FARM CREDIT ADMINISTRATION

AGREED-UPON PROCEDURES REPORT:
FEDERAL INFORMATION SECURITY
MANAGEMENT ACT EVALUATION

SEPTEMBER 30, 2004

HARPER, RAINS, KNIGHT & COMPANY, P.A.
CERTIFIED PUBLIC ACCOUNTANTS
RIDGELAND, MISSISSIPPI

CONTENTS

PAGE

HRK

HARPER, RAINS, KNIGHT
& COMPANY

Independent Accountant's Report
on Applying Agreed-Upon Procedures

The Inspector General
Farm Credit Administration

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 FY 2004 evaluation of the Farm Credit Administration's (FCA) security program and practices. This engagement was conducted in accordance with Statements on Standards for Attestation engagements 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.

The system evaluations were performed in accordance with NIST Self-assessment guide. The Office of Inspector General, 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 through:

Review of information security policies and procedures;
Inquiries of FCA personnel;
Observation of system access controls;
Review of system documentation including security plans, software change requests and approvals, security logs and audit trails.

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 to perform our evaluation.

In our evaluation we considered the following mission critical systems:

Federal Financial System (FFS)
Personnel/Payroll System
Consolidated Reporting System
Windows 2000 Network
Lotus Domino (Notes)

Our procedures did not reveal any information security control matters that we deemed to be significant deficiencies that must be reported under FISMA. The results of our information security program and practices evaluation are summarized in Exhibit II.

We were not engaged to, and did not conduct an examination, the objective of which would be the expression of an opinion on the Farm Credit Administration's 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 30, 2004

Exhibit I - Objectives, Scope and Methodology

The Office of Inspector General, 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 for FY 2004.

A. General Overview

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 (System). FCA promulgates regulations to implement the Farm Credit Act of 1971, and examines System institutions for compliance with the Act, regulations, and safe and sound banking practices.

FCA has less 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.

B 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 FY04 and FY03, 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 the major application that supports all FCA 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 (USGS)/National Business Center (NBC), and American Management Systems, Inc. (AMS). The FFS software is owned and maintained by AMS. AMS 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 (OCFO) is responsible for managing security access control to the FFS agency application. The FFS was placed in production in June 2001.

b. Payroll Services from National Finance Center (NFC)

USDA's National Finance Center (NFC) located in New Orleans, Louisiana provides the Personnel/Payroll System (PPS) 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 the Chief Administrative Officer (OCAO) maintains a security plan for the remote system at FCA that incorporates provisions of the master security plan.

c. Consolidated Reporting System (CRS)

CRS is a major application that supports FCA operations. CRS is an Oracle relational 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 Farm Credit System (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 Farm Credit System (FCS) Lender Institutions. Institutions submit the data quarterly to the FCA via diskette or zip file. The loan data are loaded using SQLLoader, and are then verified and validated by FCA personnel.

  Web-based CRS Reports is an FCA developed application using the JavaScript front-end interface and an Oracle database back-end application. The reports are built via using e-Reporting Suite, and 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.

2. Mission Critical General Support Systems

a. Windows 2000

Windows 2000 is an operating system or the core program of a computer that allows the other programs and applications to operate. Windows 2000 is fully integrated with networking capabilities and was designed for client/server computing to facilitate user workstation connections to servers and the sharing of information and services among computers.

Windows 2000 Server is the primary operating system installed on substantially all servers in the FCA network. Additionally, Windows 2000 and XP are installed on agency laptop and desktop computers where they function as a client to the FCA network as well as a stand-alone operating system for the client hardware. Through Windows 2000/XP, users can access network services such as file servers, e-mail, the Internet, applications and shared hardware such as printers.

b. Lotus Domino (Notes)

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

C. Methodology

The system evaluations were performed in accordance with NIST Self-assessment guide. The Office of Inspector General, 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 evaluation 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, 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 evaluations. 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.

Our procedures did not reveal any information security control matters that we deemed to be significant deficiencies that must be reported under FISMA.

During FY 2004 FCA OIG performed an inspection of the Office of the Chief Financial Officer's project management practices over two information systems that are currently in the implementation phase. That inspection revealed several weaknesses that OIG has communicated to management in a separate report. We considered OIG's findings during this evaluation and determined that they do not indicate significant deficiencies that must be reported under FISMA. However, OIG's findings are indicative of reportable conditions that OCFO must address in a POA&M.

