United States
Department of Agriculture

Office of the Chief Information Officer

DM 3300-005

POLICIES FOR PLANNING AND MANAGING WIRELESS TECHNOLOGIES IN USDA

POLICIES FOR PLANNING AND MANAGING WIRELESS TECHNOLOGIES IN USDA

TABLE OF CONTENTS

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

DEPARTMENTAL MANUAL	**Number:** 3300-005
SUBJECT: Policies for Planning and Managing Wireless Technologies in USDA	**DATE:** November 10, 2010
	OPI: Office of the Chief Information Officer

CHAPTER 1

GENERAL INFORMATION

1. PURPOSE

The widespread adoption of wireless technologies within USDA represents a paradigm shift from telecommunications landline technologies. This shift introduces management challenges due to the pervasive availability of wireless consumer products in the marketplace and the tendency for USDA to treat wireless acquisitions as commodity buys. The most significant business challenges associated with a commodity approach to buying wireless technologies occur when the lack of a central acquisition strategy results in fractionalized purchases of non-standard products and services. Each wireless hardware purchase such as a cellular telephone or Personal Digital Assistant (PDA) also requires a service plan. Once established, service plans automatically renew each year with little oversight. As this practice continues, the Department loses visibility and control of wireless assets. This Departmental Manual (DM) has been developed to promote policies that encourage a more strategic, centralized management of wireless assets enterprise-wide. It provides a series of chapters, which span a broad range of wireless telecommunications topics. The online version is available at:

http://www.ocionet.usda.gov/ocio/tso/tmd/telecom_policy.html.

2. SPECIAL INSTRUCTIONS

This DM replaces the following Departmental Notices (DNs) last re-issued by the USDA Office of the Chief Information Officer (OCIO) on May 19, 2008:

a. DN3300-010, *Commercial Wireless Technologies in USDA - The Assignment of Roles and Responsibilities for the Management of USDA Commercial Wireless Technologies*, April 20, 2006;

b. DN3300-011, *Commercial Wireless Technologies in USDA - Acceptable Use Policy*, April 20, 2006;

c. DN3300-012, *Commercial Wireless Technologies in USDA - Unclassified Security Requirements for Wireless Networks in Unlicensed Frequencies*, April 20, 2006;

d. DN3300-013, *Commercial Wireless Technologies in USDA - Unclassified Security Requirements for Wireless Devices*, April 20, 2006;

e. DN3300-014, *Commercial Wireless Technologies in USDA - Acquisition*, April 20, 2006;

f. DN3300-015, *Commercial Wireless Technologies in USDA - Asset Management*, April 20, 2006;

g. DN3300-016, *Commercial Wireless Technologies in USDA - Training and Development*, April 20, 2006; and

h. DN3300-017, *Commercial Wireless Technologies in USDA - Pilot Tests*, April 20, 2006.

Policies on management and technical controls to protect wireless technologies from security vulnerabilities are issued by OCIO, Cyber and Privacy Policy and Oversight (CPPO). CPPO policies can be found in the Series 3500 guidelines posted on the USDA Directives Web site.

3. POLICY

The USDA OCIO Managers responsible for telecommunications and CPPO oversight, agency Administrators, staff Directors, Chief Information Officers (CIOs), and Technology Officers shall work together to improve the management of USDA's wireless technologies and future wireless investments. In doing so, those USDA managers shall adhere to their respective Roles and Responsibilities according to the *Applicability and Scope* found in each chapter of this DM. Overall, managers responsible for wireless management shall review and realign functions and re-structure internal organizations as necessary to promote wireless implementation prioritization; secure communications; the adoption of USDA wireless standards; wireless network configuration management; wireless aggregated purchases; shared resources; streamlined processes; joint testing of emerging wireless technologies; sound financial management; ongoing asset tracking and inventory control; consistent recordkeeping; accurate reporting; workforce development; and training.

The following chapters of this DM provide detailed guidelines that constitute the minimum requirements for managing wireless technologies:

a. Chapter 2, *Roles and Responsibilities for the Management of Wireless Technologies in USDA*
b. Chapter 3, *Wireless Technologies: USDA Acceptable Use Policy*
c. Chapter 4, *Telecommunications Management of Wireless Networks in USDA*
d. Chapter 5, *USDA Guidance for the Management of Government-Issued Wireless Tools*
e. Chapter 6, *USDA Acquisition of Wireless Technologies*
f. Chapter 7, *Wireless Asset Management*
g. Chapter 8, *Wireless Training and Development in USDA*
h. Chapter 9, *Wireless Pilot Tests*

All policy regarding wireless security controls may be found in the USDA Series 3500 CPPO directives.

4. APPLICABILITY AND SCOPE

This chapter applies to all Government personnel. References to "Government personnel" throughout this policy shall be interpreted to include all USDA agency and staff office personnel, including non-Government personnel authorized to use USDA wireless networks. This directive has precedence over agency and staff office policies, procedures or other agency and staff office guidance.

It applies to all wireless tools and technologies used for Government business that transmit, receive, process or store voice and data including video. This includes but is not limited to Portable Electronic Devices (PEDs) such as laptop computers, tablets and Personal Digital Assistants (PDAs) with wireless capability; cellular/Personal Communications System (PCS) devices; paging devices; Global Positioning System (GPS) telemetry devices; receivers; Radio Frequency Identification (RFID) devices; Infrared (IR) devices; removable components such as Personal Computer Memory Card International Association (PCMCIA) cards; embedded chips; and any other wireless device capable of transmitting, receiving, processing, or storing information; as well as associated software and services. It also applies to infrastructure installed to support agency/staff office implementations of Wireless Wide Area Networks (WWANs); Wireless Metropolitan Area Networks (WMANs); Wireless Local Area Networks (WLANs); and equipment associated with Wireless Personal Area Networks (WPANs). Services include, but are not limited to, contract labor acquired to plan, design, install and manage wireless technologies; Government Full Time Equivalent (FTE) personnel dedicated to planning, designing installing and managing wireless technologies; and recurring wireless transmission rate plans sold through commercial providers, sometimes negotiated through Service Level Agreements (SLAs). Software includes utility software and protocols that support wireless voice and data transmissions.

This policy does not address classified communications.

5. DEFINITIONS

a. Asset Management. A process that promotes the long-term management of assets throughout their life cycle in a manner that enables the organization to: track them, determine their value and cost effectiveness; optimize their use, evaluate alternatives that may be more cost effective, and ensure delivery of benefits to stakeholders.

b. Collaborative Programs. Joint ventures between two or more organizations for sharing information, ideas, views, and costs to reduce technology risks and lower costs.

c. Designated Agency Representative (DAR). DARs are designated by the Chief Information Officer (CIO) or the lead Information Technology Officer within each agency or staff office in coordination with the agency/staff office Telecommunications Mission Area Control Officer (TMACO). DARs are delegated authority under USDA's Departmental Regulation DR3300-001 to place orders for telecommunications products and services on behalf of the agencies/staff or staff offices they represent. Telecommunications Services and Operations (TSO) within the Office of the Chief Information Officer (OCIO) establishes ordering limitations and guidance for USDA DARs within the context of authorized, pre-existing contracts that clearly state delegations of authority and terms. In order to be authorized to place orders, DARs must complete vendor training through the General Services Administration (GSA).

d. Emergencies. An emergency is any unplanned event that can cause death or significant injury to employees or the public; that can shut down or disrupt operations; or that can cause physical or environmental damage, such as National or Declared Emergencies, fires, hazardous materials incidents, storms, communications failure, disaster recovery, and similar situations. Note: Failure to engage in proper and timely planning for a requirement per USDA guidelines, does not constitute an emergency.

e. Federal Acquisition Regulation (FAR) System. The FAR system established for the codification and publication of uniform policies and procedures for acquisition by all executive agencies.

f. Media Access Control (MAC). The hardware address of a device connected to a network that uniquely identifies it.

g. Personal Use. An activity conducted for purposes other than accomplishing official or otherwise authorized activity. Executive Branch employees are specifically prohibited from using Government issued equipment to maintain or support a personal private business. The ban on using Government issued equipment to support a personal private business also includes employees using Government issued equipment to assist relatives, friends, or other persons in such activities. Employees may, however, make limited use under Chapter 3 of this policy of

Government office equipment to check their Thrift Savings Plan (TSP) or other personal investments, or communicate with a volunteer charity organization.

h. Pilot Test. A small-scale implementation of technology designed and implemented prior to full implementation. Pilot tests are a part of sound project management practice. A pilot test or a series of pilot tests can be used to collect useful data and to solve problems prior to full implementation. Well-planned pilots can substantially reduce project risks. As the term implies, pilots often steer or control the course of future experiments or development.

