UNITED STATES DEPARTMENT OF AGRICULTURE
AGRICULTURAL MARKETING SERVICE

DIRECTIVE 3130.7 12/15/2005

INFORMATION TECHNOLOGY SECURITY

Table of Contents

1 Policy

1.1 What is the purpose of this policy?

This policy describes the U.S. Department of Agriculture (USDA), Agricultural Marketing Services (AMS) Cyber-Security Program, which details requirements for Information Security, Network Security, and Computer Security programs and provides guidance on the implementation of Cyber-Security counter-measures within AMS.

1.2 What is the AMS policy on cyber-security?

All personnel that require access to AMS's computer and telecommunications hardware and software components are required to protect the confidentiality, integrity, and availability of these resources. This policy includes access to AMS networks, desktop computers (PCs), workstations, laptop computers, servers, network devices, handheld Personal Electronic Devices (PEDs), Blackberry, office automation equipment (such as copiers and fax machines), whether owned or leased.

1.3 What directives and requirements is this policy based on?

This policy incorporates the requirements of Public Laws, OMB Circulars, NIST Publications, and Department and Agency regulations listed in Appendix A.

1.4 What happens if personnel do not follow this policy?

Personnel that fail to comply with this policy are subject to appropriate actions by the Agency, to include administrative disciplinary actions and restriction of IT operations that can include termination of network connectivity.

1.5 Why is computer security so important?

A security breach on one AMS computer can potentially compromise the entire AMS network. As long as the AMS computers are attached to the Internet, they are at risk and will be attacked. We must all take the necessary precautions to defend against these attacks. If everyone does their job in protecting our AMS information assets, we will be less vulnerable to these attacks. Attacks can range in severity from being a nuisance to a complete shutdown of the AMS network, leading to a significant loss in productivity, time, and money.

2 User Responsibilities

2.1 What are my responsibilities as a user of AMS computer information systems?

You must comply with the user responsibilities described in this section and sign the User Certification on the Request for AMS Wide Area Network User Account, AMS Form 3130.7. The User Certification statement is completed once by each user and can be hand carried, mailed, or faxed to the Information Technology Group (ITG) Technical Resource Branch (TRB). If you are a new user, you will not receive a network user account or password until you have completed and submitted this form.

2.2 What are the security awareness training requirements?

The Computer Security Act of 1987 and OMB Circular A-130 require AMS to provide periodic training in computer security awareness and accepted computer security practices for all employees who manage, use, or operate a Federal computer system. This includes contractors and volunteers, as well as AMS employees.

New users must also agree to complete the annual security awareness training provided by the AMS ITG Cyber-Security Branch (CSB) within 60 days of receiving network access.

All users are required to take annual refresher security training as determined necessary by the Agency, typically at least once each calendar year.

Additional security training may be necessary when there is a significant change in the Agency's information security environment or procedures, or if your job requires additional security training.

The Cyber-Security Branch will provide guidance, instructions, and information on training requirements. They will also monitor the status and completion of training and report the status to Agency and Department officials.

2.3 What are the AMS User account name requirements?

Network user accounts are assigned only for use by one user. You must not allow any other user to use your user account.

2.4 What are the AMS Password requirements?

1) Passwords shall have a minimum length of eight characters;

2) Password complexity shall consist of at least three of the following four characters: Upper case letters, lower case letters, numbers, and special characters, such as !, $, #, %;

3) Passwords must be changed at least every 90 days;

4) Passwords should be changed anytime you know or feel that someone else may know it;

5) **Do not** use a Password that is easily associated with you, such as your name, Social Security number, tag number, telephone number, street address, username, spouse, significant other, child, or pet;

6) **Do not** use a password that contains common words from an English dictionary or a dictionary of another language with which you are familiar;

7) **Do not** use a password that contains commonly used proper names, including the name of any fictional character or place;

8) **Do not** use a password that you have recently used before. NOTE: The AMS network will not allow you to reuse one of your previous five passwords;

9) **Do not** give your password to anyone over the phone. NO ONE representing AMS in any official capacity should ever ask you for your password.

