U.S. DEPARTMENT OF AGRICULTURE
WASHINGTON, D.C. 20250

DEPARTMENTAL REGULATION	Number: DR 3180-001
SUBJECT: Information Technology Network Standards	DATE: September 30, 2008
	OPI: Office of the Chief Information Officer

1. PURPOSE

The objectives of the United States Department of Agriculture's (USDA) Information Technology (IT) Network requirements are to: (a) ensure cyber security protection, (b) increase effectiveness in acquiring and administering resources by promoting compatibility and interconnectivity of hardware and applications, (c) ensure that these standards are aligned with the enterprise architecture business goals and processes of USDA, and (d) meet the policy requirements of the Office of Management and Budget (OMB) Circular A-130.

2. SPECIAL INSTRUCTIONS/CANCELLATIONS

This regulation will remain in effect until superseded. Appendices are forthcoming.

3. BACKGROUND

The Clinger-Cohen Act of 1996 (40 U.S.C. 1401(3)), the Information Technology Management Reform Act (ITMRA) and OMB Circular A-130 require Federal agencies to build and maintain a Profile of Standards and Technical Reference Model that support IT investment management and development of enterprise architecture.

4. POLICY

This policy requires the agencies under the administrative oversight of the Department of Agriculture to follow a set of standards regarding communications, connectivity, hardware, applications, and the network environment. The Chief Information Officer of the USDA (CIO USDA) is required to establish standards to ensure the cyber security of the agencies, Department, and government-wide networks.

The IT Network standards are contained as appendices to this general policy. Each appendix is to be reviewed quarterly in the first year of this policy and annually in the following years. The annual review of each appendix is to be conducted in the first month of the third quarter; reviewed for comment by the agencies for 30 days; and finalized prior to the end of the third quarter.

During the annual review, the CIO USDA shall consider whether the following standards are being met:

a. support to the USDA programs for the continuity of operations;

b. focus areas and training to maximize the use of the standard applications and databases;

c. there exists centralized support of critical program systems, mixed financial systems, and systems that contain personally identifiable information;

d. establishing an enterprise architecture standard;

e. IFSM and other government-wide cyber security requirements are met;

f. achieving discounts by volume purchasing;

g. supporting logical and physical access to systems through smartcard based security and E-Authentication;

h. supporting the Department's thin client, mobile technology, and teleworking policy;

i. creating a lower cost, more functional network infrastructure;

j. minimize the number of system and application interfaces;

k. ensure applications and databases are delinquent by no more than one version;

l. require that all critical and mix financial applications are on versions fully supported by the vendor;

m. manage the replacement of major solutions, systems, and hardware; and

n. compliance with USDA's Five Year Information Technology Plan.

Agencies of the United States Department of Agriculture shall operate network infrastructure, communications, applications, interfaces, and data centers consistent with the standards identified in the appendices of this regulation. Exceptions to these standards may be requested through specific procedures identified in Paragraph 7 of this regulation.

IT Network standards are rules or specifications designed to simplify, unify or rationalize the design, interoperability, portability, and scalability of IT infrastructure components (e.g., hardware, application and systems software). The following appendices provide the detailed selection specifications for conforming to the policy requirements of this regulation:

a. Appendix A, Communications Standards
b. Appendix B, Hardware - Cabling and Connectivity Standards
c. Appendix C, Hardware - Wireless Networking Standards
d. Appendix D, Hardware - Firewall, Hubs, and Routers Standards
e. Appendix E, Hardware - Servers Standards
f. Appendix F, Hardware - Midrange Standards
g. Appendix G, Hardware – Mainframes Standards
h. Appendix H, Hardware - Storage Standards
i. Appendix I, Operating System Standards
j. Appendix J, Database Standards
k. Appendix K, Department-wide Application Standards
l. Appendix L, Other Application Standards
m. Appendix M, Physical Security, Operating Environments, and Data Centers
n. Appendix N, Other Information Technology Standards
o. Appendix O, Information Technology Network Security Standards

5. BENEFITS

The benefits from the IT Network to the Department, agencies, and users through the standardization of the information systems, applications, and hosting; ensure the required security for the government's networks, continuity of system operations, protection of information, support of USDA telework and mobile computing technologies, adherence to FISMA security requirements, lower operating costs, and volume-based purchasing discounts.

USDA uses IT to assist the Department in achieving program objectives and reporting requirements. Consistency in USDA's IT allows the development of safe, efficient and cost-effective methods for supporting programs and in planning for upgrades, migrations, staff training, and future technology installations. In addition, these standards also promote cross-agency information sharing, increase interoperability, and improve Departmental communication and collaboration.

