REPORT ON AUDIT OF FLRA SECURITY PROGRAMS

SEPTEMBER 2004

Task Order No. FLRA-IG-2004-1

Cotton & Company LLP
Auditors • Advisors
333 North Fairfax Street, Suite 401
Alexandria, Virginia 22314
703.836.6701
chayward@cottoncpa.com

CONTENTS

REPORT ON AUDIT OF
FLRA SECURITY PROGRAMS

EXECUTIVE SUMMARY

Cotton & Company LLP, on behalf of the Federal Labor Relations Authority (FLRA), Office of Inspector General, conducted an independent assessment of the agency's security programs. This work was designed to assess FLRA's compliance with the Federal Information Security Management Act of 2002 (FISMA) and Federal security requirements.

FLRA has established adequate security controls in some areas. Overall, however, its information security programs do not meet responsibilities required for Federal agencies stipulated in FISMA, Section 3544, Federal Agency Responsibilities. The weaknesses identified by this audit focus on lack of security policy, access controls, system software controls, service continuity controls, and contingency plans to recover critical operations when interruptions occur. Other common vulnerabilities involve insufficient resources, lack of contemporary training, lack of internal controls, lack of cyclic testing procedures, and general lack of employee awareness of the importance of information security and other types of security.

The objectives of this audit were to evaluate the quality and compliance of FLRA's security programs in accordance with prevailing Federal security regulations. Our evaluation considered aspects of the agency's physical and information technology security functions.

This report, which was prepared jointly by the Inspector General and Cotton & Company, discusses in detail the weaknesses identified. Weaknesses taken as a whole are considered material and should be included in FLRA's Fiscal Year (FY) 2004 FISMA report to the Office of Management and Budget (OMB) and Congress.

REPORT ON AUDIT OF
FLRA SECURITY PROGRAMS

Cotton & Company LLP, on behalf of the Federal Labor Relations Authority (FLRA), Office of Inspector General, conducted an independent assessment of the agency's security programs. This work was designed to assess FLRA's compliance with the Federal Information Security Management Act of 2002 (FISMA) and Federal security requirements.

This report, which was prepared jointly by the Inspector General and Cotton & Company, is presented under the following captions to meet requirements of Task Order No. FLRA IG-2004-1:

- Introduction
- Background
- Methodology
- Statutory and Related Requirements
- Findings and Recommendations
- Management Comments
- Risk Assessment

INTRODUCTION

Effective security is an essential element of Federal programs and should be integrated into every program management from the onset of strategic planning. Since 9/11, Federal agencies have focused on improving the security structure of their environments. Much focus has been placed on physical security, health and safety programs, and cybersecurity. Most Federal agencies have updated their policies and procedures and increased security training for employees.

Driving factors should go beyond the 9/11 level and ensure the safety and security of all public and private-sector individuals. The appropriate perspective for system and information security should relate to how vital the information is to an organization's mission, and what would happen if the information were lost or even altered. System and information security should be addressed at the level warranted by mission-critical product or service thresholds, not solely on the basis of classification or sensitivity.

As the transformation to a digital government continues to unfold, Federal agencies will need to address how information technology will reshape public-sector strategies. Computer information systems must be developed to facilitate interoperability, application portability, and scalability of computerized applications across networks of heterogeneous hardware, software, and communication platforms. Agencies need to prioritize and maximize interagency interoperability and customer needs before buying or otherwise acquiring new technology to maximize the return on investment. No longer is computer technology just a technical program. In the Federal government and the private sector, computer information has become a management program as well.

Both private and public organizations must ensure accessibility to their systems and develop an information technology architecture that provides a framework for strategic, operational, and capital planning, which includes a complete inventory of equipment, personnel, and funds devoted to information technology. The use of more off-the-shelf software, instead of internally developed programs, is increasing, and management must focus on getting the best return on investment.

Information technology resources have become an issue of concern in the Federal sector. Sufficient numbers of qualified personnel are difficult to retain as the result of private-sector competition and higher salaries. Computer technology is constantly changing, and Federal agencies have difficulty maintaining current hardware and software, because of budget restrictions. Federal government strategic planning and budget formulation in non-technical agencies do not sufficiently emphasize the importance of information technology. This results in insufficient resources and the failure to perform routine risk analyses.

As a result of studies performed in 24 Federal agencies, the U.S. Government Accountability Office (GAO) noted that, while operations, systems, and risks vary relative to agencies, system control weaknesses are similar, and poor security planning and management is the commonality rather than the exception. Rather than taking actions to control risk cost effectively, most Federal agencies react only after a violation has been detected, and, by then, costs may have risen substantially compared to costs of implementing more timely solutions before a violation occurs.

The weaknesses identified by this audit focus on lack of security policy, access controls, system software controls, service continuity controls, and contingency plans to recover critical operations when interruptions occur. Other common vulnerabilities involve insufficient resources, lack of contemporary training, lack of internal controls, lack of cyclic testing procedures, and general lack of employee awareness of the importance of information security and other types of security.

