UNITED STATES DEPARTMENT OF AGRICULTURE
Farm Service Agency
Washington, D.C. 20250

Notice IRM-307

For: FSA, FAS, and RMA Employees and Contractors

Information Systems Security Program

Approved by: Deputy Administrator, Management

1 Implementing the Information Systems Security Program

A
Background

It is the policy of USDA and FFAS to protect USDA and FFAS resources from accidental or deliberate unauthorized access, use, modification, or disclosure by employing adequate security measures through cost-effective technical and management controls.

As defined in DR 3300-1, "Telecommunications and Internet Services and Use" (Figure MB-1, CIO Council Review Approval of Limited Personal Use Policy), Government office equipment including information technology includes but is not limited to:

- PC's and related peripheral equipment and software
- library resources
- telephones
- facsimile machines
- photocopiers
- office supplies
- Internet connectivity and access to Internet services
- e-mail.

B
Purpose

This notice provides policy for implementing the FFAS Information Systems Security Program (ISSP). Notice IRM-300 is obsolete.

Continued on the next page

Disposal Date	Distribution
December 1, 2001	All FSA, FAS, and RMA Employees and Contractors; State Offices relay to County Offices

1 Implementing the Information Systems Security Program (Continued)

C
Policy Information

This policy:

- defines authorities, responsibilities, and security controls for implementing the FFAS Information Systems Security Program

- provides adequate security measures and safeguards to protect information resources from unauthorized access, use, modification, and disclosure

  Note: This includes information collected, processed, transmitted, stored, or disseminated in general support systems and major applications.

- is consistent with Government-wide policies, standards, and procedures issued by:

  - USDA
  - OMB
  - National Institute of Standards and Technology (NIST)
  - GSA
  - OPM.

D
Policy Intent

This policy will ensure that:

- development, implementation, and operations of automated information systems (AIS) and computing environments are secure, efficient, and cost-effective, based on analyses of security risks and vulnerabilities

- all AIS processing, storing, or transmitting sensitive or nonsensitive information must meet the requirements of this policy through automated or manual means

  Note: More stringent requirements may be imposed based on a risk analysis.

- appropriate and cost-effective safeguards are employed to protect information resources from unauthorized access, use, modification, and disclosure

- information security management and technology issues are properly addressed, implemented, and enforced.

Continued on the next page

1 Implementing the Information Systems Security Program (Continued)

E
Policy Contents

This policy states:

- the importance and value of computer and information resources and the need to preserve and protect their integrity, confidentiality, and availability
- that all employees and contractors are required to protect information resources from accidental or deliberate unauthorized access, use, modification, or disclosure by employing adequate security measures through cost-effective technical and management controls
- the assignment of responsibilities for information systems security
- the requirement to provide mandatory computer security awareness training to employees who are involved in managing, using, or operating AIS according to the Computer Security Act of 1987 and OMB Circular A-130, Appendix III
- that all employees and contractors shall be personally accountable for information resources entrusted to them to use them for authorized purposes (official business use or limited personal use)
- the requirement to assess information systems security measures and safeguards shall be performed through risk analyses, inspections, and audits.

Continued on the next page

F
General Policy Statement

Information resources include AIS, hardware, software, communications, and computing facilities that are owned, leased, or operated by or for FFAS.

USDA DR 3300-1, “Telecommunications and Internet Services and Use”, states that the use of telecommunications equipment and services (telephones, FAX, electronic messaging, computer equipment, and the Internet) by all USDA employees shall be in accordance with the requirements of 5 CFR, Part 2635, Subpart G, Sections 704 and 705, and the United States Office of Government Ethics document, "Standards of Ethical Conduct for Employees of the Executive Branch."

All FFAS information resources shall be for official business and limited personal use as described in the USDA DR 3300-1, “Telecommunications and Internet Services and Use”, and FFAS policies.

FFAS shall implement at least the minimum security requirements as identified in this policy to protect information resources (sensitive and nonsensitive data) processed, stored, or transmitted by AIS. Based on risk analyses, additional security safeguards shall be applied to provide the most restrictive set of controls that permits the performance of authorized tasks.

All AIS processing, storing, or transmitting sensitive information must be accredited in major applications and general support systems.

