THE FARM CREDIT ADMINISTRATION

AGREED-UPON PROCEDURES:
GISRA REVIEW

August 31, 2001

TABLE OF CONTENTS

PAGE

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Independent Accountant's Agreed-Upon Procedures Report

To the Inspector General of the
Farm Credit Administration

We have performed the procedures summarized below and presented in more detail in Exhibit B which 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) security program and practices. This agreed-upon procedures 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.

We performed the procedures that determined the critical elements which represent tasks that are essential for establishing compliance with Government Information Security Reform Act (GISRA), 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 audit 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, the CIO Council Framework, and information gleaned during the review of any FCA security incidents that may have occurred at the agency during the evaluation period.

Centerpark I
4041 Powder Mill Road, Suite 410
Calverton, Maryland 20705-3106
tel: 301-931-2050
fax: 301-931-1710

www.cliftoncpa.com

In our review we considered the following mission critical systems:

- Federal Financial System (FFS)
- Consolidated Reporting System (CRS)
- Lotus Notes
- WindowsNT
- Firewall System
- FCA Web site

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.

This report is intended solely for the information and use of the FCA's Office of Inspector General and is not intended to be and should not be used by anyone other than this specified party.

Clifton Gunderson LLP

Calverton, Maryland
August 31, 2001

Centerpark I
4041 Powder Mill Road, Suite 410
Calverton, Maryland 20705-3106
tel: 301-931-2050
fax: 301-931-1710

www.cliftoncpa.com

EXHIBIT A: GISRA EXECUTIVE SUMMARY

In accordance with Memorandum M-01-24
Reporting Instructions for the
Government Information Security Reform Act

The Office of Inspector General, supported by a contract with Clifton Gunderson LLP performed an independent evaluation of the Farm Credit Administration's (FCA or Agency) information security program and practices of the agency.

1. Introduction

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.

The Farm Credit Administration has approximately 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.

2. Mission critical systems under evaluation

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 accordance with FY 2001 Defense Authorization Act, Section X, Subtitle G, which contains the Government Information Security Reform Act (GISRA), we evaluated the following mission critical systems.

a. Federal Financial System (FFS)

FFS is one of the major applications of FCA that supports all the core accounting systems including budget execution, accounts payable, disbursements, purchasing, travel, accounts receivable, general ledger, document tracking, project cost accounting, and external reporting. The 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 System, 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 security administrator 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 an relational database containing financial and statistical information on active and inactive Farm Credit Institutions. CRS contains three distinct subsystems including 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, and the data are quarterly submitted to the FCA via diskette or zip file. The loan data was loaded, verified and validated by two designed FCA personnel.

- Web-based CRS Reports – is an in-house 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 selected FCA users who are authorized to view their institution data.

c. Lotus 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.

d. Mission Critical General Support Systems.

FCA has three mission critical general support systems.

- WindowsNT

  Windows NT 4.0 operating system is the core program of a computer, which allows the other programs and applications to operate. The operating system is installed on all agency servers and Micron Client Pro workstations. WindowsNT is fully integrated with networking capabilities. WindowsNT was designed for client/server computing, which facilitates user workstations to connect to servers and share processing information between computers.

- Firewall System

  The firewall is physically housed in the Computer Center of FCA Headquarter, McLean, Virginia. The system allows control access between the internal network and the World Wide Web. Firewall provides maximum perimeter security without compromising network performance. It provides strong protection against unwanted intrusion, while allowing approved business traffic to cross the FCA's network.

- FCA Web Site

  The FCA web site presents Agency information on the Internet.

3. GISRA review methodology

The Office of Inspector General, supported by Clifton Gunderson LLP (CG), the independent evaluator, determined the critical elements that represent tasks are essential for establishing compliance with GISRA, 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, the evaluator determined the associated objectives, risks, and critical activities, as well as related control techniques and audit 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, the CIO Council Framework, and information gleaned during the review of any FCA security incidents that had occurred at the agency during the evaluation period. We used this information to evaluate FCA's practices and addressed the above five control areas to be considered in determining compliance with GISRA. 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 GISRA evaluations in accordance with Federal guidance, e.g., *NIST Self-Assessment Guide for Information Technology Systems*.

4. Material weaknesses identified and reported under existing law

In the *Independent Auditors Report on Internal Control on Compliance with Laws and Regulations Report* the auditors stated that "The Office of Chief Financial Officer's financial management system, FINASST, could not be relied on to produce financial statements for the fiscal year ended September 30, 2000. During the implementation of the new system, difficulties in maintaining functionality of all accounting cycles required FCA to manually reconcile all FY 2000 activity and rely on a manual trial balance to prepare the annual financial statements." The problem resulted in excessive delays in producing financial statements for the fiscal year ended September 30, 2000. "These delays extended into March 2001. The financial management system was a serious challenge facing the Agency".

FCA has resolved the material weakness. FCA initiated corrective action by establishing a cross-servicing agreement with the Department of Interior, National Business Center for the financial management system used by the Department of the Interior. According to management representation the system was successfully implemented at FCA on June 4, 2001, and is compliant with FFMIA. Management reported that implementation remedied the deficiency noted in the Independent Auditor's Report on Compliance with Laws and Regulations and took the place of the requirement to submit a remediation plan.

5. Performance measures for assessing risk

The assessment of risk at FCA is done at multiple levels both strategic and operational, and the program has been geared to review the many issues involved on 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 written according 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 within each application, processed by, or transmitted by a system that provides a basis for the value of the system and is one of the major 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 additional security measures required mitigating or eliminating the potential that those threats/vulnerabilities could have on the system or its assets.

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

In May 2001, the OCIO performed a review of security controls in place for FCA Web site. As results of the review, the OCIO established a Lotus Notes database to collect information on publicly announced security vulnerabilities relating to the software and hardware currently in use within the Agency.