6. RESPONSIBILITIES

a. The CIO USDA is:

(1) The final, approving authority on the adoption of IT standards to the security of Government networks, maximize the benefit of technology purchases, and minimize investment and operating expense.

(2) The final reviewer and approver to exceptions to the network standards when requested by the agencies or staff offices.

b. The Office of the Chief Information Officer (OCIO) will:

(1) Develop basic policies and standards for the network environment.

(2) Provide management and oversight activities related to network configurations, including but not limited to:

(a) Providing periodic updates to all network configurations to network security posture is maximized;

(b) Reviewing and monitoring compliance with established network policy;

(c) Testing all configurations in a non-production environment to compatibility with legacy applications;

(d) Supporting the agencies with testing of network software;

(e) Creating a software update architecture that is able to receive and approve patches and updates from the Department of Homeland Security for deployment to the Department's enterprise;

(f) Creating and maintaining a security configuration guide for each network; and

(g) Reporting compliance and deviations to OMB.

(3) Establish enterprise-wide contracts for standard network hardware and software.

(4) Establish and maintain the green policy, recycle policy, and energy conservation policy for network components.

c. Department agencies and staff offices will:

(1) Adopt the policies and standards for the network environment by:

(a) Establishing procedures and controls to the use of these standards;

(b) Ensuring effective communication between local network administrators and OCIO; and

(c) Incorporating these standards in each agency's capital planning and investment control process.

(2) Implement and maintain network and security configuration settings by:

(a) Scanning and providing periodic updates to all network configurations to network security posture is maximized;

(b) Documenting all deviations from these standard network settings with a detailed rationale for the deviations, and request for a waiver from Cyber Security;

(c) Providing corrective action plans for the timely remediation of issues not authorized as an approved deviation;

(d) Ensuring only qualified and trained personnel are granted elevated privileges;

(e) Ensuring that elevated privileged accounts are not mail or internet enabled;

(f) Ensuring all custom or commercial off the shelf (COTS) applications are written to be run as "user";

(g) Creating an authorized software list that includes all the software that can be used on these configurations; and

(h) Employing the use of the National Institute of Standards and Technology (NIST) Security Content Automation Protocol (S-CAP) tool to help evaluate providers and perform self evaluations.

(3) Procure standard network hardware and software from enterprise–wide contracts as they are made available.

(4) Request acquisition of network hardware and software standards using the Acquisition Approval Request (AAR) process prior to any procurement. The AAR must identify whether or not the acquisition of network hardware or software to be procured meets the USDA standards, the contracts to be used and must provide a detailed rationale if the product(s) being purchased does not meet the standard, regardless of whether the standard is a product or a specification(s).

(5) Review and implement the appendices to this regulation.

7 EXCEPTION REQUEST PROCESS

Some agencies may have special conditions or requirements that prevent full compliance with this regulation. Agencies may request a special exception by submitting written justification to the CIO USDA for review and decision. The justification must include the business reasons that show a different option is in the

best interest of the agency and USDA for cyber security, technology development, and expense reduction. All requests, including appeals, must be signed by the Agency CIO.

The written exception is to be in the form of a decision memorandum and is to include:

i. Indication of Request for Exception
ii. Name of submitting agency
iii. Name and contact information of submitting person
iv. Information technology description (hardware/software exception)
v. Justification to show good cause for the exception. The request should document the justifications for the exception and the impact of granting versus not granting the request.
vi. Cyber security management plan
vii. Technology development summary
viii. Technology refresh plan
ix. Cost justification
x. Signature of Agency CIO.
xi. Date of the request.

End

Appendix O
Information Technology Network Security Standards

1.0 Information Technology Network Security Standards

The purpose of this appendix is to establish the requirements for implementing standards for the security of network infrastructure, communications, applications, interfaces, and data centers (hereafter referred to in this appendix as networks) used throughout the United States Department of Agriculture (USDA). This access control policy guidance is designed to protect information systems and data within the USDA.

2.0 User Account Management

Each agency, staff office, or shared service provider must establish and administer a user account management program for controlling access to USDA networks. This program must include procedures to establish, activate, modify, review, disable, and remove user accounts. All user account administration for agency networks will be performed by appropriately trained and authorized system security personnel in accordance with technical direction provided by the agency Information Systems Security Program Manager (ISSPM), Department policy, and Federal regulations. All user accounts are required to be documented and made available for audit by the USDA Office of the Chief Information Officer or other authorized parties.

