UNITED STATES OF AMERICA

FEDERAL LABOR RELATIONS AUTHORITY
OFFICE OF THE INSPECTOR GENERAL

WASHINGTON, D.C. 20424-0001

September 2004

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 2004 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 Ainformation 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 security reviews and provide independent and objective information on this subject matter. In order to comply with FISMA, the Inspector General has conducted an audit of FLRA's current security information technology's compliance with the FISMA requirements.

Attached you will find the FLRA Inspector General Audit of the FY 2004 Security Programs which identified that the FLRA Information Security Program has material weaknesses. FLRA management has not sufficiently addressed previous identified FLRA Inspector General and Gartner & Associate findings and recommendations. In order to comply with the Federal Information Security Management Act of 2002, FLRA management needs to focus on improving information security deficiencies as quickly as possible. The OMB standardized evaluation should be submitted with the Agency Executive Summary due to OMB on October 2004.

OMB has specifically identified FISMA reporting requirements for agencies and Inspectors General.

I am attaching the Inspector General review for inclusion in the Agency 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 2004
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 Computer Information Security Audits conducted in 2001 and 2003 revealed that the FLRA had substantial security vulnerabilities in its Computer Information Program. The Inspector General 2004 evaluation of FLRA=s information technology revealed that management had begun to focus on its technology and computer information security programs, however, several critical issues still exist. An example relates to an extensive amount of e-mail scams including pornographic material.

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.

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 still does not maintain a proper information security program The FLRA=s information technology systems are essential for its mission and still needs more attention to ensure that there is no loss, misuse, unauthorized access, or modification of the information in the information technology system. 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, 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 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/Acting Director of Information Resource Management) who reports to the CIO/Acting Director of Information Resource Management and carries out the security information responsibilities. The FLRA has not yet complied with these requirements. The FLRA has not yet implemented 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 FLRA CIO/Acting Director of Information Resource Management currently has contractors working on implementing a new network (Windows 2000) in September 2004. After the network is implemented throughout the FLRA, appropriate filters are planned to be added.

The FLRA CIO/Acting Director of Information Resource Management does perform annual review, the FLRA computer information systems and has properly submitted required FISMA quarterly reports. The FLRA systems are not yet certified or accredited but the FLRA CIO/Acting Director of Information Resource Management is focusing on this requirement. The same is true for the completion of the migration to Windows 2000 and elimination of cams and viruses. The FLRA still does not have policy for implementing patches to the network servers and does not have a test lab to assess the effect of patches which are implemented. Also, the FLRA has no policy for change control or systems development life cycle policies which address configuration management and guiding the acquisition and maintenance of hardware, software and commercial, off the shelf products. By not having this plan, the FLRA has a high risk for cost overruns, rework, implementation failures and other substantive problems that are likely to lead to the waste of resources. The FLRA did hire an additional computer technology employee during FY 2004 as well as contractors to address FLRA=s material weaknesses. The Information Resource Management staff, still lacks an Information Security Officer, and has not separated of duties of the CIO/Acting Director of Information Resource Management who has also been the Acting Director of the Information Resource Management Division for over 2 2 years.

Policy drafted by the FLRA CIO/Acting Director of Information Resource Management includes the FLRA CIO/Acting Director of Information Resource Management has also created interim policy for performing the back up of network file sand mail servers, but FLRA is still not in compliance with the NIST Contingency Planning Guide for Information Technology Systems, Back Up Methods. The FLRA has not yet implemented Information Security Continuity of Operations Plans for its major systems and applications to ensure that the network could be restored in the event of a disruption. These are serious risks which could have a severe adverse effect on the FLRA=s operations and mission capability. However, FLRA has begun to address these items. The FLRA also needs to develop and implement formal change control policy which outlines procedures to ensure that system configuration changes are properly documented, authorized, approved and tested prior to being implemented. The FLRA does not have user account maintenance polices to effectively manage user accounts. .

