UNITED STATES OF AMERICA

FEDERAL LABOR RELATIONS AUTHORITY

OFFICE OF THE INSPECTOR GENERAL

WASHINGTON, D.C. 20424-0001

2007 FLRA MANAGEMENT FISMA SURVEY RESULTS

INTRODUCTION:

In July 2007, the FLRA Inspector General conducted a Federal Information Security Management Act survey provided to all FLRA managers. All managers, except 3 responded. As a result of this survey, the following majority information is being provided to the Chairman, FLRA so that best practices as well as concerns are noted and hopefully will be addressed.

SURVEY RESULTS:

Most FLRA mangers felt that the former CIO/Information Resource Management Director and current staff were proactive in addressing information security controls and basic security activities but have not been supported by senior FLRA management. Most Headquarter managers felt that proper basic information security controls are installed and their information technology systems have no major errors. Most Headquarter managers had direct and rapid contact and response with Information Resource Management staff as well as productive interaction. Regional Office Managers did not have a significant amount of contact with either the Information Resource Management Director or Staff. Although they previously received daily notices via e-mails from Information Resource Management regarding information technology issues, they no longer receive such notices and know very little of what controls are in place and what is working.

Most FLRA managers stated that lots of hardware and software decisions are made without input from those who actually use the equipment. FLRA managers basically felt that Information Resource Management employees were sincere and tried to respond to issues brought to their attention but did not feel they were empowered or supervised in a proper way to address any issues. FLRA managers felt that even though there has been some improvement to information security technology, the FLRA has a long way to go.

Although the former FLRA CIO/Information Resource Management Director stated to the FLRA Inspector General that information security technology assessments were done yearly, FLRA managers stated they did not receive annual assessment. Headquarters managers affirmed that the former CIO/Information Resource Management met with them annually but they did not consider it an assessment. Regional Office managers stated that they did not have assessments annually at all. Most FLRA managers affirmed that, as supervisors, they periodically checked with their employees to make sure there computer systems were working properly. Several FLRA managers stated that they checked daily to make sure that at the end of the day all computers were signed out and closed.

FLRA managers as well as employees had information security training in 2004, 2005 and 2006 but have not had such training so far in 2007 except for the Administrative Judge Office employees. However, training was provided on August 23 and 25 after this survey were completed. In addition, since the former CIO/Information Resource Management Director or staff do not provide information to FLRA manager or employees, FLRA managers felt that Information Resource Management focuses on "checking in on the box" without any reference to the users.

Several Regional Office managers stated that they were having problems with their new laptops which included not being able to pull down any external information to the laptop even though they could search on it. A few Regional Office managers stated that their laptops were heavy and it was difficult for them to carry. They also stated that there were different versions of Flash players on their lab tops which made getting information from other government websites difficult. Also, there is no access to the systems if in a travel status because the new Regional Office computer systems do not have a wireless internet capability nor dialup access.

Regional Office managers stated that they needed more direct contact with Information Resource Management. They stated that everything they do has to go through Headquarters. If a file is searched for on a Regional Office computer, when the document is opened up, the computer has to seek and obtain the file from a Headquarters computer. Since the Regional servers were moved to Headquarters, their systems are very slow and sometimes non responsive. Also, the integration of computer and telephone systems has resulted in significant communication shortcomings in the past two years. Placing the services at Headquarters also applies to printing out documents which can take a long time (over 10 minutes) because print outs come from all Regional Office computers and are addressed in the order they are received.

Most FLRA managers referred back to the to the FLRA Technology Committee and IRM Governance Board which no longer have the authority to meet (stopped in 2003) or assist any FLRA managers or employees with information security technology issues. Several FLRA managers stated that the current anti spam system software has blocked some spams, other e-mails which are not related to spams are also blocked and requested e-mail information/responses are not received.

Several Regional Office Managers stated that FLRA created a security deficiency when they purchased new computer equipment for the FLRA Regional Offices without any input from the Regional Office Managers to make sure the proper needs of their staffs were addressed. The computer equipment purchased was not what was needed and after several contentious memos over several weeks, additional equipment was purchased to address the issues of concern. The new Regional Office computers were installed in April 2007 and are all on Eastern Time because they must be accessed through an FLRA Headquarters computer.

All FLRA managers affirmed that their security activities performed were signing in and using a password to access their computers. They agreed that the login process appeared to be secure for each FLRA individual but some individuals have difficulty logging in and out and they don't know why. FLRA managers also affirmed that they had another password which had to be used to certify time and attendance.

Most FLRA managers stated they could no longer access the FLRA website from their home computers and some could not even access their e-mails from home computers. The Virtual Private Networking capability that used to be available and allowed FLRA employees to access network drives from their home computers has been disabled. However, even though dial-up is available from laptops, accesses to network drives are extremely slow. Most managers were aware of information security instructions on the FLRA intranet and stated that the instructions were outdated.

INFORMATION TECHNOLOGY ISSUES NEEDING ATTENTION:

Based on this survey, the FLRA Inspector General suggests that FLRA senior management addresses the following issues.

- Feedback mechanism needs to be established so that employees can provide their concerns directly to Information Resource Management and receive responses to their concerns personally.

- FLRA should address compliance with the Government Paperwork Elimination Act so that FLRA's document management infrastructure would support electronic filing of charges and communication with parties. This requirement would better serve the public and facilitate the ability of FLRA to perform its mission and customer needs.

- FLRA line managers should be involved in issues regarding/relating to their computer systems.

- To enable work during travel and allowing FLRA employees to work on their laptops while on flights, wireless internets and dial up access should be created.