NATIONAL
ENDOWMENT
FOR THE ARTS

OFFICE OF INSPECTOR GENERAL

REVIEW OF NATIONAL ENDOWMENT FOR THE ARTS' CONTROL OVER COMPUTER-RELATED EQUIPMENT

Report No. R-11-02

January 25, 2011

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.

BACKGROUND

During the FY 2010 Evaluation of the National Endowment for the Arts' (NEA) Compliance with the Federal Information Security Management Act of 2002 (FISMA), the Office of Inspector General (OIG) became aware of a computer security incident involving the theft of a laptop computer ("laptop") from the office of an NEA employee. While it does not appear that this incident resulted in any identity theft or other damage to the Agency or persons involved, we felt it was critical to understand the factors and circumstances that led to the theft of the laptop and identify what needs to be done to strengthen controls over the Agency's computer-related equipment.

Our review of the incident noted several weaknesses in the computer security incident reporting process and physical security of laptops. As a result, we increased the scope of the review to include reported computer security incidents involving laptops during the past five years.

OBJECTIVE/SCOPE

The objective of the review was to determine whether NEA was processing and reporting computer security incidents, specifically those involving laptop thefts, in accordance with its policies and federal guidance such as the National Institute of Standards and Technology's (NIST) Special Publication (SP) 800-61, *Computer Incident Handling Guide*. A computer incident within the federal government, as defined by NIST SP 800-61, is a violation or imminent threat of violation of: computer security policies, acceptable use policies, or standard computer security practices. NIST guidance and NEA's *Computer Security Incident Policy* further describe thefts of hardware or software as computer incidents.

Our scope was computer security incidents involving the theft of laptops reported from FY 2005 to present. The review was conducted in accordance with the Council of the Inspectors General on Integrity and Efficiency Quality Standards for Inspections and Evaluations, as applicable.

METHODOLOGY

We interviewed NEA staff from Information and Technology Management (ITM), Administrative Services Office (ASO), and other affected personnel. We held discussions with General Service Administration staff and contractors responsible for building operations and security at the Old Post Office Building (OPO). We also held discussions with officials at the Federal Protective Service. We obtained and reviewed NEA policies and the NIST guidelines for reporting computer security incidents. NEA has two internal policies that define procedures for reporting computer security incidents:

1. NEA Directive Number 1355, Revision No. 2, *Security of Arts Endowment Offices*, effective 2/14/06
2. NEA ITM *Computer Security Incident Policy*, rev. 11/15/10

NEA's Information and Technology Management (ITM) provided us with a list of computer security incidents, involving laptops, reported since FY 2005. In total, there were seven laptops stolen and one listed as "issued and never returned" by a staff member who is no longer employed at the Agency. We reviewed each incident and applicable guidelines to determine NEA's compliance with computer security incident reporting requirements. Details are presented below.

INCIDENT NOTIFICATION

An organization's ability to respond to computer-related security incidents is necessary for rapidly detecting incidents, minimizing loss and destruction, and mitigating weaknesses. Timely reporting and notification is essential to effective handling of computer security incidents to allow both external and internal parties to execute their responsibilities to ensure quick resolution.

Since FY 2005, there have been eight reportable computer security incidents at the NEA. Of the eight incidents, two were not reported to the ITM Information System Security Officer (ISSO), one was not reported to the FPS and none were reported to the OIG. According to NEA's ITM *Computer Security Incident Policy*, both "NEA's Administrative Services Office and the Federal Protective Service are to be notified of all computer-related thefts." ITM's policy, however, did not include notification to the OIG. The Office of Management and Budget (OMB) Memorandum, M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information (PII)*, states, in part, that agencies should notify law enforcement agencies and Inspectors General of actual or suspected breaches involving PII. *We discussed this finding with the ITM Information System Security Officer (ISSO) and the policy was subsequently revised to include notification to the OIG*.

During our discussions with ITM and the ASO staff, we found inconsistencies in the staff's understanding of notification and reporting responsibilities. ITM's *Computer Security Incident Policy* clearly delegates the responsibility for investigating and reporting computer incidents to the Computer Security Incident Team (CSIT), which, according to its policy, consists of three members from ITM; the Deputy Chief Information Officer, Network Administrator, and the ISSO. However, we found that ITM delegates the responsibility for reporting computer-related incidents (e.g. FPS) to the ASO.

We recommend that ITM assumes responsibility for notification and reporting of any computer-related incidents as required by its policy.

We also identified several inconsistencies in the Agency's written policies governing reporting computer-related incidents. For example:

Directive 1355, Section V. D.8, instructs employees to report theft and vandalism of Federal or personal property first to the FPS, and immediately thereafter to the ASO or ITM as relevant. However, this is in direct conflict with ITM's *Computer Security Incident Policy* which only instructs employees to report the incidents to the Help Desk via e-mail (or phone if e-mail is not available).