2.5 What are some of the unacceptable uses of AMS Internet and E-mail systems?

1) Using Government office equipment for personal commercial purposes or in support of other external enterprises such as outside employment or businesses, such as selling real estate, preparing tax returns, or trading stock;

2) Viewing, downloading, storing, transmitting, or copying material that is sexually explicit or sexually oriented, related to gambling, illegal weapons, terrorist activities or any other prohibited activities;

3) Using Government office equipment to engage in any outside fund raising activities, endorsing any product or service, or participating in lobbying or prohibited partisan political activities, such as expressing opinions about candidates and distributing campaign literature;

4) Creating, copying, or transmitting any material or communication that is illegal or offensive to fellow employees or to the public, such as hate speech, material that ridicules others based on race, creed, religion, color, sex, disability, national origin or sexual orientation;

5) Creating, copying, or transmitting chain letters or other mass mailings, regardless of the subject matter;

6) Engaging in e-mail practices that involve ongoing message receipt and transmission, referred to as "instant messaging," unless the use of the feature has been approved by a supervisor for official business or as an accommodation;

7) Using large files while engaging in limited personal use of Government equipment. For example, sending or receiving greeting cards, video, sound, interactive games or other large file attachments that may hinder the performance of a network. You should not subscribe to Internet services that automatically download information, such as sports scores, stock prices or other continuous data streams, such as music or videos;

8) Loading personal software onto your computer or making configuration changes. For example, computer games and personal tax programs may not be loaded on Agency computers;

9) Using Government equipment as a staging ground or platform to gain unauthorized access to other systems;

10) Acquiring, reproducing, transmitting, distributing or using any controlled information, such as computer software and data protected by copyright, trademark, privacy laws, or other intellectual property rights beyond fair use; or export-controlled software or data.

Additional information about appropriate use of Government equipment can be found in AMS Directive 3300.1, Use of Government Office Equipment.

2.6 What are the restrictions on the use of copyrighted software?

Copyrighted software must be used in accordance with the license agreement. A valid license must be purchased for all commercially available copyrighted software used on an AMS system.

Copyrighted software is software that is provided under licensing agreements as authorized by Title 17 of the U.S. Code. Section 106 of this Title gives copyright owners exclusive rights to reproduce and distribute their material. Section 504 states that copyright infringers can be held financially liable for damages to the copyright owner. Title 18, U.S. Code, Section 2319 also imposes criminal penalties for some types of software copyright violations.

2.7 What are the requirements to connect a computer system to the AMS Network?

All computer systems (personal computers, laptops, and servers), whether AMS- or contractor-owned, that are connected to the AMS network must:

1) Be scanned for vulnerabilities and updated with the current/latest patches, fixes, and service packs. System Administrators are responsible for ensuring that the systems are patched and do not have vulnerabilities;

2) Have an approved anti-virus program installed and running with current virus data definition files. System Administrators are responsible for setting up the automatic updates to these files;

3) Use locked screen savers, requiring a password to gain access if inactive for 15 minutes;

4) Use one of the Agency’s standard operating systems as specified by AMS Directive 3130.5, Information Technology Standards, found on the AMS intranet site.

5) **Not** run Internet-aware hosting services, such as a Web service (Internet Information Service (IIS), e-mail services (SMTP), or file hosting services, without an approved waiver in writing from the AMS CIO;

6) **Not** have a modem on a computer connected to a phone line and an AMS network at the same time. However, computers at a remote worksite may use a modem only to dial out to a public phone line to access the network through the AMS Virtual Private Network

(VPN) service; Computers **must not** have a modem configured to allow any incoming calls;

7) **Not** connect personally owned computer systems to any Government-owned networks or telecommunications equipment;

8) **Not** use or install any Peer to Peer (P2P) file sharing applications, such as Kazaa, Napster, Gnutella, or Morpheus.

