UNITED STATES OF AMERICA

FEDERAL LABOR RELATIONS AUTHORITY

OFFICE OF THE INSPECTOR GENERAL

WASHINGTON, D.C. 20424-0001

September 11, 2002

TO: Dale Cabaniss
Chairman, FLRA

FROM: Francine Eichler
Inspector General

SUBJECT: Inspector General Review of the Federal Labor Relations Authority Security Program, August, 2002

References: (a) Government Information Security Reform Act (GISRA)
(b) OMB Guidance for FY 2002 Security Reviews

As a result of the first year reporting under the Government Information Security Act, the Office of Management and Budget (OMB) has provided specific instructions for Federal Agencies and Inspectors General to report the results of annual security reviews. This year's reporting is based on high-level management measures and requires that Agencies include empirical data that will support the OMB's executive level review. Agencies are required to use the NIST Self Assessment and review all systems. The Agency Executive Summary is due to OMB on September 16, 2002. This year's guidance specifically states that the Agency submit the Inspector General's evaluation and related audits along with the Agency's Executive Summary .

OMB's FY02 guidance focuses on three major areas:

1. Agency progress in remediating security weaknesses identified in FY 01.
2. Disclosing the results of FY 02 reviews and Inspector General Evaluations.
3. Identifying specific performance measures for Agency officials to ensure Accountability for their performance

Attached, you will find the FLRA Inspector General evaluation of the FLRA's Security Program and a copy of the FLRA Inspector General Computer Information Security Audit. Should you need additional information or have any questions, feel free to contact me at Ext. 217.

FLRA Inspector General FY 2002 Security Reform Act Submission
September 11, 2002

Introduction: The Government Information Security Reform Act (Security Act) requires Inspectors General to perform annual independent evaluations of Agency security programs and practices. The FLRA Inspector General generally reviews security controls in all program audits and evaluations. Several security vulnerabilities such as the lack of FLRA security policy, failure to keep legal files in locked facilities, improper use of the Internet, customer violence, lack of employee training in security and admission of non-FLRA employees into the FLRA office without validating who they are and who they are planning to meet with, have all been surfaced in previous FLRA Inspector General program audits and evaluations. 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 focus on its security programs to ensure protection for all FLRA resources and assets.

As a follow-up to the Inspector General audit recommendations, FLRA management engaged the services of a 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.

After the September 11, 2001 disaster, FLRA management also focused on the weaknesses in its physical and personnel security program. A Headquarters security committee, Coordinating Committee on Emergency Procedures (CCEP) was established and charged with the responsibility of preparing security guidance and training for the FLRA employees which would include contemporary security issues including terrorism, biological warfare and cyber security. An Information Resource Management Governance Board (IRMGB) was also created to serve as a senior management advisory committee to the Chairman and develop a strategic plan for information resources. The existing FLRA Technology Committee's responsibilities were broadened to include research on specific technology issues for the IRMGB.

Over this past year, FLRA leadership has prioritized information security as well as personnel security and has taken actions which support some of the Office of Management's Information Security Goals. These goals and recent FLRA actions to achieve them are:

1. Increasing senior management attention: The FLRA has addressed this ongoing goal.

2. Establish security information performance measures for managers. The FLRA has not addressed this goal.

3. Improve security information education and awareness. FLRA has done this by creating a CCEP Committee and providing several security training sessions however, employee attendance has been minimal. Senior management must make this training

mandatory for all personnel. and require annual security training to keep all personnel aware of current and ongoing security requirements. Security training is also provided to new employees during FLRA Orientation Sessions.

4. Integrate security information into Agency capital planning and investment controls.

The FLRA has not yet made security information a specific part of Agency wide capital (strategic) panning and capital investments. It is, however, a part of the FLRA's Information Resource Management Division's program planning.

5. Improve security of contractor services. The former FLRA Director, Administrative Services Division has made this a part of the FLRA contracting process but has not documented this requirement in the Agency's contracting policy.

