UNITED STATES OF AMERICA
FEDERAL LABOR RELATIONS AUTHORITY
OFFICE OF THE INSPECTOR GENERAL
WASHINGTON, D.C. 20424-0001

FLRA Inspector General FY 2006 Evaluation of FLRA's Compliance With The Federal Information Security Management Act of 2002

Background: The Federal Information Security Management Act of 2002 requires Inspectors General to perform annual independent evaluations of Agency security programs and practices. The FLRA Inspector General performed a comprehensive Computer Information Security Audit in FY 2001 which revealed that the FLRA had substantial security vulnerabilities in its Computer Information Program and that management needed to immediately focus on its technology and computer information security programs to ensure protection of FLRA information as well as to be able to implement e-government in the future.

The E Government Act passed in December 2002 recognized the importance of information security while the Federal Information Security Management Act (FISMA) emphasize the need of Federal agencies to develop, document and implement an enterprise wide program to provide information security for information and information systems that support Agency systems. The minimum-security requirements are applicable to all information within the Federal government other than those pursuant to Executive Order 12958. The minimum-security requirements for Federal agencies pertain to 17 securities related areas, which are:

1. access control;
2. awareness and training;
3. audit and accountability;
4. certification, accreditation and authentication;
5. configuration management;
6. contingency planning;
7. identification and authentication;
8. incident response;
9. maintenance;
10. media protection;
11. physical and services acquisition;
12. system and communication protection;
13. planning;
14. personnel security (personally identifiable information);
15. risk assessment;
16. Systems information integrity, and
17. Information integrity

The FLRA Inspector General requested a copy of the FLRA's 2005 E-Government submission from the FLRA Executive Director which was not provided.

2006 Inspector General Evaluation:

The FLRA Inspector General conducted an evaluation of the FLRA's FISMA compliance using Federal quality standards for inspections and audits. This evaluation was conducted related to the President's Council on Integrity and Efficiency, (PCIE) and Executive Council on Integrity and Efficiency (ECIE) to determine the current status of the FLRA's information security program, policies and guidance, and provide feedback to management through this report. The FLRA Inspector General also requested that management provide the Inspector General sufficient budget in 2007 so that an extensive security information technology contracted audit could be conducted in 2007 to provide independent and objective testing for FISMA, NIST, and OMB security information technology requirements. The Inspector General is waiting for a response from the Chairman, FLRA.

As a follow-up to the Inspector General audit recommendations in FY 2001, FLRA management engaged the services of private sector consultants to perform a detailed review of the FLRA=s information technology support structure which included specific assessments of the Information Resource Management Division (IRMD) organization, staffing resource levels, funding levels, strategies, information technology, and performance management. As a result of this consultation, FLRA management was provided detailed technically oriented recommendations to support the FLRA=s Information Technology Program. In FY 2004, the FLRA Inspector General contracted a Security Audit which included security information technology and affirmed that very little information technology metrics had been implemented to address security requirements and that the FLRA had a material weakness related to this issue.

In FY 2005, the FLRA CIO/Director of Information Resource Management drafted planning, policy and procedures, which were submitted to the FLRA Executive Director to maintain a proper information security program in compliance with OMB Circular A-130. As of this date, information security policies have not been approved and, thus, have not been implemented. The FLRA did address several procedures to address the FLRA's information technology systems which included several essential requirements which were essential for improving the FLRA technology system.

As a result of a request to Federal Inspectors General by the President, PCIE/ECIE/ Deputy Director, Office of Management Budget, the FLRA Inspector General conducted an evaluation of FLRA=s information technology security controls related to personally identifiable information on the FLRA website and remote websites. This evaluation affirmed that the FLRA does not conduct mission related Federal labor management complaints, cases or appeals online although this information is not considered sensitive. The only sensitive information kept on the FLRA website is administrative and it is internal and not accessible externally. The FLRA does currently provide some personal payroll information to the Department of Interior National Business Center and financial information to the Department of Treasury. Both of these connections are properly encrypted and no problems have occurred.

This evaluation verified that the FLRA has installed proper security information controls and has addressed most previously identified information technology security issues and material weaknesses. The FLRA information technology is in compliance with most National Institute of Standards and Technology information security requirements and Office of Management and Budget M-06-16 requirements. The only major issue that needs to be addressed is the implementation of current FLRA Information Technology Policy which was created in 2005, the creation of policy for Behavioral issues, and improving the security patches on the Microsoft Outlook e-mail site to eliminate an extensive amount of spasm. The FLRA still needs to assign the responsibility of security to a qualified person who would function as a Security Officer, create a security plan for all systems and major applications, providing annual security information technology training for managers and all staff, include independent testing of security controls, implement updated information technology policy and require appropriate authorization before processing new procedures.