2.8 What are the requirements for using a Personal Electronic Device (PED)?

Portable/mobile electronic computing devices, such as personal digital assistants (PDAs), notebook computers, Word Pads, and Blackberrys, approved for connectivity shall:

1) Employ password protection for access to devices;

2) Employ virus protection software on supportable portable devices. Note: Blackberrys currently do not have anti-virus protection;

3) Employ encryption technology on portable devices that are capable of doing so to protect sensitive information that may be present.

2.9 How do I report a security incident?

Report all security incidents such as those below to your program area Information Systems Security Officer (ISSO). If you are unable to get in touch with your ISSO, you can contact the ITG Cyber-Security Branch:

In Person: Room 1761 or 1757 – South Building
1400 Independence Ave., SW
Washington, DC 20250-0204

By E-mail: AMS.CyberSecurity@usda.gov, or
WashingtonDCSTITCSB@usda.gov,

By Phone: 202-720-1108 (ISSPM), or
202-690-4868 (Alternate ISSPM)

By Fax: 202-690-1145

The AMS Cyber-Security Branch is responsible for reporting information security incidents to the USDA Cyber-Security Associate Chief Information Officer, and to the Federal Computer Incident Response Center (FEDCIRC).

A **security incident** is any act that violates an explicit or implied security policy within AMS or its operating units. More specifically, an incident is any adverse event that threatens the security of information resources. Incidents may include, but are not limited to:

1) **Compromise of integrity -** when a virus or malicious code, such as worms, Trojans, backdoors, scripts, mass-mailers, etc, infects a system or network;

2) **Loss of accountability/misuse -** when an authorized or unauthorized user uses an account or a system for unauthorized or illegal purposes;

3) **Unauthorized Access -** when an unauthorized outsider gains or is suspected of gaining access to AMS IT resources;

4) **Damage to any part of the system –** intentional or unintentional damage to or destruction of hardware, software, or data;

5) **Denial of service attack (DOS)** - when an attacker has disabled a system or a network worm has used all available network bandwidth;

6) **Reconnaissance Scans/Probes/Attempted Denial of Service -** report all unauthorized network scans/probes/attempted denial of service, if the reporting site considers the scans significant or unusually persistent.

3 AMS Cyber-Security Program

3.1 What are the Administrator’s Program responsibilities?

1) Communicate the importance of IT Security in the Agency’s mission;

2) Ensure that AMS has an established IT Security Program;

3) Ensure that available funding and resources are available for staffing, training, and implementation of system safeguards as required for Agency IT operations in support of AMS’s Cyber-Security Program;

4) Ensure that Deputy Administrators provide adequate resources to protect data and systems within the programs in accordance with the AMS Cyber-Security Program.

3.2 What are the Deputy Administrator’s Program responsibilities?

1) Ensure that your program area complies with the requirements of the AMS Cyber-Security Program to protect your information technology resources;

2) Communicate to all personnel working in your program area that Cyber-Security is critical to the successful delivery of our services;

3) Serve as the Designated Approving Authority (DAA), accepting operating risk for all systems and applications that support your program’s mission;

4) Assign security and management responsibilities of IT systems in your program area to responsible program officials;

5) Designate in writing to the AMS Information Systems Security Program Manager the names of your Information Systems Security Officer (ISSO) and two alternates. Segregation of duties should be taken into consideration when you assign security functions to the various program level personnel. Segregation of duties provides:

   – A system of checks and balances; a compensating control over the mere appearance of impropriety by those in a position to bypass IT security controls.

   – The best compromise between usability and security -- the separation enables each person involved to accomplish their individual duties, resulting in a reasonable compromise between usability and security with many people working to keep the balance.

