Office of Inspector General

FISMA Evaluation

Evaluation of the Federal Labor Relations Authority Compliance with the Federal Information Security Management Act

Fiscal Year 2011

Report No. ER-12-01

November 2011

Federal Labor Relations Authority
1400 K Street, N.W. Suite 250, Washington, D.C. 20424

TABLE OF CONTENTS

PURPOSE

Dembo, Jones, Healy, Pennington & Marshall, P.C. (Dembo Jones), on behalf of the Federal Labor Relations Authority (FLRA), Office of Inspector General, conducted an independent evaluation of the quality and compliance of the FLRA security program with applicable federal computer security laws and regulations. Dembo Jones' evaluation focused on FLRA's information security required by the Federal Information Security Management Act (FISMA).

This report was prepared in conjunction with the Inspector General and Dembo Jones. The weaknesses discussed in this report should be included in FLRA's Fiscal Year (FY) 2011 report to the Office of Management and Budget (OMB) and Congress.

BACKGROUND

On December 17, 2002, the President signed into law H.R. 2458, the E-Government Act of 2002 (Public Law 107-347). Title III of the E-Government Act of 2002, commonly referred to as FISMA (the Federal Information Security Management Act), focuses on improving oversight of federal information security programs and facilitating progress in correcting agency information security weaknesses. FISMA requires federal agencies to develop, document, and implement an agency-wide information security program that provides security for the information and information systems that support the operations and assets of the agency. This program includes providing security for information systems provided or managed by another agency, contractor, or other source. FISMA assigns specific responsibilities to agency heads and Inspectors General (IGs). It is supported by security policy promulgated through Office of Management and Budget (OMB), and risk-based standards and guidelines published in the National Institute of Standards and Technology (NIST) Special Publication (SP) series.

Under FISMA, agency heads are responsible for providing information security protections commensurate with the risk and magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems. FISMA directs federal agencies to report annually to the OMB Director, Comptroller General, and selected Congressional committees on the adequacy and effectiveness of agency information security policies, procedures, and practices and compliance with FISMA. In addition, FISMA requires agencies to have an annual independent evaluation performed of their information security programs and practices and to report the evaluation results to OMB. FISMA states that the independent evaluation is to be performed by the agency IG or an independent external auditor as determined by the IG. Implementing adequate information security controls is essential to ensuring an organization can effectively meet its mission. The IG plays an essential role in supporting federal agencies in identifying areas for improvement. In support of that critical goal the Chief Information Officer is developing a strategy to secure the FLRA computing environment which centers on providing confidentially, integrity, and availability.

SCOPE AND METHODOLOGY

The scope of our testing focused on the FLRA network General Support System (GSS), however the testing also included the others systems in the FLRA system inventory. We conducted our testing through inquiry of FLRA personnel, observation of activities, inspection of relevant documentation, and the performance of technical security testing. Some examples of our inquiries with FLRA management and personnel included, but were not limited to, reviewing system security plans, access control, the risk assessments, and the configuration management processes. We also utilized a software tool for identifying vulnerabilities on the network, as well as computers attached to the FLRA network.

SUMMARY

During our FY 2011 evaluation, we noted that FLRA has taken steps to improve the information security program. We also noted that FLRA does take information security weaknesses seriously. FLRA took action to remediate several weaknesses within specific control areas. During the FY 2011 FISMA evaluation Dembo Jones performed a Vulnerability Assessment on the FLRA network, which included the servers, firewalls, and routers. This review also included testing 21 workstations that were connected to the FLRA network. Also included in the FISMA testing were controls from several families within the NIST 800-53 Rev. 3 publication.

This year's FISMA testing resulted in seven new findings. The areas of weakness are as follows:

1. Outdated patches and service packs, as well as transmission means that are not secure (Vulnerability Assessment Results).
2. Audit settings.
3. Data Center access.
4. Contingency Plans and Testing.
5. Incident Response training.
6. Homeland Security Presidential Directive (HSPD) – 12.
7. Privacy.

This year's FISMA testing included a follow up of all prior year deficiencies. There were a total of twenty prior issues. Each of those issues has many elements that make up each finding. If any one of the elements is open, then that issue remains open. The areas of prior year issues being open are as follows:

1. Ports and services on the network.
    a. Prior Issue # 5
    b. Part of Current Year Issue # 1

2. Contingency Plan testing.
    a. Prior Issue # 6
    b. Part of Current Year Issue # 4
3. Incident Response training.
    a. Prior Issue # 8
    b. Part of Current Year Issue # 5
4. Privacy.
    a. Prior Issue # 11
    b. Part of Current Year Issue # 7
5. Denial of Service attacks.
    a. Prior Issue # 15
    b. Part of Current Year Issues # 1 and # 7

SYS-01 Vulnerability Assessment Results (PY POA&M # 5 & 15)

Condition:

Dembo Jones performed a Vulnerability Assessment utilizing Nessus, which is a commercial software tool. This software deployed the latest plug-ins, which allowed for the scan to identify the latest vulnerabilities on both the network (servers, routers, firewalls, etc.) and a sample of desktops connected to the network. The results of this scan were as follows:

1. The servers and workstations were not configured with the latest client application security patches.
2. Several hosts were running an outdated version of HP System Management Homepage. A web server was running an outdated version of Apache Tomcat 4.1.12.
3. The SYSDBA account of the Firebird server was configured with default credentials.
4. The host is running a clear text service (RSH).

Criteria:

1. **NIST 800-40 Procedures for Handling Security Patches, section 2.1 states** "We recommend creating a "Patch and Vulnerability Group" (PVG). The size of the PVG will vary depending on the size and complexity of the organization. The PVG may consist of full-or part-time personnel. The personnel involved should have broad knowledge of patches, systems administration, and computer vulnerabilities. In addition, it is helpful to have specialists in particular operating systems, applications, and servers. Personnel who already provide system or network administration functions, perform vulnerability scanning or who operate intrusion detection systems are likely candidates for this group. The duties of the PVG will be to support local administrators in finding and fixing vulnerabilities in the organization's software. The PVG will generally not patch vulnerabilities themselves; rather they will work with a local administrator to apply and test patches. Generally speaking, the main function of the PVG groups should be to ensure consistency across an organization."
2. **NIST 800-123 Guide to General Server Security, section 3.3 states** "Organizations should develop standardized secure configurations for widely used OSs and server software. This will provide recommendations to server and network administrators on how to configure their systems securely and ensure consistency and compliance with the organizational security policy. Because it only takes one insecurely configured host to compromise a network, organizations with a significant number of hosts are especially encouraged to apply this recommendation." **Section 4.1 states** "Once an OS is installed, applying needed patches or upgrades to correct for known vulnerabilities is essential. Any known vulnerabilities an OS has should be corrected before using it to

host a server or otherwise exposing it to untrusted users. To adequately detect and correct these vulnerabilities, server administrators should do the following:

- Create, document, and implement a patching process.
- Identify vulnerabilities and applicable patches.
- Mitigate vulnerabilities temporarily if needed and if feasible (until patches are available, tested, and installed).
- Install permanent fixes (patches, upgrades, etc.)

3. **NIST 800-123 Guide to General Server Security, section 4.2.2 states** "The default configuration of the OS often includes guest accounts (with and without passwords), administrator or root level accounts, and accounts associated with local and network services. The names and passwords for those accounts are well known. Remove (whenever possible) or disable unnecessary accounts to eliminate their use by attackers, including guest accounts on computers containing sensitive information. For default accounts that need to be retained, including guest accounts, severely restrict access to the accounts, including changing the names (where possible and particularly for administrator or root level accounts) and passwords to be consistent with the organizational password policy. Default account names and passwords are commonly known in the attacker community."
4. **NIST 800-123 Guide to General Server Security, section 4.2.2 states** "Enabling authentication by the host computer involves configuring parts of the OS, firmware, and applications on the server, such as the software that implements a network service. In special situations, such as high-value/high-risk servers, organizations may also use authentication hardware, such as tokens or one-time password devices. Use of authentication mechanisms where authentication information is reusable (e.g., passwords) and transmitted in the clear over an untrusted network is strongly discouraged because the information can be intercepted and used by an attacker to masquerade as an authorized user."