Both GAO and OMB have advised Federal agency management to raise the level of employee awareness to the importance of security issues, ensure that policies and management controls are current and operating effectively, routinely monitor the security of computer information with automated tools, and ensure that adequate and qualified resources are administering agency computer information security, physical security, and homeland security programs.

BACKGROUND

The most recent FLRA Inspector General audit of computer information security was performed in FY 2000. This audit, conducted by Cotton & Company, revealed significant vulnerabilities in FLRA’s information technology control. In response, FLRA consulted with Gartner & Associates to provide specific ways to address and correct findings and address recommendations. Most corrective actions and recommendations have not, however, been implemented.

Over the past 5 years, several FLRA Inspector General internal reviews revealed additional security vulnerabilities. Of note, FLRA’s evacuation plan lacks specific information on where employees should go in case of a biological or terrorist attack, lacks provisions for adequate maintenance of sufficient and accessible safety and protective equipment, lacks continuity of operations plans, and does not require that all FLRA facilities undergo annual security checks.

Further, FLRA Inspector General Audit Report No. 98-01, *Telecommunications Management*, issued in September l998, indicated procedural problems with information security. In l998, the FLRA Inspector General, in response to an employee complaint, verified that two FLRA employees were accessing pornography on the internet, and one was using the internet extensively for personal activities. Information Resource Management responded immediately by inserting a firewall to prevent access to pornography and other non-ethical material and provided guidance to FLRA on the appropriate use of government equipment.

Subsequently, the Director of Information Resources Management accelerated work on creating FLRA computer information security policies. An FLRA Inspector General report titled *Internal Management Review of the FLRA Case Control Office*, issued in June l999, revealed hardware and software problems and the limited interoperability of computer systems within the agency, and even within the Case Control Office itself. This review also revealed vulnerabilities in data and information integrity.

A former FLRA Inspector General issued a Management Letter in May 1, 1992, that contained four recommendations regarding LAN security that were still not fully implemented at the time of this audit. The l992 audit was a limited audit of the security of the Local Area Network Computer System. Major concern was expressed for the absence of policies and guidelines dealing with computer security, use of computer systems for personal or non-work purposes, and use of unauthorized software and games. In addition, the audit found that some users were installing their own commercial software not provided or approved by FLRA.

Another 1992 FLRA audit, Inspector General Audit Report 92-02, *ADP Procurement Plans*, recommended that management focus on its LAN security plan and make it more specific by relating security requirements and countermeasures to the FLRA operating environment. The report specifically advised FLRA management to identify the nature of information processed, define the level of risk as it relates to the protection requirements of confidentiality, assess integrity and availability, identify system vulnerabilities, identify impacts from threat activity, and identify security measures to meet these threats.

METHODOLOGY

We conducted this audit in conformance with Federal government standards and relevant portions of GAO's *Government Auditing Standards* and President's Council on Integrity and Efficiency and the Executive Council on Integrity and Efficiency (PCIE/ECIE) audit standards. We conducted this audit in four phases, which are listed below along with primary objectives of each:

- **Planning:** Develop the evaluation program.
- **Internal Control Evaluation, Risk Assessment, and Compliance Phase:**
    - Review and evaluate the existence and effectiveness of internal controls and compliance with Federal laws and regulations.
    - Assess FLRA's risks.
- **Substantive Testing:** Conduct penetration tests and network configuration analysis for compliance with FISMA and other Federal security requirements.
- **Reporting:** Convey the evaluation program results.

Our testing of FLRA physical security considered the following items:

- Entry and egress points for FLRA work areas, building, and garage.
- Access into the building's common areas and garage during normal business hours, non-business hours, and over the weekend and holidays
- Tracking access into the building work areas and garage records after normal business hours and during the weekend.
- Physical access intrusion detection system and alarms (type and location of each).
- Fire and smoke detection and suppression devices within the building common areas and

- Type and frequency of tests conducted of the physical access intrusion detection system and fire and smoke detection systems.

- Physical security controls within FLRA work areas for critical information storage areas for paper documents.

- Procedures for conducting building evacuation tests

- Whether FLRA has assigned fire drill responsibilities to specific personnel such as office fire marshal

- Documentation defining roles and responsibilities for evacuating building.

- Responsibilities for issuing, deactivating, and destruction of badges and access cards and or keys for personnel granted access to FLRA work areas for:

- Building access control over visitors during normal business hours and non-business hours.

To accomplish our tests of FLRA's information security, we primarily used modified procedures from GAO's *Federal Information System Controls Audit Manual* (FISCAM) to evaluate specific security program requirements contained in National Institute of Standards and Technology (NIST) Special Publications 800-14 and 26. We did not conduct penetration testing, because management stated that the agency would soon be implementing migration to Microsoft 2000. This planned migration did not, however, occur before the end of this audit.