In summary, those who manage and fund the operation of an IT resource must accept the risks associated with that system and the responsibility for securing that system's resources.

3.3 What are the Chief Information Officer (CIO) Program responsibilities?

1) Oversee the AMS Cyber-Security Program and associated policies;

2) Ensure appropriate procedures are in place for Certification and Accreditation (C&A) of major systems and applications;

3) Monitor, evaluate, and report to the Administrator and Associate Administrator on the status of Cyber-Security within the Agency.

3.4 What are the Information Systems Security Program Manager (ISSPM) Program responsibilities?

The Chief of the AMS Cyber-Security Branch serves as the AMS ISSPM. This position is to:

1) Develop security policy for AMS, to include standards, practices, and related guidance;

2) Perform annual compliance reviews of program level IT Security Programs and system controls, including reviews of security plans, risk assessments, and the C&A process;

3) Advise the AMS CIO and program level ISSOs of advances in security technology;

4) Track, through the implementation of corrective actions, agency-wide security deficiencies and program area weaknesses reported through self-assessments, inspections, and reviews;

5) Work cooperatively with the USDA Office of the Chief Information Officer (OCIO), the USDA Office of the Inspector General (OIG), the AMS programs areas, and other entities to ensure that AMS has an effective Cyber-Security Program;

6) Plan and chair regular meetings with the ISSO's and security representatives as a forum for exchange on AMS security issues.

3.5 What are the Information System Security Officer (ISSO) Program responsibilities?

1) Serve as your program area's central point of contact for the Cyber-Security Program;

2) Implement security policies, procedures, standards, and guidance consistent with Agency, Department, and Federal requirements;

3) Provide information to system administrators and others concerning risks, vulnerabilities, or potential threats to systems;

4) Ensure that all program area system vulnerabilities identified by vulnerability scans are promptly resolved in accordance with established time frames;

5) Ensure that your program area systems have all required patches installed;

6) Ensure that your program area systems have up-to-date anti-virus protection;

7) Ensure that all systems are scanned for viruses and other forms of malicious code at least once a week;

8) Ensure that all major systems have the following security documentation and that the documentation is reviewed annually and updated as required:

    a. A qualitative risk assessment;

    b. Current IT System Security Plan (SSP) that accurately reflects system status;

    c. Current system Certification and Accreditation (C&A) documentation;

    d. Annual system self-assessments;

    e. Current contingency plans that have been tested.

9) Ensure that all personnel in the program area fulfill all security training requirements, including any specialized training, such as for system administrators;

10) Act as the program area's central point of contact and coordinate with the AMS Cyber-Security Branch (CSB), as appropriate, concerning Cyber-Security incidents, potential threats, and other security concerns.

3.6 What are the System Administrator (SA) Program responsibilities?

1) Ensure all required patches are on all systems that you are responsible for;

2) Keep anti-virus protection up-to-date on all systems you are responsible for;

3) Ensure that the Domain Admin Group is added to the Local Admin Group on all computers (servers, desktops, laptops).

4) Assist your program area ISSO in the development and maintenance of security plans and contingency plans for all general support systems and major applications in your program area;

5) Participate in annual risk assessments to evaluate the sensitivity of your program area's main systems, the security risks and their respective mitigation strategies;

6) Participate in the C&A processes and the development of documentation for your program area's main systems;

7) Know the sensitivity of the data your systems handle and take appropriate measures to protect it;

8) Evaluate, develop, and maintain system administration operational procedures and security manuals that assure proper integration and continuity with other system operations;

9) Take appropriate action to mitigate risks associated with all systems you are responsible for.