i. Subject Matter Expert (SME). The SME is an individual who exhibits the highest level of expertise in performing a specialized job, task, or skill within the organization. A SME might be a software engineer, a systems engineer, a helpdesk support operative, an accounts manager, a scientific researcher, or a Telecommunications Mission Area Control Officer (TMACO).

j. Wireless Assets. Hardware, software and services associated with the wireless transmission of voice and data. This includes but is not limited to Portable Electronic Devices (PEDs) such as laptop computers, tablets and Personal Digital Assistants (PDAs) with wireless capability; cellular/Personal Communications System (PCS) devices; paging devices; Global Positioning System (GPS) telemetry devices; receivers; Radio Frequency Identification (RFID) devices; Infrared (IR) devices; removable components such as Personal Computer Memory Card International Association (PCMCIA) cards; embedded chips; and any other wireless device capable of transmitting, receiving, processing, or storing information; as well as associated software and services. It also applies to infrastructure installed to support agency/staff office implementations of Wireless Wide Area Networks (WWANs); Wireless Metropolitan Area Networks (WMANs); Wireless Local Area Networks (WLANs); and equipment associated with Wireless Personal Area Networks (WPANs). Services include, but are not limited to, contract labor acquired to plan, design, install and manage wireless technologies; Government Full Time Equivalent (FTE) personnel dedicated to planning, designing installing and managing wireless technologies; and recurring wireless transmission rate plans sold through commercial providers, sometimes negotiated through Service Level Agreements (SLAs). Software includes utility software and protocols that support wireless voice and data transmissions.

k. Wireless Tools. Wireless hardware, and associated software and services capable of transmitting, receiving, processing or storing information across a wireless medium. Wireless tools may also process and/or store data transmitted across a wireless medium. Wireless tools are considered to be wireless technologies. Examples include, but are not limited to Portable Electronic Devices (PEDs) such as laptop computers, tablets and Personal Digital Assistants (PDAs) with wireless capability; cellular/Personal Communications System (PCS) devices; paging devices; Global Positioning System (GPS) telemetry devices; receivers; Radio Frequency Identification (RFID) devices; Infrared (IR) devices; removable components such as Personal Computer Memory Card International Association

(PCMCIA) cards; embedded chips; and any other wireless device capable of transmitting, receiving, processing, or storing information; as well as associated software and services.

l. Wireless Technologies. Wireless tools and methods that permit the active or passive transfer of information between separated points without physical connection. For example, audio or data can be transmitted using IR, acoustic, Radio Frequency (RF) and optical transmission mediums, however, as technology evolves wireless could use other transmission mediums as well.

m. Workforce Development. A focused effort to improve and standardize the knowledge, skills, and abilities of Federal employees.

n. Workforce Development Plans. A plan or plans that prescribe courses and related on-the-job units of instruction based on USDA's wireless requirements. Staff use the plan to annotate their training schedule and to document the completion of formal and on-the-job training.

6. ABBREVIATIONS

900 Call	Premium-rate telephone numbers for which extra charges are assessed
AAR	Acquisition Approval Request
AGAR	Agriculture Acquisition Regulation
AP	Access Point
AUPA	Acceptable Use Policy Agreement
BPA	Blanket Purchase Agreement
CFO	Chief Financial Officer
CFR	Code of Federal Regulations
CIO	Chief Information Officer
COOP	Continuity of Operations
CPIC	Capital Planning and Investment Control Process
CPPO	Cyber and Privacy Policy and Oversight
DAR	Designated Agency Representatives
DHS	Department of Homeland Security
DM	Departmental Manual
DN	Departmental Notice
DR	Departmental Regulation
EA	Enterprise Architecture
FAR	Federal Acquisition Regulation
FASA	Federal Acquisition Streamlining Act
FFMIA	Federal Financial Management Improvement Act
FMFIA	Federal Manager's Financial Integrity Act
FMR	Federal Management Regulation
FOIA	Freedom of Information Act
FTE	Full Time Equivalent

GAO	Government Accountability Office
GPS	Global Positioning System
GRS	General Records Schedule
GSA	General Services Administration
IR	Infrared
IT	Information Technology
ITMRA	Information Technology Management Reform Act
MAC	Media Access Control
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NTIA	National Telecommunications and Information Administration
OCFO	Office of the Chief Financial Officer
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
OPPM	Office of Procurement and Property Management
OSTP	Office of Science and Technology Policy
PAN	Personal Area Network
PCMCIA	Personal Computer Memory Card International Association
PCS	Personal Communications System
PDA	Personal Digital Assistant
PED	Portable Electronic Device
POC	Point of Contact
QoS	Quality of Service
RF	Radio Frequency
RFID	Radio Frequency Identification
ROI	Return on Investment
SLA	Service Level Agreement
SME	Subject Matter Expert
SOP	Standard Operating Procedure
TMACO	Telecommunications Mission Area Control Officer
TMD	Telecommunications Management Division
TSO	Telecommunications Services and Operations
TSP	Thrift Savings Plan
USC	United States Code
USDA	United States Department of Agriculture
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Network
WPAN	Wireless Personal Area Network
WWAN	Wireless Wide Area Network

7. INQUIRIES

Direct all questions concerning this notice to the Telecommunication Management Division (TMD), Telecommunications Services and Operations (TSO), Office of the Chief Information Officer (OCIO).

CHAPTER 2

ROLES AND RESPONSIBILITIES FOR THE MANAGEMENT OF WIRELESS TECHNOLOGIES IN USDA

1. PURPOSE

Chapter 2 of Departmental Manual (DM) 3300-005 was created to provide stakeholders with a broad overview of their respective roles and responsibilities for the effective management of wireless technologies in the United States Department of Agriculture (USDA). The additional roles and responsibilities that appear in subsequent chapters of this DM are not intended to duplicate or replace the roles and responsibilities that appear in Chapter 2, but rather, further delineate them by topic.

2. SPECIAL INSTRUCTIONS

Policies on management and technical controls to protect wireless technology from security vulnerabilities are issued by the Office of the Chief Information Officer (OCIO), Cyber and Privacy Policy and Oversight (CPPO). CPPO policies can be found in the Series 3500 guidelines posted on the USDA Directives Web site.

3. POLICY

The USDA OCIO Managers responsible for telecommunications and CPPO oversight, agency Administrators, staff Directors, Chief Information Officers (CIOs), and lead Technology Officers shall work together to improve the management of USDA's wireless technologies and future wireless investments. In doing so, those USDA managers shall adhere to the high level *Roles and Responsibilities* found in Section 5 of this chapter according to the *Applicability and Scope* as defined in Section 4. Overall, managers responsible for managing wireless technologies shall review and realign functions and re-structure internal organizations as necessary to promote wireless implementation prioritization; secure communications; the adoption of USDA wireless standards; wireless network configuration management; wireless aggregated purchases; shared resources; streamlined processes; joint testing of emerging wireless technologies; sound financial management; ongoing asset management that includes inventory control, consistent recordkeeping, and accurate reporting; workforce development; and training.

4. APPLICABILITY AND SCOPE

This chapter applies to all Government personnel. References to "Government personnel" throughout this policy shall be interpreted to include all USDA agency/staff office personnel, including non-Government personnel authorized to use USDA wireless networks. This directive has precedence over agency/staff office policies, procedures or other agency/staff office guidance

It applies to all wireless tools and technologies used for Government business that transmit, receive, process or store voice and data including video. This includes but is not limited to Portable Electronic Devices (PEDs) such as laptop computers, tablets and Personal Digital Assistants (PDAs) with wireless capability; cellular/Personal Communications System (PCS) devices; paging devices; Global Positioning System (GPS) telemetry devices; receivers; Radio Frequency Identification (RFID) devices; Infrared (IR) devices; removable components such as Personal Computer Memory Card International Association (PCMCIA) cards; embedded chips; and any other wireless device capable of transmitting, receiving, processing, or storing information; as well as associated software and services. It also applies to infrastructure installed to support agency/staff office implementations of Wireless Wide Area Networks (WWANs); Wireless Metropolitan Area Networks (WMANs); Wireless Local Area Networks (WLANs); and equipment associated with Wireless Personal Area Networks (WPANs). Services include, but are not limited to, contract labor acquired to plan, design, install and manage wireless technologies; Government Full Time Equivalent (FTE) personnel dedicated to planning, designing installing and managing wireless technologies; and recurring wireless transmission rate plans sold through commercial providers, sometimes negotiated through Service Level Agreements (SLAs). Software includes utility software and protocols that support wireless voice and data transmissions.

This policy does not address classified communications.

