FEDERAL LABOR RELATIONS AUTHORITY

OFFICE OF INSPECTOR GENERAL

Evaluation of the Federal Labor Relations Authority's Compliance with the Federal Information Security Management Act FY 2010 Report No. ER-11-01

For Official Use Only

TABLE OF CONTENTS

PURPOSE

Txdel, 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. Txdel's 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 Txdel. The weaknesses discussed in this report should be included in FLRA's Fiscal Year (FY) 2010 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 included FLRA Information Technology System, the only FLRA information technology system that is subject to FISMA reporting requirements.
We conducted our testing through inquiry of FLRA personnel, observation of activities, inspection of relevant documentation, and the performance of limited technical security testing. Some examples of our inquiries with FLRA management and personnel included, but were not limited to, reviewing system security plan, access control, the risk assessments, configuration management process. Examples of our observations included, but were not limited to, identifying areas were offices contained privacy information. Some examples of the documents inspected included, but were not limited to, reviewing the FLRA certification and accreditation artifacts. We also performed a vulnerability and modified penetration test of FLRA network infrastructure. Our testing includes commercially available tools that tests networked information resources for commonly known vulnerabilities. We provided the results of this testing to FLRA management separately.

FINDINGS

During our FY 2010 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 this year's assessment, we identified areas where FRLA could improve upon its Access Control, Awareness Training, Audit and Accountability, Certification, Accreditation, and Security, Configuration Management, Contingency Planning, Identification and Authentication, Incident Response, Maintenance, Media Protection, Physical and Environmental Protection, Planning, Personnel Security, Risk Assessment, System and Services Acquisition, System and Communications Protection, and System and Information Integrity.

In addition, we conducted network vulnerability and modified penetration test of key FLRA system and network devices. Our tests revealed vulnerabilities related to insecure system protocols, and configurations. While FLRA has developed an information security handbook the policies and procedures are not consistently implemented. Specifically FLRA personnel did not always follow this guidance to ensure that network devices were appropriately secured as prescribed. We believe the lack of resources and training only compound this issue.
We have provided the details of the network vulnerability and modified penetration test to FLRA management separately.

Access Control

- The information system does not enforce separation of duties through assigned access authorizations.
- The organization does not supervise and review the activities of users with respect to the enforcement and usage of information system access controls.

- The organization does not authorize, monitor, and control all methods of remote access to the information system.

Awareness Training

- 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.
- 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.

Audit and Accountability

- The information system does not generate audit records for the following events: [Assignment: organization-defined auditable events].
- 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.
- The organization does not allocate sufficient audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.
- 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: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)].
- 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.
- The information system does not provide an audit reduction and report generation capability.
- The information system does not provide time stamps for use in audit record generation.
- The information system does not protect audit information and audit tools from unauthorized access, modification, and deletion.
- The information system does not provide the capability to determine whether a given individual took a particular action.
- 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.

Certification, Accreditation, and Security

- 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.
- 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
- The organization does not monitor the security controls in the information system on an ongoing basis.

Configuration Management

- The organization does not develop, document, and maintain a current baseline configuration of the information system.
- The organization does not authorize, document, and control changes to the information system.
- The organization does not monitor changes to the information system conducting security impact analyses to determine the effects of the changes.
- 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.
- 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.
- 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].
- The organization does not develop, document, and maintain a current inventory of the components of the information system and relevant ownership information.

Contingency Planning

- 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.

- 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].
- 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.
- 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.
- The organization does not identify an alternate storage site and initiates necessary agreements to permit the storage of information system backup information.
- 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.
- 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.
- 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.
- 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.

Identification and Authentication

- 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.
- The information system does not employ authentication methods that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module.

Incident Response

- 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].
- 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.
- The organization does not implement an incident handling capability for security incidents that include preparation, detection and analysis, containment, eradication, and recovery.
- The organization does not track and document information system security incidents on an ongoing basis.
- The organization does not promptly report incident information to appropriate authorities.
- 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.

Maintenance

- 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.
- 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.

Media Protection

- The organization: (i) does not affix external labels to removable information system media and 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]
- The organization does not physically control and securely store information system media within controlled areas.

- 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.
- The organization does not sanitize information system media, both digital and non-digital, prior to disposal or release for reuse.

Physical and Environmental Protection

- 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 areas designated as publicly accessible.
- 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].
- The organization does not employ appropriate management, operational, and technical information system security controls at alternate work sites.

Planning

- 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.
- The organization does not conduct a privacy impact assessment on the information system in accordance with OMB policy.
- 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.

Personnel Security

- 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].

System and Services Acquisition

- 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.
- The organization does not manage the information system using a system development life cycle methodology that includes information security considerations.
- 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.
- The organization does not obtain, protect as required, and make available to authorized personnel, adequate documentation for the information system.
- The organization does not design and implement the information system using security engineering principles.
- 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.

System and Communications Protection

- 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 attacks or reference to source for current list].
- 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.
- The information system does not protect the integrity of transmitted information.
- The information system does not protect the confidentiality of transmitted information.
- 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].
- 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.
- 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.
- The information system does not protect the integrity and availability of publicly available information and applications.