3.7 What are the key counter-measures used by the AMS Cyber-Security Program?

No one measure by itself can effectively protect all information in AMS. However, taken together and effectively applied, AMS intends to use the following measures to mitigate cyber-security risks to acceptable levels:

1) Vulnerability Scanning

2) Patch Management

3) Anti-Virus management

4) Certification and Accreditation (C&A)

5) Change Management

6) Contingency Planning

7) Incident Response Procedures

8) Plan of Action & Milestones (POA&M)

9) Security Awareness and Training

3.8 What is Vulnerability Scanning?

Vulnerability scanning is the process of examining network components, systems, or applications to evaluate the true risk, or exposure, of the system to known threats. Vulnerability scanning analyzes the current state of the system by reviewing the system components and searching for anomalies that might indicate vulnerabilities that could permit an attack.

Vulnerability scans are to be performed on all new and existing servers, desktops, and laptops in accordance with established procedures. Scanning will, at a minimum, test for the following:

1) Operating system, platform, or application vulnerabilities;

2) Installation of security-relevant patches, service packs, and/or fixes;

3) Assessment of procedural or technical controls susceptible to misuse;

4) Easily guessed or blank passwords and default installed accounts, such as guest and administrator.

Each program area will designate authorized personnel to respond to software and hardware vulnerabilities identified in Agency vulnerability scans. The program area will then take corrective action(s) to resolve all critical vulnerabilities reported and notify the Agency of action(s) taken each month. Program areas may also perform their own vulnerability scans on all IP addresses assigned to that program area prior to or after the Agency scans. All authorized program users must be trained in the use of the scanner software prior to conducting any network scans.

A Plan of Action and Milestones (POA&M) must be reported for any unresolved critical vulnerabilities existing for more than 30 days from the date of the last scan.

3.9 What is Patch Management?

Patch Management is a set of procedures that ensure Information Systems have a regular schedule or automated process for identifying and loading appropriate security updates, patches, or fix actions for the operating system or software applications.

All AMS systems must have the approved Agency patch management client active on each system to facilitate patching, monitoring, and reporting capabilities;

Patch Management efforts will be reviewed on a monthly basis by a central monitoring process to determine the effectiveness of the patch management efforts across the Agency.

3.10 What is Anti-Virus Management?

Anti-Virus management is a set of procedures to ensure Information Systems have implemented provisions to detect, remove, and protect against viral infections. Viruses and other forms of malicious code, such as worms, Trojans, backdoors, scripts, mass-mailers, represent a significant threat to network assets. Users must be educated about viral threats and best practices required to protect against infection.

All AMS systems must have an up-to-date Anti-Virus Client installed.

Anti-Virus Clients must be configured to ensure that the latest Anti-Virus definitions are downloaded on a daily basis or as released from the vendor.

All systems must be scanned for viruses and other forms of malicious code at least once a week.

3.11 What is Certification and Accreditation (C&A)?

C&A is a process of formal testing (certification process) and acceptance of security risks (accreditation) on major systems. C&A is the process that documents, evaluates, tests, and identifies any risk related to the operating of an IT system. All identified major systems within the Agency must have an accreditation prior to being placed into production.

3.11.1 What is the Certification process?

The certification process is a comprehensive evaluation of the technical and non-technical security features of an IT system and other safeguards (e.g., physical, personnel, procedural, and environmental) to establish the extent to which a particular design and implementation meet a set of specified security requirements. Certification is a process of security testing and evaluation that documents, analyzes, and evaluates the system in its operational or proposed operational environment.

3.11.2 Who completes the Certification process?

Certification is completed at the Program level that owns and operates the system, unless the system’s security categorization requires the use of a third party. The Certification team would typically be made up of Program management, the System Owner, the ISSO, the SA(s), and any other technical personnel involved with the system. A program-level C&A point of contact shall be identified for each major system.

3.11.3 What is Accreditation?

Accreditation is a written statement, normally an Authorization to Operate (ATO), by the Designated Approving Authority (DAA). By signing, the DAA has declared that he or she has reviewed the design, implementation, and certification testing of the system, and confirms that it meets the requirements for data security and approves it to operate at an acceptable level of risk.