Cause:

For all of the deficiencies identified above, the cause is primarily because the network had recently been upgraded, and as such, there were time constraints placed on limited personnel to identify the latest patches, and other vulnerability weaknesses.

Risk:

1. Without updated patches on systems, there is the potential for remote code execution through exploitation of buffer overflows, and other vulnerabilities. Patches are deployed to close those areas subject to exploitation. Without the latest patches being deployed, identified vulnerabilities may be exploited through known attack venues.
2. Hosts (and web servers) running outdated versions may result in a denial of service, or other exploitative attacks on the network.
3. Servers and other technologies are built with standard with default user IDs and passwords so that administrators can configure them. Attackers know the default user IDs and passwords; as this is common knowledge. It is therefore, crucial that those

default IDs and passwords be changed to prevent exploitation of weak authentication credentials.

4. Clear-text services transmit information, which is readable if one has access to the data transmission as the data moves across the network wires. For this reason, it is important to remove or disable clear-text services.

Recommendation(s):

1. Analyze which patches are missing and assess which of those can be deployed without harming the network. Once complete, deploy the patches to ensure the network is protected.
2. For those services running on the hosts that are not being used: disable them. If the services are being used, then the latest version of HP System Management Homepage and Apache should be deployed.
3. Use the application's 'gsec' utility to change the password for the 'SYSDBA' account.
4. Replace the clear-text services with more secure alternatives, such as SSH and SFTP.

Management Response:

The CIO acknowledges the vulnerabilities identified by the Auditor. Patching was performed immediately upon learning of this vulnerability. It should be understood that patching will be a perpetually changing environment and FLRA will be up-to-date and out of compliance from day to day, depending on the vendor technology. HP System Management vulnerabilities have been mitigated, Firebird has been decommissioned and the SYSDBA account issue was resolved immediately upon learning of the vulnerability. Clear text services have been replaced by SSH and SFTP. It should be noted though that SSH, SFTP and even FTP are blocked inbound/outbound by our Trusted Internet Connection (TIC) service provider, CenturyLink (formerly QWest).

Mitigation Timeline: Immediate and ongoing.

SYS-02 Audit Settings

Condition:

Dembo Jones reviewed the audit settings for the server with Domain Controller access. This is the server responsible for managing authentication of FLRA users. It was revealed that Privileged Use is set to failure. Privileged Use is a setting within the audit events that tracks administrator users. Having this set to failure means if someone attempts to change something of a privileged nature, the audit log will only capture the failure of that event and not the success. If one of the privileged users changed something or created a user ID for adverse purposes, this would not be captured on the audit log for traceability and accountability purposes, as the change will have been completed successfully.

Criteria:

NIST 800-123 Guide to General Server Security, section 4.2.3 states "Auditing should also be enabled as appropriate to monitor attempts to access protected resources."

Cause:

The cause is primarily because the network had recently been upgraded, and as such, there were time constraints placed on limited personnel to ensure that upgrades didn't change previous settings on the servers.

Risk:

If an administrator attempts to create a user ID for adverse purposes, this will not be logged, as the current setting does not track successful administrator changes. Without this setting, there are no detective controls in place, in the event of adverse actions taken.

Recommendation(s):

The audit settings should be set to "success" and "failure".

Management Response:

The CIO acknowledges the vulnerability identified by the Auditor. Administrator accounts and the improper logging of their creation and use is a very serious issue to the CIO which will be resolved by December 31, 2011.

Mitigation Timeline: December 31, 2011

SYS-03 Data Center Access

Condition:

Dembo Jones obtained a listing of users with access to the Data Center. Upon this review, it was revealed that there were several personnel (four) who are not in Information Technology with access to the Data Center.

Criteria:

NIST 800-53 Recommended Security Controls for Federal Information Systems and Organizations page F-78 (PE-3) states "The organization enforces physical access authorizations to the information system independent of the physical access controls for the facility. Enhancement Supplemental Guidance: This control enhancement applies to server rooms, media storage areas, communications centers, or any other areas within an organizational facility containing large concentrations of information system components. The intent is to provide additional physical security for those areas where the organization may be more vulnerable due to the concentration of information system components. Security requirements for facilities containing organizational information systems that process, store, or transmit Sensitive Compartmented Information (SCI) are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. See also PS-3, security requirements for personnel access to SCI. (2) The organization performs security checks at the physical boundary of the facility or information system for unauthorized exfiltration of information or information system components."

Cause:

The IT Department shares access controls with building security. As such, there have been access authorizations to personnel that are not in IT roles and responsibilities.

Risk:

Only IT personnel should have access to the Data Center. By providing access to non-IT personnel, it makes an after-the-fact investigation very difficult because one of the non-IT users could have adversely changed data directly on a server without appropriate controls in place. The non-IT personnel may also be in a position of authority. With this authority, they should not have access to the Data Center, because their access to servers is a segregation of duties violation.

Recommendation(s):

Ensure only IT related personnel have access to the Data Center.

Management Response:

The CIO acknowledges the vulnerability identified by the Auditor. However, due to the nature of the four accounts, those being personnel in the Administrative Services Division who require

access to this space as it is also an area with control of electronic and ventilation equipment, the CIO chooses to accept and mitigate the risk by ensuring all access to the Data Center is logged in the same process IRMD personnel must follow.

Mitigation Timeline: Risk accepted, however, new sign-in procedures effective immediately.

SYS-04 Contingency Plans and Testing (PY POA&M # 6)

Condition:
Dembo Jones obtained the latest Contingency Plan, as well as inquired about contingency testing in the event of a disaster. The following was noted:

- It was revealed that the latest Contingency Plan had not been signed or finalized.
- Furthermore, there have been no formalized tests of a contingency to be prepared in the event of a disaster. (PY POA&M # 6)

Criteria:
NIST 800-34 Contingency Planning for Federal Information Systems 3.6 states "To be effective, the plan must be maintained in a ready state that accurately reflects system requirements, procedures, organizational structure, and policies. During the Operation/Maintenance phase of the SDLC, information systems undergo frequent changes because of shifting business needs, technology upgrades, or new internal or external policies. Therefore, it is essential that the ISCP be reviewed and updated regularly as part of the organization's change management process to ensure that new information is documented and contingency measures are revised if required. As identified as part of RMF Step 6 (Continuous Monitoring), a continuous monitoring process can provide organizations with an effective tool for plan maintenance, producing ongoing updates to security plans, security assessment reports, and plans of action and milestone documents.

NIST 800-34 Contingency Planning for Federal Information Systems 3.5 states "Plan Testing, Training, and Exercises (TT&E) An ISCP should be maintained in a state of readiness, which includes having personnel trained to fulfill their roles and responsibilities within the plan, having plans exercised to validate their content, and having systems and system components tested to ensure their operability in the environment specified in the ISCP. In addition, as indicated in Step 4 (Assess Security Controls) of the RMF, the effectiveness of the information system controls should be assessed by using the procedures documented in NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*. NIST SP 800-84, *Guide to Test, Training and Exercise Programs for Information Technology Plans and Capabilities,* provides guidelines on designing, developing, conducting, and evaluating test, training, and exercise (TT&E) events so that organizations can improve their ability to prepare for, respond to, manage, and recover from adverse events. While the majority of TT&E activities occur during the Operations/Maintenance phase, initial TT&E events should be conducted during the Implementation/Assessment phase of the SDLC to validate ISCP recovery procedures."