Connectivity is prohibited between AIS that handle sensitive data and any other systems or networks not under FFAS authority, unless formally approved by the FFAS Chief Information Officer (CIO) who is the FFAS Accrediting Authority.

All persons who use, manage, operate, maintain, or develop AIS, applications, or data must comply with this policy.

All employees and contractors are required to protect information resources within their areas of responsibility from unauthorized access, use, modification, disclosure, destruction, or delay in service. Also, they are required to attend FFAS computer security awareness training sessions according to the Computer Security Act of 1987 and OMB Circular A-130, Appendix III.

All authorized access rights shall be terminated when they are no longer required. Departing employees and contractors shall be debriefed and must comply with this policy, including Federal laws and USDA regulations concerning the separation process.

Continued on the next page

1 Implementing the Information Systems Security Program (Continued)

G
Scope and Applicability

This policy applies to all employees, contractors, other Federal and State agencies, universities, industry, farmers, reinsured companies, and the public who access and use FFAS information resources. This includes anyone involved in the design, development, review, acquisition, installation, operation, and maintenance of FFAS information resources.

H
Program Goals

All Federal applications require some level of protection. Certain applications, because of the sensitive information in them, require special management oversight and shall be treated as major applications. Adequate security for other applications shall be provided by security of the system in which they operate.

The goals of the FFAS Information Systems Security Program are to:

- establish and maintain adequate and cost-effective security measures and safeguards to ensure data confidentiality, integrity, and operational availability of information resources that process, store, or transmit nonsensitive and sensitive information
- provide information systems security policies and standards with centralized leadership, guidance, and direction to all offices for decentralized operations and implementation
- design and implement adequate and cost-effective security measures and safeguards to protect information resources by:
  - controlling and denying unauthorized access
  - restricting legitimate users to data or processes for which they are authorized
- ensure that AIS, software and communications packages, and gateways deliver data and information messages (text, numbers, images, etc.) with the same content that was entered
- ensure that unauthorized persons cannot intercept or interfere with transactions or delay them during transmission

Continued on the next page

1 Implementing the Information Systems Security Program (Continued)

H
Program Goals (Continued)

- establish, monitor, and enforce adequate security requirements to protect information resources from unauthorized access, use, modification, or disclosure
- ensure that information systems security planning requirements are integrated into the system's development life cycle management process
- maintain continuity of operations by preventing or minimizing the impacts of events that interfere with normal information resources processing capabilities and mission-critical operations
- ensure that appropriate resources are allocated to FFAS ISSP, including personnel, training, and funding as part of each Agency's information technology budget process
- provide computer security awareness training to all employees and contractors who are involved in managing, operating, or using information resources.

I
System Usage

All employees, consultants, and contractors working for FFAS and USDA **shall not**:

- attempt to gain access to systems, applications, or data for which they have not been authorized, nor assist others in attempting to gain unauthorized access to systems, applications, or data
- knowingly destroy or modify data without permission, nor introduce malicious software (viruses or worms) or infected files
- make illegal copies of software.

J
Virus Protection

Anti-virus software will be installed and used to check microcomputer systems, LAN, servers, new software packages, and diskettes for viruses before use.

Continued on the next page

1 Implementing the Information Systems Security Program (Continued)

K
Internet Access

FFAS and USDA systems will employ robust authentication measures for dial-in and Internet access. Use of a firewall or router when the system uses TCP/IP to prevent intrusions is a centralized and convenient method of protecting FFAS and USDA systems and networks. The use of passwords alone is not an adequate method of protecting systems that are connected to the Internet. Security and LAN officials will work together to determine the adequacy of security measures in place in systems used as gateways to the Internet, including threats, risks, and vulnerabilities.

It is the responsibility of USDA, FFAS agencies, and KC offices that have or plan a gateway to the Internet to fund, implement, and maintain the prescribed protection features. All FFAS agencies, KC, and staff offices using the Internet must follow the guidance in this policy, along with USDA DR 3140-2, "USDA Internet Security Policy", and USDA DR 3300-1, "Telecommunications and Internet Services and Use".

This policy is not intended to deny access to the public data. Rather, it is intended to protect data that has not been identified for public disclosure.

L
Compliance

All users of information and AIS, including contractors working for FFAS, are responsible for complying with this policy as well as other FFAS and USDA policies and Federal laws. Anyone suspecting misuse or attempted misuse of FFAS and USDA information systems resources are responsible for reporting such activity to their immediate supervisor, management officials, and to their local Information Systems Security Officer.