6. Improve ability to detect attacks and share information with other Federal agencies.

The FLRA has an accessible website, is active with the Small Agency Council and has involved several other Federal agencies located in the Westory Building in drafting a standardized Emergency policy for the entire building's occupants. The FLRA has been updating its computer technology software systems to provide a common level for information security. The FLRA Inspector General has advised the FLRA Information Resource Management overnice Board that concurrent with the focus on improving FLRA's information security, the FLRA must focus on E- Government objectives and ensure that all current and future approved actions will comply or can be adapted to E-Government requirements.

A. General Overview:

2. Agency Security Programs and Operations Reviewed by the Inspector General

(1) FLRA Security Program

The FLRA Security Program is not yet sufficient considering the contemporary focus on and need for Homeland Security. The FLRA does not yet maintain an agency-wide proactive security program, in spite of its intent. The FLRA's only implemented Security Program Instruction focuses on employee suitability and has not been updated since l984. While the Information Resource Management Division (IRM) drafted information security policy several years ago, it has not been issued. Most IRMD information technology security procedures are issued to FLRA employees via e-mail and have not documented official policy. FLRA employees require guidance and training in all aspects of security. Although several training sessions in the form of videos have been provided over the past year, the employee attendance has been minimal. Revised and newly drafted security policies have not yet been approved and implemented, and security performance procedures and measurements have not yet been identified.

Since the September 11 disaster, the level of security at the FLRA has improved and employees have become more knowledgeable of security issues and emergency procedures. The FLRA has proactively involved both Federal agencies and private sector occupants of the Westory Building in preparing security and emergency procedures but they have not yet been officially

implemented. The FLRA has also appointed floor managers for emergency evacuation procedures.

During this past year, the Administrative Services Division (ASD) and CCEP drafted several security policies and procedures which have been sent to the Chairman, FLRA for approval. These included an Occupant Emergency Plan (Emergency Evacuation Plan) and a Personnel Security and Suitability Program. The FLRA has created and coordinated an Intranet site which will enable unified communication for security and emergency information. FLRA employee contact lists have been updated to facilitate the appropriate accounting of all FLRA employees prior to or subsequent to emergency response actions. The FLRA has also reviewed general building security and recommended several improvements to the Westory Building management. The CCEP has submitted two plans for the Chairman's consideration regarding the development of an Agency Continuity Plan.

While the Security Act emphasizes the need for program management security responsibility, the FLRA has not yet provided sufficient security training (computer information, personnel and cyber security) to managers and/or employees to support this requirement. The FLRA has not yet developed specific workable security performance measurements which should be defined and integrated into program management and operations. The fact that FLRA resources are minimal and it has not had a qualified Chief Information Officer (CIO) to oversee and manage information security has definitely affected FLRA's progress in this area. The FLRA also does not have a qualified Security Officer. Previously, the Director of the ASD was assigned this responsibility and turned most security incidents over to the General Services Administration. Fortunately, current leadership has focused on the underdevelopment of FLRA's security programs and actions have been taken to improve this critical program.

Generally, FLRA security incidents are handled in compliance with the Security Act and General Services Administration requirements. They are followed-up by the FLRA Inspector General and Director, ASD.

(2) Computer Information Security

In accordance with the Office of Management and Budget's (OMB) requirements, the FLRA's IRMD conducted an annual program review of the level and adequacy of computer security for each of its information systems. This report will be submitted with the Agency's annual budget submission. The review included the assessment of 24 FLRA information systems. While the "owners" of these systems are responsible for their security, most FLRA managers currently rely on the Information Resource Management Division for this function because of their own lack of knowledge or interest in this administrative area.

Technology for the FLRA's computer information system is funded through the Agency's Central Services Fund and is not addressed at a component or subcomponent system level. The FLRA IRMD created a Security Self-Assessment Guide in September, 2001. A review of the Information Security Plan of Action (July 31, 2002) affirmed that the FLRA has not yet formulated an Agency-wide security program. Even though information technology resources have been increased by the Chairman, FLRA the Information Resource Division still maintains it has

insufficient resources to properly address computer information security requirements. The FY 2002 Plan of Action and Milestones do not indicate the number of resources still required. Although both the Inspector General Audit of Computer Information Security (2001) and a private sector management analysis of the Information Resource Management structure (2001) determined that the FLRA's computer security training program was inadequate, an adequate level of security training has not yet been provided to FLRA personnel.