In November 1999, an independent contractor, Booze Allen & Hamilton conducted a penetration exercise targeting FCA Internet and modem pool dial-up connections. Attempts to the internal network behind the firewall and dial-up connections were unsuccessful. Brute force attacks tried during this exercise were also unsuccessful. The vendors recommended several countermeasures to strengthen security. FCA implemented the appropriate countermeasures.

In August of 1999, the independent firm of Planning Technologies, Inc. (PTI) issued a management assessment of the Agency's network infrastructure. It was determined that FCA's security policy and procedures were above industry standards and overall security policies and configuration impose no critical security risk. Recommendations were made to optimize the security structure. FCA implemented recommendations were appropriate and commensurate with the acceptable level of risk for the system.

In January 15, 1999, the Inspector General reviewed the availability of the computer network from remote locations after receiving complaints concerning accessing and maintaining access to FCA network. The results of the review stated that overall the Agency's remote access was sufficiently available to support remote users' needs.

The evaluator found the security plans including risk assessments, and level of security up-to-date on the systems and applications reviewed. The evaluator found no signification security issues.

6. Performance measures for maintaining Agency-wide security program

The Agency-wide program is documented in the Policy and Procedure Manual (PPM) number 902. FCA maintains current Agency-wide, applications and systems security plans in accordance with OMB Circular A-130, Appendix III. The security plans are reviewed and updated annually. The security plans consider data sensitivity and data integrity and 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 Chief Information Officer (CIO) is responsible for developing and obtaining the approval of the FCA's Leadership Team for an overall policy on the level of security to be achieved in the FCA operations. CIO is responsible for establishing a computer security plan which conforms with security

policies established by the FCA Board, and complies with current Federal law, 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 by or used by the Agency. The review includes analysis to ascertain that security is commensurate with the risk and magnitude of the harm resulting for the loss, misuse or unauthorized access to the Agency information.

FCA Agency-wide security program addresses the ability to respond rapidly when security breaches occur, and procedures that provide continuity of data processing support when other incidents arise that affect the availability of FCA computers and systems, and procedures to take appropriate steps to prevent a reoccurrence.

The FCA has integrated its 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 Information Resource Management (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 and Senior Management, and monitored via monthly and quarterly reports to management. All deliverables are identified along with the resources required to deliver them.

The training of staff is conducted formally and 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 is identified in reports monthly to management, quarterly performance measures reports, and in meeting completion timeframes mandated by the Agency's program and in the results of audits completed.

The evaluators found no security issues concerning the Agency-wide security program.

7. Training

As of July 30, 2001, FCA had employed 272 employees. FCA provides security training via news articles and updates in the employee newsletter and via an online security tutorial (also published in the employee newsletter). The Agency sent all employees both the news

articles and a security tutorial. As an incentive to complete the tutorial, the Agency gives the employees who complete the tutorial a "secure computing" clock. The tutorial was completed by 273 employees. The cost of providing the training was limited to the salary of the Security Officer plus $1,139 for the clocks.

The Agency technical security training for FY 2001 is $82,700. The training included seminars for 18 staff. The CIO attended the "Federal Computer Security Program Managers' Forum" other staff are attending "Accessibility Standards for IT"- National Summit, and "Designing a Secure Microsoft Windows 2000-based Network".

8. Incident Handling Procedures

The FCA Computer Security Officer (CSO) is notified of all security incidents to provide coordination of the incident response to higher levels or to outside reporting of the security incident. Several staff may be involved over the course of the incident depending on the 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 Virus Incidents, Worm Incidents, Hacker/Cracker Incidents and 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 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 (NIPC). Incidents involving fraud, system penetration, theft of Agency assets, or other suspected criminal activity are reported to the FBI. In addition, all suspected criminal activity is reported to FCA's Office of General Counsel (OGC) and Inspector General (IG), and the content of the reports to law enforcement agencies through and approved by the OFC.

During the last year, the Agency has reported one incident to the FBI.

9. Capital Planning and Investment Control Process

The Chief Information Officer (CIO) is responsible for ensuring that agency security programs integrate fully into the Agency's Enterprise Architecture (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 Information Resources Management (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 IRM Operations Committee (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 Office products.

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 also reviewed and revised as necessary during this review.

10. Methodology to identify prioritizes critical assets

An initial identification and prioritization of FCA's critical assets occurs during FCA's annual planning and budgeting process. The Office of the Chief Information Officer (OCIO) issues a Call for Agency input on future information resource needs – hardware, software, development, maintenance, and training. The IRM Operations Committee (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 EA. This rating identifies and prioritizes critical assets within the EA including 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.

11. Ensure security plan is practiced

The FCA Chairman and CEO measure the performance of the information security plan thorough 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.

12. 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 Office of the Chief Administrative Officer. The COOP is the primary document for FCA's critical infrastructure protection responsibilities. Second, the OCIO reviews Office submission to ensure that equipment required to protect critical infrastructure (including such things as cell phones for the Board) is included in the IRM Planning Call and is budgeted for appropriately.

13. Contractor Provided Services.

a. IT Services Provided By Other Agencies

- Federal Financial System (FFS)

FFS provided by the Department of the Interior National Business Center. The FFS is proprietary financial management system software owned and maintained by American Management Systems, Inc. (AMS). The FFS is made available to FCA through an inter-agency agreement with the Department of Interior (DOI), National Business Center. The FFS is a mainframe computer financial management system that meets the requirements of OMB Circular A-127, Financial Management Systems.

Initially, the FFS was housed in the NBC data center in Reston, Virginia. In January of 2001, the NBC data centers were consolidated and processing of the FFS was relocated to the NBC data center in Denver, Colorado. An independent audit of the DOI, NBC controls and set-up is conducted annually in accordance with OMB Circular A-127. The NBC center in Denver is in the process of the review. An audit of the Reston Data center, "Report on Controls Placed in Operations and Tests of Operating Effectiveness" was conducted by KPMG.

The FFS is located on a mainframe computer in Denver, Colorado. FCA users connect to the FFS over the Internet.

