Office of
Inspector General

Farm Credit Administration
Federal Information Security Management Act (FISMA) Evaluation

Agreed-Upon Procedures

September 10,2003

CONTENTS PAGE

INDEPENDENT ACCOUNTANT'S REPORT ON APPLYING AGREED-UPON PROCEDURES 1

FISMA REPORT 3

HARPER, RAINS, KNIGHT & COMPANY
Certified Public Accountants
A Professional Association

The Inspector General
Farm Credit Administration
Washington, D. C.

Independent Accountant's Report on Applying Agreed-Upon Procedures

We have performed the procedures summarized below that were agreed to by the Farm Credit Administration's Office of Inspector General, solely to assist you with the annual evaluation of the Farm Credit Administration's (FCA) information security program and practices. This engagement was conducted in accordance with consulting standards established by the American Institute of Certified Public Accountants. The sufficiency of these procedures is solely the responsibility of those parties specified in this report.. Consequently, we make no representation regarding the sufficiency of the procedures described below either for the purpose for which this report has been requested or for any other purpose.

Our procedures included determination of the critical elements which represent tasks that are essential for establishing compliance with Federal Information Security Management Act (FISMA), and guidelines issued by OMB, GAO, CIO Council, and NIST for each control category, including:

- documented security policies;
- documented security procedures;
- implemented security procedures and controls;
- tested and reviewed security procedures and controls; and
- fully integrated security procedures and controls.

For each control category, we determined the associated objectives, risks, and critical activities, as well as related control techniques and evaluation concerns specific to FCA's information technology environment.

We used the requirements and criteria found in GAO's Federal Information System Controls Audit Manual (FISCAM), OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources," current NIST guidance, and the CIO Council Framework.

In our review we considered the following mission critical systems:

- Federal Financial System (FFS)
- Consolidated Reporting System (CRS)
- Lotus Domino
- Personnel/Payroll System
- Windows 2000

We were not engaged to, and did not conduct an examination, the objective of which would be the expression of an opinion on the FCA's information security program and practices. Accordingly, we do not express such an opinion. Had we performed additional procedures, other matters might have come to our attention that would have been reported to you.

Harper, Rains, Knight & Company, P.A.

September 10, 2003

FISMA REPORT

In accordance with Memorandum Reporting Instructions
for the Government Information Security Reform Act and
Updated Guidance on Security Plans of Actions and Milestones

A.1 IT Security Spending to Protect Government Operations and Assets

A.1. Identify the agency's total IT security spending and each individual major operating division or bureau's IT security spending as found in the agency's FY03 budget enacted. This should include critical infrastructure protection costs that apply to the protection of government operations and assets. Do not include funding for critical infrastructure protection pertaining to lead agency responsibilities such as outreach to industry and the public.	
Bureau Name	**FY03 IT Security Spending ($ in thousands)**
To be Prepared by Agency Only	N/A
Agency Total	N/A

A.2 Identity and Number of Agency Programs and Systems and Those Reviewed

A.2a. Identify the total number of programs and systems in the agency, the total number of systems and programs reviewed by the program officials and CIOs in FY03, the total number of contractor operations or facilities, and the number of contractor operations or facilities reviewed in FY03. Additionally, IGs shall also identify the total number of programs, systems, and contractor operations or facilities that they evaluated in FY03.						
	FY03 Programs		**FY03 Systems**		**FY03 Contractor Operations or Facilities**	
Bureau Name	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Number Reviewed
Farm Credit Administration	1	1	5	5	4	4
Agency Total	1	1	5	5	4	4
b. For operations and assets under their control, have agency program officials and the agency CIO used appropriate methods (e.g., audits or inspections) to ensure that contractor provided services or services provided by another agency for their program and systems are adequately secure and meet the requirements of FISMA, OMB policy and NIST guidelines, national security policy, and agency policy?	Yes		Yes			
c. If yes, what methods are used? If no, please explain why.	See Below					
d. Did the agency use the NIST self-assessment guide to conduct its reviews?	Yes			Yes		
e. If the agency did not use the NIST self-assessment guide and instead used an agency developed methodology, please confirm that all elements of the NIST guide were addressed in the agency methodology.	N/A			N/A		

The Office of Inspector General (OIG), supported by a contract with Harper, Rains, Knight & Co. P.A., performed an independent evaluation of the Farm Credit Administration's (FCA or Agency) information security program and practices.

