



UNITED STATES OF AMERICA
FEDERAL LABOR RELATIONS AUTHORITY
OFFICE OF THE INSPECTOR GENERAL

WASHINGTON, D.C. 20424-0001

**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 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 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 FISRA 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 a 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 Director, Information Resource Management (IRM) , who is also the CIO, 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 worked with two contractors to develop information security policy and procedures, which will strengthen the FLRA's computer information security, when implemented.

The FLRA CIO does perform annual review, the FLRA systems and has submitted required FISMA quarterly reports. The FLRA systems are not yet certified or accredited but FLRA management is focusing on this requirement. The same is true for the completion of the migration to Windows 2000 and elimination of scams and viruses. The FLRA 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 written change control and 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.

During FY 2004 the FLRA Inspector General obtained security audit contractors to once again, conduct a comprehensive Security Program Audit which focused significantly on information security. The audit has revealed that the FLRA has material weaknesses and high risks in several information security areas. Part of the cause of material weaknesses is that FLRA management has not sufficiently addressed corrective actions related to information security that were recommended in FY 2001 and FY 2002. Another significant cause of FLRA's material weakness is the lack of a sufficient and qualified staff, the lack of an Information Security Officer, and the lack of separation of duties of the CIO who has also been the Acting Director of the Information Resource Management Division for over a year and one half..

The FY 2004 Inspector General Audit of FLRA's Security Programs revealed that even though the FLRA currently has interim policy for performing back up of network file and mail servers, it is not in compliance with the NIST Contingency Planning Guide for Information Technology

Systems, Back Up Methods. The FLRA has not yet created/implemented Information Security Continuity of Operations Plans for its major systems and applications to ensure that the network can be restored in the event of a disruption. This is a serious risk which could have a severe adverse effect on the FLRA's operations and mission capability. FLRA's network infrastructure has not yet received documented authorization for the use of each support system by a senior management official via an accreditation or formal certification based on an acceptance of risks identified within the system certification process. 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 also does not have user account maintenance policies to effectively manage user accounts. Periodic reviews should be conducted to examine the levels of access that FLRA employees (and contractors) have to ensure that active user accounts for individuals no longer employed are removed immediately at the time of their departure.

The FY 2004 Inspector General Audit of FLRA's Security Programs revealed that the information contained in the FLRA September 2003 Information Security Program Report to OMB lacked accurate and complete information on the status of the FLRA's Information Security Program nor sufficient internal controls to manage, track and report on the program and effectiveness of the controls.

FLRA reported it had not identified any reportable Information Technology security weaknesses in FY 2002 and identified only one weakness (patch management control) in FY 2003. Both the FLRA Inspector General Audit of FLRA's Information Security Program and the subsequent management study performed by Gartner Consultants were not reported to OMB. Very few of the recommendations contained in the FLRA IG's audit report and Gartner's management report have been resolved. During the FY 2004 Inspector General Audit of 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 will be done in 2005.

The FLRA still has not implemented a clear cut operational information security plan, adequate annual standardized training for agency employees (and contractors) and has not yet implemented an agency-wide system POA&M (related to function). The draft operational information security plan reviewed during the FY 2004 Audit of FLRA's Security Program revealed that the current draft lacks several requirements and appendices listed in NIST 800-14 and OMB guidance. Without a fully implemented system security program plan, responsibility and accountability with respect to information security internal controls are not sufficient. Also, the FLRA still needs to improve its filter and patch management to reduce penetration risks and implement appropriate software to support penetration testing. The working relationship between the CIO and FLRA management also needs to be improved. FLRA information security policy and a contingency plan still need to be established. Security training still needs to be provided for all FLRA managers and employees. From the training aspect, the FLRA did provide Windows 2000 training for all employees during FY 2004 but the training did not include information security.

Over this next year, the FLRA must 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 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 Continuity of Operations Plans to mitigate risks associated service disruptions. Policies and procedures need to be implemented training need to be conducted. Senior management needs to focus on the material weaknesses identified by the FY 2004 Inspector General Security Program audit, provide the FLRA Information Resource Management Division with proper staff, including an Information Security Officer, and ensure that budget needs are allocated.

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 continues to have significant deficiencies and a significant amount of material risks. FLRA management must immediately focus on this program to improve it and eliminate 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.	9/30/2002	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.	9/30/2002 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	Open
	Revised date to be determined	
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	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 and certify systems.	9/30/2002	Open
	Revised date to be determined.	
2e. Develop & establish agency-wide information security policy through the consolidation of existing instructions.	9/30/2002	Open
	Revised date to be determined.	
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	Open
	Revised date to be determined	
2h. Define rules of behavior for each system based in management's defined level of acceptable risk.	9/30/2002	Open
	Revised date to be determined	
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	Open
	Revised date to be determined	
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 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	Open
2n. Obtain new software to monitor external 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 Revised date to be determined	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: hardware, software, and security controls; client server and Oracle databases; and systems security controls.	4/30/03 Revised to 6/30/2003	Open
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.	3/17/2003	Closed
<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.	9/30/2002 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 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 be determined.	Open
2d. Ensure that system owners and program offices perform periodic risk and vulnerability assessments and certify systems.	9/30/2002 Revised date to be 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 Open 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	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 external access to the network and alert IRMD security Personnel of suspicious activities.	3/31/2002 9/2001	Closed
2o. Dedicate funding to identify, review, and evaluate critical business functions for developing a business contingency and recovery plan.	4/30/03 Revised date to be determined	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: hardware, software, and security controls; client server and Oracle databases; and systems security controls.	4/30/03 Revised to 6/30/2003	Open
3c. Develop a System Development 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	12/30/01 Closed Revised to 9/31/03 3/17/2003	
vendor payments to the Department of Treasury to a more secure location away from the General work area into an area of limited access.		

Internal Review of the Office of the General Counsel's

3. 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	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	Awaiting decision of new General Counsel	Open