Full volume tape backups are performed weekly by the NBC data center in Denver, Colorado, and are sent to an off-site tape storage facility. Two incremental backups are performed daily and are maintained on-site. The DOI Disaster Recovery Plan

includes recovery procedures for the support of the resident applications including FFS and the subsystems it incorporates. Data can be reconstructed from the tape backups mentioned above. A dial-up connection to the FFS from FCA was tested successfully and can be used in case of a disaster at FCA.

Front End Security is used by NBC to restrict access to the financial information contained in the FFS application. To gain access to an FFS application a user must pass several security checkpoints or levels of security access.

- Payroll Services from National Finance Center (NFC)

  The Personnel/Payroll System (PPS) is provided to FCA by USDA's National Finance Center located in New Orleans, Louisiana. 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 Office of the Chief Administrative Officer (OCAO) for the remote system at FCA references the master security plan.

  FCA's PPS 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. Security requirements associated with dial-in are addressed in the NFC security plan.

  Design review and testing was conducted on the NFC system. The review and test consisted of a compliance verification of the system configuration with established guidelines identified in the appropriate Security Compliance Checklist. The National Finance Center Configuration Management Group uses configuration management software that includes version control, testing, impact analysis, change identification and documentation of modifications made to systems and applications.

  In addition, ongoing security review and testing is conducted at the National Finance Center in New Orleans. The NFC also coordinates contingency planning for all client agencies, including FCA, to ensure that adequate contingency systems are in place.

  The NFC operating system has access controls that limit who can logon, what resources will be available, what each user can do with these resources, and when and from where access is available. Management, security, LAN, and key user personnel cooperate closely to implement access controls. The NFC operating system procedures, network operating system security procedures, user security, network file access, console security, and network security are described in the security plan for FCA's PPS.

Currently, NFC software updates are either installed on the mainframe system located in New Orleans or available for download from NFC's web site. Software is password protected at the point of download and only available to previously authorized individuals. Request for such access must go through FCA's NFC Security Officer.

An audit log is maintained on the NFC Personnel/Payroll System to effectively trace actions affecting the security of the system to the responsible individual. The log is protected from unauthorized modification, destruction, and access by the limited rights assigned by the primary NFC System in New Orleans. The audit logs are reviewed on a regular basis for instances of possible abuse.

- The Electronic Certification System

  The Electronic Certification System (ECS) is maintained by the Department of Treasury (Treasury), Financial Management Service (FMS). ECS is a system that agencies use to certify proper payments to Treasury. The Federal Financial System 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 a 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. The three primary functions separated by FCA are:

  - Security Administrator – brings the system up and down each day and is responsible for daily trouble shooting, Treasury liaison, and issuing authorization forms to Treasury for user's access
  - Certifying Officer (CO) – reviews payment information and certifies that payments are valid
  - Data Entry Operator (DEO) – loads the summary payment information into ECS

b. Contractor Provided Services

The contractors utilized by FCA are:

- Arcus Data Security

  Arcus Data Security (Arcus) provides offsite storage services for FCA's backup tapes. The adequacy of its security was evaluated by onsite inspection by OCIO technical personnel.

Arcus is a division of Iron Mountain, a recognized leader in data security services. Iron Mountain has been protecting business records since 1951 for a diversified customer base, which includes more than half of the Fortune 500 companies. Arcus Data Security was added to Iron Mountain's data security division in January 1998. Arcus 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, Arcus Data Security has provided secure, offsite vaulting for disaster recovery and archival data. It serves more than 25,000 companies in over 50 locations.

Arcus states that "Every component of our offsite vaulting service is designed with one thing in mind; eliminating risk." Arcus locates its facilities away from exposures like flood plains and railroad tracks. It constructs its buildings with non-combustible materials and protects them with state-of-the-art physical security. Its vehicles are built specifically to transport magnetic media. It carefully screens its employees and provides them with comprehensive training on all aspects of data security and protection.

- UUNet Division of WorldCom

  UUNet Division of WorldCom is the Internet service provider for FCA. Its services are procured through the Farm Credit System Building Association. FCA does not look to UUNet to provide security. FCA considers the Internet to be inherently insecure and provides internal security up to the firewall through its internal infrastructure - hardware, software, and personnel. The security plans for the firewall, NT network, and other general support systems provide information on FCA's security measures.

- Rental Systems, Inc. Rentsys, formerly Wang disaster recovery services

  Rental Systems provides disaster recovery services for FCA. The service provided can be triggered in the wake of a catastrophic event that might render the Headquarters building or computer center unusable. The service provides a "mobile recovery facility" (MRC) that consists of a self-contained 50-foot trailer that can be delivered to any location FCA specifies. The MRC possesses its own electrical power generator, and climate control and, if needed, can provide satellite communications links to provide voice and data services. The MRC was tested off site in August 2000 to determine if the hardware furnished by the vendor, in combination with FCA's software and backup tapes could be relied on to provide basic client server and network services - within the programmed recovery timeframe of not greater than three business days. The test was successful, and we determined that one and a half business days would be adequate to configure the equipment, restore user files and provide access to client server services.

EXHIBIT B: GISRA REVIEW

FARM CREDIT ADMINISTRATION

We used the NIST Special Publication 800-XX, Self-Assessment Guide for Information Technology Systems (Draft) dated March 9, 2001 as a guide for our procedures. We considered the following mission critical systems:

- Federal Financial System (FFS)
- Consolidated Reporting System (CRS)
- Lotus Notes
- WindowsNT
- Firewall System
- FCA Web site

In performing our procedures, as suggested by NIST, we used five performance measures:

Level 1 – control objective documented in a security policy;
Level 2 – security controls documented as procedures;
Level 3 – procedures have been implemented;
Level 4 – procedures and security controls are tested and reviewed; and
Level 5 – procedures and security controls are fully integrated into a comprehensive program.

The NIST publication builds on the Federal IT Security Assessment Framework (Framework) developed for the Chief Information Officers (CIO) Council. The Framework established the groundwork for standardizing on five levels of security status and criteria agencies could use to determine if the five levels were adequately implemented.

