



OFFICE OF INSPECTOR GENERAL

EVALUATION REPORT

FISCAL YEAR 2011 EVALUATION OF

NEA'S COMPLIANCE WITH THE

FEDERAL INFORMATION SECURITY

MANAGEMENT ACT OF 2002

REPORT NO. R-12-01

November 15, 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.

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 NEA's 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. 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-11-33, dated September 14, 2011, entitled *FY 2011 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 2011 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 (FISCAM)*.

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 (LAN). These are the Grants Management System (GMS), which contains information on grant applications and the Automated Panel Bank System (APBS), which contains information on panelists who review grant applications. NEA has contracted with the Department of Transportation (DOT) Enterprise Service Center to host its Financial Management System (FMS) through DOT's Delphi Financial Management System and the U.S. Department of Agriculture (USDA) National Finance Center for payroll services. NEA has also contracted with other providers for email, grant application process and its personal identity verification program (PIV). ITM operates support systems for internet and intranet services.

The Chief Information Officer (CIO) is responsible for developing policies and procedures to ensure that security is provided over 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

The NEA Office of Inspector General (OIG) issued a report entitled Fiscal Year 2010 Evaluation of NEA's Compliance with the Federal Information Security Act of 2002 (Report No. R-11-01) dated November 15, 2010. The report had seven (7) recommendations, all of which NEA has implemented corrective actions.

We considered the results of our Review of NEA's Control Over Computer-Related Equipment, Report No. R-11-02, dated January 25, 2011. The review 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. As of August 24, 2011, NEA had implemented corrective actions for seven of the eleven recommendations.

We also considered the independent risk assessment report 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 policy 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 (FDCC).

EVALUATION RESULTS

In June 2011, 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 the specified program areas during the Fiscal Year 2011 FISMA evaluation period.

This report presents our completed DHS checklist for the NEA. We determined the level of performance (a, b, or c) that the NEA had achieved for each of the program areas listed. NEA program areas were designated as an "a" status where we determined that the NEA met all the program attributes specified by the DHS. NEA program areas were designated as a "b" status where we determined that one or more conditions listed by the DHS needed significant improvement at the NEA. Due to time and resource constraints, we were unable to test all conditions listed by the DHS in the "b" sections. Therefore, it is possible that more of these conditions exist at the NEA than those we have checked. NEA program areas were designated as a "c" status where we determined that NEA has not yet established the program area.

The FY2011 FISMA evaluation concluded that NEA's Office of Information and Technology Management (ITM) have established a security program for protecting its information technology (IT) infrastructure and is generally compliant with FISMA legislation, however improvements are needed. The most recent risk assessment identified several areas which need to be addressed by NEA to strengthen its security program and increase its compliance with FISMA requirements, OMB policy and applicable NIST guidelines. Some of the issues are related to improvements in policies and procedures, documentation, system vulnerabilities and risk assessments performed by ITM.

We determined that the following program areas met the level of performance specified by DHS's Fiscal Year 2011 FISMA checklist:

1. Risk Management
2. Configuration Management
3. Incident Response and Reporting
4. Security Training
5. Identity and Access Management
6. Continuous Monitoring Management
7. Contractor Systems

We determined the following program areas were not fully effective as a result of the conditions identified that need improvement.

1. Remote Access Management
2. Plan of Action & Milestones (POA&Ms)
3. Contingency Planning

We determined that NEA does not have a program in place for the following:

Security Capital Planning

Details of our evaluation are presented in the following narrative.

Risk Management

Overall, NEA has established and is maintaining a risk management program that is consistent with FISMA requirements, OMB policy and applicable NIST guidelines. However, some improvement opportunities have been identified. EmeSec Information Assurance (EmeSec) performed the latest risk assessment; the results of which were issued on September 23, 2011. The review concluded that while NEA has begun implementing a consistently improving Security Program, “NEA would benefit from a prioritized approach that addresses some of the most significant compliance requirements as a means of reducing the compliance and potential security risk(s) faced by the NEA Chairman, the CIO and the NEA-IG.” The assessment identified the following weaknesses:

1. Establish system ownership and security management that is consistent with NIST requirements.
2. Formally categorize the General Support System (GSS).
3. Move the apps.NEA.gov server into a demilitarized zone (DMZ).
4. Fully implement FDCC.
5. Modify web application code to sanitize all user input.
6. Apply all security patches.
7. Update policies and/or develop separate procedure(s) in support of each policy and specifics related to activities, task, and performances.
8. Update the System Security Plan (SSP) and the Certification & Accreditation (C&A) package in the proper format.
9. Document the risks related to NEA Network System including showing those risks that can be mitigated and those that cannot be mitigated.
10. Remove security policy and procedure development from the legal approval process.
11. Conduct regular security assessments.
12. Some technical enhancements
 - use stronger passwords for all account
 - enable Administrator accounts on network printers

- disable unnecessary ports and services
- apply patches and hot-fixes on all servers and workstations
- create unique administrator accounts for each administrator
- upgrade unsupported operating systems.

The system vulnerability assessment identified 20 internal system vulnerabilities which were categorized as critical and 363 vulnerabilities, both internal and external were categorized as high risk. The report also identified several medium to low risk vulnerabilities.

Subsequent to our evaluation, ITM included the weaknesses and vulnerabilities identified by the risk assessment in its Plan of Actions and Milestones (POA&Ms). In addition, ITM recently implemented Nessus, a continuous monitoring tool which identifies network vulnerabilities.

We recommend that NEA implement corrective actions for recommendations in the Risk Assessment Report issued September 23, 2011 by EmeSec. The corrective actions should address all of the recommended policy, administrative and technical improvements including vulnerabilities identified. NEA should also use a prioritized approach based on the categorization of risk to implement corrective actions for system vulnerabilities.

Configuration Management

NIST 800.53 (Rev.3) defines the configuration management plan as detailed processes and procedures for how configuration management is used to support system development life cycle activities at the information system level. The plan describes how to move a change through the change management process, how configuration settings and configuration baselines are updated, how the information system component inventory is maintained, how development, test, and operational environments are controlled, and finally, how documents are developed, released, and updated. The plan should also define roles and responsibilities.

During our review of NEA's configuration management program, we determined that NEA has established and is maintaining a security configuration management program. However, several areas of improvement were identified during the independent risk assessment and the FISMA evaluation. The assessment concluded that "NEA had no detailed configuration management policy; no configuration control board" and was not "fully FDCC compliant."

Our review of NEA's Change Management Program determined that in some cases, the requestor, reviewer and approver for changes to the system or software were the same person. The independent risk assessment also identified the same segregation of duties issue.

We recommend that NEA revise its change management policy to provide for adequate segregation of duties. The policy should ensure that the request, review and approval for potential and/or actual changes to hardware or software are not performed and approved by the same staff person.

Incident Response and Reporting

During the FY 2010 FISMA evaluation, we identified several areas in need of improvement in NEA's Computer Security Incident Reporting Program. We issued a report, NEA's Control Over Computer-Related Equipment (Report No. R-11-02) which contained eleven recommendations. The report also included seven recommendations by the NEA Information System Security Officer (ISSO) to the CIO to address weaknesses found in its program.

Appendix III to OMB Circular A-130 states:

When faced with a security incident, an agency should be able to respond in a manner that both protects its own information and helps to protect the information of others who might be affected by the incident. To address this concern, agencies should establish formal incident response mechanisms.

As of August 24, 2010, NEA had implemented corrective actions for seven of the eleven OIG recommendations and for five of the seven ISSO recommendations. *Subsequent to our evaluation, ITM informed us that corrective actions for three of the remaining OIG recommendations have been implemented and awaiting management concurrence.*

Although there are areas in need of improvement, NEA has established and is maintaining an incident response and reporting program that is consistent with FISMA requirements, OMB policy and applicable NIST guidelines.

We recommend that NEA implement corrective actions for the remaining six recommendations in Report No. R-11-02, NEA's Control over Computer-Related Equipment.

Security Training

NIST Special Publications 800-50, *Building an Information Technology Security Awareness and Training Program* and 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model* provide the standards for security awareness and training. NEA administered its FY 2011 Annual Refresher Training August 10, 2011.

We obtained and reviewed the FY 2011 *IT Security and Privacy Awareness Refresher* training materials and notification sent to employees by email. We determined that the date of completion requirement, which was recommended by the OIG in the FY 2010 FISMA evaluation, was included. However, we noted that while the training included

reporting computer-related equipment theft, it did not include computer security incident and reporting as recommended and agreed to by ITM.

Appendix III to OMB Circular A-130 states, in part:

Awareness and training for individuals with access to the system should include how to use the system's incident response capability.

