



OFFICE OF INSPECTOR GENERAL

**FISCAL YEAR 2012 EVALUATION OF
NEA'S COMPLIANCE WITH THE
FEDERAL INFORMATION SECURITY
MANAGEMENT ACT OF 2002**

REPORT NO. R-13-01

December 17, 2012

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 Office of Inspector General on its agency's information security programs and practices. This report presents the results of our evaluation of National Endowment for the Arts' (NEA) information security program and practices for protecting its information technology 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-12-20, dated September 27, 2012, entitled *FY[Fiscal Year] 2012 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 2012 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, *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*. In addition, guidance is found in the Government Accountability Office publication, *Federal Information System Controls Audit Manual*.

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). These are the Grants Management System, which contains information on grant applications and the Automated Panel Bank System, 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 through DOT's Delphi Financial Management System and the U.S. Department of Agriculture National Finance Center for payroll services. NEA has also contracted with other providers for email, grant application process and its personal identity verification(PIV) program. 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

We reviewed prior evaluation reports on NEA's FISMA compliance, information technology security program and any follow-up documentation to determine the status of prior recommendations. Details are presented below:

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.

NEA has implemented corrective actions for eight of the eleven recommendations. NEA is in the process of implementing corrective actions to address the remaining three recommendations in the report.

1. Implement corrective actions for recommendations in the Risk Assessment Reported issued September 23, 2011 by EmeSec.

2. Develop and implement written policies and procedures to ensure that it establishes an Information System Contingency Plan in compliance with NIST SP 800-34, Revision 1.
3. Establish and maintain a security capital planning and investment control process program for information security.

Review of NEA's Control Over Computer-Related Equipment, Report No. R-11-02, dated January 25, 2011

The review of NEA's control over computer-related equipment was to determine whether NEA was processing and reporting computer security incidents in accordance with its policies and federal guidance. The report contained eleven recommendations from the OIG, all of which NEA has implemented corrective actions.

Risk Assessment Report conducted by EmeSec Information Assurance, dated September 23, 2011

NEA contracted with EmeSec Information Assurance to review and assess the security architecture supporting NEA's enterprise network to meet certification and accreditation. The assessment included reviewing and examining documentation including policies, procedures and plans for compliance with FISMA requirements, OMB policies and applicable NIST guidelines. EmeSec also tested security controls by conducting specific vulnerability assessment and penetration testing on the system network and applications and NEA's compliance with Federal Desktop Core Configuration. EmeSec stated in its report that "implementing a consistently improving Security Program is a two to five year process." NEA is in the process of implementing corrective actions to address the recommendations in the report.

As part of our evaluation, we also obtained technical assistance from the International Trade Commission, Office of Inspector General (ITC OIG). An 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 and will provide a report of the results under separate cover to the NEA OIG.

EVALUATION RESULTS

In March 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 2012 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
8. Remote Access Management
9. Contingency Planning
10. Contractor Systems

The FY 2012 FISMA evaluation concluded that NEA has established a security program for protecting its IT infrastructure and is compliant with FISMA legislation. We determined that all of the specific program areas met the level of performance as indicated in DHS's FY 2012 FISMA checklist. This report presents our completed DHS checklist for NEA. (Attachment A)

Although, we did not identify any material weaknesses in the program areas, we did identify areas for improvement in the following programs:

1. Identity and Access Management
2. Risk Management

Identity and Access Management

Federal Personal Identity Verification Program

NEA has established and is maintaining a program for identity and access management. However, NEA has not developed a policy as to how the agency will implement the use of the Federal PIV smartcard credentials as the common means of authentication for access to the agency's networks and information systems.

Homeland Security Presidential Directive 12 (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractors*, was issued on August 12, 2004. HSPD-12 requires a mandatory, government-wide standard for secure and reliable forms of identification, issued by the federal government to its employees and employees of federal contractors, for access to federally-controlled facilities and networks. Based upon this directive, the NIST developed Federal Information Processing Standards Publication 201, which includes minimum requirements for a Federal PIV system. Subsequently, additional implementation guidance was issued by DHS, OMB and NIST.

OMB Memorandum M-11-11, *Continued Implementation of Homeland Security President Directive 12 - Policy for a Common Identification Standard for Federal Employees and Contractors*, dated February 3, 2011, further discusses the implementation of HSPD-12. It included a memorandum from Homeland Security, which directed each agency to develop and issue an implementation policy by March 31, 2011, through which the agency will require the use of the PIV credentials as the common means of authentication for access to that agency's facilities, networks, and information systems. To be effective in achieving the

goals of HSPD-12, and realizing the full benefits of PIV credentials, the memorandum included certain requirements for the agency's implementation policy.

NEA is compliant with the requirement for the use of PIV smartcard credentials for physical access and during FY 2012 NEA issued new computer systems to employees which can enable the use of the PIV smartcard. However, NEA has not implemented the use of the PIV smartcard credentials for access to its networks and information systems.

Recommendation

NEA should develop an implementation policy to require the use of PIV smartcard credentials for logical access to its networks as directed by HSPD-12. In addition, NEA should implement the use of the PIV smartcard credentials for access to its network and information systems.

Risk Management

Encryption of Data on Mobile Computers/Devices

Overall, NEA has established and is maintaining a risk management program that is consistent with FISMA requirements, OMB policies and applicable NIST guidelines. However, during our evaluation, we identified an area for improvement to its information security program.

During FY 2011, we evaluated NEA's control over computer-related equipment. As a result of the review, the Information Systems Security Officer (ISSO) submitted seven recommendations to the CIO which were included in the OIG's final report entitled, *Review of NEA's Control Over Computer-Related Equipment, Report No. R-11-02*. We reviewed the corrective actions for the ISSO's recommendations and determined that six of the seven recommendations were implemented. However, we do not believe that the corrective action implemented for Recommendation No. 1, regarding encryption of information on all mobile computers/devices, meets the intent of OMB guidance. OMB Memorandum M-06-16, *Protection of Sensitive Agency Information*, dated June 23, 2006, states:

All departments and agencies "**encrypt all data** on mobile computers/devices which carry agency data unless the data is determined to be non-sensitive, in writing, by your Deputy Secretary or an individual he/she may designate in writing."

NEA implemented the Microsoft Windows 7 Encryption File System method. However, this method does not encrypt all data automatically. Only *files and folders*, selected by the user can be encrypted. Encryption must be activated or de-activated by the user. Therefore, the agency must rely on users to encrypt agency data, which could also include personally identifiable information (PII). Agency data and PII continue to be at risk if users simply choose not to encrypt data. Lastly, there are no policies and procedures in place that require employees to encrypt data on mobile computers/devices.

Recommendation

NEA should implement an automatic encryption method which includes all data on all mobile computers/devices that carry agency information to ensure PII and sensitive information is not compromised. NEA should also develop and implement policies and procedures requiring the encryption of all data on mobile computers/devices.

EXIT CONFERENCE

We provided a draft copy of this report to NEA ITM officials on December 5, 2012. The officials concurred with our findings and recommendations and agreed to initiate corrective actions.

RECOMMENDATIONS

We recommend that the National Endowment for the Arts, Office of Information and Technology Management:

1. Develop an implementation policy to require the use of PIV smartcard credentials for logical access to its networks as directed by HSPD-12.
2. Implement the use of the PIV smartcard credentials for access to its network and information systems.
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 is not compromised.
4. Develop and implement policies and procedures requiring the encryption of all data on mobile computers/devices.