United States Department of Agriculture
Research, Education, and Economics

ARS □ NIFA □ ERS □ NASS

Policies and Procedures

Title:	ARS Cybersecurity Program
Number:	253.3.v2-ARS
Date:	May 7, 2012
Originating Office:	Office of the Chief Information Officer, ARS
This Replaces:	P&P 253.3-ARS dated August 19, 1998
Distribution:	ARS Headquarters, Areas, Locations

This P&P is a complete revision of the version dated August 19, 1998. It establishes the supporting program goals, and the assignment of responsibilities for the management, implementation, and operation of the ARS Information Systems Security Program. It also defines the vision and mission of the Information System Security Program and removes references to ARS' old organization. Finally, this P&P reflects the National Institute for Standards and Technology new guidance to authorize the operation of an information system.

Table of Contents

1 Introduction

The purpose of this document is to authorize the ARS IT Security office and program, to reinforce management's commitment to information security, and to assign security roles and responsibilities within the agency.

The use of distributed information systems to store, process, and communicate sensitive information and the integration of computer and telecommunication technologies has made Cybersecurity more complex and essential than ever before. Using this technology must be accompanied by the implementation of an Information Systems Security Program (ISSP) that reduces the associated security risks to an acceptable level. It is understood that the mission of a Cybersecurity program is to maintain the integrity, availability, and confidentiality of ARS wide systems, networks, and data for our customers. The program must provide responsive security support with a centralized focus for policy and enterprise-wide security solutions that are necessary to carry out ARS' scientific mission. The program is authorized by the ARS Office of the Chief Information Officer.

1.1 Cybersecurity Vision

The vision of ARS's Cybersecurity leadership is to "*Promote information assurance to ensure the integrity, availability, and confidentiality of ARS information*." Information assurance denotes maintaining the appropriate level of integrity of information so that it is trustworthy. It also speaks to the availability of information systems to the consumer in a timely manner. Finally, information assurance protects the confidentiality of the information so that it is accessible only to authorized consumers. Information assurance should permeate the entire life cycle of an information system and its components as they are created, processed, transmitted, stored, or retired.

1.2 Cybersecurity Mission Statement

ARS Cybersecurity provides leadership and guidance to support the ARS mission and promote Information Assurance throughout ARS by:

- collaborating with each System Owner to ensure ARS' information systems are in compliance with all applicable Federal laws and regulations;
- implementing meaningful metrics for cost effective and risk-based security;
- promoting Information Assurance through ARS' workforce by implementing an effective Security Education, Training, and Awareness (SETA) program; and
- ensuring the integrity, availability, and confidentiality of the data that is created, processed, transmitted, or stored on ARS Information Technology resources.

2 Authorities

- Computer Security Act of 1984
- Federal Information Security Management Act (FISMA) of 2002
- Office of Management and Budget (OMB) Circular A-123, "Internal Control Systems"

- Office of Management and Budget (OMB) Circular A-130, Appendix III, “Security of Federal Automated Information Systems”
- 5 C.F.R. PART 2635 Standards of Ethical Conduct for Employees of the Executive Branch
- Departmental Regulation (DR) 3300-001, Telecommunications & Internet Services
- Departmental Regulation (DR) 3180-001, Information Technology Network Standards
- Departmental Regulation (DR) 3140-001, Information System Security (ISS) Policy.
- Departmental Regulation (DR) 1495-001, New Media Roles, Responsibilities, and Authorities
- Departmental Manual (DM) 3545-002, USDA Information Systems Security Program

3 General Policy

It is the policy of ARS to establish and maintain an effective Information Systems Security Program (ISSP) that complies with applicable Federal and Departmental information systems security policies and addresses ARS requirements for integrity, availability, and confidentiality. IT security procedures that support a particular mission or goal will be promulgated through the issuance of Cybersecurity guidances and bulletins as an extension of this policy. Due to the dynamic nature of IT technologies, Cybersecurity guidances and bulletins will be established and revised as necessary. Some guidance and bulletins will pertain to all ARS Information Systems, while others may pertain to a subset, for example, a particular branch, application, or to a certain functional area. The guidances and bulletins will convey IT security policies, procedures, and information in standardized format.