The establishment of an Information Resource Management Governance Board (IRMBG) which is authorized to analyze technology costs and funding allocations for information technology strategies and projects, including information security is a step toward integrating security into capital planning and investments. The FLRA has not yet specifically integrated security into individual program management although several previous Inspector General internal reviews of programs identified weaknesses in this area. However, some progress has been made over this past year in developing a life cycle technology methodology which includes security and is in compliance with the Office of Management and Budget (OMB) and National Institute of Standards and Technology (NIST) requirements for creating new systems and enhancing existing systems.

In August, 2002 Inspector General Review of IRM D's progress in correcting the 22 deficiencies noted in the FY 2002 Computer Security Audit revealed that only 4 out of 22 findings were corrected, 4 were in the process of being corrected and 14 have not been addressed. The Director, Information Resource Management Division stated that the lack of sufficient funding prevented him from correcting these 14 deficiencies. A review of 2 security findings from oversight initiatives in the Office of the General Counsel was also performed. These findings were corrected.

In April, 2002, The Inspector General met with IRMB managers to discuss specific areas that the Inspector General would be looking at for the FLRA Inspector General Security Act submission. This included a request for IRMD to perform intrusion testing and assess its technology security. This testing was not performed as of this date. The Inspector General also reviewed copy of the FY 2002 IRMD NIST Self-Assessment which provided the baseline for IRMD's FY 2002 response to the Security Act. The FY 2002 Assessment was very similar to the FY 2001 Assessment and affirms that the FLRA still has many requirements to fulfill.

(3) Information Resource Management Governance Board

The Chairman, FLRA created the Information Resource Management Governance Board (IRMGB) in February, 2002. The purpose of this Board is to review information technology proposals and provide recommendations for approval or disapproval to the Chairman, FLRA. The Board Members represented the major FLRA components. The Director, IRMD and FLRA Inspector General attend these meetings as non-voting consultants.

The Board was active for the first two months after its creation, did not meet regularly for five months but has recently become reactivated. The FLRA has created a Chief Information Officer position which will Chair the IRMBG and properly manage information security.

(4) Coordinating Committee on Emergency Procedures:

The Chairman, FLRA assigned 11 specific tasks to this Headquarters CCEP as a result of the September 11, 2002 incident. This committee has met twice a month to address these tasks beginning October 1, 2002, which are as follows:

TASK	STATUS
Review, revise, and coordinate with other Federal Agencies and Building management to create a viable Headquarters Occupant Emergency Plan.	Submitted to Chairman for approval
Review existing Occupant Emergency Plans for FLRA Regional Offices.	In progress
Develop an Employee Preparedness Handbook to address emergency situations and relevant Agency procedures.	In progress
Create telephone contact lists to enable appropriate contact and accounting of FLRA employee prior to or after emergency situations.	Completed
Solicit input from Regional Directors on concerns, issues to be addressed by the Continuing Committee for Emergency Procedure.	Completed
Revise, update, FLRA Instruction Number 1600.1A, FLRA Security Program.	Submitted to Chairman for approval
Coordinate a unified communication vehicle for security and emergency notices.	In progress
Recommend/provide employee briefing/training on safety and security issues.	Ongoing
Review general building security and recommend proposed safety and security changes to Westory building management.	In progress
Develop an Agency Continuity of Operations Plan.	Options submitted to Chairman for Approval
Engage in other related activities at the discretion and direction of the Chairman.	Ongoing

As of this date, two of the eleven tasks have been officially implemented. Some security video training has been provided (employee attendance not officially required) to FLRA employees and a telephone contact list has been developed with employee home numbers for emergency contact. The Committee is also currently reviewing Federal Agencies' identification badges in order to address and strengthen the FLRA with its building security.

B. Material Weaknesses in Policies, Procedures and Practices

The FLRA Instruction 16001.A, Security Program was created in l984 and is outdated. A new instruction, Personnel Security and Suitability Program has been created and is being reviewed by the Chairman. This draft instruction states that the Chairman, FLRA will delegate the responsibility of implementing and maintaining the FLRA Security Program to the Executive Director. The Executive Director then delegates the responsibility for supervision and execution of personnel security and suitability programs and compliance with Federal laws and regulations which affect the FLRA's program to the Director, ASD who functions as the FLRA Security Officer.