A. <u>General Overview</u>

FCA is an independent agency in the executive branch of the U. S. Government. It is responsible for the regulation and examination of the banks, associations, and related entities that collectively comprise what is known as the Farm Credit System (FCS). FCA promulgates regulations to implement the Farm Credit Act of 1971 (the Act), and examines System institutions for compliance with the Act, regulations, and safe and sound banking practices. FCA has fewer than 300 employees. The Agency headquarters are in McLean, Virginia. It has field examination offices in McLean, Virginia; Bloomington, Minnesota; Dallas, Texas; Denver, Colorado; and Sacramento, California.

1. Mission Critical Systems

FCA is a single program agency with five mission critical systems. Mission critical systems are defined as any telecommunications or information system used or operated by an agency or by a contractor of an agency, or organization on behalf of an agency that processes any information, the loss, misuse, disclosure, or unauthorized access to or modification of, would have a debilitating impact on the mission of an agency. In FY03 and FY02, all mission critical systems were evaluated.

In accordance with the Federal Information Security Management Act (FISMA) and OMB's implementation guidance, we evaluated the following mission critical systems.

Major Applications

a. Federal Financial System (FFS)

FFS is a major application that supports FCA's entire core accounting functions including budget execution, accounts payable, disbursements, purchasing, travel, accounts receivable, general ledger, document tracking, project cost accounting, and external reporting. FFS is a mainframe computer financial management system. FFS is processed by the United States Geological Survey/National Business Center (NBC), and American Management Systems Inc. The FFS software is owned and maintained by American Management Systems. American Management System is responsible for providing development activities including regular upgrades, fixes, and requested enhancements to maintain the core FFS software. NBC personnel are responsible for defining and developing processes to retrieve or receive data from external sources to develop corresponding programs that enable FFS to load the data accordingly. FCA's FFS security administrator, located in the Office of Chief Financial Officer is responsible for managing security access control to the FFS agency application. The FFS was placed in production in June 2001.

b. Consolidated Reporting System (CRS)

CRS is a major application that supports FCA operations. CRS is a database containing financial and statistical information on active and inactive Farm Credit Institutions. CRS contains three distinct subsystems that are Call Report, Loan Account Reporting System (LARS), and Web-based CRS Reports:

- Call Report is comprised of financial information including a statement of condition, statement of income, and supporting schedules that is collected quarterly from the FCS Institutions. Call Report subsystem is monitored, analyzed, and assessed by FCA examiners and financial analysts to ensure that the integrity and confidentiality of financial data are maintained.

- LARS database contains specific loans of FCS Lender Institutions. Institutions submit the data quarterly to the FCA.

- Web-based CRS Reports is an FCA developed application. The reports are available on the FCA's Web site. The Freedom of Information Act (FOIA) versions of the reports are available to the public. The non-FOIA versions of the reports are available to users who are authorized to view their institution data.

c. Lotus Domino

Lotus Domino (Notes) is a database system application owned and maintained by FCA. The application supports routine administrative tasks including e-mail, group discussion, calendaring and scheduling, database management, forms, and workflow.

d. Payroll Services from National Finance Center (NFC)

United States Department of Agriculture's (USDA) NFC located in New Orleans, Louisiana provides the Personnel/Payroll System to FCA. The NFC provides distributed application and telecommunications support for the remote site located in McLean, Virginia. NFC developed a "master security plan" for the general support system in New Orleans. FCA's Office of Chief Administrative Officer (OCAO) maintains a security plan for the remote system at FCA that incorporates provisions of the master security plan.

General Support System

FCA has one mission critical general support system.

- Windows 2000

  FCA migrated from Windows NT 4.0 operating system to Windows 2000 during FY 2003. Windows 2000 is the core program of a computer, which allows the other programs and applications to operate. The operating system is installed on agency servers. Windows 2000 is fully integrated with networking capabilities. Windows 2000 was designed for client/server computing, that facilitates user workstation connections to servers and the sharing of information and services among computers.