The goal of the Framework is to provide a standardized approach to assessing a system. The Framework strives to blend the control objectives found in the many requirement and guidance documents. Specific attention was made to mapping as closely as possible to the control activities found in the General Accounting Office's (GAO) Federal Information System Control Audit Manual (FISCAM). FISCAM is the document GAO auditors and agency inspector generals use. When FISCAM is referenced in the report the major category initials along with the control activity number are provided, i.e., *FISCAM SP-3.1*.

The review considered seventeen areas of control, such as those pertaining to authentication and contingency planning. In our review, we found no significant security issues. However, we found 2 minor issues:

1. Procedures for employees' transfers can be improved.

   We found that the security plans reviewed did not address employee transfer procedures. FISCAM states: 'The security plan should include policies related to the security aspects of hiring, terminating, and *transferring* employees and assessing their job performance.

We recommend that FCA include procedures for transferred employees in the application security plans.

2. Applications reconciliation process can be improved.

   We found several non-reportable findings in the Management Letter issued for the year ended September 30, 2000 addressing reconciliation deficiencies. We recommend that FCA resolve these issues.

The above security issues are identified in the assessments found on the following pages.

FARM CREDIT ADMINISTRATION
GISRA REVIEW
AUGUST 31, 2001

1. Management Controls

Specific Control Objectives	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated
A. Risk Management *OMB Circular A-130, III*					
Critical Element 1: Is risk periodically assessed?					
• Are risk assessments performed and documented on a regular basis or whenever the system, facilities, or other conditions change? *FISCAM SP-1*	✔	✔	✔	✔	✔
• Has data sensitivity and integrity of the data considered? *FISCAM SP-1*	✔	✔	✔	✔	✔
• Has threat sources, both natural and manmade, been identified? *FISCAM SP-1*	✔	✔	✔	✔	✔
Critical Element 2: Do program officials understand the risk to systems under their control and determine the acceptable level of risk?					
• Are final risk determinations and related management approvals documented and maintained on file? *FISCAM SP-1*	✔	✔	✔	✔	✔
• Has a mission/business impact analysis been conducted? *NIST SP 800-XX*	✔	✔	✔	✔	✔
B. Review of Security Controls *OMB Circular A-130, III* *FISCAM SP-5* *NIST SP 800-18*					
Critical Element 1: Have the security controls of the System and interconnected systems been reviewed?					
• Has the system been subjected to periodic reviews? *FISCAM SP-5.1*	✔	✔	✔	✔	✔
• Has an independent review been performed in the past three years or when a significant change occurred? *OMB Circular A-130, III* *FISCAM SP-5.1* *NIST SP 800-18*	✔	✔	✔	✔	✔
• Have routine self-assessments been conducted in the past three years? *NIST SP 800-18*	✔	✔	✔	✔	✔
• Has the operating system been periodically reviewed to ensure the configuration prevents circumvention of the security software and application controls? *FISCAM SS-1.2*	✔	✔	✔	✔	✔
• Are tests and examinations of key controls routinely made, i.e., network scans, analyses of router and switch setting, penetration testing? *OMB Circular A-130, 8B3* *NIST SP 800-18*	✔	✔	✔	✔	✔
• Are security alerts and security incidents analyzed and					

Level 1 – control objective documented in a security policy (L.1)
Level 2 – security controls documented as procedures (L.2)
Level 3 – procedures have been implemented (L.3)
Level 4 – procedures and security controls are tested and reviewed (L.4)
Level 5 – procedures and security controls are fully integrated into a comprehensive program (L.5)

FARM CREDIT ADMINISTRATION
GISRA REVIEW
AUGUST 31, 2001

1. Management Controls

Specific Control Objectives	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated
remedial actions taken? *FISCAM SP 3-4* *NIST SP 800-18*	✔	✔	✔	✔	✔
Critical Element 2: Does management ensure that corrective actions are effectively implemented?					
• Is there a process for reporting significant weakness and ensuring effective remedial action? *FISCAM SP 5-1* *NIST SP 800-18*	✔	✔	✔	✔	✔
C. Life Cycle *OMB Circular A-130, III* *FISCAM CC-1.1*					
Critical Element 1: Has a system development life cycle methodology been developed?					
Initiation Phase					
• Has the sensitivity of the system been determined? *OMB Circular A-130, III* *FISCAM AC-1.1 & 1.2* *NIST SP 800-18*	✔	✔	✔	✔	✔
Development/Acquisition Phase					
• During the system design, were security requirements identified? *NIST SP 800-18*	✔	✔	✔	✔	✔
• Was an initial risk assessment performed to determine security requirements? *NIST SP 800-XX*	✔	✔	✔	✔	✔
• Were security controls consistent with and an integral part of the IT Architecture of the agency? *OMB Circular A-130, 8B3*	✔	✔	✔	✔	✔
Implementation Phase					
Critical Element 2: Are changes controlled as programs progress through testing to final approval?					
• Were design reviews and system tests run prior to placing the system in production? *FISCAM CC-2.1* *NIST SP 800-18*	✔	✔	✔	✔	✔
• Were the tests documented? *FISCAM CC-2.1* *NIST SP 800-18*	✔	✔	✔	✔	✔
• Was certification testing of security controls conducted and documented? *NIST SP 800-18*	✔	✔	✔	✔	✔
Operation/Maintenance Phase					
• Has a system security plan been developed and approved? *OMB Circular A-130, III* *FISCAM SP 2-1* *NIST SP 800-18*	✔	✔	✔	✔	✔

Level 1 – control objective documented in a security policy (L.1)
Level 2 – security controls documented as procedures (L.2)
Level 3 – procedures have been implemented (L.3)
Level 4 – procedures and security controls are tested and reviewed (L.4)
Level 5 – procedures and security controls are fully integrated into a comprehensive program (L.5)