"Organizations should conduct TT&E events periodically, following organizational or system changes, or the issuance of new TT&E guidance, or as otherwise needed. Execution of TT&E events assists organizations in determining the plan's effectiveness, and that all personnel

know what their roles are in the conduct of each information system plan. TT&E event schedules are often dictated in part by organizational requirements. For example, NIST SP 800-53 includes a control (CP-4) for federal organizations to conduct exercises or tests for their systems' contingency plans around an organization-defined frequency. Section 3.5.4 provides guidance on the type of TT&E identified for each FIPS 199 impact level."

"For each TT&E activity conducted, results are documented in an after-action report, and Lessons Learned corrective actions are captured for updating information in the ISCP. While NIST SP 800-84 provides detailed information on how to plan and conduct TT&E activities for information systems, the following sections provide summarized details."

Cause:
The cause is primarily because the network had recently been upgraded, and as such, there were time constraints placed on limited personnel to perform contingency testing on the newly deployed technologies.

Risk:
In the event of a disaster, the FLRA will likely be unprepared, because testing has not occurred. Although data is being backed up and stored off-site, this provides for data reconstitution only and not necessarily ongoing live administration. The current setting for FLRA may not allow for continuous connectivity in the event of a disaster, because this has not been tested.

Recommendation(s):
Ensure that the Contingency Plan has been reviewed and signed off as final. Also, ensure that the IT Department performs a contingency test, training, and exercise in accordance with NIST 800-34.

Management Response:
The CIO acknowledges the vulnerability identified by the Auditor. FLRA has procured services from the Bureau of Public Debt who will assist in developing the formal Contingency Plan. We have also procured an emergency notification from Everbridge. We aim to have a complete Contingency Plan tested agency-wide by June 2012.

Mitigation Timeline: June 2012

SYS-05 Incident Response Training (PY POA&M # 8)

Condition:
Dembo Jones inquired about incident response with IT personnel. It was revealed that there is no Incident Response training for IT personnel.

Criteria:
NIST 800-53 Recommended Security Controls for Federal Information Systems and Organizations page F-61 (IR-2) states "(1) The organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations. (2) The organization employs automated mechanisms to provide a more thorough and realistic training environment."

Cause:
The cause is primarily the result of there being a lack of personnel and/or the budget to provide for IT-wide incident response training.

Risk:
In the event of an incident, the FLRA will likely be unprepared, because incident response training has not been provided to the IT personnel that manage the network.

Recommendation(s):
Ensure that IT personnel are properly trained with regard to Incident Response prevention, detection, and correction.

Management Response:
The CIO acknowledges the vulnerability identified by the Auditor. However, FLRA will resolve this issue via in-house training, working with the Bureau of Public Debt and peering with CISO' from across the government on best practices by the end of the calendar year 2011. A formal Incident Response Plan will be communicated agency-wide by February 2012.

Mitigation Timeline: February 2012

SYS-06 HSPD-12

Condition:
It was revealed that the FLRA has not implemented the Homeland Security Presidential Directive (HSPD)-12 requirements across the agency.

Criteria:
NIST 800-116 Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS) section 2.2 states "HSPD-12 mandates the establishment of a government-wide standard for identity credentials to improve physical security in Federally controlled facilities2. To that end, HSPD-12 requires all government employees and contractors be issued a new identity credential based on the FIPS 201 on PIV. Following FIPS 201, this credential is referred to herein as a PIV Card3."

"HSPD-12 explicitly requires the use of PIV Cards "in gaining physical access to Federally controlled facilities and logical access to Federally controlled information systems." [HSPD-12] The PIV Card employs microprocessor-based smart card technology, and is designed to be counterfeit-resistant, tamper-resistant, and interoperable across Federal government facilities. Additionally, the FIPS 201 standards suite defines the authentication mechanisms as transactions between a PIV Card and a relying party. FIPS 201 does not, however, elaborate on the uses and applications of the PIV Card. This document provides guidelines on the uses of PIV Cards with PACS."

Cause:
The cause is primarily the result of there being a lack of personnel and/or the budget to provide for agency-wide implementation of the HSPD-12 requirements. This will have to be rolled out to the field offices as well and this can be very costly.

Risk:
The HSPD-12 requirements ensure that authentication is stronger, thus decreasing unauthorized access into the network. Without implementation of the HSPD-12, the FLRA deploys two-factor authentication only and is not complemented by the PIV cards. This increases the risk of unauthorized access to data and systems.

Recommendation(s):
Implement HSPD-12 requirements for the Washington DC location, as well as the field offices for the agency as a whole.

Management Response:

The CIO acknowledges the vulnerability identified by the Auditor. However, FLRA has purchased the technology to implement an HSPD-12 compliant Physical Access Control System (PACS) in

those regional offices which are not slated to relocate over the next two years. The implementation of an internal PKI and Certificate Authority is scheduled for completion by December 31, 2011. Also, IRMD is scheduled to upgrade all FLRA workstations to Windows 7 by this time, which will aid greatly in implementing the HSPD-12 compliant Logical Access Control System (LACS).

Mitigation Timeline: December 31, 2011

SYS-07 Privacy (PY POA&M # 11 & 17)

Condition:
Privacy Threshold Assessments (PTA) need to be performed for those systems without PTAs. The PTA is a process to identify any and all Personally Identifiable Information (PII) elements. If any of those elements (alone or in combination) can be traced to an individual, the PII is then considered Information in Identifiable Form (IIF). PIAs are required for systems that have IIF. Further, once the Privacy Impact Assessment (PIA) is completed, the IIF should be categorized as either low, moderate, or high.

Criteria:
"Perform a PTA when a new system development is initiated, or an enhancement or modification is undertaken on an existing system to determine if Identification in Identifiable Form (IIF) is present and is either from or about the public" **(TD 25-07, section 4a)**.

This publication uses the definition of PII from OMB Memorandum 07-16, which is information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. To distinguish an individual is to identify an individual" **(NIST 800-122 section 2.1).**

- Name, such as full name, maiden name, mother's maiden name, or alias
- Personal identification number, such as SSN, passport number, driver's license number, taxpayer identification number, patient identification number, and financial account or credit card number
- Address information, such as street address or email address
- Asset information, such as Internet Protocol (IP) or Media Access Control (MAC) address or other host-specific persistent static identifier that consistently links to a particular person or small, well-defined group of people
- Telephone numbers, including mobile, business, and personal numbers
- Personal characteristics, including photographic image (especially of face or other distinguishing characteristic), x-rays, fingerprints, or other biometric image or template data (e.g., retina scans, voice signature, facial geometry)
- Information identifying personally owned property, such as vehicle registration or identification number, and title numbers and related information
- Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, or employment, medical, education, or financial information).