Exhibit OMB FISMA Reporting Template

Section A: System Inventory and IT Security Performance
NOTE: ALL of Section A should be completed by BOTH the Agency CIO and the OIG.
To enter data in allowed fields, use password: fisma

A.1. By bureau (or major agency operating component), identify the total number of programs and systems in the agency and the total number of contractor operations or facilities. The agency CIOs and IG's shall each identify the total number that they reviewed as part of this evaluation in FY04. NIST 800-26, is to be used as guidance for these reviews.

A.2. For each part of this question, identify actual performance in FY04 for the total number of systems by bureau (or major agency operating component) in the format provided below.

	A.1						A.2									
	A.1.a. FY04 Programs		A.1.b. FY04 Systems		A.1.c. FY04 Contractor Operations or Facilities		A.2.a. Number of systems certified and accredited		A.2.b. Number of systems with security control costs integrated into the life cycle of the system		A.2.c. Number of systems for which security controls have been tested and evaluated in the last year		A.2.d. Number of systems with a contingency plan		A.2.e. Number of systems for which contingency plans have been tested	
Bureau Name	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Percent of Total	Total Number	Percent of Total	Total Number	Percent of Total	Total Number	Percent of Total	Total Number	Percent of Total
Farm Credit Administration	1	1	5	5	5	5	0	0.0%	5	100.0%	5	100.0%	4	80.0%	4	80.0%
Agency Total	1	1	5	5	5	5	0	0.0%	5	100.0%	5	100.0%	4	80.0%	4	80.0%

Comments:

During the prior year FISMA evaluation OIG questioned whether FCA had established an appropriate certification and accreditation (C&A) process. Specifically, OIG found that FCA largely relied on procedures related to annual security plan updates to provide system C&A. While their process included assessment steps customarily associated with certification and accreditation, FCA did not document them within a formal C&A package. FCA management stated that their procedures, when considered collectively, provided a de facto compliant C&A process. FCA OCIO subsequently filed a POA&M to formalize its C&A procedures and ensure a compliant process. At present, FCA has developed formal C&A procedures and is in the process of procuring independent certifying agent services to complete the POA&M.

FCA has contingency plans covering four of the five systems evaluated. The recovery time of the fifth system, after an unplanned disruption, is not time critical. FCA may have up to 30 days to recover. As a result, the fifth system does not have a documented contingency plan.

A.3

A.3. Evaluate the degree to which the following statements reflect the status in your agency, by choosing from the responses provided in the drop down menu. If appropriate or necessary, include comments in the Comment area provided below.

Statement	Evaluation
a. Agency program officials and the agency CIO have used appropriate methods 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.	Almost Always, or 96-100% of the time
b. The reviews of programs, systems, and contractor operations or facilities, identified above, were conducted using the NIST self-assessment guide, 800-26.	Almost Always, or 96-100% of the time
c. In instances where the NIST self-assessment guide was not used to conduct reviews, the alternative methodology used addressed all elements of the NIST guide.	Almost Always, or 96-100% of the time
d. The agency maintains an inventory of major IT systems and this inventory is updated at least annually.	Almost Always, or 96-100% of the time
e. The OIG was included in the development and verification of the agency's IT system inventory.	Almost Always, or 96-100% of the time
f. The OIG and the CIO agree on the total number of programs, systems, and contractor operations or facilities.	Almost Always, or 96-100% of the time
g. The agency CIO reviews and concurs with the major IT investment decisions of bureaus (or major operating components) within the agency.	Almost Always, or 96-100% of the time
Statement	**Yes or No**
h. The agency has begun to assess systems for e-authentication risk.	No
i. The agency has appointed a senior agency information security officer that reports directly to the CIO.	Yes

Comments:
FCA management is aware of the e-authentication risk assessment requirements contained in OMB Memorandum M-04-04 and the related technical guidance provided by NIST Special Publication 800-63. At present FCA has performed preliminary consideration of its e-government systems and believes that none of the systems would rise above level 2 described in the OMB guidance. Given that level of system risk FCA must be compliant with M-04-04, with regard to its existing systems. by September 15, 2005. The agency is also aware that new authentication systems should begin to be categorized by September 2004, however no new systems are planned for development in that timeframe. FCA OCIO is currently scheduling the resources and actions necessary to obtain compliance.