M
Noncompliance

Any person who willfully or knowingly violates or fails to comply with the provisions of this policy shall be subject to appropriate disciplinary actions, such as suspension or dismissal.

Continued on the next page

N
Disciplinary Actions

All managers, supervisors, and contractors shall:

- take the necessary disciplinary actions according to standard personnel procedures
- notify HRD and OIG if required.

Authorized personnel, such as directors, contracting officers, information systems security officials, LAN administrators, and supervisors, may take possession of any FFAS-owned information resources or unauthorized resources at the instruction of appropriate management official or legal authority to examine the contents for violations of this policy including Federal laws and FFAS and USDA policies.

2 Authorities

A Legislation

The following laws, policies, and guidelines are applicable to this policy:

- Computer Fraud and Abuse Act of 1986 (Pub. L. 99-474)
- Computer Matching and Privacy Protection Act of 1988 (Pub. L. 100-503)
- Computer Security Act of 1987 (Pub. L. 100-235)
- Copyright Act (U.S.C., Title 17)
- Electronic Communications Privacy Act of 1986 (Pub. L. 99-508)
- Electronic Freedom of Information Act Amendments of 1996 (Pub. L. 104-231)
- Federal Managers' Financial Integrity Act of 1982 (Pub. L. 97-255)
- Federal Records Act, 44 U.S.C. 3101
- FOIA of 1980 (Pub. L. 93-502)
- Privacy Act of 1974 (Pub. L. 93-579), 5 U.S.C. 552a, July 14, 1987
- Executive Order 10450 of April 27, 1954, Security Requirements for Government Employment
- Executive Order 12958 of April 17, 1995, Classified National Security Information
- Executive Order 13103 of September 30, 1998, Computer Software Piracy
- Presidential Decision Directive 63, May 22, 1998, Critical Infrastructure Protection
- U.S. Office of Government Ethics, Standards of Ethical Conduct for Employees of the Executive Branch.

Continued on the next page

2 Authorities (Continued)

B
OMB Circulars and Bulletins

The following OMB Circulars and Bulletins apply to this policy:

- OMB Circular A-130, Appendix III
- OMB Circular A-123
- OMB Circular A-127.

C
Departmental Regulations

The following Department Regulations apply to this policy:

- USDA Departmental Manual (DM) 3140-1
- USDA DM 3140-2, Draft
- USDA DM 3140-3, Draft
- USDA DM 3140-4, Draft
- USDA DM 3140-5, Draft
- USDA DM 3140-6, Draft
- USDA DM 3140-7, Draft
- USDA DM 3140-8, Draft
- USDA DM 3200-1
- USDA DM 3200-2
- USDA DM 3440-1
- USDA DR 3140-1
- USDA DR 3140-2
- USDA DR 3220-3
- USDA DR 3220-4
- USDA DR 3300-1
- USDA DR 3400-4
- USDA DR 3430-1
- USDA DR 3440-1
- USDA DR 3450-1
- USDA DR 3450-2
- USDA OHRM Personnel Bulletin 735-1

Continued on the next page

2 Authorities (Continued)

D Other Authorities

Following are other authorities that apply to this policy:

- Union contracts and/or agreements
- Department of State, Foreign Affairs Manual (FAM), Volume 12, Chapter 500 (12 FAM 500), Information Security
- Department of State, FAM, Volume 12, Chapter 600 (12 FAM 600), Information Security Technology
- Department of State, Foreign Affairs Handbook (FAH), 12 FAH-6, OSPB [Overseas Security Policy Board] Security Standards and Policy Handbook
- Department of State cable issued May 1998, 98 STATE 083902, Overseas Storage of Classified Information

  Note: Department of State regulations apply to users at foreign posts and users and systems connecting to Department of State systems.

- Federal Information Processing Standards and NIST special publications.

3 Responsibilities

A Agency Administrators Responsibilities

FSA, FAS, and RMA Administrators shall establish and support a consolidated FFAS Information Systems Security Program that ensures compliance with established and mandated Federal laws and FFAS and USDA policies.

B CIO Responsibilities

CIO shall:

- staff and fund FFAS Information Systems Security Program to ensure compliance with established and mandated Federal laws and FFAS and USDA policies
- exercise responsibility for managing, budgeting, directing, and implementing the program with cooperation and support from all offices.