FARM CREDIT ADMINISTRATION
GISRA REVIEW
AUGUST 31, 2001

1. Management Controls

Specific Control Objectives	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated
• Is the system security plan kept current? *OMB Circular A-130, III* *FISCAM SP 2-2* *NIST SP 800-18*	✔	✔	✔	✔	✔
Disposal Phase					
• Were official electronic records properly disposed/archived? *NIST SP 800-18*	✔	✔	✔	✔	✔
• Is information or media purged, overwritten, degaussed, or destroyed? *FISCAM AC-3.4* *NIST SP 800-18*	✔	✔	✔	✔	✔
D. Authorize Processing (Certification & Accreditation) *OMB Circular A-130, III* *FIPS 102*					
Critical Element 1: Has the system been certified/rectified and authorized to process (Accreditation)?					
• Has a technical and/or security evaluation been completed or conducted in the past three years or when a significant change occurred? *NIST SP 800-18*	✔	✔	✔	✔	✔
• Has a risk assessment been conducted in the past three years or when a significant change occurred? *NIST SP 800-18*	✔	✔	✔	✔	✔
• Have Rules of Behavior been established and signed by users? *NIST SP 800-18*	✔	✔	✔	✔	✔
• Has a contingency plan been developed and tested? *NIST SP 800-18*	✔	✔	✔	✔	✔
• Has a system security plan been developed, updated, and reviewed? *NIST SP 800-18*	✔	✔	✔	✔	✔
Critical Element 2: Is the system operating on an interim authority to process?					
• Has management initiated prompt action to correct deficiencies? *NIST SP 800-18*	✔	✔	✔	✔	✔
E. System security plan *OMB Circular A-130, III* *NIST SP 800-18* *FISCAM SP-2.1*					
Critical Element 1: Is a system security plan documented for the system and all interconnected systems?					
• Is the system security plan approved by key affected parties and management? *FISCAM SP-2.1*	✔	✔	✔	✔	✔

Level 1 – control objective documented in a security policy (L.1)
Level 2 – security controls documented as procedures (L.2)
Level 3 – procedures have been implemented (L.3)
Level 4 – procedures and security controls are tested and reviewed (L.4)
Level 5 – procedures and security controls are fully integrated into a comprehensive program (L.5)

FARM CREDIT ADMINISTRATION
GISRA REVIEW
AUGUST 31, 2001

1. Management Controls

Specific Control Objectives	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated
NIST SP 800-18					
• Does the plan contain the topics prescribed in NIST Special Publication 800-18? *NIST SP 800-18*	✔	✔	✔	✔	✔
• Is a summary of the plan incorporated into the strategic IRM plan? *OMB Circular A-130, III* *NIST SP 800-18*	✔	✔	✔	✔	✔
Critical Element 2: Is the plan kept current?					
• Is the plan reviewed periodically and adjusted to reflect current conditions and risks? *FISCAM SP-2.1* *NIST SP 800-18*	✔	✔	✔	✔	✔

Level 1 – control objective documented in a security policy (L.1)
Level 2 – security controls documented as procedures (L.2)
Level 3 – procedures have been implemented (L.3)
Level 4 – procedures and security controls are tested and reviewed (L.4)
Level 5 – procedures and security controls are fully integrated into a comprehensive program (L.5)

FARM CREDIT ADMINISTRATION
GISRA REVIEW
AUGUST 31, 2001

2. Operational Controls

Specific Control Objectives	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated
A. Personnel Security *OMB Circular A-130, III*					
Critical Element 1: Are controls such as separation of duties, least privilege, and individual accountability incorporated into security-related policies?					
• Are there documented job descriptions that accurately reflect assigned duties and responsibilities and that segregate duties? *FISCAM SD-1.2*	✔	✔	✔	✔	✔
• Are sensitive functions divided among different individuals? *OMB Circular A-130, III* *FISCAM SD-1*	✔	✔	✔	✔	✔
• Are distinct systems support functions performed by different individuals? *FISCAM SD-1.1*	✔	✔	✔	✔	✔
• Are mechanisms in place for holding users responsible for their actions? *OMB Circular A-130, III* *FISCAM SD-2 & 3.2*	✔	✔	✔	✔	✔
• Are hiring, transfer, and termination procedures established? *FISCAM SP-4.1* *NIST SP 800-18*	See Issue 1.	See Issue 1.	See Issue 1.	See Issue 1.	See Issue 1.
• Is there a process for requesting, establishing, issuing, and closing user accounts? *FISCAM SP-4.1* *NIST 800-18*	✔	✔	✔	✔	✔
Critical Element 2: Is appropriate background screening for assigned positions completed prior to granting access?	✔	✔	✔	✔	✔
B. Physical and Environmental Protection					
Physical Access Control					
Critical Element 1: Have adequate physical security controls been implemented that are commensurate with the risks of physical damage or access?					
• Is access to facilities controlled through the use of guards, identification badges, or entry devices such as key cards? *FISCAM AC-3* *NIST SP 800-18*	✔	✔	✔	✔	✔
• Are deposits and withdrawals of tapes and other storage media from the library authorized and logged? *FISCAM AC-3.1*	✔	✔	✔	✔	✔
Fire Safety Factors					
• Are fire suppression and prevention devices installed and working? *FISCAM SC-2.2* *NIST SP 800-18*	✔	✔	✔	✔	✔

Level 1 – control objective documented in a security policy (L.1)
Level 2 – security controls documented as procedures (L.2)
Level 3 – procedures have been implemented (L.3)
Level 4 – procedures and security controls are tested and reviewed (L.4)
Level 5 – procedures and security controls are fully integrated into a comprehensive program (L.5)