The FLRA CIO/Acting Director of Information Resource Management has addressed several of the recommendations contained in the FLRA IG=s previous information security audits and evaluations. A list of these is attached to this evaluation. During 2004 the FLRA Security Program, system configuration testing was not performed because the FLRA was in the process of migrating to

Windows 2000 and it was not completed. This testing is planned to be conducted in FY 2006

The FLRA still has not implemented adequate annual, standardized training for agency employees (and contractors) and has not yet implemented an agency-wide system POA&M (related to function.) Without a fully implemented system security program plan, responsibility and accountability with respect to information security internal controls are not sufficient. Also, as previously mentioned, the FLRA still needs to improve its filter and patch management to reduce penetration risks and implement appropriate software to support penetration testing.

Over this next year, the FLRA must still focus on creating a risk based, cost-effective approach to secure its information systems, and resolve its identified information technology security weakness and risks as well as protect its information technology systems against future vulnerabilities and threats. The FLRA must still focus on improving its computer technology and information security. The CIO/Acting Director of Information Resource Management should 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 implementing appropriate training needs.

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 FISMA compliance has affirmed that the FLRA information security systems are being addressed. However, FLRA management must continue to focus on this program to improve it and eliminate its high risks and major deficiencies.

Audit of Computer Information Security **February 2001**	**1 a. Fund, develop, implement an information security program that complies with OMB Circulars A-123, A-127, and A-130.be determined**	**9/30/2002** **Revised date to**	**Open**
	1 b. Establish senior management oversight committee to Demonstrate senior management=s commitment to and Support of an effective, efficient security program.	9/30/20/02 1/2002	Closed
	1.c. Ensure procedures are established to monitor/report FLRA=s progress in resolving weaknesses and developing an efficient/effective information system security system.	9/30/02	Closed
	2 a. Establish a security awareness program that all employees must attend annually.	**2/30/02** **Revised date to be determined**	**Open**
	2b. Delegate authority to IRMD that clearly assigns responsibilities and requirements; coordinate information Security control with systems outside IRMD and assist/control with other Program offices during development and implementation if new systems and enhancements to existing systems.	**9/30/2002** **Revised date to be determined**	**Open**
	2.c. Revise current instructions for HRD and BFD to include security administration responsibilities for respective systems & require coordination with IRMD.	**9/30/2002** **Revised date to to be determined**.	**Open**
	2d. Ensure that system owners and program offices perform periodic risk and vulnerability assessments	**9/30/2002** **Revised date determined.**	**Open**
	2e. Develop & establish agency-wide information security policy through the consolidation of existing instructions.	**9/30/2002** **Revised date to be determined.**	**Open**
	2f. Centralize management responsibilities for development of security policy procedures and practices, but retain daily security administration with program offices.	9/30/2002	Closed
	2g. Develop procedures to maintain a current inventory of authorized users for each system and for remote access.	**9/30//2002** **Revised date to be determined**	**Open**
	2h. Define rules of behavior for each system based in management=s defined level of acceptable risk.	**9/30/2002** **Revised date to be determined**	**Open**
	2i. Develop procedures to ensure that security Officials, systems, and data owners establish and formalize procedures for granting appropriate access and system privileges.	**9/30/2002** **Revised date to be determined**	**Open**
	2j. Conduct an agency-wide assessment Of information contained within the various systems to identify/classify the sensitivity of information an the security level needed.	9/30/2002	Closed