Continued on the next page

3 Responsibilities (Continued)

C Deputy Administrators, Directors, Managers, and Supervisors Responsibilities

Deputy administrators, directors, managers, and supervisors shall:

- implement and enforce USDA and FFAS information systems security policies and procedures to protect information resources within their areas of responsibility
- monitor and report on compliance with Federal laws and FFAS and USDA policies
- assist in the development and implementation of a comprehensive risk management program to identify and evaluate security risks and vulnerabilities
- promote and support computer security awareness training for employees and contractors
- review proposed procurement requests to ensure that adequate and cost-effective security measures and safeguards are addressed
- participate in internal and external reviews and inspections to:
  - ensure compliance with established policies and procedures
  - monitor the correction of deficiencies identified in audits and reports
- issue appropriate instructions needed to implement provisions of information systems security policies and standards
- investigate and report all suspected and actual computer viruses, incidents, violations, or attempts to gain unauthorized access to information resources to appropriate officials; such as the immediate supervisor, CIO, the local information systems security officer, the Federal Protective Service (FPS), and OIG if required.

Continued on the next page

3 Responsibilities (Continued)

D
Director, HRD Responsibilities

The Director, HRD shall:

- be aware of and consider the criticality, privacy, confidentiality, and sensitivity of information under her/his domain which is processed, transmitted, and stored using information technology
- develop job descriptions for personnel, which include requirements for the protection of critical, confidential, privacy, or sensitive information as performance elements
- administer a personal security program that identifies, categorizes, and defines personnel security requirements for FFAS entities, and requires appropriate background investigations/security clearances for employees and contractors alike
- advise the Agency's CIO and the FFAS and FSA KC office ISSPM's of any personnel regulation changes that can affect the ISSP
- provide authorization for disciplinary actions for noncompliance with this policy.

E
Information Systems Security Program Officials Responsibilities

Information Systems Security Program officials shall:

- provide overall management, leadership, and direction for the FFAS ISSP
- formulate, coordinate, maintain, implement, and enforce appropriate security policies and standards to protect information resources from unauthorized access and disclosure
- monitor and report on compliance with Federal laws and FFAS and USDA information systems security policies

Continued on the next page

E Information Systems Security Program Officials Responsibilities (Continued)

- formulate a comprehensive risk management program to identify and evaluate security risks and vulnerabilities

  Note: This includes the development and coordination of sensitive systems security plans, contingency plans, risk assessments, and the certification and accreditation of sensitive systems.

- be the principal point of contact on information systems security activities with the Department, FFAS management officials, other Federal agencies, and industry

- develop and implement a computer security awareness training program for all employees and contractors

- serve as a member of the Agency's acquisition review team to ensure that adequate and cost-effective security requirements are addressed

- participate in internal and external reviews, inspections, and audits to ensure compliance with Federal laws and FFAS and USDA policies

- monitor management decisions for corrective actions of deficiencies that were identified in audit reports

- investigate and report all suspected and actual computer viruses, incidents, breaches, and violations to appropriate FFAS and USDA officials; such as CIO, Departmental Information Systems Security Program Manager, FPS, and OIG if required

- formulate, coordinate, and publish the FFAS Annual Information Resources Management Security Program Status Reports, Sensitive Systems Security Plans, and the Security Strategic Plan.

Continued on the next page

3 Responsibilities (Continued)

F
LAN Administrators Responsibilities

LAN administrators shall:

- plan, install, operate, and manage the day-to-day operations, security, and maintenance activities to safeguard and protect information resources from theft, damage, and unauthorized access

- monitor, report, and maintain information resources to include LAN and other computing environments and access by:

  - monitoring usage, traffic, and intruder lockout capabilities to identify any suspicious or attempted illegal access

  - generating operations and systems audit reports and audit trails that list appropriate information and violations

  - automatically suspending user identification codes that have been inactive for 30 calendar days

- manage and implement appropriate LAN and computer technology practices in conjunction with the FFAS Information Systems Security Program policies and standards including:

  - adding, updating, and deleting users from various computing environments
  - resetting passwords for users

- work closely with the information systems security officers in reviewing, evaluating, and recommending appropriate information systems security measures and safeguards to protect information resources from unauthorized access, use, and disclosure

- report all suspected and actual viruses, breaches, incidents, violations, or attempts to gain unauthorized access or misuse of any resource in the LAN administrator's areas of responsibility to appropriate officials; such as the immediate supervisor, CIO, information systems security officer, FPS, and OIG if required.