- The information system does not reliably associate security parameters with information exchanged between information systems.
- 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.
- 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.
- 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.

System and Information Integrity

- The organization does not identify, report, and correct information system flaws.
- The information system does not implement malicious code protection.
- 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.
- 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.
- 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.
- The information system does not detect and protect against unauthorized changes to software and information.
- The information system does not check information for accuracy, completeness, validity, and authenticity.
- The information system does not identify and handles error conditions in an expeditious manner without providing information that could be exploited by adversaries.

Privacy Program

- The organization does not establish adequate policies, processes, and procedures for establishing a privacy program.
- The organization does not identify, report, and correct privacy weaknesses.

Remote Access Program

- The organization does not adhere to established policies, process, and procedures for establishing a remote access.
- The organization does not identify, report, and correct remote access weaknesses.
- The organization does not protect against unauthorized connections or subversion of authorized connections.

Entity-wide Continuous Monitoring Program

- The organization does not ensure establish adequate policies, process, and procedures for establishing a continuous monitoring program
- The organization does not identify, report, and corrects continuous monitoring program weaknesses
- The organization has not establishes continuous monitoring program oversight

Program to Oversee Contactor Systems

- The organization does not establish adequate policies, process, and procedures for establishing a contractor systems oversight.

RECOMMENDATIONS

	Recommendation	Issue Date	Number	Status	Management Comment	Mitigation Timeline
Access Control	Develop a **robust** access control program in accordance with *NIST Special Publication 800-53 Revision 3 Recommended Security Controls for Federal Information Systems*	7/20/2009	1	Open	Accept Risk - Separation of roles with an IT staff our size isn't feasible. All IT personnel assist with all IT efforts. Staff outside IRMD has rights only to what their job requires.	7/2011
	NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans				Systems monitoring technologies currently aren't in place. The CIO has a plan for correcting this deficiency.	
	NIST Special Publication 800-116 A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)				Systems monitoring technologies currently aren't in place. The CIO has a plan for correcting this deficiency.	
Awareness Training	Develop a **robust** awareness and training program in accordance with *NIST Special Publication 800-53 Revision 3 Recommended*	7/20/2009	2	Open	IRMD will develop Training equivalent to staff roles and provide said training on a quarterly basis, and when the employee starts. Due to staffing issues, our CISO role is vacant. The CIO has a plan for correcting this deficiency.	7/2011

	Security Controls for Federal Information Systems					
	NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans					
	NIST Special Publication 800-50 Building an Information Technology Security Awareness and Training Program					
	NIST Special Publication 800-16 Information Technology Security Training Requirements: A Role and Performance-Based Model					

Audit & Accountability	Develop a **robust** audit and accountability program in accordance with *NIST Special Publication 800-53 Revision 3 Recommended Security Controls for Federal*	7/20/2009	3	Open	Systems monitoring technologies currently aren't in place. The CIO has a plan for correcting this deficiency.	7/2011

	Information Systems					
	NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans					

Certification, Accreditation & Security	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*	7/20/2009	4	Open	FLRA uses the Bureau of Public Debt for our information security needs and have recently scheduled annual reviews of security controls for our GSS. This agreement did not include contractor systems. IRMD is investigating how elements of our contract with a vendor can be modified to address these issues	
	NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans				This issue is resolved. We are formally tracking issues via a POA&M	7/2011
	NIST Special Publication 800-37 Guide for the Security Certification and Accreditation of				We just recently formalized a continuous monitoring plan with the Bureau of Public Debt to address this shortcoming.	

	Federal Information Systems					
Configuration Management	Develop a **robust** configuration management program in accordance with *NIST Special Publication 800-53 Revision 3 Recommended Security Controls for Federal Information Systems*	7/20/2009	5	Open	FLRA is planning on moving to standardized builds for laptops, servers and infrastructure which follow STIGS to ensure compliance with this requirement. FLRA is looking into change management technologies to determine the financial cost this requirement would impose. New network monitoring solutions will be used to capture changes for forensic purposes. Currently, changes to information systems are solely for functionality sake. Once we correct our CISO staffing issues, this will be addressed prior to the next FISMA evaluation. Systems monitoring technologies currently aren't in place. The CIO has a plan for correcting this deficiency.	7/2011
	NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans					
Contingency Planning	Develop a **robust** contingency planning program in accordance with *NIST Special Publication 800-53 Revision 3 Recommended Security Controls for Federal Information Systems*	7/20/2009	6	Open	FLRA is currently working with a vendor to resolve the issues contained herein before the next annual FISMA evaluation. FLRA uses a 3rd party vendor to store data offsite in a manner supporting operational needs and timely recovery of sensitive data. Internet connectivity is available via one ISP. Essential personnel are	9/2011

	NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans				empowered with portable devices to provide communications and internet connectivity in the event LAN access is lost. FLRA does conduct daily and weekly backups. Backups are stored offsite and retrievable in a timely manner.	
	NIST Special Publication 800-34 Contingency Planning Guide for Information Technology Systems					

Identification & Authentication	*NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans*	7/20/2009	7	Open	FLRA will be upgrading our Active Directory and PIV authentication technologies to comply with this requirement.	7/2011
	NIST Special Publication 800-120 DRAFT Recommendation for EAP Methods Used in Wireless Network Access Authentication					
	NIST Special Publication 800-63 Electronic Authentication Guideline					