We also obtained and reviewed the list of employees who had completed the FY 2011 security awareness training and determined that 99% of the staff completed the training (165 completed, 1 did not complete).

Although NEA has established and is maintaining a security training program we recommend that ITM includes computer security incident and reporting in its annual security awareness training in accordance with OMB Circular A-130.

Plans of Action and Milestones (POA&Ms)

OMB's instructions direct Inspectors General to review the status of the agency's POA&Ms program. The program should be consistent with FISMA requirements, OMB policy and applicable NIST guidelines and include written policies for managing security weaknesses. OMB Memorandum M-02-01 describes a POA&M as a corrective action plan, a tool that identifies tasks that need to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the task and scheduled completion dates for the milestones. The purpose is to assist agencies in identifying, assessing, prioritizing and monitoring the progress of corrective efforts for security weaknesses found in programs and systems. The program should also include reports to the CIO, on a regular basis, at least quarterly, on the progress of remediation.

The independent risk assessment concluded that although NEA has an established POA&M program, it is not being implemented consistently. The assessment stated that the POA&Ms reviewed were "from the previous Office of Inspector General audit and not accurate."

During our FY 2010 FISMA evaluation, we recommended areas of improvement for the POA&Ms program. We recommended that ITM develop and implement written policies and procedures for its POA&Ms program consistent with FISMA requirements, OMB policy and applicable NIST guidelines. We also recommended that the policy include procedures for regular reporting on the progress of remediation to the CIO, at least quarterly. ITM developed the policy; however, it has not been consistently implemented. As a repeated finding (FY 2008-2010 FISMA Evaluations), we believe NEA needs to make significant improvements in its tracking and monitoring of information security weaknesses.

We recommend that ITM implement procedures for its POA&Ms program in accordance with FISMA requirements, OMB policy and applicable NIST guidelines to accurately

track and monitor information security weaknesses consistently. ITM should also document notification to the CIO, at least quarterly, of remediation progress.

Remote Access Management and Identity and Access Management

NEA has established and is maintaining a program for remote access and identity and access management. NEA has developed policies and procedures for its remote access and identity and access management programs. However, those policies are not consistently implemented and several areas of improvement were identified during our review.

The FY 2011 Risk Assessment recommended that the policies for Remote Access and Access Control be incorporated to reduce the likelihood of inconsistent guidance and/or requirements. The review also recommended that the policies should define roles and responsibilities and ensure that defined technical requirements are FDCC compliant.

During our review of the Remote Access Policy, we found that there was no requirement for employees to complete authorization forms. We also found that the authorization forms were not available on the NEA Intranet Forms webpage and not all employees with remote access had completed and submitted forms to ITM. In addition, we requested the names of employees who have remote access and authorizations on file. We determined from the information provided by ITM that of the 88 employees had remote access 39 had authorizations file.

We also found that NEA-owned cell phones (Blackberry) are maintained and issued through the NEA's Office of Administration. Therefore, ITM does not issue or maintain authorization for remote access using these devices. The Blackberry is considered a consumer device which has web-based remote access. NIST SP-800-46, Section 4.2 states, in part:

Given the similarity between the functions of consumer devices, particularly as they become more advanced, and PCs, organizations should strongly consider treating them similar to, or the same as, PCs. This means that organizational policies for PCs may simply be extended to consumer devices; if the two policies are kept separate, the policy documents should heavily cross-reference each other.

We believe NEA needs to make significant improvements to its Remote Access Program. We recommend that NEA implement corrective actions to address the following:

- Recommendations of the FY 2011 Risk Assessment.
- Revise its policy for Remote Access to include the requirement and procedures to complete and submit authorization forms to ITM. Policies and procedures should ensure that employees complete the process before remote access is granted.
- Authorization forms should be made available to employees on the NEA Intranet Forms webpage.

- Revise its Remote Access policy to include any consumer devices, such as phones which provide remote access and ensure authorizations are maintained by ITM.

Continuous Monitoring Management

OMB's FY 2011 instructions states continuous monitoring programs and strategies should address: (i) the effectiveness of deployed security controls; (ii) changes to information systems and the environments in which those systems operate; and (iii) compliance to federal legislation, directives, policies, standards and guidance with regard to information security and risk management. Continuous monitoring of security controls is required as part of the security authorization process to ensure controls remain effective over time in the face of changing threats, missions, environments of operation, and technologies. A robust and effective continuous monitoring program will ensure important procedures included in an agency's security authorization package (e.g., as described in system security plans, security assessment reports, and POA&Ms) are updated as appropriate and contain the necessary information for authorizing officials to make credible risk-based decisions regarding the security state of the information system on an ongoing basis.