The system reviews were performed in accordance with NIST Self-assessment guide. The OIG, supported by Harper, Rains, Knight & Co. P.A., the independent evaluator, determined the critical elements that represent essential tasks for establishing compliance with FISMA, and the guidelines issued by OMB, GAO, CIO Council, and NIST for each control category, including:

- documented security policies;
- documented security procedures;
- implemented security procedures and controls;
- tested and reviewed security procedures and controls; and
- fully integrated security procedures and controls.

For each control category, the evaluator determined the associated objectives, risks, and critical activities, as well as related control techniques and evaluation concerns specific to FCA's information technology environment.

The review was conducted in accordance with the requirements and criteria found in GAO's FISCAM, OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources," current NIST guidance, and the CIO Council Framework. We used this information to evaluate FCA's practices and addressed the above five control areas to be considered in determining compliance with FISMA. For each critical element, the evaluator made a summary determination as to the effectiveness of FCA's related controls. If the controls for one or more of each category's critical elements were found ineffective, then the controls for the entire category are not likely to be effective. The evaluator exercised its professional judgment in making such determinations.

The evaluation focused on the actual performance of the Agency's security program and practices and not on how the Agency measures its performance in its own annual reviews. The Agency's security controls were evaluated for programs and practices including testing the effectiveness of security controls for Agency systems or a subset of systems as required. The evaluator performed

FISMA evaluations in accordance with Federal guidance, e.g, NIST Self-Assessment Guide for Information Technology Systems.

2. Services Provided by Contractors or Other Agencies

   a. FFS

      FFS is provided by the Department of the Interior, National Business Center. FFS is proprietary financial management system software owned and maintained by American Management Systems, Inc. The FFS is made available to FCA through an inter-agency agreement with the Department of the Interior, National Business Center. The FFS is a mainframe computer financial management system that meets the requirements of OMB Circular A-127, Financial Management Systems. FCA relies on annual SAS 70 and other operational reviews to ensure that National Business Center's program and systems are adequately secure and meet the requirements of FISMA, OMB policy and NIST guidelines, national security policy, and agency policy.

   b. Payroll Services from National Finance Center (NFC)

      USDA's NFC located in New Orleans, Louisiana provides the Personnel/Payroll System to FCA. The NFC provides distributed application and telecommunications support for the remote site located in McLean, Virginia. A "master security plan" was developed for the general support system in New Orleans by the responsible NFC organization. The security plan developed by the FCA's OCAO for the remote system at FCA references the master security plan.

      FCA's Personnel/Payroll System provides connectivity to the applications and resources located at the NFC in New Orleans. This permits designated employees of FCA's OCAO to perform the data input and output functions necessary to record personnel actions and accurately calculate pay for employees. The Personnel/ Payroll System at FCA rely on a secure tunnel to exchange information with the NFC in New Orleans via the Internet. Dial-in capabilities are accomplished through the FCA firewall. Security requirements associated with dial-in are addressed in the NFC security plan. FCA relies on annual SAS 70 and other operational reviews to ensure that NFC's program and systems are adequately secure and meet the requirements of FISMA, OMB policy and NIST guidelines, national security policy, and agency policy.

   c. The Electronic Certification System

      The Electronic Certification System (ECS) is maintained by the Department of Treasury (Treasury), Financial Management Service. ECS is a system that agencies use to certify proper payments to Treasury. The FFS electronically transmits data to Treasury. FCA uses ECS to confirm that payment information is correct and can be released by Treasury to the recipients. The ECS is proprietary financial management payment system software owned and maintained by Treasury.

      FCA ensures that the system has adequate security by reviewing the "Electronic Certification Reference Guide" prepared by Treasury. Both FCA and Treasury also separate duties to reinforce security.

   d. Data Security

      A contractor provides offsite storage services for FCA's backup tapes. In 2002 the vendor completed construction and placed into operation a new tape storage facility. The contractor is a recognized leader in data security services that has been protecting business records since 1951 for a diversified customer base, which includes more than half of the Fortune 500 companies. The contractor operates over 50 dedicated data protection facilities in the United States. These sites are staffed with more than 1,200 trained personnel. For over 30 years, the contractor has provided secure, offsite vaulting for disaster recovery and archival data. It serves more than 25,000 companies in over 50 locations.