Section B: Identification of Significant Deficiencies
NOTE: ALL of Section B should be completed by BOTH the Agency CIO and the OIG.
To enter data in allowed fields, use password: fisma

B.1. By bureau, identify all FY 04 significant deficiencies in policies, procedures, or practices required to be reported under existing law. Describe each on a separate row, and identify which are repeated from FY03. In addition, for each significant deficiency, indicate whether a POA&M has been developed. Insert rows as needed.

B.1.

	FY04 Significant Deficiencies			
Bureau Name	Total Number	Total Number Repeated from FY03	Identify and Describe Each Significant Deficiency	POA&M developed? Yes or No
Farm Credit Administration			N/A	
Agency Total	0	0		

Comments: There were no significant deficiencies or material weaknesses identified during the OIG or agency FISMA evaluations for FY 2004. Additionally, none were identified for the fiscal years ended September 30, 2003 or September 30, 2002.

Section C: OIG Assessment of the POA&M Process
NOTE: Section C should *ONLY* be completed by the OIG. The CIO should leave this section blank.
To enter data in allowed fields, use password: fisma

C.1. Through this question, and in the format provided below, assess whether the agency has developed, implemented, and is managing an agency-wide plan of action and milestone (POA&M) process. This question is for IGs only. Evaluate the degree to which the following statements reflect the status in your agency by choosing from the responses provided in the drop down menu. If appropriate or necessary, include comments in the Comment area provided below.

C.1

Statement	Evaluation
a. Known IT security weaknesses, from all components, are incorporated into the POA&M.	Almost Always, or 96-100% of the time
b. **Program officials** develop, implement, and manage POA&Ms for systems they own and operate (systems that support their program or programs) that have an IT security weakness.	Almost Always, or 96-100% of the time
c. Program officials report to the CIO on a regular basis (at least quarterly) on their remediation progress.	Almost Always, or 96-100% of the time
d. **CIO** develops, implements, and manages POA&Ms for every system they own and operate (a system that supports their program or programs) that has an IT security weakness.	Almost Always, or 96-100% of the time
e. CIO centrally tracks, maintains, and reviews POA&M activities on at least a quarterly basis.	Almost Always, or 96-100% of the time
f. The POA&M is the authoritative agency **and** IG management tool to identify and monitor agency actions for correcting information and IT security weaknesses.	Almost Always, or 96-100% of the time
g. System-level POA&Ms are tied directly to the system budget request through the IT business case as required in OMB budget guidance (Circular A-11).	Almost Always, or 96-100% of the time
h. OIG has access to POA&Ms as requested.	Almost Always, or 96-100% of the time
i. OIG findings are incorporated into the POA&M process.	Almost Always, or 96-100% of the time
j. POA&M process prioritizes IT security weaknesses to help ensure that significant IT security weaknesses are addressed in a timely manner and receive appropriate resources.	Almost Always, or 96-100% of the time

Comments:

FCA OCIO has developed comprehensive procedures for monitoring system security controls and implementing corrective actions. The procedures provide for identification of system vulnerabilities through monitoring of existing security controls, scrutiny of system vulnerability alerts issued by US-CERT and vendors, annual internal assessment of security controls and consideration of information security control related findings from OIG audits and inspections. Once vulnerabilities or control weaknesses are identified the associated risks and potential magnitude of harm are assessed, a priority schedule is established, required resources are allocated and a POA&M is created. For each POA&M, specific personnel are assigned to each required task and progress is monitored until resolution. At present FCA has one POA&M resulting from findings identified in OIG's 2003 independent FISMA evaluation. FCA has made substantive progress on the POA&M and has exhibited continuous monitoring capabilities including quarterly updates filed with OMB.

C.1 OIG Assessment of the Certification and Accreditation Process

Section C should only be completed by the OIG. OMB is requesting IGs to assess the agency's certification and accreditation process in order to provide a qualitative assessment of this critical activity. This assessment should consider the quality of the Agency's certification and accreditation process. Any new certification and accreditation work initiated after completion of NIST Special Publication 800-37 should be consistent with NIST Special Publication 800-37. This includes use of the FIPS 199, "Standards for Security Categorization of Federal Information and Information Systems," to determine an impact level, as well as associated NIST documents used as guidance for completing risk assessments and security plans. Earlier NIST guidance is applicable to any certification and accreditation work completed or initiated before finalization of NIST Special Publication 800-37. Agencies were not expected to use NIST Special Publication 800-37 as guidance before it became final.