The FY 2011 risk assessment recommended that the policy for Continuous Monitoring could be strengthened by defining roles and responsibilities and defining specific timeframes/frequencies of tasks (i.e., daily, weekly monthly, quarter and/or at least annually).

We determined that NEA has established and implemented a continuous monitoring program which assesses the security state of information systems that is consistent with FISMA requirements, OMB policy and applicable NIST guidelines. However, we recommend that NEA revise its Continuous Monitoring Policies to include the recommendations of the risk assessment.

Contingency Planning

NEA has established and is maintaining an enterprise-wide business continuity/disaster recovery program that is consistent with the FISMA requirements, OMB policy and applicable NIST guidelines. However, the FY 2011 independent risk assessment recommended that NEA develop a comprehensive Information System Contingency Plan (ISCP) based on NIST SP 800-34, Revision 1.

According to NIST SP 800-34, Revision 1, the contingency plan is different from the Continuity of Operations Plan (COOP) and should define roles and responsibilities, define specific recovery time objectives, training, test planning and documenting testing results. It further states that once the disaster recovery plan has successfully transferred an information system site to an alternate site, each affected system would then use its respective ISCP to restore, recover, test systems, and put them into operation.

We recommend that NEA develop and implement written policies and procedures to ensure that it establishes an Information System Contingency Plan in compliance with NIST SP 800-34 Revision1.

Contractor Systems

OMB's FY 2011 FISMA instructions, states that "each agency must ensure their contractors are abiding by FISMA requirements. Section 3544(a)(1)(A)(ii) describes Federal agency security responsibilities as including information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency." Therefore, Federal security requirements continue to apply and the agency is responsible for ensuring appropriate security controls (see OMB Circular A-130, Appendix III). Agencies must develop policies for information security oversight of contractors and other users with privileged access to Federal data. Agencies must also review the security of other users with privileged access to Federal data and systems."

We obtained and reviewed agreements, including Interconnection Security Agreements and Memoranda of Understanding (MOU) with NEA's service providers. We found that there were agreements in place for all interconnected providers, except the service provider Xecu.net which houses NEA's backup systems.

We determined that overall NEA has established and maintains a program to oversee systems operated on its behalf by contractors or other entities. However, we recommend that NEA immediately execute an MOU and/or interconnectivity agreement with Xecu.net, as required by FISMA requirements, OMB policy and applicable NIST guidelines.

Financial Management System

NEA has an agreement with the U.S. Department of Transportation (DOT) to utilize the Enterprise Service Center's (ESC) Oracle Federal Financial System, Delphi, as their financial management system.

OMB requires that such service organizations provide client agencies with an independent report describing system controls. To comply with this requirement, DOT OIG hired an independent contractor, Clifton Gunderson, LLP, to conduct a review on the computer controls over the information technology and data processing environment, as well as the input process, and output controls built into the Delphi system, which is used by multiple Federal agencies.

The audit concluded that management's description fairly presents, in all material respects, the ESC's system was "designed and implemented throughout the period October 1, 2010 to June 30, 2011." In addition, the report, dated August 1, 2011, stated that "controls are suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period."

Payroll System

NEA uses the U.S. Department of Agriculture (USDA) National Finance Center (NFC) as its payroll provider. In September 2011, the USDA OIG issued its *Statement on Standards for Attestation Engagements No. 16 Report on Controls at the National Finance Center*.¹ The review concluded that the NFC's "description fairly presents NFC payroll/personnel processing and application hosting systems that were designed and implemented throughout the period from October 1, 2010, to July 31, 2011." Also, in their opinion, "the controls included in the description were suitably designed and operating effectively to provide reasonable assurance that the associated control objectives would be achieved." There were no recommendations in the report.

