of the reporting period. Evaluation of proposed corrective actions are in progress.

NEA offices are scheduled for relocation in February-March 2014. The relocation will divert ITM resources through the completion of the move, therefore, the implementation of corrective actions and the evaluation of those corrective actions will be impacted.

EVALUATION RESULTS

In November 2012, the Department of Homeland Security (DHS) issued a checklist for use by Offices of Inspectors General to assess the level of performance achieved by agencies in specific program areas during the FY 2013 FISMA evaluation period. The specific program areas to be assessed were:

1. Continuous Monitoring
2. Configuration Management
3. Identity and Access Management
4. Incident Response and Reporting
5. Risk Management
6. Security Training
7. Plan of Action & Milestones (POA&M)
8. Remote Access Management
9. Contingency Planning
10. Contractor Systems

The FY 2013 FISMA evaluation concluded that ITM has established a security program for protecting its IT infrastructure and is generally compliant with FISMA legislation. We determined that most of the specific program areas met the level of performance as indicated in DHS's FY 2013 FISMA checklist. We did not identify any material weaknesses in the program areas, however, we did identify improvement opportunities in the following programs:

1. Plan of Action and Milestones (POA&Ms) Program
2. Contingency Planning Program
3. Risk Management Program - Inventory Controls

Details of our evaluation are presented in the following narrative.

PLAN OF ACTION AND MILESTONES PROGRAM

OMB's FY 2013 instructions direct Inspectors General to review the status of the agency's Plan of Action and Milestones (POA&Ms) program. The program should be consistent with FISMA requirements, OMB policy and applicable NIST guidelines and include written policies for managing security weaknesses. OMB Memorandum M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, describes a POA&M as a corrective action plan, a tool that identifies tasks that need to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the task and scheduled completion dates for the milestones. The purpose is to assist agencies in identifying, assessing, prioritizing and monitoring the progress of corrective efforts for security weaknesses found in programs and systems. The program should also include reports to the CIO, on a regular basis, at least quarterly, on the progress of remediation.

During our FY 2011 FISMA evaluation, we recommended areas of improvement for the POA&Ms program. We recommended that ITM develop and implement written policies and procedures for its POA&Ms program consistent with FISMA requirements, OMB policy and applicable NIST guidelines. We also recommended that the policy include procedures for regular reporting on the progress of remediation to the CIO, at least quarterly. ITM developed the policy; however, it has not been consistently implemented. As a repeated finding (FY 2008-2011 FISMA Evaluations), we believe NEA POA&Ms program lacks adequate tracking and monitoring of information security weaknesses. Reports were not issued quarterly, as required and were not updated as to the status of prior weaknesses identified. As a result, there was no effective audit trail to determine whether weaknesses previously identified were resolved.

We recommend that NEA implements its POA&Ms program in accordance with its internal policy and NIST SP 800-37. The POA&Ms reports should include the status of prior security weaknesses identified to provide an audit trail of progress.

CONTINGENCY PLANNING PROGRAM

Our review concluded that although NEA has generally established an enterprise-wide business continuity/disaster recovery program, its program is not consistent with FISMA requirements, OMB policy, and applicable NIST guidelines.

OMB's FY 2013 instructions direct Inspectors General to determine whether the organization has incorporated the results of its system's Business Impact Analysis (BIA) into the analysis and strategy development efforts for the organization's Continuity of Operations Plan (COOP), Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP). NEA has the required COOP, however, NEA has not developed an Information System Contingency Plan, as recommended in the FY 2011 evaluation. We also found that NEA's Disaster Recovery Plan included obsolete information.

We recommend that NEA revise its Disaster Recovery Plan to ensure that the information is accurate and complete, in accordance with NIST SP 800-34.

RISK MANAGEMENT PROGRAM -Inventory Controls

NEA provided us with an inventory of its computer system equipment that was updated as of June 2013. Our review found that although the listing included required information on equipment and software, it did not include excess equipment. According to NEA's inventory policy, excess equipment information should be maintained for three years.

We recommend that ITM fully implements its policies and procedures for inventory to ensure that its inventory information is accurate and complete.

EXIT CONFERENCE

We provided a draft copy of this report to ITM officials on January 8, 2014. The officials generally concurred with our findings and recommendations and agreed to initiate corrective actions.

RECOMMENDATIONS

We recommend NEA implement corrective actions for all open recommendations from prior OIG reports. We also recommend NEA:

1. Implement its POA&M program in accordance with its internal policy and NIST SP 800-37. The POA&M reports should include the status of prior security weaknesses identified to establish an audit trail of progress.
2. Revise its Disaster Recovery Plan to ensure that the information is accurate and complete, in accordance with NIST SP 800-34.

3. Fully implement its policies and procedures for inventory control to ensure that its inventory information is accurate and complete.