	NIST Special Publication 800-25 Federal Agency Use of Public Key Technology for Digital Signatures and Authentication					

Incident Response	Develop a **robust** incident response program in accordance with *NIST Special Publication 800-53 Revision 3 Recommended Security Controls for Federal Information Systems*	7/20/2009	8	Open	IRMD will develop Training equivalent to staff roles and provide said training on a quarterly basis, and when employees start. The CIO has a plan for this deficiency. FLRA is working with a 3rd party vendor to develop a solution that will address all Incident Response concerns raised during this evaluation. We have also worked with BPD to draft an Incident Response Plan that will go in effect for FY2011.	9/2011
	NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans					
	NIST Special Publication 800-86 Guide to Integrating Forensic Techniques into Incident Response					

Maintenance	Develop a **robust** maintenance program in accordance with *NIST Special Publication 800-53 Revision 3 Recommended Security Controls*	7/20/2009	9	Open	The current patching solution has been deemed deficient. FLRA is looking into an alternative patching solution that will address both Microsoft and 3rd party vendor applications.	7/2011

	for Federal Information Systems					
	NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans				FLRA is creating a account management database to ensure proper notice of expiring accounts. An end result will be forewarning, as well as budget consideration for expiring services.	7/2011

Media Protection	Develop a **robust** media protection program in accordance with *NIST Special Publication 800-53 Revision 3 Recommended Security Controls for Federal Information Systems*	7/20/2009	10	Open	FLRA needs to address the proper materials labeling procedures.	7/2011
	NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans				This action is performed when systems are being "excessed". However, media that is being re-used is not sanitized, and should be. This is a procedural/policy change that will take place in FY11	7/2011
	NIST Special Publication 800-88 Guidelines for Media Sanitization					

Physical & Environmental	Develop a **robust** planning program in accordance with *NIST Special Publication 800-53 Revision 3 Recommended Security Controls for Federal Information Systems*	7/20/2009	11	Open	This is a procedural change that will be corrected in FY2011. We will have a login book that captures access by unauthorized users.	7/2011
	NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans				FLRA has 6 Regional Offices. We will be looking into how access to those offices can better be managed so as to address this finding.	7/2011

Planning	Develop a **robust** personnel security program in accordance with *NIST Special Publication 800-53 Revision 3 Recommended Security Controls for Federal Information Systems*	7/20/2009	12	Open	FLRA will be correcting this by reviewing the Plan quarterly. The FLRA SAOP will be addressing this moving forward in FY2011.	7/2011
	NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans					

Personnel Security	Develop a **robust** risk assessment program in accordance with *NIST Special Publication 800-53 Revision 3 Recommended Security Controls for Federal Information Systems*	7/20/2009	13	Open	IRMD will work with ASD to create a personnel risk categorization matrix that defines what impact a person could have based on their role.	9/2011
	NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans					
	Develop a **robust** physical security program in accordance with *NIST Special Publication 800-53 Revision 3 Recommended Security Controls for Federal Information Systems*					
	NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans					

System and Services Acquisition	Develop a **robust** system and services acquisition program in accordance with *NIST Special Publication 800-53 Revision 3 Recommended Security Controls for Federal Information Systems*	7/20/2009	14	Open	This specifically speaks to our use of Intuit QuickBase for our Case Tracking System. We do not have a formal relationship with them as their service is a EULA. We are working to correct this with a formal SOW that addresses key deficiencies which are requirements for federal government information systems.	7/2011
	NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans				Current SDLC practices are not mature and as such, security is added as an afterthought rather than a primary objective. This will be corrected in FY2011	7/2011
	NIST Special Publication 800-23 Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products				A key deficiency that will be resolved soon is the hiring of a new CISO to help address this concern.	7/2011

System and Communication	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*	7/20/2009	15	Open	FLRA is moving in several directions to mitigate the risks posed by deficiencies in these areas, namely our NetworX MTIPS contracts that are in process now, establishing two-factor authentication and HSPD-12 compliant authentication mechanisms.	7/2011

	NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans				In collaboration with the FLRA SAOP, we will be determining what data on our systems has PII, and what protections are in place to ensure their protection, as well as whether that data should be on the network at all.	7/2011
	NIST Special Publication 800-13 Telecommunications Security Guidelines for Telecommunications Management Network					
System and Information Integrity	Develop a **robust** system and information integrity program in accordance with *NIST Special Publication 800-53 Revision 3 Recommended Security Controls for Federal Information Systems*	7/20/2009	16	Open	FLRA is moving in several directions to mitigate the risks posed by deficiencies in these areas, namely our NetworX/MTIPS contracts that are in process now, establishing two-factor authentication and HSPD-12 compliant authentication mechanisms and systems monitoring initiatives. it is our hope that these efforts will increase our security both from within and outside FLRA.	7/2011
	NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans					
Privacy Program	Develop **a robust** privacy program in accordance with *OMB guidance in M-07-16, M-06-15, and M-06-16 for*	10/24/2010	17	Open	FLRA IRMD and SAOP will be collaborating to ensure this gets addressed in FY2011.	9/2011