5. ROLES AND RESPONSIBILITITES

This section establishes high level policy and assigns high level roles and responsibilities that pertain across a broad range of topics for the management of wireless technologies in USDA. Cross-references are provided for the key detailed topic-specific roles and responsibilities as further delineated in subsequent chapters of this DM.

a. <u>USDA CIO shall</u>:

(1) Advise the Secretary and/or Secretariat staff of significant wireless issues that could interfere with the delivery of mission critical information throughout USDA;

(2) Align wireless enterprise strategies and plans with the OCIO and USDA strategic plans, the Federal and USDA Enterprise Architectures (EAs), and, Federal guidelines promulgated by the Office of Science and Technology

Policy (OSTP), the Office of Management and Budget (OMB), the National Telecommunications and Information Administration (NTIA), the Federal CIO Council, the Department of Homeland Security (DHS), the National Institute of Standards and Technology (NIST) and other Federal organizations responsible for managing wireless technologies. Further delineation may be found in Chapter 6, *Acquisition of Wireless Technologies*, §5.a.5, and Chapter 8, *Wireless Training and Development*, §5.a.1.;

(3) Provide leadership to agency programs for the integration of wireless technologies into the existing USDA infrastructure. Further delineation may be found in Chapter 6, *Acquisition of Wireless Technologies*, §5.a.1.a-c, and Chapter 9, *Wireless Pilot Tests*, §5.a.2.d.;

(4) Set the priorities for USDA wireless programs, projects, and activities based on Department-wide business requirements and available resources. Further delineation may be found in Chapter 6, *Acquisition of Wireless Technologies*, §5.a.7-8, and Chapter 8, *Wireless Training and Development*, §5.a.3.;

(5) Obtain the financial and human resources to implement USDA wireless programs, projects and activities. Further delineation may be found in Chapter 8, *Wireless Training and Development*, §5.a.2. and §5.a.4.; and

(6) Per the Clinger Cohen Act of 1996, ensure that agencies/staff offices comply with the provisions of this directive. Further delineation may be found in Chapter 7, *Wireless Asset Management*, §5.a.2.

b. OCIO Managers responsible for Telecommunications oversight shall:

(1) Advise the CIO of wireless technology issues that could substantially affect USDA major programs and enterprise operations;

(2) Establish a formal collaboration process with USDA component agencies/staff offices to promote the cost effective sharing of wireless technology capabilities, the formulation of wireless plans and strategies, and the discussion of wireless issues. Further delineation may be found in Chapter 9, *Wireless Pilot Tests*, §5.a.2.a-d.;

(3) Develop enterprise-wide policies, processes and procedures for wireless technologies;

(4) Develop and support a life cycle approach for managing wireless technologies. Further delineation may be found in Chapter 7, *Wireless Asset Management*, §5.a.1.;

(5) Align agency/staff office wireless strategies and plans with the OCIO Strategic Plan goals, objectives and strategies for the implementation of wireless technologies, USDA EA, and, Federal guidelines promulgated by OSTP, OMB, NTIA, the Federal CIO Council, DHS, and NIST;

(6) Provide analytic support on the planning, acquisition, implementation and overall management of wireless technologies. Further delineation may be found in Chapter 6, *Acquisition of Wireless Technologies,* §5.a.2-4.;

(7) Design, develop, implement, manage and maintain the USDA wireless enterprise architecture;

(8) Develop tactical and operational plans for the implementation of wireless technologies and services for the USDA enterprise network, to include normal operations, and emergency response. Further delineation may be found in Chapter 5, *Wireless Networks*, §5.a.2.b.2-4.;

(9) Advise agencies on standards, processes, and procedures for the technical integration of wireless technologies into the USDA's telecommunications network infrastructure. Review agency/staff office wireless implementation plans for adherence to USDA standards and guidelines. Further delineation may be found in Chapter 7, *Wireless Asset Management*, §5.a.3., and Chapter 9, *Wireless Pilot Tests*, §5.a.2.d.;

(10) Centralize wireless technology acquisition, billing and inventory processes and systems in collaboration with OCIO to achieve economies of scale and promote standards for more effective management across the enterprise. Further delineation may be found in Chapter 7, *Wireless Asset Management*, §5.a.1-2.;

(11) Establish processes for agency sponsorship of centralized wireless research and development projects. Coordinate and monitor wireless technology tests, pilot programs and feasibility studies, and promote cross-organizational participation. Further delineation may be found in Chapter 9, *Wireless Pilot Tests*, §5.b.1-5.;

(12) Conduct annual training sessions for USDA staff who use or administer wireless technologies. Further delineation may be found in Chapter 8, *Wireless Training and Development*, §5.b.1-5.; and

(13) Establish processes to establish Departmental wireless standards and implement configuration management oversight throughout the department.

c. Agency Administrators or Staff Office Directors shall:

(1) Lead the cost-effective implementation of programmatic applications of wireless technologies. Further delineation may be found in Chapter 6, *Acquisition of Wireless Technologies,* §5.b.1-8., and Chapter 7, *Wireless Asset Management*, §5.b.1.;

(2) Establish cooperative or collaborative programs with other agencies to promote the cost-effective adoption of wireless technologies throughout USDA. Further delineation may be found in Chapter 9, *Wireless Pilot Tests,* §5.b.1.b-

c.;

(3) Set priority levels for internal programs, projects, and activities, that include wireless technologies; basing these priorities on business requirements and available resources;

(4) Adhere to Federal and USDA wireless strategies, policies, standards, and best practices. Further delineation may be found in Chapter 4, *Management of Wireless Networks*, §5.d-e., and Chapter 6, *Acquisition of Wireless Technologies*, §5.b.3.;

(5) Support OCIO programs to centralize wireless planning, acquisition, integration into the existing USDA enterprise network, and overall management of wireless technologies. Further delineation may be found in Chapter 5, *Management of Wireless Tools*, §5.a.1., and Chapter 6, *Acquisition of Wireless Technologies*, §5.b.2.;

(6) Comply with USDA EA and telecommunications EA standards. Further delineation may be found in Chapter 4, *Management of Wireless Networks*, §5.c.;

(7) Obtain the financial and human resources necessary to implement wireless programs, projects and activities; and

(8) Ensure that employees comply with the provisions of these directives. Further delineation may be found in Chapter 3, *Acceptable Use Policy*, §5.a-g., and Chapter 7, *Wireless Asset Management*, §5.b.3-4.

d. Agency/Staff Office CIOs or Technology Officials shall:

(1) Advise the agency Administrator or staff office Director and OCIO Telecommunications Managers of strategic plans, programs or projects that include wireless technologies and affect the management of information management and technology throughout their respective organizations;

(2) Align wireless technology planning, acquisition, design, integration and management plans with the OCIO Strategic Plan; USDA EA; USDA standards; Departmental regulations; and, Federal guidelines promulgated by OSTP, OMB, NTIA, the Federal CIO Council, DHS, NIST, and other Federal organizations that manage wireless technologies. Further delineation may be found in Chapter 4, *Management of Wireless Networks*, §5.c. and §5.e.;

(3) Assess, design, implement, manage and maintain a wireless network architecture that is compatible and fully integrated with the USDA enterprise network backbone. Further delineation may be found in Chapter 4, *Management of Wireless Networks*, §5.c.;

(4) Follow established Departmental policies and guidelines for the planning and

acquisition of all dedicated wireless telecommunications equipment and services including Capital Planning and Investment Control Processes (CPIC) established by OCIO. Further delineation may be found in Chapter 4, *Management of Wireless Networks*, §5.a.1-2., and Chapter 7, *Wireless Asset Management*, §5.b.9.;

(5) Centrally manage, plan, and acquire wireless equipment components and services in alignment with USDA standards and Departmental guidance. Further delineation may be found in Chapter 4, *Management of Wireless Networks*, §5.a.1-2.;

(6) Maintain a current, centralized inventory of wireless assets, including wireless components, equipment, and services. Further delineation may be found in Chapter 4, *Management of Wireless Networks*, §5.b., and in Chapter 7, *Wireless Asset Management*, §5.b.2.;

(7) Develop and implement internal procedures aligned with USDA policy for the following:

(a) Moves, adds, and changes to the agency's wireless network architecture. Further delineation may be found in Chapter 7, *Wireless Asset Management*, §5.b.7-8.;

(b) Electronic records management and Freedom of Information Act (FOIA) procedures for wireless;

(c) Research and development, pilot tests and feasibility studies of wireless technologies. Further delineation may be found in Chapter 9, *Wireless Pilot Tests*, §5.b.1-5.;

(d) Wireless billing validation and payment. Further delineation may be found in Chapter 5, *Management of Wireless Tools*, §5.a.2.a.1-3., and Chapter 7, *Wireless Asset Management*, §5.b.4.;

(e) Wireless inventory/asset tracking. Further delineation may be found in Chapter 5, *Management of Wireless Tools*, §5.a.2.a.1-3.;

(f) Annual assessment and report to the designated Telecommunications Manager on wireless expenditures. Further delineation may be found in Chapter 4, *Management of Wireless Networks*, §5.b, Chapter 5, *Management of Wireless Tools*, §5.a.2.a.1-3, and Chapter 7, *Wireless Asset Management*, §5.b.5.;

(g) The assignment, development and training of wireless workforce personnel. Further delineation may be found in Chapter 4, *Management of Wireless Networks*, §5.f.; and

(h) Personal use of wireless assets. Further delineation may be found in

Chapter 3, *Acceptable Use Policy*, §5.a-g., and Chapter 7, *Wireless Asset Management*, §5.b.3-4., and §5.b.6.

e. Employees shall:

Comply with the policies outlined in DM 3300-005.