This audit did involve a comprehensive review of FLRA's current security programs and information security technology. It included a review of all related instructions and systems, interviews with subject-matter managers and employees at FLRA's headquarters and regional offices, and contact with several other small agencies to compare processes.

We discussed audit findings and recommendations with management and include their responses in this report.

STATUTORY AND RELATED REQUIREMENTS

Our discussion of statutory and related requirements is presented in two sections: physical security and information security.

Physical Security

Our work included consideration of the adequacy of FLRA's physical security. A well-designed physical security plan includes, but is not limited to, the following elements:

Policies and Procedures

- Written security program and emergency management plans are established.

- Security and emergency management plans are updated to reflect anti-terrorist measures.

- Security and emergency management plans are an integrated system program, including coordination with other agencies.

- Security and emergency management plans are signed, endorsed, and approved by top management.

- Security and emergency management programs are assigned to a senior-level manager.

- Security responsibilities are defined and delegated from management through to front-line employees.

- All operations and maintenance supervisors and managers are held accountable for security and emergency management issues under their control.

Training

- Security orientation or awareness materials are provided to all employees.

- Ongoing training programs on safety, security, and emergency procedures by work area are provided.

- Public awareness materials are developed and distributed.

Document Control

- Access to documents of security-critical systems and facilities is controlled.
- Access to security sensitive documents is controlled.

Access Control

- Background investigations are conducted of contractors or others who require access to security-critical facilities.
- ID badges are used for all visitors, employees, and contractors to control access to key critical facilities.

Homeland Security

Protocols have been established to respond to the Office of Homeland Security Threat Advisory Levels.

Federal agency physical security programs must conform to a number of statutory and related requirements. Our work evaluated FLRA’s information security environment against the following:

- Homeland Security Act of 2002.

- Presidential Decision Directive 63, Critical Infrastructure Protection.

- Other relevant computer security requirements promulgated within FLRA, Executive Orders, OMB bulletins, and GAO reports.

Information Security

Federal agency information security programs must conform to a number of statutory and related requirements. Our work evaluated FLRA's information security environment against FISMA requirements and the following criteria:

- Computer Security Act of 1987.
- OMB Circular A-123, *Internal Control Systems*.
- OMB Circular A-127, *Financial Management Systems*.
- OMB Circular A-130, *Management of Federal Information Resources*, Appendix III, *Security of Federal Automated Information Resources*.
- NIST Special Publications, including 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*; 800-26, *Security Self-Assessment Guide for Information Technology Systems*; and other relevant Special Publications.
- Federal Managers Financial Integrity Act of 1982.
- Paperwork Reduction and Elimination Acts.
- Clinger-Cohen Act.
- E-Government Act of 2002.
- Government Performance and Results Act of 1993.
- Other relevant computer security requirements promulgated within FLRA, Executive Orders, OMB bulletins, and GAO reports.

FINDINGS AND RECOMMENDATIONS

This audit revealed that FLRA's current security programs and information system internal controls were substantially weak, and that FLRA was not in full compliance with Federal information system and security program requirements established by OMB circulars, NIST circulars, and Homeland Security policies. Of major concern, FLRA has not recently developed or updated agency-wide security plans, policies, or programs that address physical security and information technology. The FLRA Security Program Instruction was issued in l986 and only deals with agency security levels. Also, FLRA has not fully implemented network operating system controls, does not comply with segregation-of-duties controls, and has not expanded service continuity control. These are significant material weaknesses.

This audit revealed that FLRA regional offices have more extensive building security criteria (including those not located in Federal buildings) than the FLRA Headquarters. The current location of FLRA Headquarters is about as close to the White House as its former location and is a "critical location." Although both the FLRA Headquarters and regional offices maintain safety/security equipment which is accessible, FLRA Headquarters does not maintain sufficient safety/security equipment to protect all employees. The fact that a Continuity of Operations Plan has not yet been implemented negatively affects the FLRA's physical and information security as well. Also, this audit revealed that employees have not been provided security training over the last 4 years. This audit also affirmed that, although the

FLRA does not maintain classified information, its mission-related documents are sensitive legal documents and should be handled and maintained in a secure manner.

During this audit, several FLRA managers and employees expressed their concerns about the current level of FLRA's security programs and the need of management to focus heavily on all security issues. This audit affirmed that the FLRA does not have sufficient security policy to address requirements for homeland, physical, and information security, has not sufficiently addressed previous findings and recommendations related to security, and has an abundance of high risk security areas.

We present our specific findings and recommendations in the following categories:

A. Physical Security
B. Information Technology

While these categories are designed to facilitate user disposition of reporting results, they do overlap in some areas. For instance, service disruptions often have physical causes, but mitigation depends on IT policies and procedures. In contrast, computer-room access deficiencies, while related to IT policies and procedures, primarily represent a physical security concern. Accordingly, we classified FLRA's shortcomings related to service disruption under the Information Technology category, while classifying computer-room access issues under the Physical Security category. We used similar judgment for other overlapping conditions.