	safeguarding privacy-related information					
Remote Access Program	Establish and maintaining a remote access program that is generally consistent with *NIST's and OMB's FISMA requirements*	10/24/2010	18	Open	FLRA will be making improvements to its remote access solution that will correct these deficiencies in FY2011.	7/2011
Continuous Monitoring	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*	10/24/2010	19	Open	Systems monitoring technologies currently aren't in place. The CIO has a plan for correcting this deficiency.	7/2011
Contractor Systems	Establish and maintain a program to oversee systems operated on its behalf by contractors or other entities *NIST's and OMB's FISMA requirements*	10/24/2010	20	Open	This specifically speaks to our use of Intuit QuickBase for our Case Tracking System. We do not have a formal relationship with them as their service is a EULA. We are working to correct this with a formal SOW.	7/2011

UNITED STATES OF AMERICA
FEDERAL LABOR RELATIONS AUTHORITY
WASHINGTON, D.C. 20242

November 10, 2010

Dana Rooney-Fisher, Inspector General
Federal Labor Relations Authority
1400 K Street NW
Washington, DC 20005

Dear Inspector General Rooney-Fisher:

Thank you for the recently completed FISMA evaluation of FLRA information technology systems security. We are pleased with the finding that the FLRA is moderately secure. The evaluation findings -- as well as findings from an independent management initiated review -- establish that there is a great deal of work to be done to ensure the security posture of FLRA is improved, FLRA information and systems are secure, and operations are stable.

To fully correct these issues not only for the sake of compliance, but to operate in a mature and secure manner, the FLRA is committed to, and the FLRA Chief Information Officer (CIO) is establishing, an aggressive risk mitigation plan and timeline. The FLRA is in the planning phases of updating the agency's active directory infrastructure, email services, perimeter security technologies, system/change monitoring and reporting, certification and accreditation efforts, and overall process improvements. It is our intention that the agency has an entirely revised information technology system when the next FISMA evaluation is conducted. Our goals are aggressive, yet feasible.

Set forth below is the presentation of the FLRA Management Responses to the twenty findings by NIST 800-53 Security Control Family. The findings are organized and accompanied by the FLRA's Plan of Action & Milestones that will be followed in addressing each of the issues preventing the agency from confidently reporting full FISMA compliance.

Respectfully,

Carol Waller Pope
Chairman
Federal Labor Relations Authority

Management Responses to OIG Recommendations

	Recommendation	Issue Date	Number	Status	CIO Comment	Mitigation Timeline
Access Control	Develop a **robust** access control program in accordance with *NIST Special Publication 800-53 Revision 3 Recommended Security Controls for Federal Information Systems*	7/20/2009	1	Open	Accept Risk - Separation of roles with an IT staff our size isn't feasible. All IT personnel assist with all IT efforts. Staff outside IRMD has rights only to what their job requires.	
	NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans				Systems monitoring technologies currently aren't in place. The CIO has a plan for correcting this deficiency.	7/2011
	NIST Special Publication 800-116 A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)				Systems monitoring technologies currently aren't in place. The CIO has a plan for correcting this deficiency.	
Awareness Training	Develop a **robust** awareness and training program in accordance with *NIST Special Publication 800-53 Revision 3 Recommended Security Controls for Federal Information Systems*	7/20/2009	2	Open	IRMD will develop Training equivalent to staff roles and provide said training on a quarterly basis, and when the employee starts. Due to staffing issues, our CISO role is vacant. The CIO has a plan for correcting this deficiency.	
	NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans					7/2011
	NIST Special Publication 800-50 Building an Information Technology Security Awareness and Training Program					
	NIST Special Publication 800-16 Information Technology Security Training Requirements: A Role and Performance-Based Model					

Audit & Accountability	Develop a **robust** audit and accountability program in accordance with *NIST Special Publication 800-53 Revision 3 Recommended Security Controls for Federal Information Systems*	7/20/2009	3	Open	Systems monitoring technologies currently aren't in place. The CIO has a plan for correcting this deficiency.	7/2011
	NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans					

Certification, Accreditation & Security	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*	7/20/2009	4	Open	FLRA uses the Bureau of Public Debt for our information security needs and have recently scheduled annual reviews of security controls for our GSS. This agreement did not include contractor systems. IRMD is investigating how elements of our contract with a vendor can be modified to address these issues	7/2011
	NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans				This issue is resolved. We are formally tracking issues via a POA&M	
	NIST Special Publication 800-37 Guide for the Security Certification and Accreditation of Federal Information Systems				We just recently formalized a continuous monitoring plan with the Bureau of Public Debt to address this shortcoming.	

