UNITED STATES OF AMERICA
FEDERAL LABOR RELATIONS AUTHORITY
OFFICE OF THE INSPECTOR GENERAL
WASHINGTON, D.C. 20424-0001
1400 K Street, NW
Washington, DC 20424-0001

OFFICE OF THE INSPECTOR GENERAL

2008 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 information security material weaknesses and findings and recommendations 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 evaluation also included the:

1. Assessment of security vulnerabilities;
2. The protection of computer resources;
3. Assessment of FLRA's adherence to E-government requirements;
4. Evaluation of the FLRA's information security program;
5. Required budget to update the FLRA's information security program;
6. Proper external access to FLRA mission related information for Federal and private sector employees and;
7. Response to previous information security findings and recommendations.

Background:

In 2008, 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. A letter dated December 19, 2007 was sent by the former FLRA Chairman to the

Congressional Subcommittee on financial Services and General Government requesting approval to retain 50 percent of the FLRA's fiscal year 2008 unobligated balance so that the FLRA could focus properly on information security improvements. Fortunately, this was approved by the Congressional subcommittee in January, 2008. In 2008 the new Acting Chief Information Officer started focusing on the FLRA's information technology system, ensured the privacy and security of the FLRA Inspector General's system and has spent a significant amount of time properly upgrading FLRA's information security system.

As previously stated in 2005-2007 and now the 2008 FISMA evaluations, Information Technology Security policies created by the former Chief Information Officer/Director of FLRA Information Resource Management in 2005 have still not been implemented by the FLRA even though the former CIO/Director of Information Resource Management created an extensive amount of information security technology policy in 2005. At this point, new Information Security management should review all of the 2005 policies, update or revise them and ensure that they are implemented in FY 2009.

Facts:

The FLRA Inspector General has completed an independent evaluation of information security pursuant to requirements contained in the FISMA Act. This year's review assessed compliance with FISMA, information security policies, procedures and guidelines and FLRA's progress toward correcting weaknesses and risk assessments from previous years.

During 2008, the Chief Finance Officer/Acting Chief Information Officer had the Department of Interior National Business Center conduct an inspection of the FLRA's information technology systems to provide specific information issues that needed to be addressed during FY 2009.

The FLRA Inspector General's Information Security evaluation affirmed that some progress in developing the FLRA Information Security Program and addressing some information security issues has occurred over the past year. Although some progress has occurred, there are still many areas where improvement is still needed. Successful FISMA implementation requires Federal Agencies to adopt enterprise-wide security strategy where agency missions and business functions support security requirements and related safeguards. Based on the current and prior year FLRA FISMA reviews the FLRA has not yet made the proper shift to a risk based approach and has not fully implemented information security responsibilities. However, the fact that the FLRA is a small agency with a limited and reduced staff and minimal financial resources support for Information Technology Security, it is the FLRA Inspector General's opinion that the FLRA will not be able to meet all required standards even during FY 2009.

Nevertheless, the FLRA should address NIST compliance and risk-based information security programs one step at a time. This will comply with OMB requirements and strengthen the FLRA's security issues even though it will take several more years to accomplish 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 involving detecting, reporting and responding to information security deficiencies, and ensuring continuity of operations.

This FLRA 2008 Inspector General FISMA 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 current management. The FLRA has still not addressed the requirement for hiring or appointing an Information (or regular) Security Officer which has been recommended by the FLRA Inspector General during this entire administration. The last update to NIST requirements for security configuration occurred in 2005 and has not been updated since then although FLRA Information Security Technology employees are working on these related issues. 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 2008 FISMA Review revealed that the FLRA has defined that FLRA network servers are running under Windows 2003 operation systems and desktop and laptop computers are running under Windows XP operation systems. Windows 2000 operation systems are still in use in a few old desk tops. A technical evaluation of impact levels reviewed or categorized regarding FLRA's information security systems is being addressed. During 2008, prior to the new Acting Chief Information Officer, no security control testing had occurred. However, this review did affirm that the FLRA has and adheres to Privacy Impact Policy. Security Awareness Training was provided for all FLRA employees in 2007 but has not yet been provided for 2008.