FISMA Reporting:

FISMA requires that each agency=s report includes information regarding the following former GISRA requirements:

1) Agency risk assessments
2) Security policies and procedures.
3) Individual system security plans
4) Training
5) Annual testing and evaluation
6) Corrective Action Process
7) Security Incident Reporting
8) Continuity of Operations

FISMA requires each Agency to develop specific system configuration requirements that meet there needs and ensure compliance with continuous monitoring and maintenance. This monitoring must include the testing of operational and technical controls, which is done annually by the FLRA. CIO/Director Information Resource Management Division but also needs to have independent testing by the Office of the Inspector General every few years. These reviews must also assess risks, and identify systems, which are not certified or accredited (NIST requirements.) FISMA also codifies an ongoing policy requirement that each system security program have provisions for continuity of operations. FISMA requires that each agency have a senior Information Security Officer (appointed by the agency CIO) who reports to the CIO and carries out the security information responsibilities. The FLRA has complied with most of FISMA requirements except for continuing with independent testing of security controls, hiring a Security Officer and implementing current information technology policy. In relation to personnel security requirements, the FLRA have only conducted security checks on new personnel over the past 5.years and have not established any policy for personnel security.

Most of the FLRA information systems are low impact but there some that are at the moderate level. This specific information was not provided to the FLRA Inspector General who requested it. Many of the FLRA security controls for FLRA information systems satisfy NIST security requirements, however, there are still some required security system controls and protective measures that have not yet been implemented or properly addressed. These include:

-- Implementation of current Information Technology Policy created by the FLRA CIO/Director of Information Resource Management in 2005;

-- Hiring or training a current IRM employee to serve as an Information Technology Security Officer;

-- Eliminating an excessive amount of E-Mail spasm.

The FLRA CIO Director of Information Resource Management (IRM) has implemented the majority of findings and recommendations issued by the last two Office of Inspector General contracted information technology security audits and have created a Contingency Plan and POA&M which relates to performance measures and provides a quantitative rather than just a narrative response. The information security policy and procedures created by the FLRA CIO/Director Information Resource Management Division will strengthen the FLRA's computer information technology and security and address NIST and OMB information security requirements when approved and implemented.

The FLRA has 3 Direct Mission Support Systems, 2 Administrative Support Systems, 2 Network Support Systems, and 2 Telecommunication Systems. The FLRA CIO/Director of Information Resource Management does perform annual reviews of these FLRA systems and has properly submitted required FISMA quarterly reports. All of the 17 internal systems and 6 external systems have been categorized according to FIPS 199. The FY 2004 categorized review revealed that the category of sensitivity was mostly at the medium level but a few were low and a few were still high.

The CIO Acting Director of Information Resource Management has completed draft security policy addressing existing security weaknesses and submitted them to management in June and July of 2005 and has submitted these policies to management for approval. These policies address:

-- Contingency Planning;
-- Data Backups, Incident Reporting;
-- Security Program Plan;
-- Security Program Policies and Procedures;
-- User Account Control, Segregation of Duties;
-- Security Awareness Training, Systems Certification
-- Systems Development Life Cycle and Change and Accreditation Control, and
-- Acceptable Use of Information Resources.

Until the security policies are approved and implemented, the FLRA still has a high risk for cost overruns, rework, implementation failures and other substantive problems that are still likely to lead to the waste of resources. The Inspector General >s current evaluation has revealed that although several information security improvements have been made this past year, the FLRA still has some significant problems which need to be addressed.

The most significant problem in FY 2006 is the receipt of significant infectious and pornographic e-mails on the FLRA networks even though patches have been implemented on the network servers. Also, the FLRA still does not have a proper test lab to assess the effect of patches when they are implemented.

The FLRA Inspector General=s 2006 evaluation of the FLRA=s compliance with FISMA revealed that the FLRA CIO/Acting Director of Information Resource Management did address a large amount of previous vulnerabilities and focused on correcting a large amount of FLRA's information security issues. The FLRA did use the NIST 800-70 Security Configuration Checklists Program and the Windows Server 2003 Security Guide from NIST 800-70 to upgrade the FLRA's network environment. This evaluation also affirmed that the FLRA created a POA&M, which relates to the FLRA's mission and functions and implemented Continuity of Operations Plan to mitigate risks associated service disruptions.

Without a fully implemented system security program plan and policy, FLRA's risk assessment is still high and security internal controls are still needed. The FLRA still needs to improve its filter and patch implementations to reduce penetration risks, which have not decreased even though patches have been implemented. During this past year, security information technology training was provided for FLRA employees online and required for all FLRA employees.