CHAPTER 3

WIRELESS TECHNOLOGIES: USDA ACCEPTABLE USE POLICY

1. PURPOSE

This chapter of Departmental Manual (DM) 3300-005 establishes enterprise-wide policy and assigns responsibilities for the acceptable personal use of wireless technologies in the United States Department of Agriculture (USDA).

2. SPECIAL INSTRUCTIONS

Policies on management and technical controls to protect wireless technologies from security vulnerabilities are issued by the Office of the Chief Information Officer (OCIO), Cyber and Privacy Policy and Oversight (CPPO). CPPO policies can be found in the Series 3500 guidelines posted on the USDA Directives Web site.

3. POLICY

USDA employees are authorized limited personal use of wireless tools issued by the Department for the conduct of business. Personal use is permitted on an occasional basis provided that the use involves minimal expense to the Government and does not interfere with official business. Occasional personal use of wireless tools shall normally take place during the employees' personal or off-duty time; however, official Government business always takes precedence. Agencies and staff offices shall adopt the enterprise-wide *Procedures* that appear in Section 5 of Chapter 3, and promulgate examples of acceptable and unacceptable personal use within their respective organizations.

USDA agencies and staff offices shall issue Standard Operating Procedures (SOPs) for the acceptable use of wireless tools. SOPs shall require that an Acceptable Use Policy Agreement (AUPA) be executed with the recipient of each wireless tool issued. Agencies and staff offices are encouraged to manage the AUPA process electronically whenever possible. In those instances where tools are shared, the agency/staff office shall execute an individual AUPA with each Government personnel representative authorized to use the shared tools. SOPs shall address whether Government personnel may use wireless tools that they purchased with their own funds in the conduct of Government business. SOPs shall specify how related charges for personally-owned tools shall be reimbursed; how Government personnel shall disconnect and dispose of Government-issued wireless tools; and what steps to follow when Government-issued wireless hardware is lost or stolen.

Recommended Executive Branch Model Policy/Guidance on "Limited Personal Use" of Government Office Equipment Including Information Technology, which appears in Appendix B of this DM, provides guidance from the Federal Chief Information Officer (CIO) Council and serves as a basis for this policy.

4. APPLICABILITY AND SCOPE

This chapter applies to all Government personnel. References to "Government personnel" throughout this policy shall be interpreted to include all USDA agency/staff office personnel, including non-Government personnel authorized to use USDA wireless networks. This directive has precedence over agency/staff office policies, procedures or other agency/staff office guidance

It applies to all wireless tools used for Government business that transmit, receive, process or store voice and data including video. This includes but is not limited to Portable Electronic Devices (PEDs) such as laptop computers, tablets and Personal Digital Assistants (PDAs) with wireless capability; cellular/Personal Communications System (PCS) devices; paging devices; Global Positioning System (GPS) telemetry devices; receivers; Radio Frequency Identification (RFID) devices; Infrared (IR) devices; removable components such as Personal Computer Memory Card International Association (PCMCIA) cards; embedded chips; and any other wireless device capable of transmitting, receiving, processing, or storing information; as well as associated software and services.

This policy does not address classified communications.

Agencies may further supplement this policy with more restrictive guidelines as suitable for their operational environments. Employees should review their internal agency or staff office SOPs for additional guidelines on the acceptable use of wireless tools prior to use.

5. PROCEDURES

a. Establish SOPs to further delineate the guidelines that appear in this policy. At a minimum, SOPs shall describe the agency/staff office process for administering AUPAs to Government personnel issued wireless tools. Agencies shall execute a separate AUPA for every wireless tool assigned to Government personnel. AUPAs shall further delineate acceptable/unacceptable use of wireless tools commensurate with the operational environments they support. AUPA's shall include each of the following provisions and subparts that appear in Sections 5. (b) - (g). Agency/Staff Office SOPs and AUPAs may include more stringent guidelines. Exceptions to the minimum requirements that appear in this policy shall be submitted by the

agency/staff office CIO and approved by the USDA CIO. Exception requests shall be approved prior to issuing tools and include the following information:

(1) The specific provision(s) to be addressed;

(2) The type of wireless tools (e.g. hardware, software and/or service) to be provided;

(3) A description of the business requirements for the wireless tool(s) in question;

(4) The reason for requesting an exception;

(5) Consequences if the request is not approved; and

(6) Contact information [phone number(s) and email address] of the requestor and Agency/Staff Office Telecommunications Area Mission Control Officer (TMACO).

b. Permit the use of wireless tools for limited personal use if practices satisfy the following criteria:

(1) It does not adversely affect the performance of official Government duties;

(2) It is of reasonable duration and frequency;

(3) Authorization was granted to use wireless tools for official Government business before they were made available for personal use. Note that the USDA is not required to supply wireless tools if they are not necessary in the conduct of official Government business;

(4) It could not have been reasonably accomplished at another time; or

(5) It is provided for in a collective bargaining agreement.

c. Annually publish and distribute to all agency or staff office Government personnel, a list of acceptable personal uses of Government issued wireless tools. At a minimum the list shall include the following personal uses permitted by the Department:

(1) Notification to family, doctor, etc., when an employee is injured on the job;

(2) Notification to family members of a schedule change while traveling on Government business and delays which occur due to official business or transportation;

(3) While traveling on Government business, a brief call to the employee's residence (but not more than an average of one call per day);

(4) Calls to advise family members of a change in schedule, or to make alternate transportation or child care arrangements;

(5) Brief daily calls to speak to spouse, minor children, or other family members whose "close association" constitutes a "family relationship" (or those responsible for them, e.g., school or day care center);

(6) Brief calls to service providers that can be reached only during working hours, such as local Government agencies or physicians, or to arrange for emergency repairs to his or her residence or automobile assuming calls require local, as opposed to long distance telecommunications transmission; and

(7) Access to the Internet or brief calls made during business hours while on business travel to obtain local visitor information such as driving directions, transportation options, restaurant listings or locations, gymnasiums, and libraries.

d. Annually publish and distribute to all agency or staff office Government personnel, a list of prohibited personal uses of Government-issued wireless tools. At a minimum, the list of prohibited personal uses shall include the following Departmental controls:

(1) "900" calls are prohibited. This includes dialing a toll free number which will switch to a “900" call, either on or off a Federal Government network;

(2) Use of Government provided wireless tools for other than official business, with the exception of those acceptable uses described in this policy;

(3) Use of camera cellular phones to illegally convey photographic images;

(4) Personal use of expensive satellite tools without the written permission of a permanent (non-acting) Senior Executive. This does not include GPS services;

(5) Making unauthorized calls or using unauthorized data services with the intent to later reimburse the Government;

(6) Frequent or lengthy personal phone calls or personal texting;

(7) Initiating transmissions that result in continuous electronic data streams that degrade the network;

(8) The creation, transmission, or retransmission of unauthorized mass mailings (i.e., to lists of multiple unknown recipients where no official business relationship exists) regardless of the subject matter using Government-issued equipment;

(9) The unauthorized downloading, acquisition, use, reproduction, transmission, and distribution of wireless software or other material protected by national

and international copyright laws, trade marks or other intellectual property rights;

(10) Use of Government telecommunications or services for the creation, downloading, viewing, storage, copying or transmission of material pertaining to:

(a) Sexually explicit or sexually oriented content;

(b) Illegal gambling;

(c) Illegal weapons;

(d) Workplace violence; and

(e) Other activities prohibited by law or regulation.

(11) Using Government-issued wireless tools for activities that are inappropriate or offensive that if done absent use of such equipment would be deemed misconduct (e.g., hate speech, offensive jokes, stories, and language);

(12) Use of Government-issued wireless tools for commercial purposes or in support of "for profit" personal activities or in support of other outside employment or business activity (e.g., consulting for pay, sales or administration of personal business/financial transactions, or sales of goods or services);

(13) Use of Government-issued wireless tools to engage in:

(a) Any outside fundraising activity;

(b) Endorsing any product or service; or

(c) Participating in any lobbying activity or partisan political activity unless authorized by law or labor contract.