This 2008 review did affirm that the amount of spam's had reduced but have not totally been eliminated. This review affirmed that the FLRA's security system issues Spam Quarantine e-mails to FLRA employees stating that the e-mailed messages were removed because they appeared to be spam's and would be permanently deleted in 13 days. This Spam Quarantine Summary also provided employees the direction to access these spam's prior to them being removed if they felt it was necessary.

This review also affirmed that the log on information security process is still secure for each employee. There was no indication that a 2008 risk assessment has taken place or that a Plan of Action and Contingency Plan have been created. As

previously stated, the FLRA's security policy on the FLRA intranet is outdated. Also, the FLRA has not yet fully implemented its security program throughout the Agency. Also, there is no information security technology stated on the FLRA's strategic plan. 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.

The FLRA Inspector General's evaluation identified the following 2008 issues:

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. A few FLRA managers who were unaware of the policy went on line (as a result of the 2007 FLRA Inspector General's Information Technology Survey) and stated the policy was outdated and not relevant to the current FLRA agency. This is still true in 2008 and has not yet been addressed. Therefore, the FLRA does not demonstrate adherence to documented FLRA policy regarding IT Security or wireless Communications Policy.

1. The FLRA has still not produced Contingency Plans for FLRA systems. Nor has it appointed a Senior Information Officer or Information Security Officer. As previously mentioned, the FLRA has not yet included information technology and E-government in its FLRA Strategic Plan.

2. There is still no mechanism in place to identify what internal controls have been implemented and provided, however, FLRA management and employees have been made aware of several new security issues that have been implemented and the required activities to sign in and enter a required password to FLRA computers have been very good to support security.

3. The FLRA has no Information Resource Management feedback mechanism since the FLRA Technology Committee has been eliminated. Most FLRA managers stated that the former FLRA 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. Now that NBC will be handling FLRA's information technology, a better environment should be created in FY 2009.

4. 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.

5. 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**. They were traveling because they had no wireless internet capability or dialup access.

6. 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.

7. Although FLRA Information Resource Security employees are now focusing on correcting former FLRA Inspector General Information security recommendations, FLRA former management did not perform sufficient follow up activities identified by previous auditors and the FLRA Inspector General, however, current new FLRA management is focusing on improving all required Issues, and will explain why any of the FISMA recommendation are no longer necessary.

8. Security Technology is a necessary and critical consideration for the FLRA to carry out its mission especially because there is significant external Federal Agency and Union access to FLRA's internet 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. Understanding the overall effectiveness of security controls implemented in the information system is essential in determining the risk to FLRA's operations and assets to FLRA individuals and other organizations resulting from the use of the system. Because the FLRA Inspector General did not receive a system inventory, an accurate account of the **i**nformation system inventory can not yet be provided.

9. Now that the FLRA is properly focusing on information technology, risk assessments should be conducted and updated at least once a year or whenever the system undergoes a significant change. If additional corrective actions are needed as a result of the risk assessment, they should be added to the POA&M. Although the FLRA Inspector General will provide corrective actions to the FLRA as a result of this FISMA evaluation, the FLRA Acting Chief Information Officer should also create 2009 policy which will list corrections that will be addressed in 2009 and estimate the dates of other requirements.

10. 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.

11. 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 FISMA audit in 2009 to provide management with independent and objective findings and recommendations, to address vulnerabilities and increase FLRA's adherence to FISMA, OMB and NIST requirements.

OMB Reporting Template for Inspectors General:

1. FISMA System Inventory

The FLRA currently has 3 Agency technology information systems. Network servers are under Windows 2003, desktop and laptop computers are under Windows XP operating systems and a few old desktops are Windows 2000.

2. Certification and Accreditation, Security Control Testing and Contingency Plan Testing.

The numbers of systems certified and accredited are Security control testing was performed this year in response to the FLRA Inspector General's request.

3. Evaluation of Agency Oversight of Contractor Systems and Agency System Inventory.

The FLRA information systems do not yet meet all of the requirements of FISMA, OMB policy, NIST guidelines, security and agency policy. Current management will be addressing these issues in 2009 as much as possible. The small size of the Agency and low available information security budget will limit the ability to address all requirements, but as much as possible will be addressed. The FLRA is currently developing an inventory of major information and security systems which will improve the FLRA's contracted system. Recently, FLRA has contracted with NBC to handle information technology for the FLRA.

