ART WORKS.

National
Endowment
for the Arts
arts.gov

## OFFICE OF INSPECTOR GENERAL

# FISCAL YEAR 2014 EVALUATION OF

# NATIONAL ENDOWMENT FOR THE ARTS' COMPLIANCE WITH THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT OF 2002

## REPORT NO. R-15-01

**November 14, 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 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 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices.* The memorandum identifies current Administration information security priorities, provides agencies with Fiscal Year (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 establishes new policy guidelines to improve Federal information security posture. It also introduces new requirements based on assessments of emerging threat activities, to include the introduction of: enhanced FISMA metrics; a proactive vulnerability scanning process; and updated incident response procedures.

The *Government Performance Results and Modernization Act of 2010* (P.L. 111-352) established Cross-Agency Performance Goals (CAP Goals)[1] as tools used by agency leadership to accelerate progress on a limited number of Presidential priority areas. As with previous CAP Goals, cybersecurity was identified as one of the priorities for FY 2014 with focus on Information Security Continuous Monitoring and Identity, Credential, and Access Management, and Anti-Phishing and Malware Defense.

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 systems 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 an agreement with the U.S. 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 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.

[1] http://www.performance.gov/node/3401/view?view=public#overview

## 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 December 2, 2013, the U.S. Department of Homeland Security (DHS) issued a checklist for Offices of Inspectors General to assess the level of performance achieved by agencies in specific program areas during the FY 2014 FISMA evaluation period. The specific program areas to be assessed were:

1. Continuous Monitoring Management
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&Ms)
8. Remote Access Management
9. Contingency Planning
10. Contractor Systems
11. Security Capital Planning

## PRIOR FISMA EVALUATION AND OTHER REPORTS

NEA OIG has issued prior reports which address 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 are open recommendations from prior evaluation reports:

- Implement the use of the PIV smartcard credentials for access to its network and information systems.
- Perform scheduled, routine scanning of the perimeter on at least a monthly basis.
- Perform perimeter scans after new hardware or software is introduced to the NEA perimeter network.

Although NEA continues to make progress, completion of corrective actions should remain a priority to improve the monitoring and defense of its information systems.

## EVALUATION RESULTS

The FY 2014 FISMA evaluation concluded that NEA has established a security program for protecting its IT infrastructure and is generally compliant with FISMA legislation. We determined that the specific program areas, as indicated in DHS' FY 2014 FISMA OIG checklist, met the level of performance. We did not identify any material weaknesses in the program areas. However, our evaluation concluded that NEA should improve its management of contractor systems.

During the evaluation, we noted that the agreement with DOT for financial services expired in November 2013. We were informed by NEA that the renewal was submitted to DOT and several attempts have been made to obtain an executed agreement. Although we understand that NEA must work collaboratively with service providers through the agreement process, NEA should ensure that the process is implemented timely to prevent the memoranda of understanding (MOU) and interconnection security agreements (ISA) from lapsing.

NIST Special Publication 800-47*, Security Guide for Interconnecting Information Technology Systems*, provides guidance for planning, establishing, maintaining, and terminating interconnections between information technology (IT) systems that are owned and operated by different organizations. Without a MOU/ISA, providers, including Federal agencies, may not understand or have adequate security requirements in place for interconnectivity to NEA's information systems.

## RECOMMENDATION

NEA should develop policies and implement procedures to ensure that appropriate agreements (e.g., MOUs, ISAs, contracts, etc.) with service providers are current.

### ITM RESPONSE

*The Federal Aviation Administration [DOT] went through a re-organization. As a result, new approval procedures and processes were implemented. While the MOU has been approved, NEA will ensure that the signature pages are updated in a timely manner.*

## EXIT CONFERENCE

We provided a draft copy of this report to ITM officials on November 12, 2014 The officials generally concurred with our findings and recommendations and agreed to initiate corrective actions.