A.3 Material Weaknesses Identified and Reported Under Existing Law

There were no material weaknesses identified for the fiscal year ended September 30, 2002 or September 30, 2001.

A.3. Identify all material weakness in policies, procedures, or practices as identified and required to be reported under existing law in FY03. Identify the number of material weaknesses repeated from FY02, describe each material weakness, and indicate whether POA&Ms have been developed for all of the material weaknesses.

	FY03 Material Weaknesses			
Bureau Name	Total Number	Total Number Repeated from FY02	Identify and Describe Each Material Weakness	POA&Ms developed? Y/N
Farm Credit Administration	None	None	N/A	N/A
Agency Total	None	None	N/A	N/A

FCA does not currently have any identified material weaknesses or significant deficiencies requiring plans of action and milestones (POA&M). FCA's current security organization structure and program do provide the foundation for an effective POA&M program in the event that significant deficiencies in policies, procedures or practices are identified.

B. Responsibilities of Agency Head

B.1. Identify and describe any specific steps taken by the agency head to clearly and unambiguously set forth FISMA's responsibilities and authorities for the agency CIO and program officials. Specifically how are such steps implemented and enforced?	See Below
B.2. Can a major operating component of the agency make an IT investment decision without review by and concurrence of the agency CIO?	See Below
B.3. 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?	See Below
B.4. During the reporting period, did the agency head take any specific and direct actions to oversee the performance of 1) agency program officials and 2) the CIO to verify that such officials are ensuring that security plans are up-to-date and practiced throughout the lifecycle of each system?	See Below
B.5. Has the agency integrated its information and information technology security program with its critical infrastructure protection responsibilities, and other security programs (e.g., continuity of operations, and physical and operational security)?	See Below
B.6. Does the agency have separate staffs devoted to other security programs, are such programs under the authority of different agency officials, if so what specific efforts have been taken by the agency head or other officials to eliminate unnecessary duplication of overhead costs and ensure that policies and procedures are consistent and complimentary across the various programs and disciplines?	See Below

B.1 Responsibilities and Authorities for the Agency CIO and Program Officials

The Agency-wide information security program is documented in the Policy and Procedure Manual (PPM) number 902. FCA maintains current Agency-wide application and support system security plans in accordance with OMB Circular A-130, Appendix III. The security plans are reviewed and updated annually by considering data sensitivity and data integrity as well as risks of unauthorized internal and external users who may attempt to compromise the system. FCA has established security management that serves as a focal point for the Agency in evaluating the appropriateness and effectiveness of computer related controls on a day-to-day basis.

FCA has established a security organization structure. The CIO is responsible for developing and obtaining approval from the FCA leadership team for an overall policy on the level of security to be achieved in FCA operations. The CIO is responsible for establishing a computer security plan that conforms to security policies established by the FCA Board, and complies with current Federal laws, regulations, standards, and guidelines. The CIO maintains the management control processes to ensure that appropriate administrative, physical, and technical safeguards are incorporated into all newly developed computer applications, and into existing systems when significant modifications are made. The CIO is responsible for periodically reviewing the security of each computer installation and system operated or used by the Agency. The review includes analysis to ascertain that security is commensurate with the risk and magnitude of harm resulting from the loss, misuse or unauthorized access to the Agency information.

FCA's Agency-wide security program addresses the ability to respond rapidly when security breaches occur, and maintains procedures that provide continuity of data processing support when other incidents arise that affect the availability of FCA computers and systems. The security program also provides procedures to ensure that appropriate steps are taken to prevent a reoccurrence.

FCA has integrated its Information Resource Management (IRM) operational and strategic planning with the process of inventorying, classifying and security planning for all Agency hardware and software assets. Staff receives training via an annually updated security module, and periodic news articles and alerts. In short, FCA has approached its security program as one inclusive of, and one that actively engages the entire agency in planning, budgeting, conducting and performing their individual and unit roles within a comprehensive Agency computer security program.