3.1 Information Systems Security Program Framework

To meet the objectives above, ARS will establish an Information System Security Program (ISSP) as a combination of management and staff actions, operational activities, and technological control measures. Risk management includes the development and maintenance of computer security policies, procedures and plans, system accreditation and the continuous monitoring of security controls for ARS systems and applications in production. The following ISSP elements establish the framework for the ARS ISSP:

- The ISSP framework will include:
  - Policies, guidelines, bulletins and standards.
  - Assignment of security responsibilities.
  - Security authorization of information systems and applications
  - Security education, training, and awareness
  - System and System Boundary Protection

3.1.1 Policies, Guidelines, Bulletins and Standards

The foundation of the ISSP is the development and implementation of policies, standards, and guidelines in compliance with those at the Federal and Departmental level. ARS will adopt USDA cyber security Departmental Regulations (DR) and Departmental Manuals

(DM). Where specific policies are needed for issues unique to ARS, the Office of the Chief Information Officer (OCIO) will develop Policies and Procedures (P&P) through ARS' issuance process. Specific IT security procedures that support a particular ARS mission or goal will be promulgated through the issuance of Cybersecurity guidances and bulletins as an extension of this policy. The guidances and bulletins will be published and distributed to system owners and system administrators.

3.1.2 Assignment of Security Responsibilities

System owners will be notified, in writing, by the ARS Authorizing Official of their responsibilities for maintaining their system's Authorization to Operate (ATO.) System Owners will ensure that responsibilities for information systems security are clearly communicated to employees within their jurisdiction. If required by the importance of the computer resources and/or the sensitivity of the information processed, an information systems security representative may be formally designated to exercise the security management functions on behalf of the System Owner.

- Each System Owner may elect either dedicated personnel with Cybersecurity responsibilities, or use an alternative management structure where responsibilities are collateral in addition to their normal duties as long as all responsibilities are effectively executed. Assigning personnel with dedicated Cybersecurity responsibilities is the preferred management approach. The system owner should consider a separation of duties between those who will monitor for compliance and those who will administer the system.
- An alternative structure may also use contracting support to augment their security staffing as long as the security responsibilities are documented in the Statement of Work or contract.
- The ARS Chief Information Security Officer (ARS CISO) must be advised of the Cybersecurity point of contact identified for each system.

3.1.3 Security Education, Training and Awareness

Education, training, and awareness are key elements in the ISSP. Information systems managers, technical staff, and users will be familiar with established goals and their responsibilities with regards to Cybersecurity. To accomplish this, ongoing security awareness and education training will be provided to all employees.

- ARS OCIO will provide annual security awareness training in accordance with Departmental guidelines.
- System owners will promote information sharing among system administrators and security support staff.
- System owners will set aside funding to provide, on an annual basis, specialized security training for those employees with designated security roles and responsibilities.
- To successfully establish, manage and improve an agency/staff office/program area ISSP, all employees shall receive annual security training.

- All records of annual awareness training and specialized training will be recorded and tracked in the agency's learning management system.
- As new technologies are introduced into ARS's IT production environment, an assessment must be performed of any new vulnerabilities the technology may introduce.

3.1.4 Security Authorization of Information Systems and Applications

A formal security authorization process will be implemented to ensure that appropriate controls have been designed into sensitive computer applications. ARS will adopt the National Institute of Standards and Technology Federal Information Processing Standards (NIST FIPS) as its standard to establish the proper level of security categorization. An essential requirement of this process will be to include the manager of the business function for determining the proper level of security categorization and the security control requirements for the business function.

- Continuous Monitoring: ARS information systems will undergo continual security reviews as required by Federal regulations and Departmental Directives.
- The USDA official FISMA reporting tool will be the repository for collected artifacts and security authorization documentation.
- Conducting systems security audits and assessments of management practices, processes and technologies.

3.1.5 System and System Boundary Protection

New systems, as defined by FISMA, or system components, or significant changes to systems in production will be reviewed to ensure that security controls are implemented at the appropriate level for the system's security categorization. ARS will establish appropriate safeguards and procedures to detect actual or potential security violations and to counteract each threat as identified in a risk analysis. The System Owner will be responsible for mitigating risk and reducing vulnerabilities at the system level. The ARS Office of the Chief Information Officer will be responsible for mitigating risk and reducing vulnerabilities at the enterprise level. The various types of ARS-wide security procedures to reduce risk at the enterprise level will include, but not limited to, the following:

- Monitor and respond proactively to intrusion attempts using Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) tools.
- Perform patch management and vulnerability scanning.
- Maintain an incident response capability for containing, isolating, responding to security breaches and recommending a corrective course of action to mitigate future incidents.
- Perform computer forensics for the investigation of suspected misuse of Government information technology resources.

4 Sanctions for Misuse

ARS will take corrective action and/or enforce the use of penalties against any user who violates any USDA, ARS, or Federal system security policy. Disciplinary actions could include the following actions, up to removal:

- Written reprimands.
- Temporary suspension from duty.
- Reassignment, demotion or removal.
- Suspension of system privileges.
- Possible criminal prosecution.