A. Physical Security

We identified physical security weaknesses regarding computer rooms, headquarters building (interior and exterior) access, and movements within headquarters. Our results are presented under the following captions:

1. Computer-Room Security
2. Physical Access to 1400 K Street
3. Kastle Key Control

1. Computer-Room Security

FLRA does not require visitors to sign in and out upon entering or departing its computer rooms located at 1400 K Street, NW, and 800 K Street, NW (Tech World). As a result, physical security controls over data and physical assets are weak, and staff and contractor accountability is potentially eliminated. Further, an emergency contact list was not posted in either location to facilitate communication in the event of service disruption.

GAO's *Standards for Internal Control in the Federal Government* provides the following:

> *Physical and environmental security controls should be implemented to protect the facility housing system resources, the system resources themselves, and the facilities used to support their operation.*

Lack of adequate physical security controls over system resources could potentially result in unauthorized manipulation of system resources and controls, disruption or denial of service, and damage to sensitive information system assets without proper accountability.

Recommendation

We recommend that the Chief Information Officer (CIO) develop and maintain:

- A visitor's log that all data center visitors are required to sign upon arrival and departure.
- An emergency contact list.

Management Response

CIO has established visitor logs for both locations. The logs require all data center visitors to sign in and out upon arrival and departure.

The CIO has also compiled an emergency contact list to facilitate communication in the event of service disruption and posted this the list both outside and inside the computer rooms. Copies will also be provided to key managerial personnel.

Cotton & Company Evaluation

Management's comment is responsive, although we have not tested implementation of either control.

2. Physical Access to 1400 K Street

Some external and internal physical access controls are weak and need improvement to ensure that access is limited to only authorized individuals. During a walk through conducted after normal business hours, we found the following:

- The loading dock exterior door to the building parking garage was unsecured.
- Several FLRA interior offices were not secured on the second and third floors.

Although we were able to gain access to the parking garage, we were not able to access the building interior.

GAO's *Standards for Internal Control in the Federal Government* provides the following:

> *Physical and environmental security controls should be implemented to protect the facility. Physical access controls should restrict the entry and exit of personnel from an area. Further, it is important to establish controls to review the effectiveness of physical access controls in each area, both during normal business hours and at other times – particularly when an area may be unoccupied.*

FLRA's lack of adequate physical security controls could potentially result in property damage and theft of governmental equipment and sensitive documents. The unsecured exterior loading dock near the garage increases the potential for physical harm to employees.

Recommendation

We recommend that the Director of the Administrative Services Division (ASD):

- Work with building owners and maintenance personnel to ensure that the parking garage exterior doors remain locked and secured.

- Install door locks on all interior doors.

Management Response

Because FLRA does not control the loading dock exterior door, this issue has been addressed with building management on numerous occasions, most recently at a July 8, 2004, meeting (and two other earlier meetings) with the Federal Protective Service (FPS) and Trizec Building Management. At this meeting, FPS again advised Trizec that the building loading dock and garage area needed to be secured for the protection of staff and other resources. Once received, a copy of FPS's written report will be sent to Trizec management to further support our insistence that Trizec address this issue.

Cotton & Company Evaluation

Management's comment is partially responsive. It does not address our recommendation to install door locks on all interior doors.

3. Kastle Key Control

Our tests of control over Kastle Keys identified three employees who were each authorized to hold two Kastle Keys. We were also informed that FLRA does not have policies, procedures, and practices for updating and managing Kastle Keys. Accordingly, we concluded that FLRA does not have effective policies or procedures designed to assure that Kastle Keys are fully controlled once they are issued.

GAO's *Standards for Internal Control in the Federal Government* states that "…it is important to establish controls to review the effectiveness of physical access controls in each area [of the agency physical space]…."

These conditions leave FLRA vulnerable to unauthorized individuals entering the premises, thus creating security breaches that could result in the theft and destruction of government property.

Recommendation

We recommend that ASD develop effective polices for managing Kastle Keys and direct ASD security personnel to implement procedures in accord with the policies adopted.

Management Response

Although we do not have written procedures in place for updating and managing Kastle Keys, the keys are updated and managed through the Kastle website. Three ASD employees have access to this website and use the program to issue and delete keys and run reports on card key access and issuance. In July, ASD began running Card Key status reports every Monday morning. These reports are reviewed to ensure that there are no duplicate keys and no authorized individuals have access to the suites. Written policies are being developed concerning managing Kastle Keys.

Cotton & Company Evaluation

Management's comment is responsive. It did not, however, provide a date for finalizing the written policies it proposes.

B. Information Security

We identified IT weaknesses that we discuss under the following captions:

1. Disaster Recovery and Business Continuity
2. Systems Accreditation and Formalized Acceptance By Management
3. Data Back Ups
4. Security-Awareness Training
5. Security Program Plan
6. Incident Response Plan
7. Information Security Program
8. Patch Management
9. Systems Development Life Cycle and Change Control
10. Segregation of Duties
11. User-Account Control

1. Disaster Recovery and Business Continuity

Management does not have disaster recovery, IT contingency, business continuity, and continuity of operations plans fully developed and implemented to address and mitigate risks associated with ensuring the continuity of support in the event of a service disruption.