FCA's security program is integrated with the Agency's IRM program. The implementation of planned IRM initiatives has a high profile because these are also documented in the annual IRM planning cycle, approved by the IRM Operations Committee (IRMOC) and senior management, and monitored via monthly and quarterly reports to management. All deliverables are identified along with the resources required to produce them.

The training of staff is conducted and formally tracked by individual, completion date, and a course evaluation is documented from each individual receiving training. For those with specific security responsibilities, training requirements are documented in the individual's development program and employees sent to off site courses as appropriate to their responsibilities.

The actual performance of the information security program is identified in monthly reports to management, quarterly performance measure reports, assessment of the degree to which completion timeframes mandated by the Agency's program are met and in the results of audits completed.

B.2 IT Investment Decisions Without CIO Review and Concurrence

All major IT investment decisions must have review and concurrence by the CIO. The IRM Planning Process controls the IT investment process. Equipment purchases, system maintenance projects and new system requests are submitted to the IRMOC for approval.

B.3 Ensure Security Plan is Practiced

The FCA Chairman and Chief Executive Officer measure the performance of the information security plan through the annual IRM planning process. The performance measures stated in the IRM plan are monitored via monthly and quarterly reports, which are distributed to management. Security plans are updated annually for the mission critical systems. During the FISMA evaluation, the independent reviewers verified that the security plans for the mission critical systems were current.

B.5 Integration of FCA Information Technology Security Program

FCA integrates its information and information technology security program with its critical infrastructure protection responsibilities in two main ways. First, the computer disaster recovery plan is integrated into the Continuity of Operations Plan (COOP) produced by the OCAO. Second, the OCIO reviews operating unit submissions to ensure that equipment required for protecting critical infrastructure is included in the IRM Planning Call and is budgeted for appropriately.

FCA’s official COOP was last updated in conjunction with Y2K contingency preparations. A draft COOP dated May 2003 currently exists, however at the time of this evaluation, the draft plan had not been approved and officially adopted by FCA.

The COOP is the result of the business continuity planning process designed to reduce FCA's risk for an unexpected disruption of its critical functions, no matter whether these are manual or automated, and assure continuity of the minimum level of services necessary for critical operations. The planning is primarily the responsibility of senior management, as they are entrusted with the safeguarding of both the assets and the viability of FCA. Additionally, the COOP drives OCIO plans to recover information processing capabilities, as well as other unit plans to recover operational capabilities. The IS recovery plan must be consistent with and support the overall plan of the organization.

FCA's OCIO and other operating offices have prepared continuity and recovery plans that provide the capabilities to support all of the services identified by senior management in the draft COOP. However, senior management should complete the draft COOP and ensure that it is adopted as the official plan for FCA.

Without an authorized COOP based on current business continuity planning considerations, FCA cannot be sure that OCIO and other operating unit disaster recovery plans will provide the services that top management deems critical for operations.

B.6 Coordination of Security Staff, Policies and Procedures

FCA has established a security organization structure. The CIO is responsible for developing and obtaining the approval from the FCA leadership team for an overall policy on the level of security to be achieved in FCA operations. The CIO is responsible for establishing a computer security plan that conforms to security policies established by the FCA Board, and complies with current Federal laws, regulations, standards, and guidelines. The CIO maintains the management control processes to ensure that appropriate administrative, physical, and technical safeguards are incorporated into all newly developed computer applications, and into existing systems when significant modifications are made. The CIO is responsible for periodically reviewing the security of each computer installation and system operated or used by the Agency. The review includes analyses to ascertain that security is commensurate with the risk and magnitude of the harm resulting from the loss, misuse or unauthorized access to the Agency information.

FCA has Agency-wide security plans that ensure policies and procedures are consistent across systems and FCA security personnel report directly to the CIO. As a result, the Agency eliminates unnecessary duplication of overhead costs.

B.7 Identification of Critical Operations and Assets and their Interdependencies and Interrelationships

B.7. Identification of agency's critical operations and assets (both national critical operations and assets and mission critical) and the interdependencies and interrelationships of those operations and assets.				
a. Has the agency fully identified its critical operations and assets, including their interdependencies and interrelationships?	Yes			
b. If yes, describe the steps the agency has taken as a result of the review.	See Below			
c. If no, please explain why.	N/A			

FCA has five mission critical systems and their interdependencies and interrelationships are identified through the annual planning and budget process.