Statement	Evaluation
Assess the overall quality of the Agency's certification and accreditation process. Comments: As a result of the FY 2003 independent FISMA evaluation, OIG questioned whether FCA had established an appropriate certification and accreditation (C&A) process. Specifically, OIG found that FCA largely relied on procedures related to annual security plan updates to provide system C&A. While their process included assessment steps customarily associated with certification and accreditation, FCA did not document them within a formal C&A package. The primary components missing from FCA's process were documentation of the specific controls to be evaluated and the related evaluation methodologies, evidence of independent evaluation of security controls, and a formal security accreditation decision letter. Overall, OIG found that FCA's C&A procedures were adequate for continuous monitoring of security controls but that the C&A procedures should be strengthened to meet the OMB policy requiring system reauthorization (certification and accreditation) at least every three years or when significant changes are made. Based on the OIG finding and the finalization of NIST SP 800-37, FCA OCIO developed a POA&M to formalize its C&A procedures and ensure a compliant process. At present, FCA has updated control documentation, developed proposed formal C&A procedures and is in the process of procuring independent certifying agent services to complete the POA&M.	Satisfactory

Section D
NOTE: ALL of Section D should be completed by BOTH the Agency CIO and the OIG.
To enter data in allowed fields, use password: fisma

D.1. First, answer D.1. If the answer is yes, then proceed. If no, then skip to Section E. For D.1.a-f, identify whether agencywide security configuration requirements address each listed application or operating system (Yes, No, or Not Applicable), and then evaluate the degree to which these configurations are implemented on applicable systems. **For example:** If your agency has a total of 200 systems, and 100 of those systems are running Windows 2000, the universe for evaluation of degree would be 100 systems. If 61 of those 100 systems follow configuration requirement policies, and the configuration controls are implemented, the answer would reflect "yes" and "51-70%". If appropriate or necessary, include comments in the Comment area provided below.

D.2. Answer Yes or No, and then evaluate the degree to which the configuration requirements address the patching of security vulnerabilities. If appropriate or necessary, include comments in the Comment area provided below.

D.1. & D.2.

	Yes, No, or N/A	Evaluation
D.1. Has the CIO implemented agencywide policies that require detailed specific security configurations and what is the degree by which the configurations are implemented?	**Yes**	
a. Windows XP Professional	Yes	Almost Always, or 96-100% of the time
b. Windows NT	Yes	Almost Always, or 96-100% of the time
c. Windows 2000 Professional	Yes	Almost Always, or 96-100% of the time
d. Windows 2000	N/A	
e. Windows 2000 Server	Yes	Almost Always, or 96-100% of the time
f. Windows 2003 Server	N/A	
g. Solaris	N/A	
h. HP-UX	N/A	
i. Linux	N/A	
j. Cisco Router IOS	Yes	Almost Always, or 96-100% of the time
k. Oracle	Yes	Almost Always, or 96-100% of the time
l. Other. Specify:	N/A	
	Yes or No	**Evaluation**
D.2. Do the configuration requirements implemented above in D.1.a-f., address patching of security vulnerabilities?	Yes	Almost Always, or 96-100% of the time

Comments:

Workstations connected to FCA's network utilize either Windows 2000 or XP as their operating systems. FCA OCIO has developed specific security configurations that are applied to the workstations before they are delivered to the user. The configurations include local security policies that aid in protecting the workstation from unauthorized users and that prevent authorized users from making major changes to the operating system. Another example is a domain system policy that prevents the user from accessing or modifying the registry. OCIO system administrators have considered the Windows 2000 and XP configuration guidelines contained in NIST SP 800-43 and 800-68 and modified those configurations based on FCA specific environmental considerations.

Windows 2000 Server is the primary operating system installed on substantially all servers in the FCA network. Cisco is the primary supplier of routers and switches used in FCA's network. FCA OCIO has developed specific security configurations for its network equipment using baseline security measures from vendors and others sources and modified them for FCA specific environmental factors.