FARM CREDIT ADMINISTRATION
GISRA REVIEW
AUGUST 31, 2001

2. Operational Controls

Specific Control Objectives	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated
Supporting Utilities					
• Are heating and air-conditioning systems regularly maintained? *NIST SP 800-18*	✔	✔	✔	✔	✔
• Is there a redundant air-cooling system? *FISCAM SC-2.2*	✔	✔	✔	✔	✔
• Are electric power distribution, heating plants, water, sewage, and other utilities periodically reviewed for risk of failure? *FISCAM SC-2.2* *NIST SP 800-18*	✔	✔	✔	✔	✔
• Has an uninterruptible power supply or backup generator been provided? *FISCAM SC-2.2*	✔	✔	✔	✔	✔
Interception of Data					
Critical Element 2: Is data protected from interception?					
• Is physical access to data transmission lines controlled? *NIST SP 800-18*	✔	✔	✔	✔	✔
C. Production, Input/Output Controls					
Critical Element 1: Is their user support?					
• Is there a help desk or group that offers advice? *NIST SP 800-18*	✔	✔	✔	✔	✔
Critical Element 2: Are there media controls?					
• Are there procedures to ensure that unauthorized individuals cannot read, copy, alter, or steal printed or electronic information? *NIST SP 800-18*	✔	✔	✔	✔	✔
• Are there procedures for ensuring that only authorized users pick up, receive, or deliver input and output information and media? *NIST SP 800-18*	✔	✔	✔	✔	✔
• Are audit trails used for receipt of sensitive inputs/outputs? *NIST SP 800-18*	✔	✔	✔	✔	✔
• Are controls in place for transporting or mailing media or printed output? *NIST SP 800-18*	✔	✔	✔	✔	✔
D. Contingency Planning *OMB Circular A-130, III*					
Critical Element 1: Have the most critical and sensitive operations and their supporting computer resources been identified?					
• Are critical data files identified and the frequency of file backup documented? *FISCAM SC- SC-1.1 & 3.1* *NIST SP 800-18*	✔	✔	✔	✔	✔
• Are resources supporting critical operations identified? *FISCAM SC-1.2*	✔	✔	✔	✔	✔

Level 1 – control objective documented in a security policy (L.1)
Level 2 – security controls documented as procedures (L.2)
Level 3 – procedures have been implemented (L.3)
Level 4 – procedures and security controls are tested and reviewed (L.4)
Level 5 – procedures and security controls are fully integrated into a comprehensive program (L.5)

FARM CREDIT ADMINISTRATION
GISRA REVIEW
AUGUST 31, 2001

2. Operational Controls

Specific Control Objectives	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated
• Have processing priorities been established and approved by management? *FISCAM SC-1.3*	✔	✔	✔	✔	✔
Critical Element 2: Has a comprehensive contingency plan been developed and documented?					
• Is the plan approved by key affected parties? *FISCAM SC-3.1*	✔	✔	✔	✔	✔
• Are responsibilities for recovery assigned? *FISCAM SC-3.1*	✔	✔	✔	✔	✔
• Are there detailed instructions for restoring operations? *FISCAM SC-3.1*	✔	✔	✔	✔	✔
• Is there an alternate processing site; if so, is there a contract or interagency agreement in place? *FISCAM SC-3.1* *NIST SP 800-18*	✔	✔	✔	✔	✔
• Is the location of stored backups and are generations of backups identified? *NIST SP 800-18*	✔	✔	✔	✔	✔
• Has the contingency plan been distributed to all appropriate personnel? *FISCAM SC-3.1*	✔	✔	✔	✔	✔
Critical Element 3: Are tested contingency/disaster recovery plans in place?					
• Is the plan stored securely offsite? *FISCAM SC-3.1*	✔	✔	✔	✔	✔
• Are employees trained in their roles and responsibilities? *FISCAM SC-2.3* *NIST SP 800-18*	✔	✔	✔	✔	✔
• Is the plan periodically tested and readjusted as appropriate? *FISCAM SC-3.1* *NIST SP 800-18*	✔	✔	✔	✔	✔
E. Hardware and System Software Maintenance *OMB Circular A-130, III*					
Critical Element 1: Is access limited to system software and hardware?					
• Are restrictions in place on who performs maintenance and repair activities? *OMB Circular A-130, III* *FISCAM SS-3.1* *NIST SP 800-18*	✔	✔	✔	✔	✔
• Is access to all program libraries restricted and controlled? *FISCAM CC-3.2 & 3.3*	✔	✔	✔	✔	✔
Critical Element 2: Are all new and revised hardware and software authorized, tested and approved before implementation?					
• Is an impact analysis conducted to determine the effect					

Level 1 – control objective documented in a security policy (L.1)
Level 2 – security controls documented as procedures (L.2)
Level 3 – procedures have been implemented (L.3)
Level 4 – procedures and security controls are tested and reviewed (L.4)
Level 5 – procedures and security controls are fully integrated into a comprehensive program (L.5)

2. Operational Controls

Specific Control Objectives	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated
of proposed changes on existing security controls, including the required training needed to implement the control? *NIST SP 800-18*	✔	✔	✔	✔	✔
• Are system components tested and approved (operating system, utility, applications) prior to promotion to production? *FISCAM SS-3.1 & CC-2.1* *NIST SP 800-18*	✔	✔	✔	✔	✔
• Are software change request forms used to document requests and related approvals? *FISCAM CC-1.2* *NIST SP 800-18*	✔	✔	✔	✔	✔
• Are the distribution and implementation of new or revised software documented and reviewed? *FISCAM SS-3.2*	✔	✔	✔	✔	✔
F. Data Integrity *OMB Circular A-130, 8B3*					
Critical Element 1: Is virus detection and elimination software installed and activated?	✔	✔	✔	✔	✔
Critical Element 2: Are data integrity and validation controls used to provide assurance that the information has not been altered and the system functions as intended?					
• Are reconciliation routines used by applications, i.e., checksums, hash totals, record counts? *NIST SP 800-18*	See Issue 2	See Issue 2.	See Issue 2.	See Issue 2.	See Issue 2.
• Are inappropriate or unusual activity investigated and appropriate actions taken? *FISCAM SS-2.2*	✔	✔	✔	✔	✔
• Are procedures in place to determine compliance with password policies? *NIST SP 800-18*	✔	✔	✔	✔	✔
• Are intrusion detection tools installed on the system? *NIST SP 800-18*	✔	✔	✔	✔	✔
• Are the intrusion detection reports routinely reviewed and suspected incidents handled accordingly? *NIST SP 800-18*	✔	✔	✔	✔	✔
• Is system performance monitoring used to analyze system performance logs in real time to look for availability problems, including active attacks? *NIST SP 800-18*	✔	✔	✔	✔	✔
• Is penetration testing performed on the system? *NIST SP 800-18*	✔	✔	✔	✔	✔
G. Documentation *OMB Circular A-130, 8B3*					
Critical Element 1: Is there documentation that explains how software/hardware is to be used?					