4.1 Revocation of System Accreditation

Each ARS information system, as defined by FISMA, must have a current Authorization-to-Operate designated by the ARS Authorizing Official. Any system that does not have a current Authorization-to-Operate will be subject to management review that may lead to removal from the production environment. The system will not be accessible by the general public or general ARS employees. Only the Authorizing Official may reconstitute access to the system.

5 Summary of Responsibilities

Each ARS System Owner will identify a security point of contact for each system to ensure the responsibilities listed below are met.

- Implement established information security policies within their jurisdiction;
- Implement and maintain the appropriate security controls for IT systems and applications in production;
- Conduct regular risk assessments for IT systems and applications;
- Implement and maintain effective risk mitigation strategies;
- Provide information for the preparation of the annual Departmental Security Program assessment;
- Respond to regular and ad hoc reporting requirements and audits;
- Monitor for compliance to USDA, OMB, NIST and other governing bodies’ security policies;
- Monitor for compliance to the Security Awareness and Training Program and promote information systems security awareness and ethical use of automated information systems;
- Monitor for compliance to the Security Incident Response Program;
- Notify OCIO of any newly discovered vulnerabilities and threats that may impact other jurisdictions other than their own and promptly report to the ARS Incident Response Team (ARS-CyberIR@ars.usda.gov) any breaches of security or events that may indicate security violations or attempts to gain unauthorized access to computers, information systems, or data resident on information resources.
- Maintain system audit trails, controls logs and other mechanisms;

- Disseminate Agency and Department policy and procedures to location personnel;
- Monitor for compliance to system Configuration Management (CM) process of all systems;
- Assist and support the Security Authorization process (formerly known as the Certification and Accreditation (C&A) process) for the information systems;
- Develop security documentation for each general support system and major application;
- Ensure appropriate security requirements are included in the procurement lifecycle starting with the Acquisition Approval Request process.

5.1 Supervisors

- Counsel employees on the proper use of IT resources to ensure those resources are being used appropriately.
- Immediately notify the servicing Employee Relations Specialist when they are made aware of potential misuse of Government IT resources.
- Ensure all employees complete all security awareness and other IT related mandatory training.

5.2 Employee Relations Specialists

- Determine whether misuse indicated is based on appropriate law, rule, regulation, or agency policy.
- Conduct an inquiry/investigation into the extent of the misuse of IT resource(s). Please see ARS P&P 253.4 “Use of Information Technology Resources” for more information on acceptable and unacceptable use of Information Technologies.
- Provide advice and guidance on appropriate disciplinary action.

5.3 Employees, Contractors, Collaborators, Consultants, Volunteers

- Ensure that personal use of IT resources is limited to personal time, does not interfere with official business, and involves minimal additional expense to the Government.
- Notify their immediate supervisor if they have reason to believe IT resources are being used for other than authorized purposes.
- Complete all security awareness and other IT related mandatory training.
- Comply with all security requirements pertaining to the automated information resources they use.
- Practice good housekeeping with all computer equipment (i.e., computer areas should be uncluttered, and food, drinks, and smoking should be kept away from computers).
- Safeguard all user ID’s and passwords to automated information systems.
- Backup data and systems on a regular basis.

- Understand and comply with all licensed software agreements before using the software at each work area.
- Report all computer security incidents to ARS-CyberIR@ars.usda.gov.

6 Definitions

Authorization (to operate)
The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.

Availability
Ensuring timely and reliable access to and use of information.

Confidentiality
Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Information
Any representation of knowledge such as facts, data, or opinions, including numerical, graphic, or narrative maintained in any medium or form, including computerized databases, paper, microfilm, or magnetic tape.

Information System
A discrete collection of processes, data, people, and technologies organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Information System Owner (or Program Manager)
Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.

Information Technology [40 U.S.C., Sec. 1401]
Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.

Integrity

Integrity, in terms of data and network security, is the assurance that information can only be modified or updated by people or processes authorized to do so. Integrity means that data cannot be modified undetectably.

Investigation

A formal examination and evaluation of relevant facts to determine whether misconduct has taken place or, if misconduct has already been confirmed, to assess its extent and determine appropriate action.

Security Control Assessment

The testing and/or evaluation of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

Separation of Duties

Separation of duties is the security principle to manage conflict of interest, the appearance of conflict of interest, and fraud. It restricts the amount of power held by any one individual. It puts a barrier in place to prevent fraud that may be perpetrated by one individual.

Approved:

/s/

Paul R. Gibson, Chief Information Officer
Office of the Chief Information Officer

5/7/12

Date