FCA maintains an active program for identifying and remediation of security vulnerabilities. A cornerstone of the program is a Lotus Notes database utilized by OCIO for collecting information on announced security vulnerabilities relating to the hardware and software currently in use at FCA. The database also facilitates tracking of the status of efforts to patch the vulnerabilities. FCA OCIO monitors several sources for vulnerabilities including vendor and US CERT bulletins. Identified vulnerabilities are posted to the Notes database and appropriate staff is assigned to take necessary actions. Required patches are pushed to all workstations using system management software. Additionally, FCA utilizes automated methods to ensure that current updates to its anti-virus software are installed on its servers and workstations.

Section E: Incident Detection and Handling Procedures

NOTE: ALL of Section E should be completed by BOTH the Agency CIO and the OIG.

To enter data in allowed fields, use password: fisma

E.1. Evaluate the degree to which the following statements reflect the status at your agency. If appropriate or necessary, include comments in the Comment area provided below.

E.1

Statement	Evaluation
a. The agency follows documented policies and procedures for reporting incidents internally.	Almost Always, or 96-100% of the time
b. The agency follows documented policies and procedures for external reporting to law enforcement authorities.	Almost Always, or 96-100% of the time
c. The agency follows defined procedures for reporting to the United States Computer Emergency Readiness Team (US-CERT). http://www.us-cert.gov	Almost Always, or 96-100% of the time

E.2.

E.2. Incident Detection Capabilities.

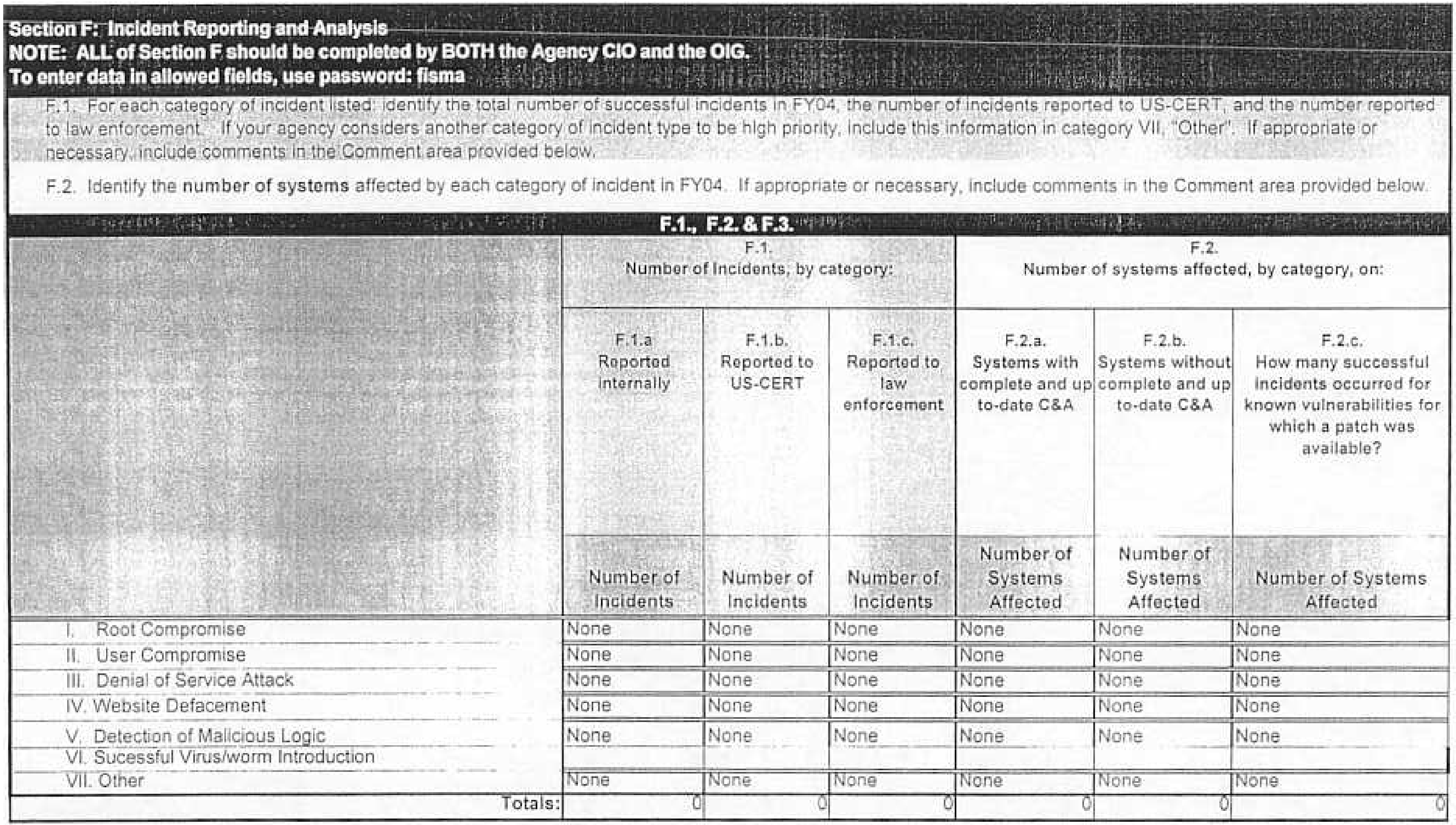
	Number of Systems	Percentage of Total Systems
a. How many systems underwent vulnerability scans and penetration tests in FY04?	1	20%