The OCIO issues a Call for Agency input on future information resource needs including hardware, software, development, maintenance, and training. The IRMOC reviews the IRM Call submissions and assigns a numeric rating to each proposed project and investment based on criteria derived from OMB guidance. The investment review process considers both risk and anticipated return and includes a review of each project's alignment with and impact on FCA's enterprise architecture (EA). This rating identifies and prioritizes critical assets within the EA including interdependencies, interrelationships and links to external systems. Based on the relative levels of each proposed project or investment, the IRMOC recommends approval of the higher priority items to senior management. The CIO submits the recommended initiatives and the IRM budget to senior management for approval of the Plan. The EA is updated annually to reflect changes due to completed IT investments and projects.

Ongoing identification and reassessment of critical assets, especially the applications and general support systems, is also conducted during the annual planning process. OCIO maintains an inventory of systems and applications. This inventory is updated each year during the IRM Planning Call. The sponsor of each system indicates whether the system is still required, needs revision, or is no longer needed. The sponsor, in consultation with OCIO staff, determines whether a system is a major application. OCIO staff uses a technical committee approach to determine which systems are general support systems. In addition, OCIO ensures that all systems are either provided adequate security by the general support systems, or are identified as a major application with a unique security plan.

B.8 Documented Procedures for Reporting Security Incidents & Sharing Information on Common Vulnerabilities

B.8. How does the agency head ensure that the agency, including all components, has documented procedures for reporting security incidents and sharing information regarding common vulnerabilities?	
a. Identify and describe the procedures for external reporting to law enforcement authorities and to the Federal Computer Incident Response Center (FedCIRC).	See Below
b. Total number of agency components or bureaus.	1
c. Number of agency components with incident handling and response capability.	1
d. Number of agency components that report to FedCIRC.	1
e. Does the agency and its major components share incident information with FedCIRC in a timely manner consistent with FedCIRC and OMB guidance?	Yes
f. What is the required average time to report to the agency and FedCIRC following an incident?	24 hours
g. How does the agency, including the programs within major components, confirm that patches have been tested and installed in a timely manner?	Logged & Monitored in "Network Security Vulnerability Database"
h. Is the agency a member of the Patch Authentication and Distribution Capability operated by FedCIRC?	Yes
i. If yes, how many active users does the agency have for this service?	5
j. Has the agency developed and complied with specific configuration requirements that meet their own needs?	Yes
k. Do these configuration requirements address patching of security vulnerabilities?	Yes

FCA has documented their incident handling procedures. The FCA Computer Security Officer (CSO) is notified of all security incidents and provides coordination of the incident response to higher levels within FCA or for reporting to external entities when appropriate. Several staff may be involved in the response to an incident depending on its type and severity. System, Network, and Database Administrators or other staff are directed to respond to the incident as appropriate. FCA has specific incident procedures for viruses, worms, hackers/crackers and responding to identified security vulnerabilities. Minor incidents may only require the actions of an administrator to resolve the issue while severe incidents may entail more staff assistance and may ultimately invoke the Disaster Recovery Plan.

Information regarding the release of a security incident is controlled. The site specific information such as account or system names, network addresses or program specific information is not released to outside agencies. All reporting of incidents is performed by the CSO. All release of information regarding an incident must be reviewed and authorized by the CIO and the CSO.

It is the Agency's policy to report all potential threats to the Federal Computer Incident Response Center (FedCIRC) and the National Infrastructure Protection Center. Incidents involving fraud, system penetration, theft of Agency assets, or other suspected criminal activity is reported to the Federal Bureau of Investigation or other duly appointed authority, such as the U.S. Secret Service. In addition, all suspected criminal activity is reported to FCA's Office of General Counsel and OIG.