Security Capital Planning

Capital Planning and Investment Control Process, as defined in OMB Circular A-139, (6)(c)" is a management process for ongoing identification, selection, control, and evaluation of investments in information resources. The process links budget formulation and execution, and is focused on agency missions and achieving specific program outcomes." The FY 2011 FISMA instruction lists the following attributes for an established program that is established and maintained:

- Documented policies and procedures to address information security in the capital planning and investment control process.
- Includes information security requirements as part of the capital planning and investment process
- Establishes a discrete line item for information security in organizational programming and documentation
- Employs a business case/Exhibit 300/Exhibit 53 to record information security resources required
- Ensures information security resources are available for expenditure as planned

NEA does not have a capital planning and investment control process program.

We recommend NEA establish and maintain a security capital planning and investment control process program for information security. The program should include written policies and procedures to ensure that the program is in compliance with FISMA requirements, OMB policy and applicable NIST guidelines.

Privacy Reporting and Privacy Impact Assessment

The FY 2011 FISMA guidance included additional questions on security and privacy policies, which requires agencies to submit information on privacy issue allegations, policies and the types of privacy reviews ITM conducted.

¹ The Statement on Standards for Attestation Engagements (SSAE) 16 reports replaced the SAS 70 reports for periods ending on or after June 15, 2011.

ITM's review of personally identifiable information (PII) holdings determined that (1) NEA collects only PII that is relevant and necessary for administrative purposes and (2) there are adequate administrative, technical and physical safeguards in place for the PII collected. NEA does not use Social Security Numbers (SSNs), truncated SSNs, or any part of SSNs as tracking numbers for its applications, grants, cooperative agreements or contracts. NEA does not share PII with outside agencies other than for processing payments. ITM indicated there have been no reported breaches or security incidents involving PII collected or maintained by the Agency. Therefore NEA is not required to conduct privacy information assessments (PIA).

FY 2011 OMB guidance states that "although neither Section 208 of the E-Government Act, nor OMB's implementing guidance mandate agencies conduct PIAs on electronic systems containing information about Federal employees (including contractors), OMB encourages agencies to scrutinize their internal business processes and the handling of identifiable information about employees to the same extent they scrutinize processes and information handling procedures involving information collected from or about members of the public (OMB Memorandum 03-22, Section II.B.3.a)."

EmeSec reviewed the NEA PIA policy and offered the following assessment:

- The document does not trace via flow the transport of PII data through the NEA General Support System.
- It does have the portion regarding what is submitted may be collected but it shows no discussion on whether the stored PII is encrypted, once collected.

We recommend that NEA revises its PIA policy to address the above assessment and ensure compliance with FISMA requirements, OMB policy and applicable NIST guidelines.

EXIT CONFERENCE

We provided a draft copy of this report to ITM officials on November 14, 2011. The officials generally 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. Implement corrective actions for recommendations in the Risk Assessment Report issued September 23, 2011 by EmeSec. The corrective actions should address all of the recommended policy, administrative and technical improvements including vulnerabilities identified. NEA should also use a prioritized approach based on

the categorization of risk to implement corrective actions for system vulnerabilities.

2. Revise its change management policy to provide for adequate segregation of duties. The policy should ensure that the request, review and approval for potential and/or actual changes to hardware or software are not performed and signed off by the same staff person.
3. Implement corrective actions for the remaining six recommendations in Report No. R-11-02, NEA's Control over Computer-Related Equipment.
4. Include computer incident and reporting in its annual security awareness training.
5. Implement procedures for its POA&Ms program in accordance with NIST, OMB and FISMA requirements to accurately track and monitor information security weaknesses consistently.
6. Document notification to the CIO, at least quarterly, of remediation progress of its POA&M program.
7. Implement corrective actions to address the following recommendations for its Remote Access program:
 - Recommendations of the FY 2011 Risk Assessment.
 - Revise its policy for Remote Access to include the requirement and procedures to complete and submit authorization forms to ITM. Policies and procedures should ensure that employees complete the process before remote access is granted.
 - Authorization forms should be made available to employees on the NEA Intranet Forms webpage.
 - Revise its Remote Access policy to include any consumer devices, such as phones which provide remote access and ensure authorizations are maintained by ITM.
8. 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.
9. Execute an MOU and/or interconnectivity agreement with Xecu.net, as required by FISMA requirements, OMB policy and applicable NIST guidelines.
10. Establish and maintain a security capital planning and investment control process program for information security. The program should include written policies and procedures to ensure that the program is in compliance with OMB, FISMA and NIST guidelines.

11. Revise its PIA policy to address EmeSec's assessment and ensure compliance with FISMA requirements, OMB policy and applicable NIST guidelines.