Continued on the next page

G
Users and Contractors Responsibilities

Users and contractors shall:

- understand and comply with all security requirements pertaining to Federal laws and FFAS and USDA policies
- comply with all security requirements pertaining to the information resources they use, and employ available and approved safeguards to protect the confidentiality, integrity, and availability of data, applications, and information resources
- request the appropriate computing environments access authorization from their immediate supervisor or oversight manager by completing the appropriate request forms
- provide correct user identification codes and use only approved and authorized computing environments, equipment, AIS, data, and information resources for official business use and limited personal use as described in USDA DR 3300-1 and FFAS policies
- refrain from using trivial and obvious password identification codes and ensure that passwords are held in strict confidence and properly safeguarded from unauthorized access, use, and disclosure
- obey all copyright and licensing laws and comply with Executive Order 13103, Computer Software Piracy
- refrain from exploiting any hardware, software, communications, or AIS weakness, such as intentionally modifying, destroying, reading, or transferring data and information in an unauthorized manner
- secure and log off from any computing environment when processing is completed

  Note: Always log off at the end of the workday.

- perform regular backups of data, software, applications, and information on computer resources using the fixed disk drive, tapes, and diskettes for disaster recovery purposes

Continued on the next page

G
Users and Contractors Responsibilities (Continued)

- refrain from introducing any unauthorized or unscanned software, data, hardware, or telecommunication devices or modifying any configurations without proper approval from CIO

- report any observed or suspected computer security virus, incident, breach, or violation to the immediate supervisor, management officials, and local information systems security officer for appropriate investigation.

Report security breaches and incidents to the addresses listed below:

USDA - FFAS Headquarters
Information Systems Security Program Manger
Attention: Information Technology Services Division (ITSD), STOP 0584
1400 Independence Avenue, S.W., Room 6967-S
Washington, D.C. 20250-0584

USDA-FSA-ISSPS STOP 9198
6501 Beacon Drive
Kansas City, MO 64133-4676

H
Facility Managers Responsibilities

Facility managers of ADP and IRM equipment, facilities, and information resources shall:

- conduct risk analyses and inspections to identify and evaluate risks and vulnerabilities

- manage daily ADP and IRM equipment, facilities, and information resources, including information systems security and physical security operations that provide appropriate:

  - physical access controls to computer rooms, facility entrances, and exits

    Note: Allow only authorized personnel to enter the facility and maintain proper logs of authorized visitors.

  - security information, reports, and evaluations about the facility to management officials, information systems security officers, and customers

Continued on the next page

3 Responsibilities (Continued)

H Facility Managers Responsibilities (Continued)

- formulate, coordinate, and submit Facility Sensitive Systems Security Plan to the FFAS Information Systems Security Program Manager
- formulate, test, and maintain contingency and disaster recovery procedures and plans
- work closely with the information systems security officers in reviewing, evaluating, and recommending appropriate computer security measures and safeguards to protect information resources from unauthorized access, use, and disclosure
- report all suspected and actual viruses, breaches, incidents, violations, or attempts to gain unauthorized access or misuse of any resource in the facility manager's area of responsibility to appropriate officials; such as the immediate supervisor, CIO, information systems security officer, FPS, or OIG, if required.

4 Minimum Security Controls

A Categories of Controls

The minimum security controls can be divided into the following 3 categories:

- physical security
- technical security
- administrative security.

The FFAS Information Systems Security Program shall integrate a combination of these information systems security controls into a comprehensive program to protect information resources from unauthorized access, use, and disclosure.

At a minimum, the FFAS Information Systems Security Program includes the set of security controls established by:

- OMB Circular A-130, Appendix III
- USDA DR 3140-1 and USDA DR 3300-1
- Computer Security Act of 1987.

Continued on the next page

4 Minimum Security Controls (Continued)

B
Physical Security

Physical security is concerned with the measures designed to:

- prevent unauthorized physical access to equipment, facilities, material, information, and documents
- safeguard them against espionage, sabotage, damage, tampering, theft, and other covert acts.

