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

DEPARTMENTAL REGULATION

Number:
3180-001

SUBJECT:
Information Technology Network Standards

DATE:
January 31, 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This regulation will remain in effect until superseded.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

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