



## OFFICE OF INSPECTOR GENERAL

# EXECUTIVE SUMMARY OF FY 2014 FISMA EVALUATION

### 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), and 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)<sup>1</sup> 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.

---

<sup>1</sup> <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.

## **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 and access management program.

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 ITM 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.

## **RECOMMENDATION**

We recommended NEA improve its management of contractor systems.