The FLRA Inspector General's review affirmed that the amount of FLRA computer systems were Microsoft Windows 2003 for most servers, Microsoft Windows NT for a few ad-hoc servers, Oracle database 10g R2 for agency wide

case tracking systems. Desktop laptop work stations involve Microsoft Windows XP operation systems. Microsoft Office suite 2003, Adobe Acrobat Reader 7, Oracle 6i forms and reports runtime software. There is still some old desktop/laptop systems located at some Regional and Headquarters Offices without disposal.

4. Evaluation if a Plan of Action and Milestones (POA&M)

The FLRA is currently developing and will be managing through NBC an Agency wide plan of actions and milestone processes which will incorporate all identified information technology security weaknesses in the FLRA information technology systems. When information security systems are identified, they will be addressed as soon as possible. As previously stated, the essential actions that must be addressed for the FLRA in 2009 include the creation of information technology, security instructions, Contingency planning, address all previous and current FLRA Inspector General Information technology findings and recommendations, and provide training and proper related information to FLRA employees.

5. IG Assessment of Certification and Accreditation Process

The FLRA has no adherence to existing policy, guidance and standards because none of this was implemented by the former current administration Head of the Agency. The FLRA Inspector General still has to rate the quality of the FLRA's certification and accreditation as poor, however, as stated many times, the new current Agency Senior Administrative Employees are aware of the situation and are devoted to improving the security plan, testing and evaluation, handling relevant information technology incidents, providing necessary security awareness training and addressing security configuration.

6. IG Assessment of the Privacy Impact Assessment Process

The FLRA has no stated or written policy, guidance or standards regarding the Privacy Impact Assessment Process. Hopefully, it will be addressed and implemented during 2009.

7. IG Assessment of Progress of the Agency Privacy Program

The FLRA created a safeguard with the National Business Center which includes protecting personal identifiable information from external accessibility. This implementation started in 2006 when additional Human Resource requirements were contracted by the FLRA to the National Business Center. So far, the FLRA Inspector General has not discovered or been informed that violations to Information security have occurred during 2008.

8. Configuration Management

The FLRA does not have an Agency wide security configuration policy which responds to the Breach of Personally Identifiable Information, therefore no qualitative assessment has been made during 2008.

New Federal Acquisition Regulation 2007-004 which modifies all contracts related to common security is available from the National Institute of Standards and Technology website. The proximate extent to which the FLRA has applicable systems that implement security configurations should be administered and handled properly in 2009'.

9. Incident Reporting

The FLRA has no Agency policy regarding incident reporting; however the FLRA Inspector General does have policy regarding reporting improper issues. FLRA employees have not reported such issues to the FLRA Inspector General during 2008. The same relates to reporting of issues regarding law enforcement issues.

10. Security Awareness Training

On September 24, 2008, the FLRA provided security awareness training for all FLRA employees.

11. Collaborative Web Technologies and Peer to Peer file Sharing

The FLRA has no subject policies regarding the use of collaborative web technologies. This subject matter also has not been brought up in FLRA ethics training or any other FLRA training in 2008.

12. E-Authentication

The FLRA has not identified all e-authentication applications in accordance with NIST Special Publication 800-63. As previously stated, FLRA Information technology will now be handled by the National Business Center and this issue should be addressed and implemented in 2009.

RECOMMENDATIONS:

As a result of this 2008 FISMA evaluation and Management Survey, the FLRA Inspector General recommends that the following issues be addressed during FY 2009:

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 senior and 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. The FLRA Acting CIO should provide information technology security reporting to the Head of the Agency on a quarterly basis that reflects the requirements of FISMA.

6. The FLRA Acting CIO should provide information technology security training to all FLRA employees at least on a yearly basis.

7. The FLRA Acting CIO (or NBC) should hire a vendor to create an FLRA Contingency Plan in 2009 which should be used to address plans, procedures and technical measures that enable the recovery of FLRA's Information technology systems, operations and data on a yearly basis.

8. The FLRA Acting CIO should begin in 2009 to create and/or update and implement FLRA Information Technology Instructions and add Information Technology to its Strategic Plan.

9. Although current management has started to focus on and improve the FLRA's Information Resource Technology System, weaknesses and identified risks should be prioritized and addressed during 2009 incompliance with OMB POA&M criteria.

10. Spam's need to be eliminated more extensively.

11. An FLRA Contingency Plan has still not been created but should be addressed in 2009.

Date Issued: September 26, 2008