The E-Government Act requires agencies to conduct a PIA before:

In general, PIAs are required to be performed and updated as necessary where a system change creates new privacy risks. For example:

- Conversions - when converting paper-based records to electronic systems;
- Anonymous to Non-Anonymous - when functions applied to an existing information collection change anonymous information into information in identifiable form;
- Significant System Management Changes - when new uses of an existing IT system, including application of new technologies, significantly change how information in identifiable form is managed in the system:
- Significant Merging - when agencies adopt or alter business processes so that government databases holding information in identifiable form are merged, centralized, matched with other databases or otherwise significantly manipulated:
- New Public Access - when user-authenticating technology (e.g., password, digital certificate, biometric) is newly applied to an electronic information system accessed by members of the public;
- Commercial Sources - when agencies systematically incorporate into existing information systems databases of information in identifiable form purchased or obtained from commercial or public sources. (Merely querying such a source on an ad hoc basis using existing technology does not trigger the PIA requirement);
- New Interagency Uses - when agencies work together on shared functions involving significant new uses or exchanges of information in identifiable form, such as the cross-cutting E-Government initiatives; in such cases, the lead agency should prepare the PIA;
- Internal Flow or Collection - when alteration of a business process results in significant new uses or disclosures of information or incorporation into the system of additional items of information in identifiable form:
- Alteration in Character of Data - when new information in identifiable form added to a collection raises the risks to personal privacy (for example, the addition of health or financial information)

OMB 03-22 section II.B.2

"The confidentiality of PII should be protected based on its risk level. This section outlines factors for determining the PII confidentiality impact level for a particular instance of PII, which is distinct from the confidentiality impact level described in Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems.20 The PII confidentiality impact level takes into account additional PII considerations and should be used to determine if additional protections should be implemented. The PII confidentiality impact level—low, moderate, or high—indicates the potential harm that could result to the subject individuals and/or the organization if the PII were inappropriately accessed, used, or disclosed. Once the PII confidentiality impact level is selected, it should be used to supplement the provisional confidentiality impact level, which is determined from information and system categorization processes outlined in FIPS 199 and

NIST Special Publication (SP) 800-60, Volumes 1 and 2: Guide for Mapping Types of Information and Information Systems to Security Categories."
(NIST 800-122, section 3, page 3-1)

"Agencies must: identify those individuals in the agency (e.g., information technology personnel, Privacy Act Officers) that have day-to-day responsibility for implementing section 208 of the E-Government Act, the Privacy Act, or other privacy laws and policies."
(OMB M-03-22, section VI, A)

Cause:
This is the result of there being a lack of personnel to prepare and manage the privacy related issue.

Recommendation:
A system inventory should be maintained and from this listing, the following should be performed:

- Identify which of those systems have PII and IIF.
- Identify which of those systems need a PIA.
- Identify which of those PIAs need to be posted on the FLRA website.
    - Identify information that needs to be redacted prior to posting of the PIA on the FLRA website.

Management Response:
The CIO acknowledges the vulnerability identified by the Auditor. The Information Resources Management Division (IRMD), in cooperation with the Senior Agency Official for Privacy (SOAP), will perform those Recommendations listed above by September 30, 2012.

Mitigation Timeline: September 30, 2012

PRIOR YEAR FINDINGS

#	Year Initiated	POA&M	Open / Closed
1	2009	**Develop a robust access control program in accordance with NIST Special Publication 800-53 Revision 3 Recommended Security Controls for Federal Information Systems.** • The information system does not enforce separation of duties through assigned access authorizations. - CLOSED • The organization does not supervise and review the activities of users with respect to the enforcement and usage of information system access controls. - CLOSED. • The organization does not authorize, monitor, and control all methods of remote access to the information system. - NO REMOTE ACCESS - N/A	Closed
2	2009	**Develop a robust awareness and training program in accordance with NIST Special Publication 800-53 Revision 3 Recommended Security Controls for Federal Information Systems.** • The organization does not identify personnel that have significant information system security roles and responsibilities during the system development life cycle, documents those roles and responsibilities, and does not provide appropriate information system security training: (i) before authorizing access to the system or performing assigned duties; (ii) when required by system changes; and (iii) [Assignment: organization-defined frequency] thereafter. - CLOSED • The organization does not establish and maintain contacts with special interest groups, specialized forums, professional associations, news groups, and/or peer groups of security professionals in similar organizations to stay up to date with the latest recommended security practices, techniques, and technologies and to share the latest security-related information including threats, vulnerabilities, and incidents. - CLOSED	Closed
3	2009	**Develop a robust audit and accountability program in accordance with NIST Special Publication 800-53 Revision 3 Recommended Security Controls for Federal Information Systems.** • The information system does not generate audit records for the following events: [Assignment: organization-defined auditable events]. - CLOSED • The information system does not produce audit records that contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events. - CLOSED • The organization does not allocate sufficient audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded. - CLOSED • The information system does not alert appropriate organizational officials in the event of an audit processing failure and does not take the following additional actions: [Assignment:	Closed

#	Year Initiated	POA&M	Open / Closed
		organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)]. - ACCEPTED RISK - CLOSED • The organization does not regularly review/analyze information system audit records for indications of inappropriate or unusual activity, does not investigate suspicious activity or suspected violations, does not report findings to appropriate officials, and does not take necessary actions. - CLOSED • The information system does not provide an audit reduction and report generation capability. - CLOSED • The information system does not provide time stamps for use in audit record generation. - CLOSED • The information system does not protect audit information and audit tools from unauthorized access, modification, and deletion. - CLOSED • The information system does not provide the capability to determine whether a given individual took a particular action. - CLOSED • The organization does not retain audit records for [Assignment: organization-defined time period] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements. - CLOSED	
4	2009	**Develop a robust certification, accreditation, and security program in accordance with NIST Special Publication 800-53 Revision 3 Recommended Security Controls for Federal Information Systems.** • The organization does not conduct an assessment of the security controls in the information system [Assignment: organization-defined frequency, at least annually] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. - CLOSED • The organization does not develop and update [Assignment: organization-defined frequency], a plan of action and milestones for the information system that documents the organization's planned, implemented, and evaluated remedial actions to correct deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system. - CLOSED • The organization does not monitor the security controls in the information system on an ongoing basis. – CLOSED	Closed

#	Year Initiated	POA&M	Open / Closed
5	2009	**Develop a robust configuration management program in accordance with NIST Special Publication 800-53 Revision 3 Recommended Security Controls for Federal Information Systems.** • The organization does not develop, document, and maintain a current baseline configuration of the information system. - CLOSED • The organization does not authorize, document, and control changes to the information system. - CLOSED • The organization does not monitor changes to the information system conducting security impact analyses to determine the effects of the changes. - CLOSED • The organization: (i) does not approve individual access privileges and enforces physical and logical access restrictions associated with changes to the information system; and (ii) does not generate, retain, and review records reflecting all such changes. - CLOSED • The organization: (i) does not establish mandatory configuration settings for information technology products employed within the information system; (ii) does not configure the security settings of information technology products to the most restrictive mode consistent with operational requirements; (iii) does not document the configuration settings; and (iv) does not enforce the configuration settings in all components of the information system. - CLOSED • The organization does not configure the information system to provide only essential capabilities and does not specifically prohibit and/or restrict the use of the following functions, ports, protocols, and/or services: [Assignment: organization-defined list of prohibited and/or restricted functions, ports, protocols, and/or services]. – **OPEN. This finding has been rolled up into a new finding – Vulnerability Assessment finding.** • The organization does not develop, document, and maintain a current inventory of the components of the information system and relevant ownership information. - CLOSED	OPEN
6	2009	**Develop a robust contingency planning program in accordance with NIST Special Publication 800-53 Revision 3 Recommended Security Controls for Federal Information Systems.** • The organization does not develop and implement a contingency plan for the information system addressing contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the system after a disruption or failure. Designated officials within the organization do not review and approve the contingency plan and distribute copies of the plan to key contingency personnel. - CLOSED • The organization does not train personnel in their contingency roles and responsibilities with respect to the information system and does not provide refresher training [Assignment: organization-defined frequency, at least annually]. - CLOSED	OPEN

