UNITED STATES OF AMERICA
FEDERAL LABOR RELATIONS AUTHORITY
Office of Inspector General
WASHINGTON, D.C. 20424-0001

August 19, 2005

TO: Dale Cabaniss
Chairman, FLRA

FROM: Francine Eichler
Inspector General

SUBJECT: Inspector General Evaluation of the Federal Labor Relations Authority’s Federal Information Security Management Act of 2002

References: (a) Federal Information Security Management Act of FY 2002
(b) OMB Guidance for FY 2005 FISMA Security Reviews

The Office of Management and Budget (OMB) has provided specific instructions for Federal agencies and Inspectors General to report the results of annual information security reviews in compliance with the Federal Information Security Management Act (FISMA) of FY 2002. FISMA applies to all Federal agencies covered by the Paperwork Reduction Act. FISMA explicitly states that each Federal agency provide security protections for “information collected or maintained by or on behalf of the agency and information systems used or operated by an agency or by a contractor of an agency or another organization on behalf of the agency.” FISMA requires Inspectors General to perform annual information security reviews and provide independent and objective information on this subject matter. Because of budget constraints, the FLRA Inspector General was not able to conduct an audit of FLRA’s current security information technology. The FLRA Inspector General did, however, conduct an evaluation of FLRA ‘s progress in completing previous information technology findings and recommendations and FLRA’s compliance with the FISMA requirements. The FLRA Inspector General Evaluation should be submitted with the FLRA’s Executive Summary due to OMB not later than October 7, 2005.

OMB has specifically identified FISMA reporting requirements for agencies and Inspectors General. I am attaching the Inspector General review for inclusion with the FLRA’s submission. I have also provided a copy of Inspector General defined vulnerabilities from the 2001 Security Audit and their current status as well as the findings and recommendations from the FY 2004 Inspector General Audit of FLRA’s Security Programs. If you have any questions, please contact me at Extension 7744.

FLRA Inspector General FY 2005 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.

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. Very few of these recommendations have been implemented.

In FY 2002, the Chairman, FLRA created a Chief Information Officer (CIO) position. The FLRA Chief Information Officer has drafted planning, policy and procedures, which still need to be approved by FLRA management before they can be implemented. The FLRA does not currently maintain a proper information security program in compliance with OMB Circular A-130. The FLRA's information technology systems are essential for its mission and needs more management attention to ensure that there is no loss, misuse, unauthorized access, or modification of the information in the application. Specific management, operational and technical security controls as well as telecommunications and network security controls must be implemented to reduce the areas of high risk. At a minimum, the FLRA needs to assign the responsibility of security to a qualified person, have a security plan for all systems and major applications, provide a yearly review and testing of security controls and require appropriate authorization before processing new procedures.

FISMA Reporting

FISMA requires that each agency's report include 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 also requires each Agency to develop specific system configuration requirements that meet their needs and ensure compliance with continuous monitoring and maintenance. This monitoring must include the testing of management, operational and technical controls. It 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 not yet complied with these requirements. Although the CIO/Acting Director, of Information Resource Management (IRM), has formulated a corrective action plan for previous FLRA Inspector General information security findings, the CIO has not yet created an agency wide Plan of Action and Milestone (POA&M) process which relates to performance measures and provides a quantitative rather than just a narrative response. The CIO has previously worked with two contractors to develop information security policy and procedures, which will strengthen the FLRA's computer information security, when implemented. Currently the FLRA is contracted with the National Business Center in Denver Colorado for finance and human resource systems and the Government Printing Office, which provides hosting services for the FLRA Internet.

The FLRA has 3 `Direct Mission Support Systems, 2 Administrative Support Systems, 2 Network Support Systems and 2 Telecommunication Systems. The FLRA CIO does perform annual reviews of the 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 some were low and high. Basically, all managers agreed with the category of sensitivity stated by the FLRA CIO and were at an acceptable and appropriate level.

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 and Accreditation, Systems Development Life Cycle and Change 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 evaluation also has revealed that although the FLRA CIO/Acting Director of Information Resource Management Division addressed and created corrections for the FLRA's material weaknesses and high risks, implementation has not occurred because the CIO/ Acting Director of Information Resource Management was still waiting for management approval and an increased budget to address the proper implementation of new requirements.

The most significant problem in FY 2005 was infections of the FLRA networks with the Trojan Virus. The FLRA still has not implemented policy for implementing patches to the network servers. However, the FLRA has created a test lab to assess the effect of patches to the network servers to assess the effect of patches when they are implemented.   Following a maintenance schedule to make sure that computers and servers are properly updated with security patches would help minimize the problems caused by viruses and pornographic e-mails, which have dramatically increased over the last year.

The FLRA Inspector General did not have a sufficient 2005 budget allocation to conduct a Information Security Program Audit.   In order to comply with FISMA's Inspector General requirements, the FLRA Inspector General conducted an evaluation which revealed that the FLRA CIO/Acting Director of Information Resource Management did significantly address previous vulnerabilities and focused significantly on correcting FLRA's information security issues identified in the Inspector General's 2004 Security Audit. The FLRA does 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. During FY 2005, FLRA management did approve and hired an additional staff member, a network manager who is fulfilling security requirements, which was a positive action for the Information Resource Management Division. However, FLRA management has not yet hired/appointed an Information Security Officer, and has not yet separated the duties of the CIO/Acting Director of the Information Resource Management Division.

During FY 2005, the FLRA CIO/Acting Director of the Information Resource Management Division analyzed user account management on FLRA's agency-wide systems and the agency network as well as conducted an impact analysis on the use of passwords, how they were being used and how they were interconnected within the FLRA's network environment. The FLRA CIO/Acting Director of the Information Resource Management Division renegotiated Microsoft License renewal through the Small and Independent Agency Council which yielded a cost savings of $108,000 over a 3 year period and obtained 13 new laptops through a warranty program to replace laptops in one of the FLRA Regional Offices which were not operating properly for the past two years.

Without a fully implemented system security program plan, responsibility and accountability with respect to information security internal controls are still not sufficient. The FLRA still needs to improve its filter and patch management to reduce penetration risks, which have increased even more over the last year. FLRA information security policy and a contingency plan need to be implemented. Security training still needs to be provided for all FLRA managers and employees. From the training aspect, the FLRA CIO/Acting Director of Information Resource Management Division did provide information security training for her Information Resource Management Staff during FY 2005. Security Information training was not provided to FLRA employees in FY 2005. In FY 2005, the FLRA's CIO/Acting Director of Information Management Resources recommended OPM online security awareness training for employees to management, which has not yet been approved.

Over this next year, the FLRA must continue to focus 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 must focus on improving its computer technology and information security, create an agency wide POA&M which relates to FLRA's mission and functions and implement a Continuity of Operations Plans to mitigate risks associated service disruptions. Policies and procedures need to be implemented, and training needs to be conducted for 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. The FLRA Inspector General's evaluation of the FLRA's FY 2005 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.

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 2004 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.