3.0 Access Authorization

Authorizations to access and use USDA information technology (IT) resources will be granted by business owners responsible for those resources. Access will be based on official business "Need to Know" and limited to the "Least Privilege" access required to perform job functions. Because of the sensitivity and vulnerability of network assets, active accounts will be reviewed at least monthly for privileged users (i.e., network operators, engineers, administrators, security personnel), and at least quarterly for general users. Account permissions will be reviewed at least annually. Any discrepancies between network users and their access shall be reconciled by requesting and processing appropriate changes in user accounts and their associated access permissions.

4.0 Remote Access

All types of access to USDA networks that are allowed via external connections, such as Virtual Private Networks (VPN) or CITRIX, must be fully documented and authorized by the individual's manager.

All methods of remote access to USDA networks are subject to the following restrictions/controls:

- All remote accesses must be controlled and monitored through a limited number of managed access control points.
- Remote access must use a two-factor authentication mechanism where one of the factors is provided by a mechanism separate from the computer gaining access.
- All remote access sessions must be protected using Federal Information Processing Standards (FIPS) 140-2 compliant encryption.
- All remote access sessions must be protected by a "time-out" function requiring user re-authentication after 15 minutes or less of inactivity.
- Remote access activity must be recorded in logs and reviewed periodically.
- Remote access privileges must be authorized and restricted to users with an operational need for access.
- Remote access for privileged functions on an information system can be authorized only for compelling operational needs and the rationale for such access must be documented in the security plan for the information system.
- All methods of remote access must be fully documented in each agency's overall agency security plan.

5.0 User Background Checks

Individuals who are to be granted access to USDA networks must first undergo the Personal Identity Verification (PIV) process mandated by USDA policy and Homeland Security Presidential Directive 12 (HSPD-12). In addition, applications for appropriate background investigations for all individuals must be submitted and processed to a degree that meets the requirements for access.

6.0 Security Awareness

Individuals must complete the paper-based or CD based (on a stand-alone system) Computer Security Awareness and Privacy Basics training prior to being granted access to any USDA networks. All employees must meet the annual training requirements for computer security awareness and the protection of personally identifiable information (PII) to retain access.

7.0 User Access Requests

Before a user account can be created or access permissions modified, a hardcopy or electronic user access request form must be completed. A hardcopy or electronic copy of each completed and processed form must be retained by the authorizing agency representative for each active user account. Each form should include at least the following:

- User first, middle, and last name.
- User ID(s).
- Description of the action requested.

- Description of the access(es) requested.
- List of networks the individual is authorized to access and what role is authorized for each system.
- User's signature verifying that the user has read, and will abide by, the system's security rules and has completed all required security and privacy training.
- Verification of background investigation status (initiated, under adjudication, or completed).
- Authorizing manager's signature.
- Authorizing network security administrator's signature (if applicable).
- Processing agent's signature (e.g., ISSPM or Information System Security Officer).

8.0 Need-to-Know

USDA information systems shall be configured to ensure that users without specific authorization to data or resources are not allowed access to them.

9.0 Password Standards

Pending implementation of USDA's LincPass environment, all USDA networks must be configured to automatically ensure that all user accounts and their associated passwords adhere to the following USDA standards:

- Maximum lifetime for a password shall be 60 days for general users and privileged users (e.g., Security Administrators, programmers, auditors, engineers).
- Access by inactive users shall be suspended by the system within 30 days (15 days for privileged users).
- User accounts shall be automatically locked out by the system after five consecutive unsuccessful logon attempts.
- Passwords must have a minimum of 12 alphanumeric and special characters (with complexity turned on), including at least one of each of the following: a number, an uppercase letter, and a lowercase letter; except for agency-documented and ACIO-CS approved exceptions where systems do not allow for compliance.
- Dictionary words cannot be used for passwords.
- System security software must enforce a password history for each user, disallowing reuse of the same password for at least 24 iterations.
- A minimum password age of one day must be enforced.
- Systems must obscure feedback of authentication information (e.g., display asterisks when a user enters a password).
- Passwords in storage and in transmission must be protected using FIPS 140-2, Security Requirements for Cryptographic Modules validated encryption.

10.0 Duty Assignment/Employment Status

Upon a change in job responsibilities, title, or location, an employee's or contractor's network accesses must be reviewed and reconciled by immediately requesting and processing appropriate changes in their user accounts and their associated access permissions.

When an employee or contractor is terminated, the employee's manager must immediately notify the appropriate agency personnel of the user's departure. All IDs and passwords or other means of accessing files or using network resources by the individual must be disabled or removed within one working day of departure.

11.0 Access Logging

USDA networks must log access control related events. Reviews of these logs for identification of potentially suspicious activities should be conducted every 30 days or more frequently depending on the sensitivity of the system and its data. High impact systems should be configured to automatically notify responsible individuals when selected suspicious actions are logged.