The FLRA has drafted an Occupant Emergency Plan (Emergency Evacuation Plan) which has been submitted to the Chairman, FLRA for approval. This plan was coordinated with other Federal Agencies located in the same building. The FLRA has not yet identified critical, physical infrastructure assets and interdependencies with different infrastructures nor created an Agency-wide critical infrastructure protection plan (contingency plan). The FLRA has not yet developed remediation plans nor performed a current Agency-wide security vulnerability assessment of Agency technical systems. Several program vulnerabilities have been surfaced through previous Inspector General audits and internal reviews and these are not being addressed sufficiently.

C. Responsibilities of Agency Head

1. Identify and describe specific steps taken by the Agency Head to address Security Act Responsibilities

The Chairman, FLRA created an Agency-wide Security Committee, the CCEP and assigned 11 specific tasks to this Committee, including the development of documented Agency procedures. These are listed in A.2, above.

The Chairman, FLRA has the authority to terminate employees, when deemed necessary for security or suitability reasons. This authority has not been delegated to a lower management level.

2. How does the Head of the Agency ensure that the Agency's Information Security Plan is practiced throughout the life cycle of each Agency system?

An Agency Information Security Plan that integrates with the life cycle of each FLRA system has not yet been implemented.

(a) Did the Agency Head take specific and direct actions to oversee the performance?

of Agency program officials and the CIO to ensure that security plans are updated and practiced?

The Chairman, FLRA has prioritized personnel security, information security and cyber security. The Chairman has recently hired a qualified Chief Information Officer who will report to the Office of the Chairman's Executive Assistant/Chief of Staff and oversee security information performance, implement contemporary policies and procedures and create an Information Security and Contingency Plan.

(b) Has the Agency Head been asked to reallocate existing resources or seek? reprogramming to close security performance gaps following the budget submission. What was the result?

As a result of the Inspector General's Computer Information Security Audit, the results of a subsequent contracted consultation on the FLRA'S Information Resource Management Division structure, the Chairman, FLRA took actions to address the critical vulnerabilities of security program performance which included the increase of resources to increase the work capability of the Information Resources Management Division.

3. How has the agency integrated its information technology security program with its critical infrastructure protection responsibilities and other security programs? Does the Agency have separate staffs devoted to other security programs and are they under the authority of different agency officials. What steps has the Agency Head or other officials taken to eliminate unnecessary duplication of costs and ensure that policies and procedures are consistent and complimentary across the various programs?

Currently, the FLRA Security Program is fragmented. The Director, IRMD is responsible for information security. The Director, ASD is responsible for personnel and cyber security. Both of these managers' report to the FLRA Executive Director. During this past year, an emphasis has been placed on the FLRA security programs. New policies and procedures have been drafted, employees have been offered some training on security issues, and managers are being held responsible for the security of their organizational components. Floor monitors and stair monitors have been designated at the Headquarters to handle emergency situations (collateral duty). The FLRA has taken the lead in drafting policy for all of the Federal and private sector organizations located in its Headquarters building for handling emergency situations. Regional Office Directors are responsible for all security aspects of their Regional Offices. Those Regional Offices located in Federal buildings have Federal Security Officers. The Director, ASD and Director, IRMD are responsible for ensuring that security policies related to their programs are consistent throughout the Agency.

4. Has the Agency undergone a Project Matrix Review? If so, describe the steps the agency has taken as a result of the review. If no, describe how the agency identifies its critical operations and assets, interdependencies and interrelationships and how the agency secures those operations and assets?

The FLRA has not undergone a Project Matrix Review from an agency-wide perspective. However an in-depth analysis of the IRMD was performed in FY 2001 by consultants a FY 2002 Work Analysis of FLRA's management positions is currently being finalized. Both of these initiatives have addressed critical operations, and assets, interdependencies and interrelationships of the Agency.