#	Year Initiated	POA&M	Open / Closed
		• The organization: (i) does not test and/or exercise the contingency plan for the information system [Assignment: organization-defined frequency, at least annually] using [Assignment: organization-defined tests and/or exercises] to determine the plan's effectiveness and the organization's readiness to execute the plan; and (ii) does not review the contingency plan test/exercise results and does not initiate corrective actions. – **OPEN – this has been rolled up to a current year finding – Contingency Plans and Testings.** • The organization does not review the contingency plan for the information system [Assignment: organization-defined frequency, at least annually] and does not revise the plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing. - CLOSED • The organization does not identify an alternate storage site and initiates necessary agreements to permit the storage of information system backup information. - CLOSED • The organization does not identify an alternate processing site and does not initiate necessary agreements to permit the resumption of information system operations for critical mission/business functions within [Assignment: organization-defined time period] when the primary processing capabilities are unavailable. – **OPEN – New Finding # 4.** • The organization does not identify primary and alternate telecommunications services to support the information system and initiates necessary agreements to permit the resumption of system operations for critical mission/business functions within [Assignment: organization-defined time period] when the primary telecommunications capabilities are unavailable. - CLOSED • The organization does not conduct backups of user-level and system-level information (including system state information) contained in the information system [Assignment: organization-defined frequency] and does not protect backup information at the storage location. - CLOSED • The organization does not employ mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to a known secure state after a disruption or failure. - CLOSED	
7	2009	**NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans.** • The information system does not obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals. - CLOSED • The information system does not employ authentication methods that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for	Closed

#	Year Initiated	POA&M	Open / Closed
		authentication to a cryptographic module. - CLOSED	
8	2009	**Develop a robust incident response program in accordance with NIST Special Publication 800-53 Revision 3 Recommended Security Controls for Federal Information Systems.** • The organization does not train personnel in their incident response roles and responsibilities with respect to the information system and does not provide refresher training [Assignment: organization-defined frequency, at least annually]. - **OPEN – this has been rolled up to a current year finding – Incident Response Training.** • The organization does not test and/or exercise the incident response capability for the information system [Assignment: organization-defined frequency, at least annually] using [Assignment: organization-defined tests and/or exercises] to determine the incident response effectiveness and does not document the results. - CLOSED • The organization does not implement an incident handling capability for security incidents that include preparation, detection and analysis, containment, eradication, and recovery. - CLOSED • The organization does not track and document information system security incidents on an ongoing basis. - CLOSED • The organization does not promptly report incident information to appropriate authorities. - CLOSED • The organization does not provide an incident response support resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents. The support resource is an integral part of the organization's incident response capability. - CLOSED	OPEN
9	2009	**Develop a robust maintenance program in accordance with NIST Special Publication 800-53 Revision 3 Recommended Security Controls for Federal Information Systems.** • The organization does not schedule, perform, document, and review records of routine preventative and regular maintenance (including repairs) on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements. - CLOSED • The organization does not obtain maintenance support and spare parts for [Assignment: organization-defined list of key information system components] within [Assignment: organization-defined time period] of failure. - CLOSED	Closed
10	2009	**Develop a robust media protection program in accordance with NIST Special Publication 800-53 Revision 3 Recommended Security Controls for Federal Information Systems.** • The organization: (i) does not affix external labels to removable information system media and	Closed

#	Year Initiated	POA&M	Open / Closed
		information system output indicating the distribution limitations, handling caveats and applicable security markings (if any) of the information; and (ii) does not exempt [Assignment: organization-defined list of media types or hardware components] from labeling so long as they remain within [Assignment: organization-defined protected environment] - CLOSED • The organization does not physically control and securely store information system media within controlled areas. - CLOSED • The organization does not protect and control information system media during transport outside of controlled areas and restricts the activities associated with transport of such media to authorized personnel. - CLOSED • The organization does not sanitize information system media, both digital and non-digital, prior to disposal or release for reuse. - CLOSED	
11	2009	**Develop a robust planning program in accordance with NIST Special Publication 800-53 Revision 3 Recommended Security Controls for Federal Information Systems.** • The organization does not review the security plan for the information system [Assignment: organization-defined frequency, at least annually] and do not revise the plan to address system/organizational changes or problems identified during plan implementation or security control assessments. - CLOSED • The organization does not conduct a privacy impact assessment on the information system in accordance with OMB policy. - **OPEN – this was rolled up into a new finding - Privacy.** • The organization does not plan and coordinate security-related activities affecting the information system before conducting such activities in order to reduce the impact on organizational operations (i.e., mission, functions, image, and reputation), organizational assets, and individuals. - CLOSED	OPEN
12	2009	**Develop a robust personnel security program in accordance with NIST Special Publication 800-53 Revision 3 Recommended Security Controls for Federal Information Systems.** • The organization does not assign a risk designation to all positions and establishes screening criteria for individuals filling those positions. The organization does not review and revise position risk designations [Assignment: organization-defined frequency]. - CLOSED	Closed
13	2009	**Develop a robust Physical and Environmental program in accordance with NIST Special Publication 800-53 Revision 3 Recommended Security Controls for Federal Information Systems.** • The organization does not control physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides other than	Closed

#	Year Initiated	POA&M	Open / Closed
		areas designated as publicly accessible. - CLOSED • The organization does not maintain visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) that includes: (i) name and organization of the person visiting; (ii) signature of the visitor; (iii) form of identification; (iv) date of access; (v) time of entry and departure; (vi) purpose of visit; and (vii) name and organization of person visited. Designated officials within the organization do not review the visitor access records [Assignment: organization-defined frequency]. - CLOSED • The organization does not employ appropriate management, operational, and technical information system security controls at alternate work sites. - CLOSED	
14	2009	**Develop a robust planning program in accordance with NIST Special Publication 800-53 Revision 3 Recommended Security Controls for Federal Information Systems.** • The organization does not determine, document, and allocate as part of its capital planning and investment control process, the resources required to adequately protect the information system. - CLOSED • The organization does not manage the information system using a system development life cycle methodology that includes information security considerations. - CLOSED • The organization does not include security requirements and/or security specifications, either explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable laws, Executive Orders, directives, policies, regulations, and standards. - CLOSED • The organization does not obtain, protect as required, and make available to authorized personnel, adequate documentation for the information system. - CLOSED • The organization does not design and implement the information system using security engineering principles. - CLOSED • The organization: (i) does not require that providers of external information system services employ adequate security controls in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, guidance, and established service-level agreements; and (ii) does not monitor security control compliance. - CLOSED	Closed
15	2009	**Develop a robust system and communications protection program in accordance with NIST Special Publication 800-53 Revision 3 Recommended Security Controls for Federal Information Systems.** • The information system does not protect against or limit the effects of the following types of denial of service attacks: [Assignment: organization-defined list of types of denial of service	Open

#	Year Initiated	POA&M	Open / Closed
		attacks or reference to source for current list]. – **OPEN – Rolled up into a new finding – Vulnerability Assessment Results.** • The information system does not monitor and control communications at the external boundary of the information system and at key internal boundaries within the system. - CLOSED • The information system does not protect the integrity of transmitted information. - **OPEN – Rolled up into a new finding - Privacy.** • The information system does not protect the confidentiality of transmitted information. - **OPEN – Rolled up into a new finding - Privacy.** • The information system does not establish a trusted communications path between the user and the following security functions of the system: [Assignment: organization-defined security functions to include at a minimum, information system authentication and re-authentication]. - CLOSED • When cryptography is not required and employed within the information system, the organization does not establish and manage cryptographic keys using automated mechanisms with supporting procedures or manual procedures. - CLOSED • For information requiring cryptographic protection, the information system does not implement cryptographic mechanisms that comply with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. - CLOSED • The information system does not protect the integrity and availability of publicly available information and applications. - CLOSED • The information system does not reliably associate security parameters with information exchanged between information systems. - CLOSED • The organization does not issue public key certificates under an appropriate certificate policy and does not obtain public key certificates under an appropriate certificate policy from an approved service provider. - CLOSED • The organization: (i) does not establish usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the information system if used maliciously; and (ii) does not authorize, monitor, and control the use of mobile code within the information system. - CLOSED • The information system that provides name/address resolution service does not provide additional data origin and integrity artifacts along with the authoritative data it returns in response to resolution queries. – CLOSED	
16	2009	**Develop a robust system and information integrity program in accordance with NIST Special**	Closed