(14) Use of Government-issued wireless tools to send or post agency information to external newsgroups, bulletin boards or other forums without authorization;

(15) Any use of Government-issued wireless tools in a manner that generates more than minimal additional expense, as determined by USDA agencies and staff offices, to the Government; and

(16) Personal use of Government-issued wireless tools in a manner that gives the appearance of acting in an official capacity or that the USDA endorses or sanctions those activities if unauthorized. For example, employees may not post USDA information to external news groups, bulletin boards or other public forums without USDA authorization.

e. Incorporate use of personal wireless tools for Government business guidelines in agency/staff office SOPs. At a minimum include management controls consistent with the following Departmental guidelines:

(1) Infrequent reimbursements for charges associated with the Government business use of wireless services acquired by Government personnel for personal use is permitted on an exception basis at the discretion of the agency or staff office, or in the absence of agency or staff office guidance, at the discretion of the employee's supervisor;

(2) Infrequent reimbursements for charges associated with the Government business use of wireless services acquired by Government personnel for personal use are permitted on an exception basis, and only for the transactions or minutes, and for related and apportioned usage-sensitive taxes and fees for Government related calls as substantiated by an itemized call detail list and copy of the invoice;

(3) Reimbursements for charges associated with the Government business use of wireless services acquired by Government personnel for personal use may not exceed 20% of the normal total monthly invoice amount. Reimbursement requests for Government use which are consistently at or near the 20% limit month-to-month may justify the assignment of a Government-issued wireless tool to the employee for Government business;

(4) Reimbursement of charges for any Government prohibited use as documented in this policy or agency/staff office SOPs is not permitted; and

(5) Reimbursement of charges for any Government business use of wireless services that does not satisfy the preservation requirements of records subject to legal discovery documented in this policy or agency/staff SOPs is not permitted.

f. Incorporate procedures in agency/staff office SOPs for the acceptable use of Government-issued wireless tools that instruct Government personnel how to report lost or stolen hardware to their supervisors.

g. Incorporate procedures in agency/staff office SOPs for the acceptable use of Government-issued wireless technologies for the disposition of Government-issued wireless technologies.

CHAPTER 4

TELECOMMUNICATIONS MANAGEMENT OF WIRELESS NETWORKS IN USDA

1. PURPOSE

This chapter of the Departmental Manual (DM) 3300-005 establishes policy for the effective business management of wireless network technologies in the United States Department of Agriculture (USDA).

2. SPECIAL INSTRUCTIONS

Policies on management and technical controls to protect wireless technologies from security vulnerabilities are issued by the Office of the Chief Information Officer (OCIO), Cyber and Privacy Policy and Oversight (CPPO). CPPO policies can be found in the Series 3500 guidelines posted on the USDA Directives Web site.

3. POLICY

Agencies are required to receive approval from USDA OCIO Telecommunications Managers prior to the purchase of any wireless network technologies regardless of the dollar amount. This includes the purchase of all software and equipment for the implementation of new wireless networks as well as upgrades or changes to existing wireless networks. This does not include Wireless Personal Area Networks (WPANs) or the purchase of external wireless devices that access wireless networks. Agency approval requests for wireless networks shall describe business and security requirements, include a cost trade off analysis between the proposed wireless network verses a hardwired network with equivalent capabilities, and provide total anticipated costs for each. OCIO shall review all wireless network approval requests for cost effectiveness. In addition, agencies are required to submit an annual report to the USDA OCIO Telecommunications Management Staff that accounts for all wireless networks and associated infrastructure and ensure that the information provided is mapped into the agency Enterprise Architecture (EA). Agencies shall ensure that technical personnel are adequately trained to oversee the planning, development, implementation and management of wireless networks in order to maintain an acceptable USDA Quality of Service (QoS) consensus standards.

4. APPLICABILITY AND SCOPE

This DM applies to all Government personnel. References to "Government personnel" throughout this policy shall be interpreted to include all USDA agency/staff office personnel, including non-Government personnel authorized to use USDA wireless networks.

It applies to all wireless technologies associated with the implementation of Wireless Wide Area Networks (WWANs); Wireless Metropolitan Area Networks (WMANs); and Wireless Local Area Networks (WLANs); and associated software and services. Services include, but are not limited to, contract labor acquired to plan, design, install and manage wireless technologies; Government Full Time Equivalent (FTE) personnel dedicated to planning, designing installing and managing wireless technologies; and recurring wireless transmission rate plans sold through commercial providers, sometimes negotiated through Service Level Agreements (SLAs). Software includes utility software and protocols that support wireless voice and data transmissions.

This policy does not address classified communications.

5. PROCEDURES

a. Acquisition Approval Request (AAR). Agencies shall submit AARs prior to the purchase of hardware or software for the implementation or reconfiguration of any WWAN, WMAN or WLAN regardless of the purchase amount. Requests shall be submitted to the Office of the Chief Information Officer Telecommunications Manager designated on the OCIO Wireless Web site, and must include the following information:

(1) A description of the business requirements to be supported by a wireless network.

(2) An alternatives analysis consistent with USDA OCIO Capital Planning and Investment Control (CPIC) guidance[1] that demonstrates the Return(s)-On-Investment (ROI) associated with one or more proposed wireless network alternatives verses a hardwired network with equivalent capabilities. The total estimated costs for the proposed wireless network(s) and hardwired equivalent shall be summarized clearly and distinctly in an executive summary. The analysis shall also document delineated costs and the assumptions upon which the costs are based.

[1] USDA, *Information Technology Capital Planning and Investment Control Guide for the Fiscal Year 2011 Budget*; at 3, Executive Summary; at 14, §2.3, Process; at 16-17, §2.3.3, Develop Concept; at 17, §2.3.4, Develop Preliminary Business Case; at 18, §2.3.8, Make Final Investment Decisions; and at 21, §3.3.4, Develop Major Investment Supporting Materials; Retrieved from: http://www.ocio.usda.gov/cpic/doc/CPIC_Guide_for_FY2011_Budget_Year_Main.pdf on 04-06-10.

b. Reporting Requirements. Network managers are required to establish and maintain configuration management of all WWAN/WMAN/WLAN architectures and components, and maintain configuration records. Based on those records, network managers shall submit an annual report to a designated USDA OCIO Telecommunications Manager per instructions on the OCIO Wireless Web site that accounts for all wireless networks and associated infrastructure. At a minimum, annual reports shall include the Media Access Control (MAC) addresses for each node of every wireless network, the physical address where individual nodes are located, and the name of and contact information for the network manager/administrator responsible for operating and maintaining the network. Additionally, reports shall include the list of client devices and associated user profile data for anyone authorized to access the wireless network.

c. Enterprise Architecture (EA). Agencies shall ensure that wireless infrastructure documentation is mapped into their respective EAs.

d. Quality of Service (QoS). In order to ensure an acceptable QoS:

(1) Channel Separation. Network managers are required to maintain a separation of five channels from nearby wireless networks where feasible to prevent interference, consistent with National Institute of Standards and Technology (NIST) recommendations.

(2) Radio Frequency Interference. Radio frequency interference detection and handling of the interference shall be an inherent part of the wireless network.

(3) Access Point (AP). APs shall be configured to uniformly comply with enterprise-wide QoS standards established through a consensus process.

e. Standards. Interface standards shall be established that address all layers of a wireless network. Additionally network administrators must validate that client software tools interoperate effectively with existing WWAN/WMAN/WLAN network software prior to purchase.

f. Training. Agencies/staff offices are required to provide annual training on configuration management and current standards requirements for Technical Specialists and Managers overseeing the technical planning, design, implementation, operations or maintenance of WWAN/WMAN/WLAN technologies. Training shall address advances in wireless protocols, standards, hardware and software including components, configurations, and overall architectures.

CHAPTER 5

USDA GUIDANCE FOR THE MANAGEMENT OF GOVERNMENT-ISSUED WIRELESS TOOLS

1. PURPOSE

This chapter of Departmental Manual (DM) 3300-005 instructs United States Department of Agriculture (USDA) agencies/staff offices to establish Standard Operating Procedures (SOPs) for the management of Government-issued wireless tools.

2. SPECIAL INSTRUCTIONS

Policies on management and technical controls to protect wireless technologies from security vulnerabilities are issued by the Office of the Chief Information Officer (OCIO), Cyber and Privacy Policy and Oversight (CPPO). CPPO policies can be found in the Series 3500 guidelines posted on the USDA Directives Web site.

3. POLICY

USDA agencies/staff offices shall establish SOPs and associated processes for the management of wireless tools. Agency/staff office SOPs must conform to Federal and USDA regulations, guidelines and policies for information technology and telecommunications standards, acquisitions, asset management, and training.