Information security is an ongoing process and websites need to be up to date with all security measures. Vulnerabilities must be addressed when they are identified to prevent the development of future significant deficiencies and material weaknesses. Over this next year, the FLRA needs to continue focusing on creating a risk based, cost-effective approach to secure its information systems, and resolve its identified information technology security weaknesses and risks as well as protect its information technology systems against future vulnerabilities and threats. The FLRA Inspector General's evaluation of the FLRA's FY 2006 FISMA compliance has affirmed that the FLRA has focused on correcting and improving its information security systems and has focused on FISMA compliance to correct its previously identified vulnerabilities. While the FLRA security technology systems still have vulnerabilities, the fact that improvements have been made is a positive step.

FY 2006 Update on FLRA Inspector General
Security Information Findings & Recommendations

Audit of Computer Information Security FY 2001

Audit of Computer Information Security February 2001	1. Fund, develop, and implement an information security program that complies with OMB Circulars A-123, A-127, and A-130.	06/27/05	Closed
	2. Establish senior management oversight committee to demonstrate senior management's commitment to and support of an effective, efficient security program.	01/02	Closed
	3. Ensure procedures are established to monitor/report FLRA's progress in resolving weaknesses and developing an efficient/effective information system security system.	09/30/02	Closed
	4. Establish a security awareness program that all employees must attend annually.	07/05/05	Closed
	5. Delegate authority to IRMD that clearly assigns responsibilities and requirements; coordinate information security control with systems outside determined IRMD and assist/control with other program offices during development and implementation if new systems and enhancements are added to existing systems.	06/27/05	Closed
	6. Revise current instructions for HRD and BFD to include security administration responsibilities for respective systems that also require coordination with IRMD.	06/27/05	Closed
	7. Ensure that system owners and program offices perform periodic risk and vulnerability assessments and certify systems.	09/30/02	Closed
	8. Develop & establish agency-wide information security policy through the consolidation of existing instructions.	06/27/05	Closed
	9. Centralize management responsibilities for development of security policy procedures and practices, but retain daily security administration with program offices.	06/27/05	Closed
	10. Develop procedures to maintain a current inventory of authorized users for each system and for remote access.	06/27/05	Closed
	11. Define rules of behavior for each system based in management's defined level of acceptable risk.	**12/30/05**	**Open**
	12. Develop procedures to ensure that Security Officials, systems, and data owners establish and formalize procedures for granting appropriate access and system privileges.	9/30/02	Closed
	13. Conduct an agency-wide assessment of information contained within the various systems to identify/classify the sensitivity of information and the security level needed.	9/30/02	Closed

Note: Periodic risk and vulnerability assessment conducted yearly since September 2002.

FY 2001 Audit of FLRA Security Programs	1. Formalize incident response procedures to identify/report on apparent/actual security breaches. Revised date for security breaches. Include instructions on proper procedures for reacting to security breaches in security awareness programs.	06/27/05	Closed
	2. Develop procedures for periodically evaluating user privileges and in granting initial access and revised date to privileges to systems software and data.	06/27/05	Closed
	3. Obtain new remote access software sufficient to preclude unlimited remote dial in access to FLRA network.*(CISCO - Virtual Private Network (VPN))	12/31/03	Closed
	4. Obtain new software to monitor eternal access to the network and alert IRMD security personnel of suspicious activities.	3/31/02	Closed
	5. Dedicate funding to identify, review, and evaluate critical business functions for developing a business contingency and recovery plan.	06/27/05	Closed
	6. Document procedures for programmers' access to the production environment and management's compensating controls to detect unauthorized activities**.**	06/27/05	Closed
	7. Document the network configuration: hardware, software, and security controls; client server and Oracle databases; and systems security controls.	04/16/03	Closed
	8. Develop a System Develop Life Cycle Methodology compliant with OMB and NIST requirements for developing new systems and enhancing existing systems	04/16/03	Closed
	9. Review costs and benefits of relocating the computer used for entering and authorizing vendor payments to the Department of Treasury to a more secure location away from the general work area into an area of limited access.	3/17/03	Closed

Internal Review of the Office of the General Counsel	1. To acknowledge and comply with information security and assurance case files should be marked with “For Official Use Only” or “Confidential” and be locked after hours and during major time absences of investigation agents to protect confidentiality/sensitivity of information.	10/02	Closed
	2. Refrain from using e-mail to transmit any type of investigation documentation. Until software is encrypted or other appropriate information Security software is installed unless parties are aware of potential disclosure and agree to use the e-mail even though there is the possibility of information disclosure/compromise.	**9/02 Awaiting decision of new General Counsel**	Open
	3. FLRA is in the process of procuring VeriSign SSL 128-bit certificate for an external server.	10/30/05	Closed
Summary	**Line items with 06/27/05 and 07/05/05 have been completed and currently being reviewed by management. Once approved, plans and policies will be implemented.**		

Note: Information will be re-assessed this year to ensure compliance with new NIST Publication 53 in regards to internal controls (low, high, and medium) outlined in FIPS 199.