3.11.4 Who completes the Accreditation documentation process?

The AMS Cyber-Security Branch will work with the system owners to prepare the Accreditation documentation for signatures. Accreditation is granted by the Designated Approving Authority (DAA), who is the program official with management, operational, and budget control over the IT system to be accredited. To ensure separation of duties in AMS, the DAA **must** be an Administrator, Associate Administrator, or Deputy Administrator.

When operational need or mission criticality requires a system to become operational and the system does not provide adequate safeguards, the DAA may grant an accreditation with conditions or an Interim Authorization to Operate (IATO). Any approved IATOs **are not to exceed one year duration,** and shall be reviewed on a quarterly basis.

3.11.5 How often must C&A be accomplished?

Each major system must be re-accredited every three years, or when significant security relevant changes are made to the system.

3.11.6 What government guidance is available on the C&A process?

All systems shall be certified and accredited in accordance with USDA, AMS, and National Institute of Science and Technology (NIST) Guidelines (Special Publication 800-37, *Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems*,) prior to being placed into operation. Please contact the AMS Cyber-Security Branch for additional guidance and assistance with the C&A process.

3.11.7 What are the initial steps of the C&A process?

First, the C&A Security Categorization must be completed to determine the appropriate levels of protection required for each system. The Federal Information Processing Standards Publications (FIPS PUB) 199 provides guidance for assigning security categorization factors for information processed on federal systems. In order to assign the appropriate security categorization to the major system or application, you must determine the level of concern (**Low**, **Moderate**, or **High**) for the following three factors:

Confidentiality (C) - provides assurance that the system data is protected from disclosure to unauthorized personnel, processes, or devices.

Integrity (I) - provides assurance that the data processed by the system is protected from unauthorized, unanticipated, or unintentional modification or destruction.

Availability (A) - provides assurance that the system data and resources will be available to authorized users on a timely and reliable basis.

3.11.8 What are the C&A phases?

The C&A process consists of three phases: the pre-certification phase, the certification and accreditation phase, and the post-accreditation phase.

Phase 1 (the pre-certification phase) - defining the scope of the C&A effort, identifying existing security controls**,** reviewing any approved Interconnection Security Agreements (ISA), conducting a Privacy Impact Assessment (PIA), reviewing the System Security Plan (SSP), reviewing the initial risk assessment, and negotiating with the participants;

Phase 2 (the certification and accreditation phase) - conducting the Security Test & Evaluation (ST&E), updating the risk assessment with findings from the ST&E, updating the SSP, documenting the certification findings, and forwarding the certification findings to the C&A team, the Department's Cyber-Security Group, and then to the DAA for an accreditation decision;

Phase 3 (the post-accreditation phase) - consists of managing the configuration of the system and re-accreditation.

3.11.9 What C&A documentation is required?

Depending on the security categorization of the system the following documentation would be required for the C&A effort:

Documents Required	Security Categorization	
	C-I-A = One or More High or Medium	C-I-A = all Low
System Security Plan	Required	Required
Self - Assessment	Required	Required
Risk Assessment	Required	Required
Accreditation letter from DAA	Required	Required
Contingency, Disaster Recovery plan	Required	Required
Privacy Impact Assessment (PIA)	Required	Required
Third-Party Security Test & Evaluation Plan	Required	
Third-Party Security Test & Evaluation Report	Required	
Configuration Management Plan	Required	
Trusted Facility Manual (TFM)	Required	
Security Features Users Guide (SFUG)	Required	
Additional support documentation (vendors manuals, user manuals, others)	Required	

3.12 What are the Configuration and Change Management requirements?

All systems requiring C&A shall follow configuration management described below. Each system owner shall:

1) Ensure all changes are documented, tested, and approved by management before being placed into production. Normal Windows patches, updates, and antivirus updates are not subject to this requirement;

2) Ensure that changes to the system are added to the C&A documentation.