Level 1 – control objective documented in a security policy (L.1)
Level 2 – security controls documented as procedures (L.2)
Level 3 – procedures have been implemented (L.3)
Level 4 – procedures and security controls are tested and reviewed (L.4)
Level 5 – procedures and security controls are fully integrated into a comprehensive program (L.5)

FARM CREDIT ADMINISTRATION
GISRA REVIEW
AUGUST 31, 2001

2. Operational Controls

Specific Control Objectives	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated
• Is there vendor-supplied documentation of software? *NIST SP 800-18*	✔	✔	✔	✔	✔
• Are there standard operating procedures for all the topic areas covered in this document? *NIST SP 800-18*	✔	✔	✔	✔	✔
• Are there user manuals? *NIST SP 800-18*	✔	✔	✔	✔	✔
• Are there emergency procedures? *NIST SP 800-18*	✔	✔	✔	✔	✔
• Are there backup procedures? *NIST SP 800-18*	✔	✔	✔	✔	✔
Critical Element 2: Are there formal security and operational procedures documented?					
• Is there a system security plan? *OMB Circular A-130, III* *FISCAM Pp-2.1* *NIST SP 800-18*	✔	✔	✔	✔	✔
• Is there a contingency plan? *NIST SP 800-18*	✔	✔	✔	✔	✔
• Are there risk assessment reports? *NIST SP 800-18*	✔	✔	✔	✔	✔
• Are there certification and accreditation documents and statements authorizing the system to process? *NIST SP 800-18*	✔	✔	✔	✔	✔
H. Security Awareness, Training, and Education *OMB Circular A-130, III*					
Critical Element 1: Have employees received adequate training to fulfill their security responsibilities?					
• Have employees received a copy of the rules of behavior? *NIST SP 800-18*	✔	✔	✔	✔	✔
• Is employee training and professional development documented and monitored? *FISCAM SP-4.2*	✔	✔	✔	✔	✔
• Is there mandatory annual refresher training? OMB Circular A-130, III	✔	✔	✔	✔	✔
• Are methods employed to make employees aware of security, i.e., posters, booklets? *NIST SP 800-18*	✔	✔	✔	✔	✔
• Have employees received a copy of or have easy access to agency security procedures and policies? *NIST SP 800-18*	✔	✔	✔	✔	✔
I. Incident Response Capability *OMB Circular A-130, III* *FISCAM SP-3.4* *NIST 800-18*					
Critical Element 1: Is there a capability to provide help to users when a security incident occurs in the system?					
• Is a formal incident response capability available?					

Level 1 – control objective documented in a security policy (L.1)
Level 2 – security controls documented as procedures (L.2)
Level 3 – procedures have been implemented (L.3)
Level 4 – procedures and security controls are tested and reviewed (L.4)
Level 5 – procedures and security controls are fully integrated into a comprehensive program (L.5)

2. Operational Controls

Specific Control Objectives	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated
FISCAM SP-3.4 *NIST SP 800-18*	✔	✔	✔	✔	✔
• Is there a process for reporting incidents? *FISCAM SP-3.4* *NIST SP 800-18*	✔	✔	✔	✔	✔
• Are incidents monitored and tracked until resolved? *NIST SP 800-18*	✔	✔	✔	✔	✔
• Are personnel trained to recognize and handle incidents? *FISCAM SP-3.4* *NIST SP 800-18*	✔	✔	✔	✔	✔
• Are alerts/advisories received and responded to? *NIST SP 800-18*	✔	✔	✔	✔	✔
• Is there a process to modify incident handling procedures and control techniques after an incident occurs? *NIST SP 800-18*	✔	✔	✔	✔	✔
Critical Element 2: Is incident related information shared with organizations?					
• Is incident information and common vulnerabilities or threats shared with interconnected systems? *OMB A-130, III* *NIST SP 800-18*	✔	✔	✔	✔	✔
• Is incident information shared with FedCIRC [3] concerning incidents and common vulnerabilities and threats? *OMB A-130, III* *GSRA*	✔	✔	✔	✔	✔
• Is incident information reported to FedCIRC, NIPC [4], and local law enforcement when necessary? *OMB A-130,III* *GSRA*	✔	✔	✔	✔	✔

Level 1 – control objective documented in a security policy (L.1)
Level 2 – security controls documented as procedures (L.2)
Level 3 – procedures have been implemented (L.3)
Level 4 – procedures and security controls are tested and reviewed (L.4)
Level 5 – procedures and security controls are fully integrated into a comprehensive program (L.5)