#	Year Initiated	POA&M	Open / Closed
		Publication 800-53 Revision 3 Recommended Security Controls for Federal Information Systems. • The organization does not identify, report, and correct information system flaws. - CLOSED • The information system does not implement malicious code protection. - CLOSED • The organization does not employ tools and techniques to monitor events on the information system, detect attacks, and provide identification of unauthorized use of the system. - CLOSED • The organization does not receive information system security alerts/advisories on a regular basis, does not issue alerts/advisories to appropriate personnel, and does not take appropriate actions in response. - CLOSED • The information system does not verify the correct operation of security functions [Selection (one or more): upon system startup and restart, upon command by user with appropriate privilege, periodically every [Assignment: organization-defined time-period]] and [Selection (one or more): does not notify system administrator, does not shut the system down, and does not restart the system] when anomalies are discovered. - CLOSED • The information system does not detect and protect against unauthorized changes to software and information. - CLOSED • The information system does not check information for accuracy, completeness, validity, and authenticity. - CLOSED • The information system does not identify and handles error conditions in an expeditious manner without providing information that could be exploited by adversaries. - CLOSED	
17	2010	**Develop a robust privacy program in accordance with OMB guidance in M-07-16, M-06-15, and M-06-16 for safeguarding privacy-related information.** • The organization does not establish adequate policies, processes, and procedures for establishing a privacy program. – CLOSED • The organization does not identify, report, and correct privacy weaknesses. - **OPEN – rolled up into a new finding - Privacy.** (Comment Part of Prior Year Issue # 11)	Open (Part of Prior Year # 11)
18	2010	**Establish and maintaining a remote access program that is generally consistent with NIST's and OMB's FISMA requirements.** • The organization does not adhere to established policies, process, and procedures for establishing a remote access. - CLOSED • The organization does not identify, report, and correct remote access weaknesses. - CLOSED	Closed

#	Year Initiated	POA&M	Open / Closed
		• The organization does not protect against unauthorized connections or subversion of authorized connections. - CLOSED	
19	2010	**Establish an entity-wide continuous monitoring program that assesses the security state of information systems that is generally consistent with NIST's and OMB's FISMA requirements.** • The organization does not ensure establish adequate policies, process, and procedures for establishing a continuous monitoring program. - CLOSED • The organization does not identify, report, and corrects continuous monitoring program weaknesses. - CLOSED • The organization has not establishes continuous monitoring program oversight. - CLOSED	Closed
20	2010	**Establish and maintain a program to oversee systems operated on its behalf by contractors or other entities NIST's and OMB's FISMA requirements.** • The organization does not establish adequate policies, process, and procedures for establishing a contractor systems oversight. - CLOSED	Closed

APPENDIX A – MANAGEMENT RESPONSES

UNITED STATES OF AMERICA
FEDERAL LABOR RELATIONS AUTHORITY
WASHINGTON, D.C. 20424

November 10, 2011

Dana Rooney-Fisher
Inspector General
Federal Labor Relations Authority
1400 K Street NW
Washington, DC 20424

Dear Ms. Rooney-Fisher:

The Federal Labor Relations Authority (FLRA) extends its appreciation for the recently completed Federal Information Security Management Act (FISMA) evaluation of the FLRA information technology systems security. The FLRA takes information security very seriously. The previous year's Inspector General Audit reported twenty vulnerabilities ranging in severity from "Low" to "High." I am pleased to report that all "High" impact vulnerabilities have been fully addressed and are resolved, and that the seven remaining issues set forth below are identified only as "Low to Moderate:"

1. Outdated patches and service packs, as well as transmission means that are not secure;
2. Audit settings;
3. Data Center access;
4. Contingency Plans and Testing;
5. Incident Response Training;
6. Homeland Security Presidential Directive (HSPD) – 12; and
7. Privacy.

We have developed a Plan of Action and Milestones (POA&M) that we are confident will effectively address each of the remaining issues. The POA&M, provided below, includes Management Responses and anticipated resolution dates, and reflects the satisfactory resolution of vulnerabilities reported in previous years. We look forward to working with you on the resolution of the remaining issues over the course of Fiscal Year 2012.

Thank you for your continued support of this effort.

Respectfully,

Carol Waller Pope
Chairman
Federal Labor Relations Authority

Management Responses to OIG Recommendations

1	**Risk:** 1. Without updated patches on systems, there is the potential for remote code execution through exploitation of buffer overflows, and other vulnerabilities. Patches are deployed to close those areas subject to exploitation. Without the latest patches being deployed, identified vulnerabilities may be exploited through known attack venues. 2. Hosts (and web servers) running outdated versions may result in a denial of service, or other exploitative attacks on the network. 3. Servers and other technologies are built with standard with default user IDs and passwords so that administrators can configure them. Attackers know the default user IDs and passwords; as this is common knowledge. It is therefore, crucial that those default IDs and passwords be changed to prevent exploitation of weak authentication credentials. 4. Clear-text services transmit information, which is readable if one has access to the data transmission as the data moves across the network wires. For this reason, it is important to remove or disable clear-text services. **Government Requirement:** 1. **NIST 800-40 Procedures for Handling Security Patches, section 2.1** 2. **NIST 800-123 Guide to General Server Security, section 3.3** 3. **NIST 800-123 Guide to General Server Security, section 4.2.2**	The CIO acknowledges the vulnerabilities identified by the Auditor. Patching was performed immediately upon learning of this vulnerability. It should be understood that patching will be a perpetually changing environment and FLRA will be up-to-date and out of compliance from day to day, depending on the vendor technology. HP System Management vulnerabilities have been mitigated, Firebird has been decommissioned and the SYSDBA account issue was resolved immediately upon learning of the vulnerability. Clear text services have been replaced by SSH and SFTP. It should be noted though that SSH, SFTP and even FTP are blocked inbound/outbound by our Trusted Internet Connection (TIC) service provider, CenturyLink (formerly QWest).	Mitigated
2	**Risk:** If an administrator attempts to create a user ID for adverse purposes, this will not be logged, as the current setting does not track successful administrator changes. Without this setting, there are no detective controls in place, in the event of adverse actions taken. **Government Requirement:** 1. **NIST 800-123 Guide to General Server Security, section 4.2.3**	The CIO acknowledges the vulnerability identified by the Auditor. Administrator accounts and the improper logging of their creation and use is a very serious issue to the CIO which will be resolved by December 31, 2011.	12/31/2011
3	**Risk:**	The CIO acknowledges the vulnerability identified	Mitigated