B.9 Security Incidents Reported During FY 2003

<table>
<tr><th colspan="3">B.9. Identify by bureau, the number of incidents (e.g., successful and unsuccessful network penetrations, root or user account compromises, denial of service attacks, website defacing attacks, malicious code and virus, probes and scans, password access) reported and those reported to FedCIRC or law enforcement.</th></tr>
<tr><td>Bureau Name</td><td>Number of incidents reported</td><td>Number of incidents reported externally to FedCIRC or law enforcement</td></tr>
<tr><td>Farm Credit Administration</td><td></td><td>None</td></tr>
<tr><td></td><td></td><td></td></tr>
</table>

During the reporting period, FCA was not the target of attacks other than those considered routine. FCA was not adversely affected, or embarrassed, due to any security incident, routine or otherwise.

The bulk of the incidents fell into the category of viruses, worms, etc., proliferated by malicious e-mails and their associated attachments. These were predominantly handled by FCA’s total virus defense implementation.

The OCIO firewall logs reflected a significant increase in various types of scans. None constituted successful attempts to gain access to unauthorized services. The activity did not result in penetration of FCA’s firewall or rise to the level of persistence or volume that OCIO thought warranted reporting to FedCIRC or law enforcement.

While not actually security incidents, FCA did forward hundreds of various Internet scam type fraudulent e-mail solicitations to the U.S. Secret Service.

C.1 Risk Assessment, Appropriate Level of Security, Security Planning & Evaluation of Controls

C.1. Have agency program officials and the agency CIO: 1) assessed the risk to operations and assets under their control; 2) determined the level of security appropriate to protect such operations and assets; 3) maintained an up-to-date security plan (that is practiced throughout the life cycle) for each system supporting the operations and assets under their control; and 4) tested and evaluated security controls and techniques? By each major agency component and aggregated into an agency total, identify actual performance in FY03 according to the measures and in the format provided below for the number and percentage of total systems.

Bureau Name	Total Number of Systems	Number of systems assessed for risk and assigned a level or risk		Number of systems that have an up-to-date IT security plan		Number of systems certified and accredited		Number of systems with security control costs integrated into the life cycle of the system		Number of systems for which security controls have been tested and evaluated in the last year		Number of systems with a contingency plan		Number of systems for which contingency plans have been tested	
		No. of Systems	% of Systems	No.	%	No.	%	No.	%	No.	%	No.	%	No.	%
FCA	5	5	100	5	100	*	*	5	100	5	100	4	80	4	80
Agency Total	5	5	100	5	100	*	*	5	100	5	100	4	80	4	80

*FCA does not have a formal certification and accreditation (C&A) process. FCA relies on its system security plan update procedures to provide the assurances required for system certification and accreditation. While FCA does not have a formal C&A process, its current procedures do ensure that management, operational, and technical controls are assessed by management prior to a system being placed in service and that those controls are reevaluated on a periodic basis. Additionally, FCA's current procedures ensure that the minimum security controls, required by OMB Circular A-130, that must be in place prior to authorizing a system for processing are present. FCA management continues to evaluate the need for a formal C&A process in conjunction with evolving guidance from OMB and NIST.

The assessment of risk at FCA is done at multiple levels both strategic and operational, and the program entails review of pertinent factors on at least an annual basis. Security plans for all major applications are being updated annually, and a risk assessment component is associated with each update. The security plans conform to NIST SP 800-18 guidelines, which include sections on information sensitivity, risk assessment and management, review of security controls, operations and technical controls.

The security plans provide an overview of security requirements, describe the controls in place, delineate responsibilities, and expected behavior of all individuals who access the system. The plans address the sensitivity and criticality of the information stored in, processed by, or transmitted via FCA systems. This assessment of system information provides a basis for determining major systems and is one of the core factors in risk management. The risk analysis considers availability, integrity and confidentially of the information. Under each of the three categories, the risks are High, Medium and Low. Each security plan identifies threats; vulnerabilities and security measures required to adequately mitigate the risk to systems or assets posed by those threats and vulnerabilities.

FCA's risk cycle includes testing and evaluating controls, analyzing the results, and adopting appropriate countermeasures to improve security. Security is tested and evaluated periodically by FCA staff and outside vendors.

OCIO maintains a Lotus Notes database to collect information on publicly announced security vulnerabilities relating to the software and hardware currently in use within the Agency.