We recommend that ITM and the ASO collaborate to ensure that Agency directives and ITM's *Computer Security Incident Policy* are consistent and implemented. The policies should clearly outline the responsibility for notification of computer-related security incidents to both external and internal parties by ITM and security incidents involving non-computer-related equipment to the ASO. In addition, we recommend that the Agency ensures that the policies are communicated to employees and contractors.

INTERNAL CONTROLS

Accountability for NEA Computer-Related Equipment

NEA Directive 1355 Section D.12 directs employees to return all assigned Federal computer-related hardware and software to ITM upon separation from the Arts Endowment. However, ITM records indicate that in one instance, a laptop was not returned upon separation of an employee. The employee was assigned a laptop in 2003 and subsequently re-assigned it to another employee, without notifying ITM. *Employment Clearance Statements* indicated that both employees were cleared by ITM for returning all computer-related equipment, including laptops. The original assignee was cleared January 2009 and the subsequent employee was cleared in August 2007. ITM contacted both employees in February 2009 to determine the location of the laptop. The employee who separated in 2007 indicated that the laptop was returned prior to separation, however, there is no documentation to confirm that the laptop was returned to the agency. An incident report was not completed and the ISSO was not notified. We recommend that ASO and ITM collaborate to develop and implement policies and procedures to prohibit the assignment of any computer-related equipment by employees other than authorized ITM staff.

NIST SP-800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations, Appendix F-Media Protection*, recommends as a control enhancement, organizations track, document and verify media sanitation and disposal actions. ITM's inventory includes equipment classified as "retired"; however "excessed" equipment is not included. For example, the above laptop was identified in ITM's 7/16/2008 inventory as assigned to the original employee; however, a separate excess report identified the laptop as excessed on 1/10/2008. The laptop was not identified in the 2009 inventory. In addition, the excess list provided did not indicate how or to what organization the equipment was excessed.

According to ITM's *Equipment Inventory Policy*, when equipment is transferred between departments or moved to another location the information on the IT Equipment Inventory Spreadsheet must be updated to reflect the new location of the equipment. ITM or the ASO did not maintain documentation identifying the recipient of the excessed computer-related equipment.

We recommend that ITM, in cooperation with the ASO, develop and implement policies and procedures to ensure documentation on all computer-related equipment classified as excess is maintained, including the identification of the recipient organization. We also recommend that ITM include excess computer-related equipment in its inventory, in the year of excess, to improve accountability and ensure that computer-related equipment is accurately accounted for and documented.

NEA employees are not required to provide written acknowledgement for receipt of computer-related equipment; therefore, there is no documentation to support receipt of equipment. We recommend that ITM, in cooperation with ASO, develop and implement policies and procedures to ensure that computer-related equipment issued to employees or contractors is adequately documented and the employee's signature is included to acknowledge receipt.

To further strengthen controls, we recommend that ASO and ITM work with the Office of Human Resources to revise the standard employee exit form to include identification information on computer-related equipment to ensure equipment issued to employees or contractors is returned to the Agency upon separation.

The agency informed us that the standard employee exit form has been revised to include identification information for computer-related equipment, and is now in use.

We were informed by ITM that the return of assigned computer-related equipment is verified before clearing employees or contractors for separation. However, we recommend that ITM documents the identification number on the employee exit form to verify return of "assigned" equipment.

Portable and mobile computer systems, such as laptops, have an increased risk of theft and physical damage. Users can also "misplace" or leave laptops unattended. In seven of the eight reported incidents, laptops were stolen from the offices of NEA where they were left unsecured. NEA Directive 1355, states in part, that agency personnel are responsible for "returning promptly to ASO or ITM all property and equipment lent from their inventories at the conclusion of the meeting or other purpose." However, in one instance, seven laptops were authorized for an event outside of the building. At the end of the event, the laptops were packed in boxes labeled "laptops" to be returned to the agency. The boxes were stored over a weekend in an agency storeroom. According to ITM records, three laptops were stolen somewhere between the facility and storage at the NEA.

NIST 800-12, *An Introduction to Computer Security: The NIST Handbook*, recommends secure storage of laptops when not in use. The handbook recommends encryption of data files on stored media as a cost-effective precaution against disclosure of confidential information if a laptop is lost or stolen. It also recommends user security briefings on the proper security of portable computer systems and signed briefing acknowledgments.

We recommend that ITM provide all users with physical security for laptops such as "security cable locks" and ensure that users understand and acknowledge their responsibility for the security of Agency computer-related equipment. We also recommend that ITM install anti-theft software on laptops.

On January 14, 2011, ITM began installing security cable locks on desktop and laptop computers.

Removal of NEA Computer-Related Equipment

NEA Directive 1355, VII.B, states that "if the item to be removed is computer-related hardware or software, whether owned by the Federal government or the individual, the individual must obtain a special pass signed by the CIO [Chief Information Officer] or other authorized ITM official."

Directive 1355, Section VII.C states: "On departing from the OPO with the specified property, the security guard on duty will check the pass's signature against a list of authorizers' signatures. The guard also may ask to see the item. When the guard has determined the validity of the pass, the individual may leave with the item." This policy would be impossible to implement without the cooperation of employees. However, we found that employees were not requesting or displaying passes for the removal of NEA computer-related equipment. This weakness in controls over computer-related equipment increases the risk of the Agency and its employees being exposed to potential loss of Federal property and theft of PII or sensitive information.