b. Specifically, what tools, techniques, technologies, etc., does the agency use to mitigate IT security risk?

Answer:

Virus scanning software, network firewalls, automated security patching software, network intrusion detection and alert software, a proprietary database to identify and manage installation of security patches, application security logs, VPN's to encrypt WAN communications, and others

Comments:



Section F: Incident Reporting and Analysis

NOTE: ALL of Section F should be completed by BOTH the Agency CIO and the OIG.

To enter data in allowed fields, use password: fisma

F.1. For each category of incident listed: identify the total number of successful incidents in FY04, the number of incidents reported to US-CERT, and the number reported to law enforcement. If your agency considers another category of incident type to be high priority, include this information in category VII, "Other". If appropriate or necessary, include comments in the Comment area provided below.

F.2. Identify the **number of systems** affected by each category of incident in FY04. If appropriate or necessary, include comments in the Comment area provided below.

F.1., F.2. & F.3.

	F.1. Number of Incidents, by category:			F.2. Number of systems affected, by category, on:		
	F.1.a Reported internally	F.1.b. Reported to US-CERT	F.1.c. Reported to law enforcement	F.2.a. Systems with complete and up to-date C&A	F.2.b. Systems without complete and up to-date C&A	F.2.c. How many successful incidents occurred for known vulnerabilities for which a patch was available?
	Number of Incidents	Number of Incidents	Number of Incidents	Number of Systems Affected	Number of Systems Affected	Number of Systems Affected
I. Root Compromise	None	None	None	None	None	None
II. User Compromise	None	None	None	None	None	None
III. Denial of Service Attack	None	None	None	None	None	None
IV. Website Defacement	None	None	None	None	None	None
V. Detection of Malicious Logic	None	None	None	None	None	None
VI. Sucessful Virus/worm Introduction						
VII. Other	None	None	None	None	None	None
Totals:	0	0	0	0	0	0

Comments:

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.

Section G: Training
NOTE: ALL of Section G should be completed by BOTH the Agency CIO and the OIG.
To enter data in allowed fields, use password: fisma

G.1. Has the agency CIO ensured security training and awareness of all employees, including contractors and those employees with significant IT security responsibilities? If appropriate or necessary, include comments in the Comment area provided below.

G.1.

G.1.a. Total number of employees in FY04	G.1.b. Employees that received IT security awareness training in FY04, as described in NIST Special Publication 800-50		G.1.c. Total number of employees with significant IT security responsibilities	G.1.d. Employees with significant security responsibilities that received specialized training, as described in NIST Special Publications 800-50 and 800-16		G.1.e. Briefly describe training provided	G.1.f. Total costs for providing IT security training in FY04 (in $'s)
	Number	Percentage		Number	Percentage		
303	294	0.97029703	20	16	0.8	20 minute video presentation titled "Stolen Access" that addressed common security breaches.	$36,406

G.2.

	Yes or No
a. Does the agency explain policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency wide training?	Yes

Comments:
FCA provided an in-house training course presented to all employees during FY 2004. 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. FCA provided additional security awareness via articles in the employee newsletter and e-mail alerts.