FFS, Lotus Notes, Personnel/Payroll System and Windows 2000 have contingency plans. The recovery time of CRS, after an unplanned disruption, is not time critical. FCA may have up to 30 days to recover. As a result, CRS does not have a documented contingency plan.

C.2 Maintain Agency-Wide IT Security Program, Ensure Effective Implementation & Evaluate Performance

C.2. Identify whether the agency CIO has adequately maintained an agency-wide IT security program and ensured the effective implementation of the program and evaluated the performance of major agency components.

Has the agency CIO maintained an agency-wide IT security program? Y/N	Did the CIO evaluate the performance of all agency bureaus/components? Y/N	How does the agency CIO ensure that bureaus comply with the agency-wide IT security program?	Has the agency CIO appointed a senior agency information security officer per the requirements in FISMA?	Do agency POA&Ms account for all known agency security weaknesses including all components?
Yes	Yes	See Below	Yes	N/A

The CIO has adequately maintained an agency-wide security program. As stated earlier, the Agency-wide program is documented in the PPM number 902. FCA maintains current Agency-wide application and system security plans in accordance with OMB Circular A-130, Appendix III. The security plans are reviewed and updated annually. FCA has established a security organizational structure and security program that is integrated with the Agency's IRM plan.

C.3 Ensure Security Training and Awareness for all Employees and Contractors

C.3. Has the agency CIO ensured security training and awareness of all agency employees, including contractors and those employees with significant IT security responsibilities?

Total number of agency employees in FY03	Agency employees that received IT security training in FY03		Total number of agency employees with significant IT security responsibilities	Agency employees with significant security responsibilities that received specialized training		Briefly describe training provided	Total costs for providing training in FY03
	Number	Percentage		Number	Percentage		
280	268	96	14	13	93	See Below	$31,000

FCA provided an in-house training course presented to all employees during December 2002. To further employee awareness of security, FCA awarded the employees a token and conducted a reception after conclusion of the training session. For those with specific security responsibilities, training requirements are considered in the individual's development program and the employees are sent to off site courses as appropriate to their responsibilities. New employees are provided security awareness training during an orientation session. FCA provided additional emphasis on security awareness through articles in the employee newsletter and e-mail alerts.

C.4 Integrate Security into the Capital Planning and Investment Control Process

C.4. Has the agency CIO fully integrated security into the agency's capital planning and investment control process? Were IT security requirements and costs reported on every FY05 business case (as well as in the exhibit 53) submitted by the agency to OMB?				
Bureau Name	Number of business cases submitted to OMB in FY05	Did the agency program official plan and budget for IT security and integrate security into all of their business cases? Y/N	Did the agency CIO plan and budget for IT security and integrate security into all of their business cases? Y/N	Are IT security costs reported in the agency's exhibit 53 for each IT investment? Y/N
FCA	None	N/A	N/A	N/A

The CIO is responsible for ensuring that agency security programs integrate fully into the Agency's EA and capital planning and investment control processes. Security is built into and funded as part of the system architecture. The CIO develops security policy and level of security to be achieved. The Chairman and FCA Board approve the policy. The CIO develops an overall plan to achieve the security objectives and to comply with current law, regulations, and guidance.

The CIO's overall security program integrates the security program into the IRM Planning Process and into the life cycle management of each system. Before any system can be developed or modified, the Program Offices must submit a proposal during the IRM Planning Call. The IRMOC reviews the IRM Call submissions and recommends approval or disapproval of equipment purchases and system maintenance projects. It also prioritizes proposed development projects and enhancements to existing systems using criteria derived from OMB guidance. These evaluations include a review of each project's alignment with and impact on FCA's EA. Security risks and demands on the network are carefully analyzed. The budgeted costs of security appear as line items in the OCIO budget and are cross-referenced to the costs of meeting strategic goals and to the costs of specific operating Office hardware and software requests.

In addition, OCIO maintains an inventory of systems and applications. This inventory is updated each year during the IRM Planning Cycle. The sponsor of each system indicates whether it is still required, needs revision, or is no longer needed. The security level of each system is reviewed and revised as necessary during this review.