Hardware, software, telecommunications, documentation, and all sensitive information handled by AIS shall be adequately protected to prevent unauthorized access, use, modification, disclosure, or destruction. Before conducting sensitive operations at any location, security planning must consider physical security and information systems security as part of the accreditation process.

Following are types of physical security.

Type	Description
Facility Security	Security requirements for computer facilities shall include physical construction, fire protection, access controls, and environmental controls. Appropriate facility security measures shall be developed and implemented based on the level of risk to the computer and information resources as identified by a risk analysis report.
Environmental Security	Office areas that support desktop equipment shall have environmental controls specified for human safety and comfort. Facilities supporting large scale operations and telecommunications facilities may require additional physical, electrical, temperature, and humidity controls, such as fire suppression systems, uninterrupted power supply, air conditioning, and water hazard detection systems to ensure the continuity of operations for facilities and equipment.

Continued on the next page

4 Minimum Security Controls (Continued)

C
Technical Security

Technical security is the design of AIS that process, store, or transmit sensitive information that must include, at a minimum, the automated security features installed using standard hardware, software, and communications capabilities.

Following are types of technical security.

Type	Description
User Identification Code and Password	User access shall be controlled and limited based on positive user identification, password, and authentication mechanisms that support the minimum requirements of access control, least privilege, and system integrity.
Authentication	Authentication controls to verify the identity of each user may be a prerequisite to AIS access. The preferred method for verifying users is a password system where authentication is done each time the password is used.
Audit Records	AIS transactions are subject to recording and reviewing for inappropriate or illegal activity. Audit trails must be sufficient in detail to facilitate reconstruction of events if compromise or malfunction occurs.
Network Connections	Telecommunications connections between FFAS and non-FFAS networks, public and private must be authorized by CIO. FFAS operating policy requires that any access to the Internet services be provided through approved gateways.

Continued on the next page

4 Minimum Security Controls (Continued)

D Administrative Security

Administrative security consists of automated and manual controls and operational procedures used with or in place of computer security features. Administrative security controls must be documented in the Sensitive Systems Security Plan.

Following are types of administrative security.

Type	Description
Accountability and Access Control Criteria	Security access control criteria and administrative procedures must be established to limit authorized users access to information processed, stored, or transmitted, including sensitive AIS.
Personnel	FFAS personnel and contractors entrusted with the management, operation, maintenance, or use of computer resources and sensitive information shall have the required appropriate management approvals and security clearances.
Risk Management	FFAS shall implement a process for identifying, measuring, controlling, and reducing security risks to information technology resources and sensitive information. This includes a: • risk analysis to identify and analyze threats, vulnerabilities, and the effectiveness of current or proposed safeguards • cost/benefit analysis, which determines the relative value of the resource to the cost of security measures • management decision to implement selected safeguards based on the risk analysis report, including accepting residual risks.
Inspections and Reviews	All information resources shall be periodically inspected and reviewed to ensure that management, operations, personnel, and security measures, controls, and safeguards are functioning properly. The type of inspection and review shall be commensurate with the type of risk acceptable to management officials.

Continued on the next page

D Administrative Security (Continued)

Type	Description
Contingency Planning	FFAS general support systems and major applications shall have viable and logical Disaster Recovery and Contingency Operations Plans. These plans shall be routinely reviewed, tested, and updated to: • minimize damage and disruption caused by undesirable events • provide for continued performance of essential AIS and computer processing operations, services, and mission critical functions.
Accreditation	Accreditation is an acceptable level of risk for which management officials have formally assumed responsibility. The accreditation process shall ensure that adequate and cost-effective security measures and controls have been designed, tested, and implemented into sensitive AIS, LAN, and computer facilities. Every sensitive AIS covered by this policy must be re-accredited every 3 years.
Education and Training	Education and training comprise key elements in the FFAS Information Systems Security Program. Computer security awareness training shall be mandatory for all employees and contractors who are involved in the management, use, or operation of AIS.
Sensitive Systems Security Plans	Sensitive Systems Security Plans must show how the system manager or owner of data is planning to protect and safeguard AIS, data and information processing capabilities from loss, misuse, unauthorized access, and modification. Each plan must address disaster and recovery capabilities. These plans are part of the accreditation process for general support systems and major applications.