Personnel responsible for making changes on these systems should document the items listed below, and receive all appropriate management and program technical approvals for the proposed changes prior to making them.

Recommended Change Management Checklist:

1) Requestor of the change
2) Description of the change
3) Reason for the change
4) Date and time the change is scheduled
5) Describe the procedures for implementing the change
6) Impact on customers during implementation
7) Is there a system outage required? If so, what is the duration of the outage?
8) Will users be notified in advance of the proposed change? If so, how and when will they be notified?
9) What are the risks associated with the change? What problems or symptoms are likely if the implementation is not successful?
10) Who will test the change? How will it be tested? Who will review the test results?
11) Describe the back-out procedures for the change (briefly describe each back-out strategy in order of priority of use). Impact on customers if back out is necessary

3.13 What is Contingency Planning?

Contingency Planning describes the procedures to be taken in the event that system operations are disrupted and the testing of those procedures to determine their effectiveness in restoring business functions and services. Contingency Plans are required for:

1) **A temporary incident,** such as loss of power or building access interrupts operations for hours or days;

2) **A major disaster,** such as fire or flooding where operations must be relocated or shut down for days or weeks.

System owners must have Incident and Disaster Recovery Plans prepared and tested for any system that requires C&A. Contingency plans must be tested on an annual basis. Any testing deficiencies or updated plans shall be incorporated in the C&A documentation. Contingency plans shall be developed in accordance with NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*. Please contact the AMS Cyber-Security Branch for additional guidance and assistance.

3.14 What is a Plan of Action & Milestones (POA&M)

A POA&M is an executable plan of corrective actions and associated milestones intended to address security vulnerabilities that have been identified for systems or programs. Vulnerabilities can be identified through:

1) Annual FISMA reviews;
2) OIG, GAO, and financial audits;
3) Certification & Accreditation (C&A) activities;
4) Annual Self-inspection;
5) Vulnerability scans (critical vulnerabilities that are unresolved after 30 days are entered into the POA&M);
6) Security incidents

A POA&M Action Item is a task that is planned to mitigate an identified vulnerability.

A POA&M Milestone is the completion of a specific activity in an Action Item.

The ISSO of a system or application identified in the POA&M action item must report the current status of the POA&M action items and its milestones to the AMS ISSPM on a monthly basis until resolved. POA&M items are tracked in a consolidated POA&M database, which is maintained by the AMS CSB and the Department OCIO. POA&M items are included in the annual FISMA report to OMB.

3.15 What should I do if I have a system or application that cannot comply with a security requirement based on a specific business need?

If you have a system or application that requires an exception to one or more of these security practices and the security risks can be appropriately mitigated, the AMS Chief Information Officer (CIO) can grant a written waiver. You must submit your request in writing to the CIO and include the following:

1) description of the system or application that requires the waiver
2) a business case for the waiver;

3) the measures taken to mitigate any security vulnerabilities;

4) your plan and timeline to comply with the standard security practices.

All waivers must be reviewed on an annual basis for continued applicability and to determine the progress that has been accomplished to eliminate the need for the approved waiver. Contact the AMS CSB for additional assistance and guidance on submission of waivers.

/s/

Lloyd C. Day
Administrator

Attachment A:

Security References

The following is a list of the main references that are applicable to the Agency's IT security policy:

US Federal Directives/Guidance

Federal Information Security Management Act (FISMA, enacted December 2002)

Circular A-130, Appendix III *Security of Federal Automated Information Resources* (Nov 2000)

NIST Computer Security Special Publications (800 series)

NIST Federal Information Processing Standards (FIPS series)

USDA-AMS Cyber-Security Directives/Guidance

OCIO Cyber Security Guidance (OCIO Intranet site)

AMS Cyber-Security Branch (AMS Intranet site)

AMS Directives

AMS Directive 3300.1, Use of Government Office Equipment (02/09/2001)

AMS Directive 3130.5, Information Technology Standards, (04/01/2004)