5. How does the Agency Head ensure that the Agency has documented procedures for reporting security incidents and sharing information regarding common vulnerabilities? Identify and describe the procedures for external reporting. Does the agency participate in GSA's patch authentication and dissemination capability program?

The Chairman, FLRA provided direction for the creation and implementation of internal security policies and procedures. Specific security procedures for this process have not been documented into policy or procedures. The FLRA was informed by GSA that they were developing a program which would facilitate the sharing of information regarding common vulnerabilities. The FLRA has not yet been notified that this program is operational. The FLRA is not aware of the GSA's patch authentication and dissemination capability program. The ASD is currently pursuing this information.

C. Responsibilities of Agency Program Officials

1. Have Agency Program Officials assessed the risk to operations and assets under their control, determined the level of security appropriate to protect such operations, maintained an up-to date security plan for each system supporting the operations and assets under their control and tested/evaluated security controls and techniques?

FLRA program officials worked with the FLRA IRMD Data Base Manager to assess the risk to their operations and assets under their control in July, 2002. In 2001, the Director, IRMD worked directly with FLRA managers to assess the security level of information entered and released from their systems.

Thus far, the FLRA has not required Program Managers to maintain security plans for each system supporting the operations and assets under each manager's control. This will have to be accomplished in order for the FLRA to comply with the Security Act.

2. Have Agency Program Officials used appropriate methods to ensure that Contractor or other agency provided services are secure and meet the requirements of the Security Act, OMB policy and NIST guidance?

As a result of an Inspector General recommendation to the Director, IRMD, and the IRMD Data Base Manager conducted an agency wide evaluation to insure that FLRA technical systems met the requirements of the Security Act, OMB policy and NIST guidance. The FLRA still has major requirements that need to be addressed.

D. Responsibilities of Agency Chief Information Officer

1. Has the CIO adequately maintained an agency-wide security program, ensured the effective implementation of the program and evaluated the performance of major agency components, ensured the training of agency employees with significant security responsibilities, collected program statistics and created actual performance measures?

The Executive Director has been acting as the FLRA's Chief Information Officer over the past several years. FLRA Inspector General audits and assessments have affirmed that up until the current leadership, the FLRA did not appropriately focus on information technology and security requirements and those Agency employees had not been appropriately trained in this area. The current Chairman is in the process of correcting these vulnerabilities. The FLRA Chairman has focused heavily on personnel security and is committed to improving the Agency's security programs' effectiveness. It is anticipated that with the appointment of a qualified Chief Information Office, more progress and effective security program administration will be implemented and institutionalized.

2. for security operations and assets under control, has the CIO used appropriate methods to ensure that contractor services meet the requirements of the Security Act, OMB policy and NIST guidance.

The FLRA Security Officer affirmed that contractors who are involved in FLRA programs and operations must have security checks prior to being hired. This requirement, however, is not documented in any FLRA policy.

3. Has the agency CIO fully integrated security into the agency's capital planning and investment control process? Were security requirements and costs reported on FY 03 capital asset plans? How many capital asset plans & justifications will be submitted to OMB for the FY 04 budget requests?

The FLRA Security Program has not specifically been intergrated into the FLRA's strategic planning and capital asset plan even though senior management has been focusing on its importance. Information technology costs have been defined but are not specifically identified in FLRA FY 03 and FY04 budget submissions since such expenditures have been funded through the Agency's Central Services Fund. The FLRA has not yet created capital asset plans and justifications for submission to OMB with its FY 04 budget requests.

Inspector General Evaluation:

The FLRA has made some progress this past year in strengthening its security programs, however, much of it has been related to researching options and drafting policies and procedures which have not yet been implemented. Although previous Inspector General oversight activities pointed out significant weaknesses in both personnel security and computer information security, the September 11 disaster validated the reasons why security is a critical administrative program for the Agency. The Chairman, FLRA has focused on improving information security technology and a strong security program and has prioritized the improvement of these programs.

Over this past year, the FLRA has made progress toward compliance with the Security Act, but security weaknesses still exist and the Agency lacks appropriate documentation of security policy and procedures. A more proactive management focus needs to occur over this next year to ensure the implementation of contemporary security and information security programs and related policies, and that all Agency employees are trained and aware of all requirements in this area.