We recommend that ASO and ITM collaborate to revise its policies and directive to improve security requirements for removing computer-related property, such as laptops and communicate the requirements to NEA employees.

DOCUMENTATION OF INCIDENTS

ITM was unable to provide adequate documentation detailing the events for seven of the eight incidents. ITM did not complete computer security incident reports and did not maintain documentation for resolution or final disposition of the incident. ITM informed us that computer security incidents were reported to ASO by email or telephone.

NIST and the US-CERT: United States Computer Emergency Readiness Team's incident reporting guidelines provide recommendations for incident documentation. For example,

NIST SP 800.61, *3.2.5 Incident Documentation*, recommends, in part:

> **As soon as an incident response team suspects that an incident is occurring or has occurred, it is important to immediately start recording all facts regarding the incident. The incident response team should maintain records about the status of incidents, along with other pertinent information.**

ITM's *Computer Security Incident Policy* also directs the CSIT to ensure that all computer incidents are investigated in a "timely fashion." However, the policy does not include time requirements or guidance on "timely fashion." In one instance, ITM took more than two weeks before determining that there was no PII or any other sensitive information on the missing laptop.

Directive 1355, VIII.C further directs the affected employee to prepare a brief memorandum to the ASO detailing the incident. The ASO could only provide memoranda to support two incidents.

We recommend that the ITM develop and implement policies and procedures to adequately document computer security incidents. ITM should develop time requirements for investigating and reporting computer security incidents. Written notification of computer-related incidents to appropriate internal and external parties should be supported by Computer Incident Reports and employee's statement detailing events. We also recommend that the ASO and ITM collaborate to revise policies and procedures to ensure affected employees adequately document computer security incidents and submit the documentation to ITM. ITM should also include this requirement in its *Computer Security Incident Policy.*

RECOMMENDATIONS

As a result of our findings and the most recent computer incident, the ISSO submitted recommendations to the CIO to address weaknesses found in ITM's computer incident policies and procedures. The recommendations included:

1. Encryption of information on all mobile computers/devices which carry Agency information to ensure PII and sensitive information is not compromised.

2. Revising *ITM's Computer Security Incident Policy* to centralize the responsibility of notifying all parties involved of lost or stolen equipment, including time requirements for reporting incidents.

3. Developing and implementing the standard incident reporting form to include detailed information on computer equipment lost or stolen.

4. Requiring users to sign for mobile/portable computer-related equipment (e.g., laptops) and acknowledge responsibility for safeguarding equipment.

5. Developing or revising the inventory system for tracking stolen equipment and include status of encryption and whether PII or sensitive data is on equipment.

6. Developing and implementing procedures to ensure accuracy of inventory tracking system.

7. Increasing users' knowledge on computer security incident reporting.

In addition to the ISSO recommendations, the OIG recommends:

1. ITM assumes responsibility for notification and reporting of any computer-related incidents as required by its policy.

2. ASO and ITM collaborate to ensure that Agency directives and ITM's *Computer Security Incident Policy* are consistent and implemented. The policies should clearly outline the responsibility for notification to both external and internal parties by ITM for computer-related equipment and ASO for non-computer-related equipment and building operations. In addition, we recommend that the Agency ensures that the policies are communicated to employees and contractors.

3. ASO and ITM collaborate to develop and implement policies and procedures to prohibit the assignment of any computer-related equipment by anyone other than authorized ITM employees.

4. ASO and ITM collaborate to develop and implement policies and procedures to ensure documentation on all computer-related equipment classified as excess is maintained, including the identification of the recipient organization.

5. ITM include excess computer-related equipment in its inventory, in the year of excess, to improve accountability and ensure that computer-related equipment is accurately accounted for and documented.

6. ITM, in cooperation with the ASO, develop and implement policies and procedures to ensure that computer-related equipment issued to employees is adequately documented and the employee's signature is included to acknowledge receipt.

7. ITM documents the serial number of mobile/portable computer-related equipment on the employee exit form to verify return of "assigned" equipment.

8. ITM provide <u>all</u> users with physical security for laptops such as "security cable locks" and ensure that users understand and acknowledge their responsibility for the security of Agency computer-related equipment. We also recommend that ITM install anti-theft software on laptops.

9. ASO and ITM collaborate to revise Agency policies and directives to improve security requirements for removing mobile/portable computer-related property, such as laptops and communicate the requirements to NEA employees.

10. ITM develop and implement policies and procedures to adequately document computer security incidents. ITM should develop time requirements for investigating and reporting computer security incidents. Written notification of computer-related incidents to appropriate internal and external parties should be supported by Computer Incident Reports and employee's statement detailing events.

11. ASO and ITM collaborate to revise policies and procedures to ensure affected employees adequately document computer security incidents and submit the documentation to ITM. ITM should also include this requirement in its *Computer Security Incident Policy.*