FLRA management has been unable to complete these plans, because of limited personnel and higher-priority system initiatives including the Windows 2000 migration efforts.

OMB Circular A-130, Appendix III, *Security of Federal Information Resources*, requires agencies to develop and maintain continuity of support plans for general support systems and contingency plans for major applications. Once the plans are developed, Appendix III requires that personnel be trained to effectively implement the plans and plans be tested and modified as appropriate based on the testing results.

Absent these plans, and without training and testing, FLRA risks long-term network outages and substantial or complete inability to carry out its mission.

Recommendation

We recommend the CIO:

- Fully develop disaster recovery, IT contingency, business continuity, and continuity of operations plans.

- Provide training to enable personnel to effectively implement all plans, and require periodic retraining.

- After each plan is implemented, conduct and document testing to ensure that each plan is responsive, periodically reevaluate plans, and keep plans current.

Management Response

The CIO is working with the Director of ASD to develop a Disaster Recovery and Business Continuity Plan for major applications and support systems. Contract services are being procured to assist with development of a Continuity of Operations Plan. These documents will address the issues raised in the recommendations, including the training, testing, and risk assessment reevaluation matters.

The CIO will use NIST Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook*, as a guide for written policies and procedures. Disaster recovery for agency-wide major applications such as the case tracking system has been documented and tested this past year to ensure continuity of support in the event of service disruption.

Cotton & Company Evaluation

Management's comment is responsive; it did not, however, provide dates for completing any of its proposed actions.

2. Systems Accreditation and Formalized Acceptance by Management

FLRA's general support system, including its data network and major applications, have not been certified and accredited (C&A) or formally authorized for processing by management in accordance with OMB Circular A-130 and NIST criteria.

In general, IT systems utilized within Federal agencies fall into one of two categories: major applications or general support systems. OMB Circular A-130 requires all systems (major application and general support) to be authorized for processing (accredited). Accreditation must be based on an assessment of management, operational, and technical controls and risks associated with each system.

Lack of C&A may expose FLRA to risks that senior management may not be willing to assume. Management cannot put full reliance on the security of individual applications, because the general support system, which lies beneath the applications, has not been authorized for processing by an appropriate management official based on a standard C&A.

Recommendation

We recommend that the CIO:

- Perform a C&A review in accordance with NIST standards and authorize the general support system for processing.

- Ensure that a management official authorizes in writing the use of each general support system based on an acceptance of risks identified within the system certification process as described by NIST.

Management Response

NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, will be used for written policies and procedures that will address, among other things, procedures for authorizing each general support system.

FLRA is in the process of procuring contract services to conduct a risk assessment via the GSA-FTS-Millennia Lite contract. Services will include risk identification, qualitative and quantitative risk analysis, risk response planning, and risk monitoring and control as contemplated by FISMA or other follow on legislation.

Cotton & Company Evaluation

Management's comment is responsive; it did not, however, provide dates for completing any of its proposed actions.

3. Data Back Ups

FLRA has interim policies and procedures for performing system back ups of the network and mail servers. The personnel performing the back ups do not, however, follow this interim guidance.

NIST's *Contingency Planning Guide for Information Technology Systems*, Back Up Methods, Section 3.4.1, requires that system data be backed up regularly, pursuant to written policies and procedures.

Lack of adherence to a documented policies and procedures for creating back ups for the CDs and disks could potentially result in the loss of sensitive information and data and disruption or damage to sensitive information system assets.

Recommendation

We recommend that the CIO ensure that staff members adhere to a documented policies and procedures for performing backups of network file and mail servers.

Management Response

System data and network files are being backed up regularly every day. Weekly backups are completed each Friday. Back up tapes are stored offsite at the National Capital Archives, Woodbridge, Virginia. The Microsoft Exchange email database and the Oracle case-tracking database are exported each night to a storage device for easy retrieval in the event of an emergency. Written procedures for completing network and database backups are being drafted and will be tested before being implemented.

Cotton & Company Evaluation

Management's comment is responsive; it did not, however, provide a date for finalizing its proposed written procedures.

4. Security-Awareness Training

FLRA does not have a computer security awareness training program that is administered periodically to all employees in accordance with OMB requirements.

OMB Circular A-130, Appendix III, requires agencies to provide security awareness training to their employees and specialized security awareness training for system administrators.

Without effective security awareness training, users may unknowingly act in a manner to jeopardize data and system integrity.

Recommendation

We recommend that the CIO develop a program to provide annual security awareness training to all FLRA employees in accordance with OMB requirements. In addition, we recommend that FLRA develop proper procedures to accurately assess and report on the program's level of attendance and effectiveness.