All non-voice data transmissions (e.g., emails) to/from Government-issued wireless tools shall be registered with and routed through the USDA network. Agencies/staff offices shall establish continuous access monitoring and reporting capabilities that identify the Media Access Control (MAC) address for authorized users; and can be referenced to the specific wireless device, and to the user's profile. Wireless usage reports shall be analyzed by agency/staff office telecommunications subject matter experts in order to: ensure that networks are secure and engineered in a manner that maintains high Quality of Service (QoS) to USDA customers; identify usage trends to improve future acquisition decisions; and, take corrective action to address excessive, infrequent, or non-usage of Government-issued tools.

4. APPLICABILITY AND SCOPE

This chapter applies to all Government personnel. References to "Government

personnel" throughout this policy shall be interpreted to include all USDA agency/staff office personnel, including non-Government personnel authorized to use USDA wireless networks. This directive has precedence over agency/staff office policies, procedures or other agency/staff office guidance

It applies to all wireless tools and technologies used for Government business that transmit, receive, process or store voice and data including video. This includes but is not limited to Portable Electronic Devices (PEDs) such as laptop computers, tablets and Personal Digital Assistants (PDAs) with wireless capability; cellular/Personal Communications System (PCS) devices; paging devices; Global Positioning System (GPS) telemetry devices; receivers; Radio Frequency Identification (RFID) devices; Infrared (IR) devices; removable components such as Personal Computer Memory Card International Association (PCMCIA) cards; embedded chips; and any other wireless device capable of transmitting, receiving, processing, or storing information; as well as associated software and services. Services include, but are not limited to, contract labor acquired to plan, design, install and manage wireless technologies; Government Full Time Equivalent (FTE) personnel dedicated to planning, designing installing and managing wireless technologies; and recurring wireless transmission rate plans sold through commercial providers, sometimes negotiated through Service Level Agreements (SLAs). Software includes utility software and protocols that support wireless voice and data transmissions.

This policy does not address classified communications.

5. ROLES AND RESPONSIBILITIES

a. Agencies/Staff Offices shall:

(1) Establish SOPs and associated processes for the management of wireless technologies. SOPs shall further delineate the guidelines found in DM 3300–005 to address specific agency/staff office requirements.

(2) All non-voice data transmitted (e.g., emails) for Government business via Government-owned or leased wireless technologies shall be registered with and routed through the USDA network. Peer-to-peer transmissions are prohibited. Agencies/staff offices shall establish continuous access monitoring and reporting capabilities that identify the MAC address for authorized users; and can be referenced to the specific wireless hardware, and to the user's profile.

(a) Wireless usage reports shall be analyzed quarterly by agency/staff office telecommunications subject matter experts in order to:

1 Ensure that networks are engineered in a manner that maintains high QoS to USDA customers. If traffic patterns indicate a significant

increase in usage, or traffic patterns shift significantly from one location to another, contact the USDA network enterprise engineering team to determine whether a network impact assessment may be needed.

2 Identify usage trends to improve future acquisition decisions; and,

3 Take corrective action to address continuous excessive, infrequent, or non-usage of Government-issued tools, for example:

a Determine whether patterns are commensurate with the functions assigned to user(s);

b Discontinue services no longer needed; and,

c Move users to a shared plan if appropriate.

(b) Exceptions to the policy may be approved as follows:

1 *Bluetooth® transmissions on Personal Area Networks (PANs)*. Bluetooth® transmissions on PANs are permitted, subject to CPPO guidelines found in the Series 3500 policies.

2 *Use in Continuity of Operations (COOP) or emergency response operations*. USDA personnel responsible for COOP or emergency response operations must submit an annual approval request to the designated USDA OCIO Telecommunications Manager for an exception to the peer-to-peer restriction. The request must contain:

a Point Of Contact (POC). Requesting agency, office, division, business unit, or branch name and point of contact; and

b Description. Number of anticipated users; their titles and organizations; and, a description of the operational need.

3 *Emergencies*. If an emergency occurs and an alternative transmission path is necessitated by the emergency, agencies/staff offices shall notify the designated USDA OCIO Telecommunications Manager within 15 days of the initial activation using the selected alternative. Agencies/staff offices should describe the nature of the incident and the alternative transmission approach. The USDA OCIO Telecommunications Manager shall determine whether it is necessary to submit a waiver for continuing operations.

4 *Continuing and Compelling Business Use*. Agencies/staff offices with a continuing and compelling business reason for using alterative transmission paths that are non-compliant with these guidelines should submit a written request to the designated OCIO

Telecommunications Manager for a waiver. Once submitted, the Telecommunications Manager shall have 15 days to respond to approve/deny the request.

CHAPTER 6

USDA ACQUISITION OF WIRELESS TECHNOLOGIES

1. PURPOSE

This chapter of the Departmental Manual (DM) 3300-005 establishes Departmental policy for the acquisition of wireless technologies in the United States Department of Agriculture (USDA).

2. SPECIAL INSTRUCTIONS

Policies on management and technical controls to protect wireless technologies from security vulnerabilities are issued by the Office of the Chief Information Officer (OCIO), Cyber and Privacy Policy and Oversight (CPPO). CPPO policies can be found in the Series 3500 guidelines posted on the USDA Directives Web site.

3. POLICY

The USDA OCIO shall establish Blanket Purchase Agreements (BPAs) or place task orders through General Services Administration (GSA) contracts for wireless technologies and services. USDA agencies/staff offices shall limit wireless purchases to those technologies or services that are available through GSA contracts approved by the USDA Chief Information Officer (CIO). Requests for exceptions to this policy shall be submitted to a designated OCIO Telecommunications Manager according to guidelines found in Section 5.(b). of this chapter. USDA agencies/staff offices shall assign and train Designated Agency Representatives (DARs), or representatives designated by the agency/staff office Telecommunications Mission Area Control Officer (TMACO) to place orders for all wireless technologies. Agencies/staff offices shall comply with USDA and Federal acquisition policies, and establish internal Standard Operating Procedures (SOPs) that, at a minimum, incorporate the provisions found in Sections 3 and 5 of this policy.

4. APPLICABILITY AND SCOPE

This chapter applies to all Government personnel. References to "Government personnel" throughout this policy shall be interpreted to include all USDA agency/staff office personnel, including non-Government personnel authorized to use USDA wireless

networks. This directive has precedence over agency/staff office policies, procedures or other agency/staff office guidance.

It applies to all wireless tools and technologies used for Government business that transmit, receive, process or store voice and data including video. This includes but is not limited to Portable Electronic Devices (PEDs) such as laptop computers, tablets and Personal Digital Assistants (PDAs) with wireless capability; cellular/Personal Communications System (PCS) devices; paging devices; Global Positioning System (GPS) telemetry devices; receivers; Radio Frequency Identification (RFID) devices; Infrared (IR) devices; removable components such as Personal Computer Memory Card International Association (PCMCIA) cards; embedded chips; and any other wireless device capable of transmitting, receiving, processing, or storing information; as well as associated software and services. It also applies to infrastructure installed to support agency/staff office implementations of Wireless Wide Area Networks (WWANs); Wireless Metropolitan Area Networks (WMANs); Wireless Local Area Networks (WLANs); and equipment associated with Wireless Personal Area Networks (WPANs). Services include, but are not limited to, contract labor acquired to plan, design, install and manage wireless technologies; Government Full Time Equivalent (FTE) personnel dedicated to planning, designing installing and managing wireless technologies; and recurring wireless transmission rate plans sold through commercial providers, sometimes negotiated through Service Level Agreements (SLAs). Software includes utility software and protocols that support wireless voice and data transmissions.

This policy does not address classified communications.

5. ROLES AND RESPONSIBILITIES

a. OCIO shall:

(1) Establish BPAs or task orders through GSA contracts for wireless technologies that:

(a) Promote economy of scale savings;

(b) Promote the adoption of standard equipment and services to improve interoperability; and

(c) Promote the adoption of standardized billing processes and customer support by USDA vendors.

(2) Provide customer support to agencies/staff and staff offices regarding Department-level contracts for wireless technologies.

(3) Make information available regarding available wireless technologies, and the associated pricing.

(4) Serve as the Department's representative to service providers and equipment manufacturers regarding enterprise-wide wireless acquisitions.

(5) Represent the Department to oversight agencies/staff offices such as the Office of Management and Budget (OMB), Government Accountability Office (GAO), and Department of Commerce on wireless technologies.

(6) Coordinate with the GSA, service providers and equipment manufacturers to apply a standard naming convention to all USDA accounts and invoices associated with the purchase of wireless technologies in order to look up information and generate reports on all USDA wireless acquisitions.

(7) Establish Department-wide acquisition processes for wireless technologies.

(8) Provide guidance on the use of specific payment systems.

b. Agencies/staff offices shall:

(1) Follow Departmental guidelines for the acquisition of all wireless technologies.