	Only IT personnel should have access to the Data Center. By providing access to non-IT personnel, it makes an after-the-fact investigation very difficult because one of the non-IT users could have adversely changed data directly on a server without appropriate controls in place. The non-IT personnel may also be in a position of authority. With this authority, they should not have access to the Data Center, because their access to servers is a segregation of duties violation. **Government Requirement:** 1. **NIST 800-53 Recommended Security Controls for Federal Information Systems and Organizations page F-78 (PE-3)**	by the Auditor. However, due to the nature of the four accounts, those being personnel in the Administrative Services Division who require access to this space as it is also an area with control of electronic and ventilation equipment, the CIO chooses to accept and mitigate the risk by ensuring all access to the Data Center is logged in the same process IRMD personnel must follow.	
4	**Risk:** In the event of a disaster, the FLRA will likely be unprepared, because testing has not occurred. Although data is being backed up and stored off-site, this provides for data reconstitution only and not necessarily ongoing live administration. The current setting for FLRA may not allow for continuous connectivity in the event of a disaster, because this has not been tested. **Government Requirement:** 1. **NIST 800-34 Contingency Planning for Federal Information Systems 3.6** 2. **NIST 800-34 Contingency Planning for Federal Information Systems 3.5**	The CIO acknowledges the vulnerability identified by the Auditor. FLRA has procured services from the Bureau of Public Debt who will assist in developing the formal Contingency Plan. We have also procured an emergency notification from Everbridge. We aim to have a complete Contingency Plan tested agency-wide by June 2012.	Jun-12
5	**Risk:** In the event of an incident, the FLRA will likely be unprepared, because incident response training has not been provided to the IT personnel that manage the network. **Government Requirement:** 1. **NIST 800-53 Recommended Security Controls for Federal Information Systems and Organizations page F-61 (IR-2)**	The CIO acknowledges the vulnerability identified by the Auditor. However, FLRA will resolve this issue via in-house training, working with the Bureau of Public Debt and peering with CISO' from across the government on best practices by the end of the calendar year 2011. A formal Incident Response Plan will be communicated agency-wide by February 2012.	Feb-12
6	**Risk:** The HSPD-12 requirements ensure that authentication is stronger, thus decreasing unauthorized access into the network. Without implementation of the HSPD-12, the FLRA deploys two-factor authentication only and is not complemented by the PIV cards. This increases the risk of unauthorized access to data and systems. **Government Requirement:** 1. **NIST 800-116 Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS) section 2.2**	The CIO acknowledges the vulnerability identified by the Auditor. However, FLRA has purchased the technology to implement an HSPD-12 compliant Physical Access Control System (PACS) in those regional offices which are not slated to relocate over the next two years. The implementation of an internal PKI and Certificate Authority is scheduled for completion by December 31, 2011. Also, IRMD is scheduled to upgrade all FLRA workstations to Windows 7 by this time, which will aid greatly in implementing the HSPD-12 compliant Logical Access Control System (LACS).	Dec-11

7	**Risk:** The confidentiality of PII should be protected based on its risk level. **Government Requirement:** 1. **OMB 03-22 section II.B.2** 2. **NIST 800-122, section 3, page 3-1** 3. **OMB M-03-22, section VI, A**	The CIO acknowledges the vulnerability identified by the Auditor. The Information Resources Management Division (IRMD), in cooperation with the Senior Agency Official for Privacy (SOAP), will perform those Recommendations listed above by September 30, 2012.	9/2012

APPENDIX B – OIG RESPONSES REPORTED IN CYBERSCOPE

Inspector General

Section Report

2011

Annual FISMA Report

Federal Labor Relations Authority

Section 1: Risk Management

1a. The Agency has established and is maintaining a risk management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:

1.a(1). Documented and centrally accessible policies and procedures for risk management, including descriptions of the roles and responsibilities of participants in this process.

Yes

1.a(2). Addresses risk from an organization perspective with the development of a comprehensive governance structure and organization-wide risk management strategy as described in NIST 800-37, Rev.1

Yes

1.a(3). Addresses risk from a mission and business process perspective and is guided by the risk decisions at the organizational perspective, as described in NIST 800-37, Rev.1.

Yes

1.a(4). Addresses risk from an information system perspective and is guided by the risk decisions at the organizational perspective and the mission and business perspective, as described in NIST 800-37, Rev. 1.

Yes

1.a(5). Categorizes information systems in accordance with government policies.

Yes

1.a(6). Selects an appropriately tailored set of baseline security controls.

Yes

1.a(7). Implements the tailored set of baseline security controls and describes how the controls are employed within the information system and its environment of operation.

Yes

1.a(8). Assesses the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

Yes

1.a(9). Authorizes information system operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that

Section 1: Risk Management

this risk is acceptable.

Yes

1.a(10). Ensures information security controls are monitored on an ongoing basis including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials.

Yes

1.a(11). Information system specific risks (tactical), mission/business specific risks and organizational level (strategic) risks are communicated to appropriate levels of the organization.

Yes

1.a(12). Senior Officials are briefed on threat activity on a regular basis by appropriate personnel. (e.g., CISO).

Yes

1.a(13). Prescribes the active involvement of information system owners and common control providers, chief information officers, senior information security officers, authorizing officials, and other roles as applicable in the ongoing management of information system-related security risks.

Yes

1.a(14). Security authorization package contains system security plan, security assessment report, and POA&M in accordance with government policies.

Yes

Section 2: Configuration Management

2.b. The Agency has established and is maintaining a security configuration management program. However, the Agency needs to make significant improvements as noted below.

2.b(1). Configuration management policy is not fully developed (NIST 800-53: CM-1)

No

2.b(2). Configuration management procedures are not fully developed (NIST 800-53: CM-1).

No

2.b(3). Configuration management procedures are not consistently implemented (NIST 800-53: CM-1).

No

Section 2: Configuration Management

2.b(4). Standard baseline configurations are not identified for software components (NIST 800-53: CM-2).

No

2.b(5). Standard baseline configurations are not identified for all hardware components (NIST 800-53: CM-2).

No

2.b(6). Standard baseline configurations are not fully implemented (NIST 800-53: CM-2).

No

2.b(7). FDCC/USGCB is not fully implemented (OMB) and/or all deviations are not fully documented (NIST 800-53: CM-6).

No

2.b(8). Software assessing (scanning) capabilities are not fully implemented (NIST 800-53: RA-5, SI-2).

Yes

2.b(9). Configuration-related vulnerabilities, including scan findings, have not been remediated in a timely manner, as specified in Agency policy or standards. (NIST 800-53: CM-4, CM-6, RA-5, SI-2).

Yes

2.b(10). Patch management process is not fully developed, as specified in Agency policy or standards. (NIST 800-53: CM-3, SI-2).

Yes

2.b(11). Other

No

Section 3: Incident Response and Reporting

3.c. The Agency has not established an incident response and reporting program.

Section 4: Security Training

4.a. The Agency has established and is maintaining a security training program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:

4.a(1). Documented policies and procedures for security awareness training.

Section 4: Security Training

Yes

4.a(2). **Documented policies and procedures for specialized training for users with significant information security responsibilities.**

Yes

4.a(3). **Security training content based on the organization and roles, as specified in Agency policy or standards.**

Yes

4.a(4). **Identification and tracking of the status of security awareness training for all personnel (including employees, contractors, and other Agency users) with access privileges that require security awareness training.**

Yes

4.a(5). **Identification and tracking of the status of specialized training for all personnel (including employees, contractors, and other Agency users) with significant information security responsibilities that require specialized training.**

Yes

Section 5: POA&M

5.a. **The Agency has established and is maintaining a POA&M program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and tracks and monitors known information security weaknesses. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:**

5.a(1). **Documented policies and procedures for managing IT security weaknesses discovered during security control assessments and requiring remediation.**

Yes

5.a(2). **Tracks, prioritizes and remediates weaknesses.**

Yes

5.a(3). **Ensures remediation plans are effective for correcting weaknesses.**

Yes

5.a(4). **Establishes and adheres to milestone remediation dates.**

Yes

5.a(5). **Ensures resources are provided for correcting weaknesses.**

Yes

Section 5: POA&M

5.a(6). Program officials and contractors report progress on remediation to CIO on a regular basis, at least quarterly, and the CIO centrally tracks, maintains, and independently reviews/validates the POA&M activities at least quarterly.

Yes

Section 6: Remote Access Management

6.a. The Agency has established and is maintaining a remote access program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:

6.a(1). Documented policies and procedures for authorizing, monitoring, and controlling all methods of remote access.