Management Response

FLRA is in the process of procuring a web- or computer-based security awareness training course for use by all FLRA employees and contractors. In addition, specialized training, as appropriate, for IRM or other FLRA employees with security responsibilities will be procured. All employees and contractors will be required to certify in writing that they have attended training. The CIO continues to develop procedures (e.g., Use of Government Equipment, Network Administration) to supplement and reinforce security awareness. The CIO plans to conduct periodic reviews every 6 months to assess effectiveness.

Cotton & Company Evaluation

Management's comment is responsive; it did not, however, provide dates for implementing its proposed actions.

5. Security Program Plan

FLRA has prepared a draft Information Security Program Plan's (SPP) framework in accordance with OMB guidance and NIST Special Publication 800-14. This draft is incomplete, and it does not address all requirements. For instance, the draft plan:

- Is generic and lacks definitive statements in key sections that specifically address the FLRA infrastructure environment.

- Is missing all appendixes and Chapters 7 and 8.

- Lacks requisite information about:

  - Establishing operational and technical controls for the general support system.
  - Developing and implement specific rules of behavior for all system users.

- Does not document specific security activities to address the following:

  - Specific system security plans.
  - Rules of the system (rules of behaviors and password policies).
  - Specialized and security awareness training.
  - Incident response capability.
  - System interconnection.

OMB Circular A-130, *Management of Federal Information Resources*, dated November 28, 2000, provides the following guidance:

> *The head of each agency must develop internal agency information policies and procedures and oversee, evaluate, and otherwise periodically review agency information resources management activities for conformity with the policies set forth in this Circular (Section 9.a.5.).*

Without a fully developed and implemented system security program plan, responsibilities may be unclear, resulting in failure to adequately provide for system security and provide accountability for ensuring that appropriate and required computer security controls are in place.

Recommendation

We recommend that the CIO develop a complete Security Program Plan, arrange for appropriate personnel to review it, revise the plan accordingly, and obtain approval by cognizant executive management.

Management Response

FLRA is in the process of procuring contract services to assist the CIO in developing an up-to-date security plan and identifying, testing, and evaluating security controls and techniques. Upon completion of operations and assets identification and risk assessment, management will determine the level of security appropriate to protect such operations and assets.

Cotton & Company Evaluation

Management's comment is responsive; it did not, however, provide dates for implementing its proposed actions.

6. Incident Response Plan

FLRA has not developed, documented, or implemented an incident response plan to identify its responsibilities and to provide necessary guidance for addressing cyber attacks.

NIST Special Publication 800-34, *Contingency Planning Guide for Information Technology Systems*, and OMB Circular A-130, Appendix III, require agencies to establish an incident response plan to ensure the capability to provide help to users when a security incident occurs in the system and to share information concerning common vulnerabilities and threats.

In the event of a systems security breach, FLRA could be without the necessary functional direction, guidance, and system support measures to mitigate the risk of unauthorized manipulation of sensitive financial and application data.

Recommendation

We recommend that the CIO develop, document, and implement an incident response plan consistent with NIST and OMB criteria.

Management Response

FLRA is in the process of procuring contract services to assist the CIO in establishing a methodology to ensure that the FLRA, including all components, has documented procedures for reporting security incidents and sharing common vulnerabilities. The CIO will use NIST Special Publication 800-3, *Establishing a Computer Security Incident Response Capability*, and OMB criteria as guidance in developing an incident response plan.

Cotton & Company Evaluation

Management's comment is responsive; it did not, however, provide dates for implementing its proposed actions.

7. Information Security Program

FLRA does not have adequate controls in place to ensure that a cohesive entity-wide security program is implemented and maintained and adequate security is provided for assets and information collected, processed, transmitted, stored, or disseminated in its general support system and major applications. Furthermore, FLRA controls to monitor its information security program are not adequate to ensure that information systems security program procedures comply with applicable Federal laws, regulations, and standards and adequately address and mitigate risks from prior-year evaluations and audits.

OMB Circular A-130, Appendix III, requires agencies to:

> *Implement and maintain an information security program to assure that adequate security is provided for all agency information collected, processed, transmitted, stored, or disseminated in general support systems and major applications.*

OMB Circular A-130 also requires security plan monitoring:

> *The head of each agency must develop internal agency information policies and procedures and oversee, evaluate, and otherwise periodically review agency information resources management activities for conformity with the policies set forth in this Circular (Section 9.a.5.).*

Without a well-designed program, security controls may be inadequate; responsibilities may be unclear, misunderstood, and improperly implemented; and controls may be inconsistently applied through informal processes. Such conditions may lead to inadequate protection of sensitive or critical resources and disproportionately high expenditures for controls over low-risk resources.

Recommendation

We recommend that the CIO:

- Take immediate action to ensure timely development and implementation of policies and procedures necessary to establish and support FLRA's information security program.

- Develop and implement policies and procedures to track, evaluate, and monitor FLRA's information and information systems security program in accordance with OMB Circular A-130, Appendix III, and ensure proper and timely reporting to OMB and Congress.