(2) Purchase wireless technologies through GSA contracts approved by the USDA CIO. Requests for exceptions shall be sent to an OCIO designated Telecommunications Manager and shall include:

(a) Signature from the agency/staff office CIO.

(b) Description of technologies to be purchased including volume, anticipated costs including fixed and recurring service fees, funding source(s), and date(s) of purchase(s). Note that approvals will be limited to purchases made during a single fiscal year.

(c) Reason the purchase cannot be made through a GSA contract that is approved by the USDA CIO.

(d) Name of agency/staff office business unit making the request.

(e) Point of contact for the request including name, phone number(s), email address, and physical address.

(3) Purchase wireless technologies that conform to Departmental standards. Requests for exceptions shall be sent to an OCIO designated Telecommunications Manager and shall include:

(a) Signature from the agency/staff office CIO.

(b) Description of technologies to be purchased including volume, anticipated costs, funding source(s) and date(s) of purchase(s). Note that approvals will be limited to purchases made during a single fiscal year.

(c) Reason the purchase cannot conform to USDA standards.

(d) Name of agency/staff office business unit making the request.

(e) Point of contact for the request including name, phone number(s), email address, and physical address.

(4) Establish SOPs whereby wireless equipment and services are ordered only by agency/staff office DARs, or representatives designated by the agency/staff office TMACO.

NOTE: Purchases by individuals other than DARs or representatives designated by a TMACO are not permitted.

(5) Where economic benefits are realized and business requirements permit, encourage the purchase of shared usage plans as appropriate for supporting operational requirements.

(6) Comply with the provisions of USDA's *Agriculture Acquisition Regulation (AGAR) Advisory 58A* regarding the *Prohibition on Using Purchase Cards or Convenience Checks to Acquire Telecommunications*.

(7) To the maximum extent possible, purchase commercially available wireless equipment and services. Clearly indicate in each Acquisition Approval Request (AAR) submitted to OCIO whether the acquisition includes wireless technologies. If the project team plans to purchase any wireless technologies, regardless of cost, describe the wireless technologies to be purchased including: the volume, anticipated costs, funding source(s), and anticipated date(s) of purchase(s). Agencies shall submit AARs prior to the purchase of hardware or software for the implementation or reconfiguration of any WWAN, WMAN or WLAN, regardless of the purchase amount. If the acquisition includes costs for the implementation of a wireless network, requests shall be submitted to the Office of the Chief Information Officer Telecommunications Manager designated on the OCIO wireless Web site, and must include the following information:

(a) A description of the business requirements to be supported by a wireless network.

(b) An alternatives analysis consistent with USDA OCIO Capital Planning and Investment Control (CPIC) guidance[1] that demonstrates the Return(s)-On-Investment (ROI) associated with one or more proposed wireless network alternatives verses a hardwired network with equivalent capabilities. The total estimated costs for the proposed wireless network(s) and hardwired equivalent shall be summarized clearly and

[1] USDA, *Information Technology Capital Planning and Investment Control Guide for the Fiscal Year 2011 Budget*; at 3, Executive Summary; at 14, §2.3, Process; at 16-17, §2.3.3, Develop Concept; at 17, §2.3.4, Develop Preliminary Business Case; at 18, §2.3.8, Make Final Investment Decisions; and at 21, §3.3.4, Develop Major Investment Supporting Materials; Retrieved from: http://www.ocio.usda.gov/cpic/doc/CPIC_Guide_for_FY2011_Budget_Year_Main.pdf on 04-06-10.

distinctly in an executive summary. The analysis shall also document delineated costs and the assumptions upon which the costs are based.

(8) Ensure that service providers and equipment manufacturers apply a standard naming convention as defined by the USDA OCIO to accounts and invoices associated with the purchase of wireless technologies in order to look up information and generate reports on all agency/staff office wireless acquisitions.

CHAPTER 7

WIRELESS ASSET MANAGEMENT

1. PURPOSE

The Clinger-Cohen Act of 1996 (also known as the Information Technology Management Reform Act of 1996 (ITMRA)) and other Federal legislation require agencies to be accountable for information technology assets, including wireless hardware, software, and services. This chapter of the Departmental Manual (DM) 3300-005 establishes Departmental policy for wireless technology asset management in compliance with Federal regulations.

2. SPECIAL INSTRUCTIONS

Policies on management and technical controls to protect wireless technologies from security vulnerabilities are issued by the Office of the Chief Information Officer (OCIO), Cyber and Privacy Policy and Oversight (CPPO). CPPO policies can be found in the Series 3500 guidelines posted on the United States Department of Agriculture (USDA) Directives Web site.

3. POLICY

USDA agencies/staff offices shall utilize General Services Administration (GSA) service contracts approved by the USDA Chief Information Officer (CIO) to purchase services for the effective management of wireless assets.

4. SCOPE

This chapter applies to all Government personnel. References to "Government personnel" throughout this policy shall be interpreted to include all USDA agency/staff office personnel, including non-Government personnel authorized to use USDA wireless networks. This directive has precedence over agency/staff office policies, procedures or other agency/staff office guidance

It applies to all wireless tools and technologies used for Government business that transmit, receive, process or store voice and data including video. This includes but is not limited to Portable Electronic Devices (PEDs) such as laptop computers, tablets, and Personal Digital Assistants (PDAs) with wireless capability; cellular/personal

communications system (PCS) devices; paging devices; Global Positioning System (GPS) telemetry devices; receivers; Radio Frequency Identification (RFID) devices; Infrared (IR) devices; removable components such as Personal Computer Memory Card International Association (PCMCIA) cards; embedded chips; and any other wireless device capable of transmitting, receiving, processing, or storing information; as well as associated software and services. It also applies to infrastructure installed to support agency/staff office implementations of Wireless Wide Area Networks (WWANs); Wireless Metropolitan Area Networks (WMANs); Wireless Local Area Networks (WLANs); and equipment associated with Wireless Personal Area Networks (WPANs). Services include, but are not limited to, contract labor acquired to plan, design, install and manage wireless technologies; Government Full Time Equivalent (FTE) personnel dedicated to planning, designing, installing, and managing wireless technologies; and recurring wireless transmission rate plans sold through commercial providers, sometimes negotiated through Service Level Agreements (SLAs). Software includes utility software and protocols that support wireless voice and data transmissions.

This policy does not address classified communications.

5. ROLES AND RESPONSIBILITIES

a. OCIO shall:

Establish purchasing strategies and management controls that optimize the value of wireless assets throughout their total life cycle.

Generate annual analyses and reports on the status of wireless technology assets Department-wide that:

Quantify wireless expenditures to determine baseline spending;

Convey patterns and trends for validation and planning; and

Provide baseline inventory data and associated business requirements.

Establish a wireless technologies standards body that that leverages common technologies to the greatest extent possible while supporting diverse business requirements.

b. Agencies/Staff Offices shall:

(1) Implement the purchasing strategies and management controls established by the USDA OCIO.

(2) Maintain records that permit routine analyses and the generation of meaningful reports, specifically delineating overall inventory levels of wireless assets, quarterly expenditures on wireless technologies, and program business

requirements. It would be acceptable and encouraged for agencies/staff offices to process and maintain the associated records and reports electronically whenever possible. Best practices indicate that records should also include carrier or manufacturer, brand name, model name, model number, serial number, owner, location (i.e. physical address), initial cost, billing account number, type of recurring service plan, service contract type, service contract length, method of recurring payment, and documentation of quality of service problems.

(3) Maintain management controls over wireless assets to safeguard them against improper use, theft and undue deterioration.

(4) Establish and enforce procedures that require supervisors to request and review wireless bills monthly for each employee issued a wireless device, where the device is subject to recurring service fees. Supervisors should initial the monthly billing statements certifying that:

(a) The bills are accurate.

(b) Individual plans are effective.

1 Usage should not exceed the monthly plan allowance.

2 Monthly charges that routinely exceed the monthly plan allowance should be adjusted by the agency or staff office Designated Agency Representative (DAR) or Telecommunications Mission Area Control Officer (TMACO) with the approval of the employee's supervisor.

3 The monthly plan allowance should not routinely exceed the monthly charges by a significant amount.

4 Monthly plan allowances that routinely exceed the monthly charges by a significant amount should be adjusted by the agency or staff office DAR or TMACO at the request of the employee's supervisor.

(5) Establish procedures by which TMACOs and DARs annually review wireless usage throughout the agency(ies)/staff office(s) they support, and adjust usage plans to achieve the maximum benefit. For example, an agency or staff office may consider the creation of a loaner pool of wireless devices for distribution to employees on an as needed basis, as opposed to the permanent assignment of these devices to individual employees.

(6) Establish procedures to ensure that upon employee termination, Government-owned wireless assets are returned to the agency/staff office and that services are discontinued or reassigned to another employee or contractor. Procedures must require that the agency TMACO or DAR make the necessary changes or deletions to records in the appropriate billing system(s).