Configuration Management	Develop a **robust** configuration management program in accordance with *NIST Special Publication 800-53 Revision 3 Recommended Security Controls for Federal Information Systems*	7/20/2009	5	Open	FLRA is planning on moving to standardized builds for laptops, servers and infrastructure which follow STIGS to ensure compliance with this requirement. FLRA is looking into change management technologies to determine the financial cost this requirement would impose. New network monitoring solutions will be used to capture changes for forensic purposes. Currently, changes to information systems are solely for functionality sake. Once we correct our CISO staffing issues, this will be addressed prior to the next FISMA evaluation. Systems monitoring technologies currently aren't in place. The CIO has a plan for correcting this deficiency.	7/2011
	NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans					

Contingency Planning	Develop a **robust** contingency planning program in accordance with *NIST Special Publication 800-53 Revision 3 Recommended Security Controls for Federal Information Systems*	7/20/2009	6	Open	FLRA is currently working with a vendor to resolve the issues contained herein before the next annual FISMA evaluation. FLRA uses a 3rd party vendor to store data offsite in a manner supporting operational needs and timely recovery of sensitive data. Internet connectivity is available via one ISP. Essential personnel are empowered with portable devices to provide communications and internet connectivity in the event LAN access is lost. FLRA does conduct daily and weekly backups. Backups are stored offsite and retrievable in a timely manner.	9/2011
	NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans					
	NIST Special Publication 800-34 Contingency Planning Guide for Information Technology Systems					
Identification & Authentication	*NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans*	7/20/2009	7	Open	FLRA will be upgrading our Active Directory and PIV authentication technologies to comply with this requirement.	7/2011
	NIST Special Publication 800-120 DRAFT Recommendation for EAP Methods Used in Wireless Network Access Authentication					
	NIST Special Publication 800-63 Electronic Authentication Guideline					
	NIST Special Publication 800-25 Federal Agency Use of Public Key Technology for Digital Signatures and Authentication					
Incident Response	Develop a **robust** incident response program in accordance with *NIST Special Publication 800-53 Revision 3 Recommended Security Controls for Federal Information Systems*	7/20/2009	8	Open	IRMD will develop Training equivalent to staff roles and provide said training on a quarterly basis, and when employees start. The CIO has a plan for this deficiency. FLRA is working with a 3rd party vendor to	9/2011

					develop a solution that will address all Incident Response concerns raised during this evaluation. We have also worked with BPD to draft an Incident Response Plan that will go in effect for FY2011.	
	NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans					
	NIST Special Publication 800-86 Guide to Integrating Forensic Techniques into Incident Response					
Maintenance	Develop a **robust** maintenance program in accordance with *NIST Special Publication 800-53 Revision 3 Recommended Security Controls for Federal Information Systems*	7/20/2009	9	Open	The current patching solution has been deemed deficient. FLRA is looking into an alternative patching solution that will address both Microsoft and 3rd party vendor applications.	7/2011
	NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans				FLRA is creating a account management database to ensure proper notice of expiring accounts. An end result will be forewarning, as well as budget consideration for expiring services.	7/2011
Media Protection	Develop a **robust** media protection program in accordance with *NIST Special Publication 800-53 Revision 3 Recommended Security Controls for Federal Information Systems*	7/20/2009	10	Open	FLRA needs to address the proper materials labeling procedures.	7/2011
	NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans				This action is performed when systems are being "excessed". However, media that is being re-used is not sanitized, and should be. This is a procedural/policy change that will take place in FY11	7/2011
	NIST Special Publication 800-88 Guidelines for Media Sanitization					
Physical & Environmental	Develop a **robust** planning program in accordance with *NIST Special Publication 800-53 Revision 3 Recommended Security Controls for Federal Information Systems*	7/20/2009	11	Open	This is a procedural change that will be corrected in FY2011. We will have a login book that captures access by unauthorized users.	7/2011

	NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans				FLRA has 6 Regional Offices. We will be looking into how access to those offices can better be managed so as to address this finding.	7/2011

Planning	Develop a **robust** personnel security program in accordance with *NIST Special Publication 800-53 Revision 3 Recommended Security Controls for Federal Information Systems*	7/20/2009	12	Open	FLRA will be correcting this by reviewing the Plan quarterly. The FLRA SAOP will be addressing this moving forward in FY2011.	7/2011
	NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans					

Personnel Security	Develop a **robust** risk assessment program in accordance with *NIST Special Publication 800-53 Revision 3 Recommended Security Controls for Federal Information Systems*	7/20/2009	13	Open	IRMD will work with ASD to create a personnel risk categorization matrix that defines what impact a person could have based on their role.	9/2011
	NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans					
	Develop a **robust** physical security program in accordance with *NIST Special Publication 800-53 Revision 3 Recommended Security Controls for Federal Information Systems*					
	NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans					

System and Services Acquisition	Develop a **robust** system and services acquisition program in accordance with *NIST Special Publication 800-53 Revision 3 Recommended Security Controls for Federal Information Systems*	7/20/2009	14	Open	This specifically speaks to our use of Intuit QuickBase for our Case Tracking System. We do not have a formal relationship with them as their service is a EULA. We are working to correct this with a formal SOW that addresses key deficiencies which are requirements for federal government information systems.	7/2011

	NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans				Current SDLC practices are not mature and as such, security is added as an afterthought rather than a primary objective. This will be corrected in FY2011	7/2011
	NIST Special Publication 800-23 Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products				A key deficiency that will be resolved soon is the hiring of a new CISO to help address this concern.	7/2011
System and Communication	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*	7/20/2009	15	Open	FLRA is moving in several directions to mitigate the risks posed by deficiencies in these areas, namely our NetworX MTIPS contracts that are in process now, establishing two-factor authentication and HSPD-12 compliant authentication mechanisms.	7/2011
	NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans				In collaboration with the FLRA SAOP, we will be determining what data on our systems has PII, and what protections are in place to ensure their protection, as well as whether that data should be on the network at all.	7/2011
	NIST Special Publication 800-13 Telecommunications Security Guidelines for Telecommunications Management Network					
System and Information Integrity	Develop a **robust** system and information integrity program in accordance with *NIST Special Publication 800-53 Revision 3 Recommended Security Controls for Federal Information Systems*	7/20/2009	16	Open	FLRA is moving in several directions to mitigate the risks posed by deficiencies in these areas, namely our NetworX/MTIPS contracts that are in process now, establishing two-factor authentication and HSPD-12 compliant authentication mechanisms and systems monitoring initiatives. it is our hope that these efforts will increase our security both from within and outside FLRA.	7/2011
	NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans					
Privacy Program	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*	10/24/2010	17	Open	FLRA IRMD and SAOP will be collaborating to ensure this gets addressed in FY2011.	9/2011

Remote Access Program	Establish and maintaining a remote access program that is generally consistent with *NIST's and OMB's FISMA requirements*	10/24/2010	18	Open	FLRA will be making improvements to its remote access solution that will correct these deficiencies in FY2011.	7/2011
Continuous Monitoring	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*	10/24/2010	19	Open	Systems monitoring technologies currently aren't in place. The CIO has a plan for correcting this deficiency.	7/2011
Contractor Systems	Establish and maintain a program to oversee systems operated on its behalf by contractors or other entities *NIST's and OMB's FISMA requirements*	10/24/2010	20	Open	This specifically speaks to our use of Intuit QuickBase for our Case Tracking System. We do not have a formal relationship with them as their service is a EULA. We are working to correct this with a formal SOW.	7/2011

APPENDIX A

MANAGEMENT COMMENTS

APPENDIX B

OIG RESPONSES REPORTED IN CYBERSCOPE

Section 1: Status of Certification and Accreditation Program

1. Selected response is:

b. The Agency has established and is maintaining a certification and accreditation program. However, the Agency needs to make significant improvements as noted below.

1a. Areas for Improvement:

1a(1). Certification and accreditation policy is not fully developed.

No

1a(2). Certification and accreditation procedures are not fully developed, sufficiently detailed or consistently implemented.

No

1a(3). Information systems are not properly categorized (FIPS 199/SP 800-60).

No

1a(4). Accreditation boundaries for agency information systems are not adequately defined.

No

1a(5). Minimum baseline security controls are not adequately applied to information systems (FIPS 200/SP 800-53).

No

1a(6). Risk assessments are not adequately conducted (SP 800-30).

No

1a(7). Security control baselines are not adequately tailored to individual information systems (SP 800-30).

No

1a(8). Security plans do not adequately identify security requirements (SP 800-18).

No

1a(9). Inadequate process to assess security control effectiveness (SP800-53A).

No

1a(10). Inadequate process to determine risk to agency operations, agency assets, or individuals, or to authorize information systems to operate (SP 800-37).

Yes

1a(11). Inadequate process to continuously track changes to information systems that may necessitate reassessment of control effectiveness (SP 800-37).

Yes

Section 1: Status of Certification and Accreditation Program

1a(12). Other

Yes

Explanation for Other

The FLRA does not perform annual security assessments

Section 2: Status of Security Configuration Management

2. Selected response is:

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

2a. Areas for Improvement:

2a(1). Configuration management policy is not fully developed.

No

2a(2). Configuration management procedures are not fully developed or consistently implemented.

Yes

2a(3). Software inventory is not complete (NIST 800-53: CM-8).

No

2a(4). Standard baseline configurations are not identified for all software components (NIST 800-53: CM-8).

Yes

2a(5). Hardware inventory is not complete (NIST 800-53: CM-8).

Yes

2a(6). Standard baseline configurations are not identified for all hardware components (NIST 800-53: CM-2).

Yes

2a(7). Standard baseline configurations are not fully implemented (NIST 800-53: CM-2).

Yes

2a(8). FDCC is not fully implemented (OMB) and/or all deviations are not fully documented.

Yes

2a(9). Software scanning capabilities are not fully implemented (NIST 800-53: RA-5, SI-2).

No

Section 2: Status of Security Configuration Management

2a(10). Configuration-related vulnerabilities have not been remediated in a timely manner (NIST 800-53: CM-4, CM-6, RA-5, SI-2).

No

2a(11). Patch management process is not fully developed (NIST 800-53: CM-3, SI-2).

No

2a(12). Other

No

3. Identify baselines reviewed:

Operating System
None

Section 3: Status of Incident Response & Reporting Program

4. Selected response is:

b. The Agency has established and is maintaining an incident response and reporting program. However, the Agency needs to make significant improvements as noted below.

4a. Areas for Improvement:

4a(1). Incident response and reporting policy is not fully developed.

No

4a(2). Incident response and reporting procedures are not fully developed, sufficiently detailed or consistently implemented.