Management Response

The CIO has drafted a framework for implementing these recommendations. Upon completion of operations and assets identification and risk assessment and after management has determined the level of security appropriate to protect such operations and assets, the CIO will develop and implement policies and procedures necessary to establish and support FLRA's information security program. Such policies and procedures will be written in accordance with OMB Circular A-130, Appendix III, and will include policies and procedures to track, evaluate, and monitor FLRA's information security program.

Cotton & Company Evaluation

Management's comment is responsive; it did not, however, provide dates for implementing its proposed actions.

8. Patch Management

IT employees or IRM staff install patches on network servers according to an informal, undocumented regimen, rather than a properly approved and documented policy. Our tests also disclosed that patches are installed directly into the network production environment without any precautionary evaluation of patches in a test environment.

These conditions could leave FLRA's IT environment vulnerable to loss of sensitive information and data and disruption or damage to sensitive information system assets.

NIST Special Publication No. 800- 40*, Procedures for Handling Security Patches,* dated August 2002, recommends that organizations have an explicit and documented patching and vulnerability policy and a systematic, accountable, and documented process for handling patches.

Recommendation

We recommend that the CIO:

- Develop policies and procedures requiring that patches be properly tested in a test environment before being placed into production.
- Develop a test lab to adequately test patches.
- Provide training to individuals to ensure that critical functions and activities can be performed by multiple personnel.

Management Response

The CIO has proposed that a test environment be developed by the network manager to properly test patches before being placed in production. The CIO is in the process of recruiting a network manager and will address that issue once the position has been filled. It will be the primary responsibility of the network manager to patch systems under his/her control. Other network administrators will also be cross-trained to ensure continuity of operations. Appropriate training will be provided to all IT employees who have assigned tasks associated with handling patches.

During this past year, the CIO reviewed NIST Special Publication 800- 40, *Procedures for Handling Security Patches*, dated August 2002, which sets forth the process for patch management. The CIO will incorporate these standards within documented policies and procedures for handling patches.

Cotton & Company Evaluation

Management's comment is responsive; it did not, however, provide dates for implementing its proposed actions.

9. Systems Development Life Cycle and Change Control

FLRA has no formalized written change control and systems development life cycle (SDLC) policies addressing configuration management and guiding the acquisition, development, and maintenance of hardware, software, and commercial off-the-shelf (COTS) products.

OMB Circular A-130, Appendix III, provides or refers to standards specific to information systems development, which include documentation of requirements, authorizations for undertaking projects, reviews and testing, and approvals before placing systems into operation. OMB also has instructed agencies to apply NIST guidelines (particularly NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*, dated December 1998) to achieve adequate security over Federal computer systems.

FLRA plans to migrate to a Windows 2000 platform, but plans have been delayed substantially for reasons that we were unable to fully ascertain during our evaluation. Without an SDLC to guide the migration, FLRA risks cost overruns, rework, implementation failures, unacceptable post-implementation system performance, and other substantive problems that could lead to waste of government resources.

Recommendation

We recommend that the CIO:

- Develop and implement a formal SDLC methodology based on NIST guidance and ensure the policy at a minimum addresses the following elements:

    - Sensitivity of data to be processed in the system.
    - Resources required for adequately securing the system.
    - Input from the equivalent of an Investment Review Board.
    - Authorizations for software modification documentation and maintenance.
    - Budget requests to include security resources for the system.
    - Security controls consistent with and integral to senior management's standards.
    - Security requirements to be included in solicitation documentation.

- Develop and implement a formal change control policy outlining the procedures needed to ensure that system configuration changes are properly documented, authorized, approved, and tested before being moved into production or implemented.

Management Response

FLRA is in the process of procuring contract services to assist the CIO in establishing and formalizing an SDLM methodology based on NIST guidelines to provide a mechanism for monitoring and controlling tasks, completion dates, product quality, and FLRA expenditures in the customization and maintenance of COTS and government off-the-shelf (GOTS) application system software. In addition, the SLDM will incorporate appropriate security controls throughout each phase of the system's lifecycle.

The CIO will use NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*, dated December 1998, and OMB Circular A-130, Appendix III, to achieve adequate security over FLRA's computer systems.

Cotton & Company Evaluation

Management's comment is responsive; it did not, however, provide dates for implementing its proposed actions.

10. Segregation of Duties

We identified the following conditions:

- FLRA does not have a designated systems security officer (SSO). Thus, the majority of security activities fall under the purview of the CIO, which presents a separation of duties weakness.

- The CIO and acting information resource manager maintain domain-administrator privileges on FLRA's network. These privileges are incompatible with the other responsibilities of these individuals and present a severe information security concern for FLRA.

FLRA is at greater risk of compromise of network operations and loss or compromise of data as the result of these conditions. These conditions also represent noncompliance with a number of Federal criteria addressing the need to maintain segregation among incompatible duties. In accord with NIST Special Publication 800-14:

> *Organizations should strive for separation of duties between security personnel who administer the access control function and those who administer the audit trail* (Section 3.13.2).