Yes

6.a(2). Protects against unauthorized connections or subversion of authorized connections.

Yes

6.a(3). Users are uniquely identified and authenticated for all access.

Yes

6.a(4). If applicable, multi-factor authentication is required for remote access.

Yes

6.a(5). Authentication mechanisms meet NIST Special Publication 800-63 guidance on remote electronic authentication, including strength mechanisms.

Yes

6.a(6). Defines and implements encryption requirements for information transmitted across public networks.

Yes

6.a(7). Remote access sessions, in accordance to OMB M-07-16, are timed-out after 30 minutes of inactivity after which re-authentication are required.

Yes

Section 7: Identity and Access Management

7.a. The Agency has established and is maintaining an identity and access management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and identifies users and network devices. Although improvement

Section 7: Identity and Access Management

opportunities may have been identified by the OIG, the program includes the following attributes:

7.a(1). Documented policies and procedures for account and identity management.

Yes

7.a(2). Identifies all users, including federal employees, contractors, and others who access Agency systems.

Yes

7.a(3). Identifies when special access requirements (e.g., multi-factor authentication) are necessary.

Yes

7.a(4). If multi-factor authentication is in use, it is linked to the Agency's PIV program where appropriate.

Yes

7.a(5). Ensures that the users are granted access based on needs and separation of duties principles.

Yes

7.a(6). Identifies devices that are attached to the network and distinguishes these devices from users.

Yes

7.a(7). Ensures that accounts are terminated or deactivated once access is no longer required.

Yes

7.a(8). Identifies and controls use of shared accounts.

Yes

Section 8: Continuous Monitoring Management

8.b. The Agency has established an enterprise-wide continuous monitoring program that assesses the security state of information systems. However, the Agency needs to make significant improvements as noted below.

8.b(1). Continuous monitoring policy is not fully developed (NIST 800-53: CA-7).

Yes

8.b(2). Continuous monitoring procedures are not fully developed (NIST 800-53: CA-7).

No

Section 8: Continuous Monitoring Management

8.b(3). Continuous monitoring procedures are not consistently implemented (NIST 800-53: CA-7; 800-37 Rev 1, Appendix G).

No

8.b(4). Strategy or plan has not been fully developed for enterprise-wide continuous monitoring (NIST 800-37 Rev 1, Appendix G).

No

8.b(5). Ongoing assessments of security controls (system-specific, hybrid, and common) have not been performed (NIST 800-53, NIST 800-53A).

No

8.b(6). The following were not provided to the authorizing official or other key system officials: security status reports covering continuous monitoring results, updates to security plans, security assessment reports, and POA&Ms (NIST 800-53, NIST 800-53A).

No

8.b(7). Other

No

Section 9: Contingency Planning

9.b. The Agency has established and is maintaining an enterprise-wide business continuity/disaster recovery program. However, the Agency needs to make significant improvements as noted below.

9.b(1). Contingency planning policy is not fully developed contingency planning policy is not consistently implemented (NIST 800-53: CP-1).

Yes

9.b(2). Contingency planning procedures are not fully developed (NIST 800-53: CP-1).

No

9.b(3). Contingency planning procedures are not consistently implemented (NIST 800-53; 800-34).

No

9.b(4). An overall business impact assessment has not been performed (NIST SP 800-34).

No

9.b(5). Development of organization, component, or infrastructure recovery strategies and plans has not been accomplished (NIST

SP 800-34).

No

9.b(6). A business continuity/disaster recovery plan has not been developed (FCD1, NIST SP 800-34).

No

9.b(7). A business continuity/disaster recovery plan has been developed, but not fully implemented (FCD1, NIST SP 800-34).

No

9.b(8). System contingency plans missing or incomplete (FCD1, NIST SP 800-34, NIST SP 800-53).

No

9.b(9). Systems contingency plans are not tested (FCD1, NIST SP 800-34, NIST SP 800-53).

No

9.b(10). Test, training, and exercise programs have not been developed (FCD1, NIST SP 800-34, NIST 800-53).

Yes

9.b(11). Test, training, and exercise programs have been developed, but are not fully implemented (FCD1, NIST SP 800-34, NIST SP 800-53).

No

9.b(12). After-action report did not address issues identified during contingency/disaster recovery exercises (FCD1, NIST SP 800-34).

No

9.b(13). Systems do not have alternate processing sites (FCD1, NIST SP 800-34, NIST SP 800-53).

No

9.b(14). Alternate processing sites are subject to the same risks as primary sites (FCD1, NIST SP 800-34, NIST SP 800-53).

No

9.b(15). Backups of information are not performed in a timely manner (FCD1, NIST SP 800-34, NIST SP 800-53).

No

9.b(16). Backups are not appropriately tested (FCD1, NIST SP 800-34, NIST SP 800-53).

No

Section 9: Contingency Planning

9.b(17). Backups are not properly secured and protected (FCD1, NIST SP 800-34, NIST SP 800-53).

No

9.b(18). Contingency planning does not consider supply chain threats.

No

9.b(19). Other

No

Section 10: Contractor Systems

10.a. The Agency has established and maintains a program to oversee systems operated on its behalf by contractors or other entities, including Agency systems and services residing in the cloud external to the Agency. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:

10.a(1). Documented policies and procedures for information security oversight of systems operated on the Agency's behalf by contractors or other entities, including Agency systems and services residing in public cloud.

Yes

10.a(2). The Agency obtains sufficient assurance that security controls of such systems and services are effectively implemented and comply with federal and Agency guidelines.

Yes

10.a(3). A complete inventory of systems operated on the Agency's behalf by contractors or other entities, including Agency systems and services residing in public cloud.

Yes

10.a(4). The inventory identifies interfaces between these systems and Agency-operated systems.

Yes

10.a(5). The Agency requires appropriate agreements (e.g., MOUs, Interconnection Security Agreements, contracts, etc.) for interfaces between these systems and those that it owns and operates.

Yes

10.a(6). The inventory of contractor systems is updated at least annually.

Yes

Section 10: Contractor Systems

10.a(7). Systems that are owned or operated by contractors or entities, including Agency systems and services residing in public cloud, are compliant with FISMA requirements, OMB policy, and applicable NIST guidelines.

Yes

Section 11: Security Capital Planning

11.a. The Agency has established and maintains a security capital planning and investment program for information security. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:

11.a(1). Documented policies and procedures to address information security in the capital planning and investment control process.

Yes

11.a(2). Includes information security requirements as part of the capital planning and investment process.

Yes

11.a(3). Establishes a discrete line item for information security in organizational programming and documentation.

Yes

11.a(4). Employs a business case/Exhibit 300/Exhibit 53 to record the information security resources required.

Yes

11.a(5). Ensures that information security resources are available for expenditure as planned.

Yes

Contacting the Office of Inspector General

If you believe an activity is wasteful, fraudulent, or abusive of Federal funds, contact the:

HOTLINE (800)331-3572

HTTP://WWW.FLRA.GOV/OIG-HOTLINE

EMAIL: OIGMAIL@FLRA.GOV
CALL: (202)218-7970 FAX: (202)343-1072
WRITE TO: 1400 K Street, N.W. Suite 250, Washington, D.C. 20424

The complainant may remain confidential; allow their name to be used; or anonymous. If the complainant chooses to remain anonymous, FLRA OIG cannot obtain additional information on the allegation, and also cannot inform the complainant as to what action FLRA OIG has taken on the complaint. Confidential status allows further communication between FLRA OIG and the complainant after the original complaint is received. The identity of complainants is protected under the provisions of the Whistleblower Protection Act of 1989 and the Inspector General Act of 1978. To learn more about the FLRA OIG, visit our Website at http://www.flra.gov/oig

Office of Inspector General

FISMA Evaluation