	2k. Formalize incident response procedures and processes to identify/report on apparent/actual security breaches. Include instructions on proper procedures for reacting to security breaches in security awareness program.		**9/30/2002 Open Revised date to be determined**
	2l. Develop procedures for periodically evaluating User privileges and in granting initial access and privileges to systems software and data.		**12/30/2002 Open Revised date to be determined**
	2m. Obtain new remote access software sufficient to preclude unlimited remote dial in access to FLRA network.		**3/31/02 Open Revised to 09/30/2002**
	2n. Obtain new software to monitor eternal access to the network and alert IRMD security Personnel of suspicious activities.		3/31/2002 Closed
	2o. Dedicate funding to identify, review, and evaluate critical business functions for developing a business contingency and recovery plan.		**4/30/03 Open Revised date to be determined**
	3a. Document procedures for programmers= access to the production environment and management=s compensating controls to detect unauthorized activities.		**12/30/01 Open Revised to 12/31/2002 Revised target date to be determined**
	3b. Document the network configuration: hardware4, software, and security controls; client server and Oracle databases; and systems security controls.		**4/30/03 Open Revised to 6/30/2003**
	3c. Develop a System Develop Life Cycle Methodology compliant with OMB and NIST requirements for developing new systems and enhancing existing systems		**4/30/2003 Open Revised date to Be determined**
	4a. 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.		Closed 3/17/2003
<u>Audit of Computer Information Security</u> <u>February 2001</u>	**1 a. Fund, develop, implement an information security program that complies with OMB Circulars A-123, A-127, and A-130.**		**9/30/200 Open Revised date to be determined**
	1 b. Establish senior management oversight committee to Demonstrate senior management=s commitment to and Support of an effective, efficient security program.		9/30/20/02 Closed 1/2002
	1.c. Ensure procedures are established to monitor/report FLRA=s progress in resolving weaknesses and developing an efficient/effective information system security system.	9/30/02	Closed
	2 a. Establish a security awareness program that all employees must attend annually.	**2/30/02**	**Open Revised date to be determinedb.**
	Delegate authority to IRMD that clearly assigns responsibilities and requirements; coordinate information Security control with systems outside IRMD and assist/control with other Program offices during development and implementation if new systems and enhancements to existing systems.	**9/30/2002**	**Open Revised date to be determined**
	2.c. Revise current instructions for HRD and BFD to include security administration responsibilities for respective systems & require coordination with IRMD.	**9/30/2002**	**Open Revised date to be determined**.
	2d. Ensure that system owners and program offices perform periodic risk and vulnerability assessments	**9/30/2002 Revised date to**	**Open**

and certify systems.	**be determined.**	
2e. Develop & establish agency-wide information security policy through the consolidation of existing instructions.	**9/30/2002 Revised date to be determined.**	**Open**
2f. Centralize management responsibilities for development of security policy procedures and practices, but retain daily security administration with program offices.	9/30/2002	Closed
2g. Develop procedures to maintain a current inventory of authorized users for each system and for remote access.	**9/30//2002 Revised date to be determined**	**Open**
2h. Define rules of behavior for each system based in management=s defined level of acceptable risk.	**9/30/2002 Revised date to be determined**	**Open**
2i. Develop procedures to ensure that security Officials, systems, and data owners establish and formalize procedures for granting appropriate access and system privileges.	**9/30/2002 Revised date to be determined**	**Open**
2j. Conduct an agency-wide assessment Of information contained within the various systems to identify/classify the sensitivity of information an the security level needed.	9/30/2002	Closed
2k. Formalize incident response procedures and processes to identify/report on apparent/actual security breaches. Include instructions on proper procedures for reacting to security breaches in security awareness program.	**9/30/2002 Revised date to be determined**	**Open**
2l. Develop procedures for periodically evaluating User privileges and in granting initial access and privileges to systems software and data.	**12/30/2002 Revised date to be determined**	**Open**
2m. Obtain new remote access software sufficient to preclude unlimited remote dial in access to FLRA network.	**3/31/02 Revised to 09/30/2002 to be determined**	**Open**
2n. Obtain new software to monitor eternal access to the network and alert IRMD security Personnel of suspicious activities.	9/2001	Closed
2o. Dedicate funding to identify, review, and evaluate contingency and recovery plan.be determined	**4/30/03**	**Open**

	3a. Document procedures for programmers= access to the production environment and management=s compensating controls to detect unauthorized activities.	**12/30/01 Revised to 12/31/2002 Revised target date to be determined**	**Open**
	3b. Document the network configuration: hardware4, software, and security controls; client server and Oracle databases; and systems security controls.	**4/30/03**	**Open Revised to 6/30/2003**
	3c. Develop a System Develop Life Cycle Methodology compliant with OMB and NIST requirements for developing new systems and enhancing existing systems	**4/30/2003**	**Open Revised date to Be determined**
	4a. 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.	12/30/01 Revised to 9/31/03 3/17/2003	Closed
Internal Review of the **<u>Office of the General Counsel=s</u>**			
	3. To acknowledge and comply with information security and assurance, case files should be marked with AFor Official Use Only@ orAConfidential@ and be locked after hours and during major time absences of investigation agents to protect confidentiality/sensitivity of information.	10/02	3/02 Closed
	6. 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**	**Open Awaiting decision of new General Counsel**