Yes

4a(3). Incidents were not identified in a timely manner (NIST 800-53, 800-61, and OMB M-07-16, M-06-19).

No

4a(4). Incidents were not reported to US-CERT as required (NIST 800-53, 800-61, and OMB M-07-16, M-06-19).

No

4a(5). Incidents were not reported to law enforcement as required.

No

4a(6). Incidents were not resolved in a timely manner (NIST 800-53, 800-61, and OMB M-07-16, M-06-19) .

No

Section 3: Status of Incident Response & Reporting Program

4a(7). Incidents were not resolved to minimize further damage (NIST 800-53, 800-61, and OMB M-07-16, M-06-19).

No

4a(8). There is insufficient incident monitoring and detection coverage (NIST 800-53, 800-61, and OMB M-07-16, M-06-19).

Yes

4a(9). Other

No

Section 4: Status of Security Training Program

5. Selected response is:

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

5a. Areas for Improvement:

5a(1). Security awareness training policy is not fully developed.

No

5a(2). Security awareness training procedures are not fully developed, sufficiently detailed or consistently implemented.

No

5a(3). Specialized security training policy is not fully developed.

No

5a(4). Specialized security training procedures are not fully developed or sufficiently detailed (SP 800-50, SP 800-53).

No

5a(5). Training material for security awareness training does not contain appropriate content for the Agency (SP 800-50, SP 800-53).

No

5a(6). Identification and tracking of employees with login privileges that require security awareness training is not adequate (SP 800-50, SP 800-53).

No

5a(7). Identification and tracking of employees without login privileges that require security awareness training is not adequate (SP 800-50, SP 800-53).

No

Section 5: Status of Plans of Actions & Milestones (POA&M) Program

Yes

6a(6). Security weaknesses are not appropriately prioritized (OMB M-04-25).

Yes

6a(7). Estimated remediation dates are not reasonable (OMB M-04-25).

Yes

6a(8). Initial target remediation dates are frequently missed (OMB M-04-25).

Yes

6a(9). POA&Ms are not updated in a timely manner (NIST SP 800-53, Rev. 3, Control CA-5, and OMB M-04-25).

Yes

6a(10). Costs associated with remediating weaknesses are not identified (NIST SP 800-53, Rev. 3, Control PM-3 & OMB M-04-25).

Yes

6a(11). Agency CIO does not track and review POA&Ms (NIST SP 800-53, Rev. 3, Control CA-5, and OMB M-04-25).

No

6a(12). Other

No

Section 6: Status of Remote Access Program

7. Selected response is:

b. The Agency has established and is maintaining a remote access program. However, the Agency needs to make significant improvements as noted below.

7a. Areas for Improvement:

7a(1). Remote access policy is not fully developed.

No

7a(2). Remote access procedures are not fully developed, sufficiently detailed or consistently implemented.

Yes

7a(3). Telecommuting policy is not fully developed (NIST 800-46, Section 5.1).

Yes

7a(4). Telecommuting procedures are not fully developed or sufficiently detailed (NIST 800-46, Section 5.4).

Section 6: Status of Remote Access Program

Yes

7a(5). Agency cannot identify all users who require remote access (NIST 800-46, Section 4.2, Section 5.1).

Yes

7a(6). Multi-factor authentication is not properly deployed (NIST 800-46, Section 2.2, Section 3.3).

Yes

7a(7). Agency has not identified all remote devices (NIST 800-46, Section 2.1).

Yes

7a(8). Agency has not determined all remote devices and/or end user computers have been properly secured (NIST 800-46, Section 3.1 and 4.2).

Yes

7a(9). Agency does not adequately monitor remote devices when connected to the agency's networks remotely (NIST 800-46, Section 3.2).

Yes

7a(10). Lost or stolen devices are not disabled and appropriately reported (NIST 800-46, Section 4.3, US-CERT Incident Reporting Guidelines).

Yes

7a(11). Remote access rules of behavior are not adequate (NIST 800-53, PL-4).

No

7a(12). Remote access user agreements are not adequate (NIST 800-46, Section 5.1, NIST 800-53, PS-6).

Yes

7a(13). Other

No

Section 7: Status of Account and Identity Management Program

8. Selected response is:

b. The Agency has established and is maintaining an account and identity management program that identifies users and network devices. However, the Agency needs to make significant improvements as noted below.

8a. Areas for Improvement:

Section 7: Status of Account and Identity Management Program

8a(1). Account management policy is not fully developed.

No

8a(2). Account management procedures are not fully developed, sufficiently detailed or consistently implemented.

Yes

8a(3). Active Directory is not properly implemented (NIST 800-53, AC-2).

Yes

8a(4). Other Non-Microsoft account management software is not properly implemented(NIST 800-53, AC-2).

Yes

8a(5). Agency cannot identify all User and Non-User Accounts (NIST 800-53, AC-2).

No

8a(6). Accounts are not properly issued to new users (NIST 800-53, AC-2).

No

8a(7). Accounts are not properly terminated when users no longer require access (NIST 800-53, AC-2).

No

8a(8). Agency does not use multi-factor authentication where required (NIST 800-53, IA-2).