FARM CREDIT ADMINISTRATION
GISRA REVIEW
Audit Program
AUGUST 31, 2001

3. Technical Controls

Specific Control Objectives	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated
A. Identification and Authentication *OMB Circular A-130, III* *FISCAM AC-2* *NIST SP 800-18*					
Critical Element 1: Are users individually authenticated?					
• Is a current list maintained and approved of authorized users and their access? *FISCAM AC-2* *NIST SP 800-18*	✔	✔	✔	✔	✔
• Is emergency and temporary access authorized? *FISCAM AC-2.2*	✔	✔	✔	✔	✔
• Are passwords, tokens, or other devices used to identify and authenticate? *FISCAM AC-3.2* *NIST SP 800-18*	✔	✔	✔	✔	✔
• Are passwords changed at least every ninety days or earlier if needed? *FISCAM AC-3.2* *NIST SP 800-18*	✔	✔	✔	✔	✔
• Do passwords require alpha numeric, upper/lower case, and special characters? *FISCAM AC-3.2* *NIST SP 800-18*	✔	✔	✔	✔	✔
• Are inactive user identifications disabled after a specified period of time? *FISCAM AC-3.2* *NIST SP 800-18*	✔	✔	✔	✔	✔
• Are passwords not displayed when entered? *FISCAM AC-3.2* *NIST SP 800-18*	✔	✔	✔	✔	✔
• Are there procedures in place for handling lost and compromised passwords? *FISCAM AC-3.2* *NIST SP 800-18*	✔	✔	✔	✔	✔
• Are passwords distributed securely and users informed not to reveal their passwords to anyone (social engineering)? NIST SP 800-18	✔	✔	✔	✔	✔
• Are passwords transmitted and stored with one-way encryption? *FISCAM AC-3.2* *NIST SP 800-18*	✔	✔	✔	✔	✔
• Are vendor-supplied passwords replaced immediately? *FISCAM AC-3.2* *NIST SP 800-18*	✔	✔	✔	✔	✔
• Is there a limit to the number of invalid access attempts					

Level 1 – control objective documented in a security policy (L.1)
Level 2 – security controls documented as procedures (L.2)
Level 3 – procedures have been implemented (L.3)
Level 4 – procedures and security controls are tested and reviewed (L.4)
Level 5 – procedures and security controls are fully integrated into a comprehensive program (L.5)

3. Technical Controls

Specific Control Objectives	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated
that may occur for a given user? *FISCAM AC-3.2* *NIST SP 800-18*	✔	✔	✔	✔	✔
Critical Element 2: Are access controls enforcing segregation of duties?					
• Does the system correlate actions to users? *OMB A-130, III* *FISCAM SD-2.1*	✔	✔	✔	✔	✔
B. Access Controls *OMB Circular A-130, III* *FISCAM AC-3.2* *NIST SP 800-18*					
Critical Element 1: Do the logical access controls restrict users to authorized transactions and functions?					
• Can the security controls detect unauthorized access attempts? *FISCAM AC-3.2* *NIST SP 800-18*	✔	✔	✔	✔	✔
• Is access to security software restricted to security administrators? *FISCAM AC-3.2*	✔	✔	✔	✔	✔
• Do terminals automatically log off and screensavers lock system after a period of inactivity? *FISCAM AC-3.2* *NIST SP 800-18*	✔	✔	✔	✔	✔
• Are inactive users' accounts monitored and removed when not needed? *FISCAM AC-3.2* *NIST SP 800-18*	✔	✔	✔	✔	✔
Critical Element 2: Are there logical controls for Telecommunications access?					
• Has communication software been implemented to restrict access through specific terminals? *FISCAM AC-3.2*	✔	✔	✔	✔	✔
• Are insecure protocols (i.e., UDP, ftp) disabled? *PSN Security Assessment Guidelines*	✔	✔	✔	✔	✔
• Have all vendor-supplied default security parameters been reinitialized to more secure settings? *PSN Security Assessment Guidelines*	✔	✔	✔	✔	✔
• Are there controls to allow users to access the system remotely? *NIST SP 800-18*	✔	✔	✔	✔	✔
• Are network activity logs maintained and reviewed? *FISCAM AC-3.2*	✔	✔	✔	✔	✔
• Does the network connection automatically disconnect at the end of a session? *FISCAM AC-3.2*	✔	✔	✔	✔	✔
• Is dial-in access monitored?					

Level 1 – control objective documented in a security policy (L.1)
Level 2 – security controls documented as procedures (L.2)
Level 3 – procedures have been implemented (L.3)
Level 4 – procedures and security controls are tested and reviewed (L.4)
Level 5 – procedures and security controls are fully integrated into a comprehensive program (L.5)

3. Technical Controls

Specific Control Objectives	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated
FISCAM AC-3.2	✔	✔	✔	✔	✔
• Is access to telecommunications hardware or facilities restricted and monitored? *FISCAM AC-3.2*	✔	✔	✔	✔	✔
• Are firewalls or secure gateways installed? *NIST SP 800-18*	✔	✔	✔	✔	✔
• If firewalls are installed do they comply with firewall policy and rules? *FISCAM AC-3.2*	✔	✔	✔	✔	✔
Critical Element 3: If the public accesses the system, are there controls in-place and implemented to protect the integrity of the application and the confidence of the public?					
• Is a privacy policy posted on the web site? *OMB-99-18*	✔	✔	✔	✔	✔
• Is a DOJ approved standardized log-on banner displayed on the system warning unauthorized users that they have accessed a U.S. government system and can be punished? *FISCAM AC-3.2* *NIST SP 800-18*	✔	✔	✔	✔	✔
C. Audit Trails *OMB Circular A-130, III* *FISCAM AC-4.1* *NIST SP 800-18*					
Critical Element 1: Is all activity involving access to and modification of sensitive or critical files logged?					
• Does the audit trail provide accountability by providing a trace of user actions? *NIST SP 800-18*	✔	✔	✔	✔	✔
• Can the audit trail support after-the-fact investigations of how, when, and why normal operations ceased? *NIST SP 800-18*	✔	✔	✔	✔	✔
• Is access to online audit logs strictly controlled? *NIST SP 800-18*	✔	✔	✔	✔	✔
• Are off-line storage of audit logs retained for a period of time, and if so, is access to audit logs strictly controlled? *NIST SP 800-18*	✔	✔	✔	✔	✔
• Is there separation of duties between security personnel who administer the access control function and those who administer the audit trail? *NIST SP 800-18*	✔	✔	✔	✔	✔
• Are audit trails reviewed frequently? *NIST SP 800-18*	✔	✔	✔	✔	✔

Level 1 – control objective documented in a security policy (L.1)
Level 2 – security controls documented as procedures (L.2)
Level 3 – procedures have been implemented (L.3)
Level 4 – procedures and security controls are tested and reviewed (L.4)
Level 5 – procedures and security controls are fully integrated into a comprehensive program (L.5)