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

MEMORANDUM

TO: Dale Cabaniss
Chairman, FLRA

FROM: Francine Eichler
Inspector General

DATE: September 12, 2007

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
(c) NIST Special Publication 800-100
(d) NIST Special Publication 800-53

The Office of Management and Budget (OMB) has provided 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, by a contractor 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.

This 2007 FISMA evaluation was conducted by the FLRA Inspector General in compliance with the Quality Standards for Inspections and Government Auditing Standards for Federal Inspectors General. As in 2006, in spite of several requests by the FLRA Inspector General for FISMA related information (which was known to be prepared in a timely manner by the former FLRA Chief Information Officer (CIO)/Director of Information Resource Management), the FLRA Executive Director did not provide the former CIO or her own response for the requested subject information to the Inspector General. This year, the Inspector General conducted a FISMA survey with all FLRA managers in order to address current issues properly and provide FLRA Management with related issues from other FLRA line managers. This survey information is included in this Inspector General FISMA evaluation and is also being provided to you. This FLRA Inspector General

Evaluation should be submitted with the FLRA's Executive Summary due to OMB not later than October 2, 2007.

If you have any questions, please contact me at Extension 7744.

2007 Federal Labor Relations Authority Inspector General
FISMA Evaluation

Methodology:

One of the main objectives of the FLRA Inspector General's evaluation of the FLRA's adherence to FISMA requirements was to again review the correction of previous reported material weaknesses and to address the level of confidentiality, integrity and risk controls of the FLRA's information security system. This review was performed in compliance with the requirements of the Inspector General Act of l978, as amended as well as FISMA and E-Government requirements. This included the:

- Assessment of security vulnerabilities;

- The protection of computer resources;

- The assurance that one individual does not perform or control all aspects of computer operations or have unauthorized access to records;

- Assessment of disruptions to a system related to intentional or unintentional actions by employees and;

- Evaluation of the FLRA's information security program.

Background:

In 2007, the FLRA Inspector General requested budget funds from the FLRA Chairman to support an Office of Inspector General independent and objective contracted information technology audit focused on technology and security. No response to several requests was provided even though several previous contracted information security technology audits conducted through the FLRA Inspector General indicated material weaknesses. Nevertheless, this evaluation did focus on information security controls to ensure that misuse, fraudulent use, improper disclosure and destruction have been diminished from previous years. Unfortunately, in 2007, there were no significant actions performed. Information security policies created by the former Chief Information Officer/Director of FLRA Information Resource Management in 2005 have still not been implemented by FLRA even though the former CIO/Director of Information Resource Management created an extensive amount of information security technology policy in 2005.

Facts:

Information security requirements involve assessing risks, developing and implementing policies, procedures and security plans, providing security awareness training, testing and evaluating actions which address information security problems, detecting, reporting and responding to information security deficiencies and ensuring continuity of operations.

This FLRA 2007 Inspector General Review indicated that progress has taken place to support correcting previously reported weaknesses identified by the Office of Inspector General. The current status of the FLRA's information security and computer reliability are still not totally resolved, however improvement in the entire basic system has been addressed by management. The FLRA has still not addressed the requirement for a Security Officer and updated security information policy has still not been approved by FLRA management. Several Information Resource Management employees affirmed that no certification and accreditation process has been created or implemented which includes adherence to existing FISMA, OMB or NIST information technology security policy, guidance and standards. The last update to NIST requirements for security configuration occurred in 2005 and has not been updated since then. In order to meet FISMA, OMB and NIST requirements, the FLRA needs to provide a larger budget for information security and technology and update the skills of Information Resource Management staff so that they can address current vulnerabilities.

This FLRA Inspector General 2007 FISMA Review revealed that the FLRA has not specifically defined how many systems relate to the FLRA nor was an evaluation of impact levels reviewed or categorized regarding FLRA's information security systems. During 2007, no security control testing has occurred. This review did affirm that the FLRA has and adheres to Privacy Impact Policy. Security Awareness Training was provided for all FLRA employees on August 23 and August 29, 2007.

This review did affirm that the amount of spams have diminished but have not totally been eliminated. This review affirmed that in August 2007 the FLRA's security system began once again to issue Spam Quarantine e-mails to FLRA employees stating the e-mailed messages removed because they appeared to be spams and would be permanently deleted in 13 days. This Spam Quarantine Summary also provided employees the direction to access these spams prior to them being removed if they felt it was necessary.

This review also affirmed that the log on information security process is secure for each employee. There was no indication that a 2007 risk assessment has taken place or that

any systems were reviewed for security controls or contingency systems or that a Plan of Action had been created. This review did affirm that the FLRA has developed an inventory of major information systems which is updated annually. An extensive amount of Information security policy was created by the former FLRA CIO in 2005 but has still not been approved and implemented. The security policy on the FLRA intranet is outdated. No information security disaster recovery plan has yet been created. The current patch program used by the FLRA is not as effective as it should be but it has eliminated several previous problems and these needs to be considered a good action.