Yes

8a(9). Agency has not adequately planned for implementation of PIV for logical access (HSPD 12, FIPS 201, OMB M-05-24, OMB M-07-06, OMB M-08-01).

Yes

8a(10). Privileges granted are excessive or result in capability to perform conflicting functions (NIST 800-53, AC-2, AC-6).

No

8a(11). Agency does not use dual accounts for administrators (NIST 800-53, AC-5, AC-6).

No

8a(12). Network devices are not properly authenticated (NIST 800-53, IA-3).

Yes

8a(13). Other

No

Section 7: Status of Account and Identity Management Program

Section 8: Status of Continuous Monitoring Program

9. Selected response is:

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

9a. Areas for Improvement:

9a(1). Continuous monitoring policy is not fully developed.

No

9a(2). Continuous monitoring procedures are not fully developed or consistently implemented.

Yes

9a(3). Strategy or plan has not been fully developed for entity-wide continuous monitoring (NIST 800-37).

Yes

9a(4). Ongoing assessments of selected security controls (system-specific, hybrid, and common) have not been performed (NIST 800-53, NIST 800-53A).

Yes

9a(5). The following were not provided to the system 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).

Yes

9a(6). Other

No

Section 9: Status of Contingency Planning Program

10. Selected response is:

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

10a. Areas for Improvement:

10a(1). Contingency planning policy is not fully developed.

No

Section 9: Status of Contingency Planning Program

10a(2). Contingency planning procedures are not fully developed or consistently implemented.

Yes

10a(3). An overall business impact assessment has not been performed (NIST SP 800-34).

Yes

10a(4). Development of organization, component, or infrastructure recovery strategies and plans has not been accomplished (NIST SP 800-34).

Yes

10a(5). A business continuity/disaster recovery plan has not been developed (FCD1, NIST SP 800-34).

Yes

10a(6). A business continuity/disaster recovery plan has been developed, but not fully implemented (FCD1, NIST SP 800-34).

Yes

10a(7). System contingency plans missing or incomplete (FCD1, NIST SP 800-34, NIST SP 800-53).

Yes

10a(8). Critical systems contingency plans are not tested (FCD1, NIST SP 800-34, NIST SP 800-53).

Yes

10a(9). Training, testing, and exercises approaches have not been developed (FCD1, NIST SP 800-34,NIST 800-53).

Yes

10a(10). Training, testing, and exercises approaches have been developed, but are not fully implemented (FCD1, NIST SP 800-34, NIST SP 800-53).

Yes

10a(11). Disaster recovery exercises were not successful revealed significant weaknesses in the contigency planning. (NIST SP 800-34).

Yes

10a(12). After-action plans did not address issues identified during disaster recovery exercises (FCD1, NIST SP 800-34).

Yes

10a(13). Critical systems do not have alternate processing sites (FCD1, NIST SP 800-34, NIST SP 800-53).

Yes

10a(14). Alternate processing sites are subject to same risks as primary sites (FCD1, NIST SP 800-34, NIST SP 800-53).

Section 9: Status of Contingency Planning Program

Yes

10a(15). Backups of information are not performed in a timely manner (FCD1, NIST SP 800-34, NIST SP 800-53).

Yes

10a(16). Backups are not appropriately tested (FCD1, NIST SP 800-34, NIST SP 800-53).

Yes

10a(17). Backups are not properly secured and protected (FCD1, NIST SP 800-34, NIST SP 800-53).

Yes

10a(18). Other

No

Section 10: Status of Agency Program to Oversee Contractor Systems

11. Selected response is:

b. The Agency has established and maintains a program to oversee systems operated on its behalf by contractors or other entities. However, the Agency needs to make significant improvements as noted below.

11a. Areas for Improvement:

11a(1). Policies to oversee systems operated on the Agency's behalf by contractors or other entities are not fully developed.

No

11a(2). Procedures to oversee systems operated on the Agency's behalf by contractors or other entities are not fully developed or consistently implemented.

Yes

11a(3). The inventory of systems owned or operated by contractors or other entities is not sufficiently complete.

Yes

11a(4). The inventory does not identify interfaces between contractor/entity-operated systems to Agency owned and operated systems.

Yes

11a(5). The inventory of contractor/entity-operated systems, including interfaces, is not updated at least annually.

Yes

11a(6). Systems owned or operated by contractors and entities are not subject to NIST and OMB's FISMA requirements (e.g.,

Section 10: Status of Agency Program to Oversee Contractor Systems

certification and accreditation requirements).

No

11a(7). Systems owned or operated by contractor's and entities do not meet NIST and OMB's FISMA requirements (e.g., certifications and accreditation requirements).

No

11a(8). Interface agreements (e.g., MOUs) are not properly documented, authorized, or maintained.

No

11a(9). Other

No

CONTACTING THE OFFICE OF INSPECTOR GENERAL

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

Please Call

Toll Free 1-800-331-3572 or (202)218-7744 in the Washington metropolitan area

or write to:

Federal Labor Relations Authority

Office of Inspector General

1400 K Street, NW

Suite 250

Washington, D.C. 20424

Information can be provided anonymously. Federal Government employees are protected from reprisal and anyone may have his or her identity held in confidence.