12.0 Residual Data Removal

Each agency must establish and implement procedures to ensure that a user's sensitive residual data cannot be accessed by unauthorized users (see National Institute of Standards and Technology (NIST) Special Publication (SP) 800-88, Guide for Media Sanitization).

13.0 Access Warning Banner

All USDA information systems must display an approved, system use notification message before granting system access informing potential users of the following:

- The user is accessing a U.S. Government information system;
- The system usage may be monitored, recorded, and subject to audit;
- Unauthorized use of the system is prohibited and subject to criminal and civil penalties; and
- The use of the system indicates consent to monitoring and recording.

This notification must remain on the screen until the user takes explicit actions to log onto the information system.

14.0 Concurrent Sessions

High impact USDA networks must restrict the number of concurrent sessions for any user to three or a lower value as determined by the system owner and agency ISSPM.

15.0 Session Lock

All USDA networks must be configured to initiate a session lock after 15 minutes of inactivity. The session lock shall remain in effect until the user reestablishes access using appropriate identification and authentication procedures.

16.0 Portable and Mobile Devices

Portable and mobile devices used to access the USDA network must be authorized, documented, and monitored. All data on such devices must be encrypted using FIPS 140-2 validated encryption unless the data has been determined to be non-sensitive, in writing, by the system owner and validated by USDA's Office of the Chief Information Officer (OCIO).

17.0 Personally Owned Systems

The USDA prohibits the use of personally owned information systems to directly access government networks for official U.S. Government business involving the processing, storage, or transmission of federal information. Personally owned information systems can be used to interface with government web interfaces designed to accommodate communication of specific information (e.g., Employee Personal Page and Outlook Web Access).

18.0 Policy Exceptions

Exceptions to this policy will be considered only in terms of implementation time. Exceptions that are approved will be interim in nature and expire at the end of one year. Agencies shall submit all policy exception requests directly to the Office of the Chief Information Officer.

19.0 Responsibilities

19.1 The USDA CIO will:

- Publish and disseminate policy and procedures for Access Control for networks;
- Review all requests for exceptions to this policy appendix in a timely manner and coordinate the response to the agency; and
- Conduct periodic evaluations to ensure agency compliance with this policy.

19.2 The Agency Chief Information Officer (CIO) will:

- Oversee all aspects of access control within the agency;

- Ensure that separation of duties among IT staff is maintained to avoid conflicts of interest;
- Ensure that audit trails are appropriately configured and reviewed, and that irregularities are addressed; and
- Annually certify that access profiles for each employee have been reviewed and are appropriate.

19.3 The Agency ISSPM will:

- Administer all aspects of an effective access control system within the agency; and
- Verify access control is properly documented and followed within the agency.

19.4 Business and System Owners will:

- Ensure that authorizations to access the networks under their administration are based on 'Need-to-Know,' Least Privilege, and separation of duties; and
- Participate in periodic reviews of access authorizations and submit requests for changes in user accounts to reconcile any discrepancies noted.

19.5 Network Operators, Engineers, Technicians (et al) will:

- Access or attempt to access only networks and network resources to which they are specifically authorized;
- Protect passwords and all other system access methods against unauthorized disclosure; and
- Protect input/output data from casual inspection or unauthorized retrieval.

20.0 Network Security Configuration Settings

Current Security Configuration Guides for USDA network components can be found at http://www.ocionet.usda.gov/ocio/security/config_guides.html. Systems covered by these guides include:

- Microsoft Windows 2003 Member Server
- Cisco router/firewall
- Cisco Switch
- Linux Red Hat Enterprise 4
- Sun Solaris 10

21.0 Scanning and Patching

Agencies and staff offices must scan operating system software monthly, unless a waiver has been approved by the USDA CIO allowing quarterly scanning, to ensure that software updates and patches are current and that all network vulnerabilities are remediated. At a minimum, all patching must be performed on a monthly basis.

22.0 TWO-FACTOR AUTHENTICATION

USDA, along with the rest of the Federal government, is beginning to implement HSPD-12 to provide an interoperable identity card to employees and contractors who either access government computer systems or need to access government facilities that are protected with electronic access controls. USDA is going to leverage the HSPD-12 credential (also known as the USDA LincPass) to meet the two-factor authentication requirement.

The USDA LincPass environment will be implemented and deployed during FY 2008 and FY 2009. All employees and contractors who have been provisioned with a LincPass must use it to access USDA networks. The LincPass usage requirement will apply to laptop access by the end of FY 2008 and to workstation access by the end of FY 2009.