FISMA SURVEY

During FY 2007, the FLRA Inspector General conducted a FISMA survey with FLRA managers to provide specific issues related to information technology security. This survey revealed the following issues, some of which need to be addressed:

- Most FLRA Headquarters managers felt necessary security controls were in place and they did not find many obvious errors.

- Most FLRA managers were aware that FLRA Security Information Technology policy was on the intranet but it was outdated. The few FLRA managers who were unaware of the policy went on line (as a result of a related question for this survey) and also stated the policy was outdated and not relevant to the current FLRA agency.

- The majority of FLRA managers stated there was no mechanism in place to identify what internal controls have been implemented and provided.

- The FLRA has no Information Resource Management feedback mechanism since the FLRA Technology Committee has been eliminated. Most FLRA managers stated that this Technology Committee was excellent and responsive to technology and security

issues with FLRA employees. They also stated that the IRM Governance Board which was established after the Technology Committee was canceled was also stopped and this also diminished their interaction in information technology.

- Most managers stated that basic security controls have been implemented to the information technology system over the last two years which has helped both managers and employees. They all affirmed that the required activities to sign in and enter a required password to FLRA computers were very good to support security.

- The former FLRA CIO and staff have been proactive in addressing security deficiencies but much of what they recommended was not supported by senior management. FLRA managers basically felt that Information Resource Management employees were sincere and tried to respond to issues brought to their attention but they were not empowered or supervised in a proper way to address the issues.

- The spam guarantee software implemented in December 2006 has diminished spams significantly for FLRA managers as well as employees.

- In 2006, new computers were provided to FLRA Regional Offices without consulting with Regional Office managers to ensure necessary requirements were addressed. The new FLRA Regional Office computers have several different versions of Flash players. Employees can search for information on their new laptops but can not transfer it down to their computers.

- Some FLRA managers and employees can access e-mails from home computers and some can not. Access to work files from home computers was eliminated for just about all FLRA employees during this administration when the previous file server was changed to a National Office File Server.

- All Regional Office computers work through FLRA Headquarters' information technology system. All computer actions come through the Washington D.C. computer system before they appear on the Regional Office computers. Because of this system, all Regional Office time elements relate to and state Eastern Time. FLRA Regional Office Managers also stated that there was no way to access their computer systems when they were traveling because they had no wireless internet capability or dialup access.

- Although the former Information CIO/Resource Management Director stated that she conducted security technology assessments yearly, FLRA managers stated they did not receive such assessments. FLRA Headquarters managers affirmed that the former CIO/Information Resource Management met with them annually, but they did not have an assessment conducted annually. All FLRA managers affirmed that they periodically checked with their employees to make sure that their computer systems worked properly. Several managers stated that they checked their employee's computers every day after work to make sure they were properly closed.

Conclusion:

Information Security Technology is a necessary and critical consideration for the FLRA to carry out its mission especially because there is significant Federal external access to the FLRA system. Updated policy for information technology needs to be implemented to ensure that FLRA employees know what is required for this program and that it address FISMA, OMB and NIST requirements and standards more properly.

FLRA information security technology still requires the elimination of several previously defined FLRA Inspector General Audit risk assessments which definitely affects the FLRA's capability of carrying out its mission in a proper manner. Progress has been made by the FLRA developing a better information security system compared to previous years, however, FLRA management still has several challenges which relate to improving information security processes and programs, protecting website and e-mail information, and working across the FLRA's boundaries.

Although the Inspector General ended up having to conduct an evaluation once again for the FISMA Report, further technology testing and independent efforts are definitely needed to address weaknesses in the FLRA computer technology systems. Information security has been a high risk area in the FLRA as well as the Federal government since l997. It is imperative for the FLRA to permit the FLRA Inspector General to contract and conduct an extensive Information Security audit to provide management with independent and objective findings and recommendations to address vulnerabilities and increase FLRA's adherence to FISMA, OMB and NIST requirements.

As a result of this 2007 FISMA evaluation and Management Survey, the FLRA Inspector General recommends that the following issues be addressed during FY 2008:

1. A Feedback mechanism needs to be established so that FLRA employees can provide their computer information technology and security concerns directly to Information Resource Management and receive timely responses to their concerns personally.

2. FLRA should address compliance with the Government Paperwork Elimination Act so that FLRA's document management infrastructure would support electronic filing of charges and secure communication.

3. FLRA should focus on FISMA, NIST and OMB requirements and support the FLRA Inspector Generals request to have an independent and objective audit focused on information technology and security issues.

4. All FLRA line managers should be constantly involved with Information Resource Management Division to address their computer system issues. Information Resource Management Division employees should have the authority to respond to FLRA managers and employees.

5. To enable work for FLRA management and employees during travel by airplanes and/or taxies, FLRA should consider providing wireless internets and dial-up accesses to laptops taken on travel.