GAO issued *Standards for Internal Control in the Federal Government*, dated November 1999, which offers the following guidance on page 14:

> *Key duties and responsibilities need to be divided or segregated among different people to reduce the risk of error or fraud.*

Recommendation

We recommend that the Chairman:

- Suspend access or implement adequate procedures to mitigate risks associated with the CIO's access privileges to the network domain servers and local account passwords and follow through with the Windows 2000 migration and rollout initiative to ensure that current passwords that have been compromised due to the departure of the network manager do not continue to present the agency with a major security risk.

- Designate an SSO, ensure that a separation of duties exists among security personnel who administer the access control function, and assign necessary duties for the general support system and IT administer infrastructure security.

- Separate duties between user account maintenance and exception report/audit trail queries for the general support system and firewall.

Management Response

This problem will be corrected when FLRA migrates to the new Windows 2000 operating environment. Proper authorization and access controls will also be established during the migration.

The auditors have agreed to provide a list of agencies of similar size that have a separate security officer. The overall IRMD structure will be assessed to determine how best to resolve the issue raised by the auditors.

Cotton & Company Evaluation

Management's comment is responsive; it did not, however, provide dates for implementing its proposed actions.

We researched several entities similar to FLRA, and found that all maintain separation between security officers and CIOs. The agencies that have separated these key functions are: Merit Systems Protection Board, Defense Facilities Nuclear Safety Board, International Trade Commission, Federal Prison Industries (UNICOR), Equal Employment Opportunity Commission, and National Credit Union Administration.

11. User-Account Control

FLRA's network and application security personnel are not required to conduct periodic reviews of user accounts and assigned privileges to assure that accounts and privileges are legitimate and appropriate. In addition, user account maintenance policies and procedures are outdated.

Based on a sample of user accounts, we identified 23 active accounts assigned to personnel no longer employed by FLRA and several instances of generic accounts that agency personnel could not identify with specific purposes and uses.

Maintaining active user accounts for users who are no longer employed by FLRA creates the possibility that these accounts will be used inappropriately to perform fraudulent transactions or disrupt system availability. Generic accounts reduce accountability when many individuals have access to the each of the several generic accounts. In addition, without adequate procedures to periodically review user account lists and assure that user privileges are proper, management cannot be assured either that active users are authorized to access the systems and user privileges are appropriate to their *current* duties.

NIST Special Publication No. 800-14, provides the following guidance (Section 3.5.2)

> *Audit and Management Reviews—It is necessary to periodically review user account management on a system. Reviews should examine the levels of access each individual has, conformity with the concept of least privilege, whether all accounts are still active, whether management authorizations are up-to-date, whether required training has been completed, and so forth. These reviews can be conducted on at least two levels: (1) on an application-by-application basis, or (2) on a system wide basis.*

Recommendation

We recommend that the CIO:

- Develop policies and procedures requiring periodic reviews of users on the network operating system as well as their network privileges to ensure appropriate security over user access is controlled.

- Analyze generic accounts currently active on the network operating system to ensure that they are appropriate and that account access is controlled and monitored.

Management Response

The CIO has begun the process of developing policies and procedures for authorization and access controls within FLRA. The CIO plans to include provisions for periodic reviews of users on the system as well as the controls necessary to authorize or restrict the activities of users and system personnel.

The CIO is in the process of examining the issue of generic accounts on the system, with a view to determining their appropriateness and how best to assure that account access is controlled and monitored. The CIO is in the process of looking at network accounts and is analyzing the extent of the problem and will take appropriate steps to correct the problem.

Cotton & Company Evaluation

Management's comment is responsive; it did not, however, provide dates for implementing its proposed actions.

MANAGEMENT COMMENTS

The Inspector General convened an exit conference on June 24, 2004, with management and Cotton & Company representatives to discuss preliminary results. Management generally withheld comment during the exit conference pending receipt and evaluation of the formal draft report.

After the exit conference, we submitted a written draft for management consideration. Management subsequently replied to the draft in a timely manner. We incorporated these replies and our analysis with each finding.

RISK ASSESSMENT

Management ultimately is responsible for assessing risk and establishing priorities for remediating it. We considered the risk for each finding and, using FISMA criteria, assessed whether each finding represented a low, medium, or high risk (L, M, and H, respectively.) We rated all conditions as medium or high risk.

Our risk ratings by condition follow:

Finding	Description	Risk
A1	Computer-Room Security	M
A2	Physical Access to 1400 K Street	M
A3	Kastle Key Control	H
B1	Disaster Recovery and Business Continuity	H
B2	Systems Accreditation and Formalized Acceptance By Management	H
B3	Data Back Ups	M
B4	Security-Awareness Training	M
B5	Security Program Plan	H
B6	Incident Response Plan	H
B7	Information Security Program	H
B8	Patch Management	M
B9	Systems Development Life Cycle and Change Control	H
B10	Segregation of Duties	H
B11	User-Account Control	H