



**National  
Endowment  
for the Arts**  
arts.gov

**OFFICE OF INSPECTOR GENERAL**

**FISCAL YEAR 2015 EVALUATION OF  
NATIONAL ENDOWMENT FOR THE ARTS'  
COMPLIANCE WITH  
THE FEDERAL INFORMATION SECURITY  
MANAGEMENT ACT OF 2002**

**REPORT NO. R-16-01**

**October 28, 2015**

**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 National Endowment for the Arts' (NEA) 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. 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) issued Memorandum M-15-01, dated October 3, 2014, entitled *Fiscal Year (FY) 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices*. The memorandum identified Administration information security priorities, provided agencies with FY 2014-2015 FISMA and Privacy Management reporting guidance and deadlines, as required by the *Federal Information Security Management Act of 2002* (P.L. 107-347). It established new policy guidelines to improve Federal information security posture.

On December 18, 2014, the *Federal Information Security Modernization Act of 2014*, was passed to further strengthen Federal information security by updating the *FISMA*, and providing a comprehensive framework for ensuring the effectiveness of information security controls over federal information operations and assets. In the *FY 2015 CIO Annual FISMA Metrics* agencies are directed to ensure security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of government information.

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. ITM also operates support systems for Internet and intranet services. NEA has agreements with other Federal agencies to provide financial and payroll services. NEA also has agreements/contracts with other providers for email, grant application process and its Personal Identity Verification (PIV) program. NEA's Chief Information Officer 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 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.

On June 19, 2015, the U.S. Department of Homeland Security (DHS) issued FY 2015 Federal Information Security Modernization Act reporting metrics, VI.2, which includes a checklist for

Offices of Inspectors General (OIG) to assess the level of performance achieved by agencies in specific program areas.

## **PRIOR FISMA EVALUATION AND OTHER REPORTS**

NEA OIG has issued prior reports which addressed weaknesses found in NEA's information systems security program, including its continuous monitoring, *Homeland Security President Directive 12 - Policy for a Common Identification Standard for Federal Employees and Contractors* (HSPD-12) implementation, patch management, and perimeter security programs. Below is the status of open recommendations from prior evaluation reports:

### **Fiscal Year 2012 Evaluation report of NEA's Compliance with the Federal Information Security Management Act of 2002 (Report No. R-13-01)**

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

*NEA has implemented the capability to use PIV smartcard credentials for access to its network and information systems. However, use of the card is not mandatory. Therefore, the recommendation will remain open.*

### **Evaluation of NEA Perimeter Security (Report No. R-13-03)**

*Recommendation No. 1:* Perform scheduled, routine scanning of the perimeter on at least a monthly basis.

*Recommendation No. 2:* Perform perimeter scans after new hardware or software is introduced to the NEA perimeter network.

*NEA has developed policies for perimeter scanning requirements; however, the policy has not been implemented consistently.*

In January 2015, NEA ITM contracted with the US Department of Transportation, Federal Aviation Administration's Enterprise Services Center (ESC) to evaluate its information systems for compliance with the FISMA requirements. The evaluation included:

- Vulnerability scan of NEA's network and devices
- United States Government Configuration Baseline workstation compliance scans
- Database scan
- Web application scan

Overall, the evaluation identified missing critical and high security patches associated with the operating system and third party applications.

## EVALUATION RESULTS

### Continuous Monitoring and Security Configuration Management

NEA has not established a continuous monitoring or security configuration management program that is consistent with FISMA requirements, OMB policy and application NIST guidelines.

Continuous monitoring is described as the ability to provide additional visibility for organizations to identify signs of compromise to make hardware assets harder to exploit through hardware asset management, software asset management, secure configuration management and vulnerability management. In short, an effective monitoring program allows an agency to identify hardware and software connected to its network (scanning), whether authorized or unauthorized. Once vulnerabilities are identified, an effective configuration management program should provide for near-real-time capability to find and fix configuration deviations faster than they can be exploited. This includes maintaining an effective patch management process to ensure timely and secure installation of software patches. NIST Special Publication 800-40 Rev. 3, describes the importance of patch management:

*Patch management is the process for identifying, acquiring, installing, and verifying patches for products and systems. Patches correct security and functionality problems in software and firmware. From a security perspective, patches are most often of interest because they are mitigating software flaw vulnerabilities; applying patches to eliminate these vulnerabilities significantly reduces the opportunities for exploitation. Also, patches are usually the most effective way to mitigate software flaw vulnerabilities, and are often the only fully effective solution.*

In September 2015, NEA OIG contracted with US International Trade Commission (USITC) OIG to perform an analysis of NEA's network scanning results to evaluate NEA's progress in mitigating the vulnerabilities identified in previous evaluations. Consistent with the prior USITC OIG and ESC evaluations, this analysis identified a high number of missing critical and high severity patches associated primarily with third party applications, such as Adobe Acrobat, Apple Quicktime, and Oracle Java software. *NEA has not implemented an effective program to ensure timely installation of software patches. The process for patching NEA systems is ineffective and exposes the Agency's information and systems to significant risk.*

We are issuing the following recommendations as a result of the findings identified above.

*Recommendation No. 1: Report patching status monthly to agency executive management.*

*Recommendation No. 2: Conduct a risk assessment to determine a tool and implement a process that will secure (patch) all IT assets.*

*Recommendation No. 3: Apply a risk-based framework to evaluate, assess and mitigate all high or critical vulnerabilities on the day of release.*

*Recommendation No. 4: Fully patch all devices that are attached to the network.*

## **Remote Access Management**

NEA has not established an effective remote access program that is consistent with FISMA requirements, OMB policy and applicable NIST guidelines.

NEA requires only a user ID and password to remote access NEA information system and does not require the use of an authentication device such as a token or HSPD-12 PIV card for remote computer or network authentication. A single-factor authentication mechanism, such as a username and password, is insufficient to block even basic attackers.

OMB M-06-16, *Protection of Sensitive Agency Information*, dated June 23, 2006, states the following regarding two-factor authentication: "The National Institute of Standards and Technology (NIST) provided a checklist for protection of remote information...recommending all departments and agencies take the following actions:

- 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;
- Allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access;
- Use a "time-out" function for remote access and mobile devices requiring user re-authentication after 30 minutes inactivity; and
- Log all computer-readable data extracts from databases holding sensitive information and verify each extract including sensitive data has been erased within 90 days or its use is still required."

Without a fully implemented multifactor authentication process for remote access, NEA is exposed to unnecessary risks to its network.

*Recommendation No. 5:* Conduct and implement a comprehensive program for remote access, for government furnished or personal equipment, which will include the implementation of multifactor authentication.

## **EXIT CONFERENCE**

We provided a draft copy of this report to NEA officials on October 28, 2015. The officials generally concurred with our findings and recommendations and agreed to initiate corrective actions.

## RECOMMENDATIONS

*Recommendation No. 1:* Report patching status monthly to agency executive management.

*Recommendation No. 2:* Conduct a risk assessment to determine a tool and implement a process that will secure (patch) all IT assets.

*Recommendation No. 3:* Apply a risk-based framework to evaluate, assess and mitigate all high or critical vulnerabilities on the day of release.

*Recommendation No. 4:* Fully patch all devices that are attached to the network.

*Recommendation No. 5:* Conduct and implement a comprehensive program for remote access, for government furnished or personal equipment, which will include the implementation of multifactor authentication.