(7) Establish procedures to ensure that upon office closure or relocation, the agency TMACO or DAR enters the necessary modifications, changes, or deletions for wireless recurring service charges into the appropriate systems or submits them to the appropriate organizations.

(8) Establish procedures to ensure that upon office closure or relocation, Government-owned wireless assets are moved or properly discarded. Procedures for disposition of wireless assets are outlined in the Agricultural Property Management Regulations.

(9) Account for the acquisition, ongoing operations, maintenance, and refreshment of wireless technologies in Capital Planning and Investment Control (CPIC) business cases.

CHAPTER 8

WIRELESS TRAINING AND DEVELOPMENT IN USDA

1. PURPOSE

This chapter of the Departmental Manual (DM) 3300-005 establishes Departmental policy for workforce development and training to more effectively plan and manage wireless technologies.

2. SPECIAL INSTRUCTIONS

Policies on management and technical controls to protect wireless technologies from security vulnerabilities are issued by the Office of the Chief Information Officer (OCIO), Cyber and Privacy Policy and Oversight (CPPO). CPPO policies can be found in the Series 3500 guidelines posted on the United States Department of Agriculture (USDA) Directives Web site.

3. POLICY

USDA shall develop and provide ongoing training for a wireless workforce in order to promote consistency and improvement in the overall management of wireless technologies throughout the Department. OCIO shall lead the Department in identifying training requirements, setting wireless training priorities, and obtaining resources for workforce development across the broad range of existing and emerging wireless technologies.

4. APPLICABILITY AND SCOPE

This chapter applies to all Government personnel. References to "Government personnel" throughout this policy shall be interpreted to include all USDA agency/staff office personnel, including non-Government personnel authorized to use USDA wireless networks. This directive has precedence over agency/staff office policies, procedures or other agency/staff office guidance

It applies to all wireless tools and technologies used for Government business that transmit, receive, process, or store voice and data including video. This includes but is not limited to Portable Electronic Devices (PEDs) such as laptop computers, tablets, and Personal Digital Assistants (PDAs) with wireless capability; cellular/Personal

Communications System (PCS) devices; paging devices; Global Positioning System (GPS) telemetry devices; receivers; Radio Frequency Identification (RFID) devices; Infrared (IR) devices; removable components such as Personal Computer Memory Card International Association (PCMCIA) cards; embedded chips; and any other wireless device capable of transmitting, receiving, processing, or storing information; as well as associated software and services. It also applies to infrastructure installed to support agency/staff office implementations of Wireless Wide Area Networks (WWANs); Wireless Metropolitan Area Networks (WMANs); Wireless Local Area Networks (WLANs); and equipment associated with Wireless Personal Area Networks (WPANs). Services include, but are not limited to, contract labor acquired to plan, design, install, and manage wireless technologies; Government Full Time Equivalent (FTE) personnel dedicated to planning, designing, installing, and managing wireless technologies; and recurring wireless transmission rate plans sold through commercial providers, sometimes negotiated through Service Level Agreements (SLAs). Software includes utility software and protocols that support wireless voice and data transmissions.

This policy does not address classified communications.

5. ROLES AND RESPONSIBILITIES

a. The USDA Chief Information Officer (CIO) shall:

(1) Align information management and information technology workforce development plans with the USDA strategic plan; the USDA Enterprise Architecture (EA) standards; USDA telecommunications standards; Federal regulations and policy guidelines promulgated by the Office of Science and Technology Policy (OSTP), Office of Management and Budget (OMB), the National Telecommunications and Information Administration (NTIA), the Federal Chief Information Officer (CIO) Council, the Department of Homeland Security (DHS), the National Institute of Standards and Technology (NIST), the National Security Agency (NSA), and other Federal organizations responsible for wireless technologies;

(2) Integrate wireless workforce development into current training programs;

(3) Set priorities for USDA wireless workforce development based on business requirements; and

(4) Obtain the financial and human resources necessary to implement OCIO programs, projects, and activities for wireless workforce development.

b. OCIO Telecommunications Managers shall:

(1) Identify wireless training needs throughout the Department;

(2) Provide guidance to agency programs for the integration of wireless technologies into existing workforce development programs;

(3) Encourage the development of subject matter expertise to cover a broad range

of operational environments and issues including, but not limited to: normal operations, emergency response, disaster planning, and life cycle management;

(4) Develop strategies and programs for wireless workforce development; and

(5) Provide wireless training online, through USDA online learning programs whenever feasible.

CHAPTER 9

WIRELESS PILOT TESTS

1. PURPOSE

Wireless technology pilot tests are routinely conducted in United States Department of Agriculture (USDA) agencies/staff offices across the organization. However, outcomes and lessons learned are not documented and shared. As a result, the same basic tests are performed multiple times. Therefore, USDA has established a process to centrally coordinate reporting and sharing of information gathered on wireless technologies through various pilot tests. In doing so, it is USDA's goal to achieve improved collaboration and sharing among USDA agencies/staff offices about information gathered from pilot tests on commercial wireless technologies.

This chapter of the Departmental Manual (DM) 3300-005 establishes organizational policies for conducting pilot tests for wireless technologies.

2. SPECIAL INSTRUCTIONS

Policies on management and technical controls to protect USDA from security vulnerabilities associated with wireless technologies are issued by the Office of the Chief Information Officer (OCIO), Cyber and Privacy Policy and Oversight (CPPO). CPPO policies can be found in the Series 3500 guidelines posted on the USDA Directives Web site.

3. POLICY

USDA's OCIO shall facilitate the Departmental adoption of next generation wireless technologies and eliminate redundant agency/staff office pilot tests of wireless technologies. Agencies/staff offices shall follow OCIO procedures for conducting and coordinating pilot tests, and shall share test results with one another through the OCIO established processes.

4. SCOPE

This chapter applies to all Government personnel. References to "Government personnel" throughout this policy shall be interpreted to include all USDA agency/staff office personnel, including non-Government personnel authorized to use USDA wireless

networks. This directive has precedence over agency/staff office policies, procedures or other agency/staff office guidance

It applies to all wireless tools and technologies used for Government business that transmit, receive, process or store voice and data including video. This includes but is not limited to Portable Electronic Devices (PEDs) such as laptop computers, tablets, and Personal Digital Assistants (PDAs) with wireless capability; cellular/Personal Communications System (PCS) devices; paging devices; Global Positioning System (GPS) telemetry devices; receivers; Radio Frequency Identification (RFID) devices; Infrared (IR) devices; removable components such as Personal Computer Memory Card International Association (PCMCIA) cards; embedded chips; and any other wireless device capable of transmitting, receiving, processing, or storing information; as well as associated software and services. It also applies to infrastructure installed to support agency/staff office implementations of Wireless Wide Area Networks (WWANs); Wireless Metropolitan Area Networks (WMANs); Wireless Local Area Networks (WLANs); and equipment associated with Wireless Personal Area Networks (WPANs). Services include, but are not limited to, contract labor acquired to plan, design, install and manage wireless technologies; Government Full Time Equivalent (FTE) personnel dedicated to planning, designing, installing, and managing wireless technologies; and recurring wireless transmission rate plans sold through commercial providers, sometimes negotiated through Service Level Agreements (SLAs). Software includes utility software and protocols that support wireless voice and data transmissions.

5. ROLES AND RESPONSIBILITIES

a. OCIO Telecommunications Managers shall:

(1) Incorporate special provisions for wireless pilot programs in the acquisition approval process for telecommunications products and services.

(2) Develop a collaborative process to share information across the Department about pilot tests.

(a) Establish a protected Web site restricted to USDA personnel for posting information regarding wireless technology pilot tests that are planned, underway, or completed, that incorporates the inputs of all agencies/staff offices.

(b) Post summary information regarding pilot tests submitted by the Telecommunications Mission Area Control Officers (TMACOs).

(c) Distribute reports on wireless pilot test summaries submitted by the TMACOs to the Department Chief Information Officer (CIO) Council in order to use the information for planning and decision making.

(d) Establish an incentives program whereby elements of successful pilots

may be considered for adoption as USDA standards.

b. Agencies/Staff Offices shall:

(1) Follow USDA processes for initiating pilot projects including the following:

(a) The TMACOs shall prepare and submit requests for approval to deploy a pilot test for wireless technologies to the designated Telecommunications Manager.

(b) A description of the proposed pilot test should be sufficiently detailed to allow an individual to determine whether the pilot could apply to another organization. At a minimum information shall include:

1 Names, models, and versions of the wireless equipment, or a description of the commercial services proposed;

2 A description of the business requirement or the problem to be solved, and the security requirements;

3 The anticipated duration, scope, and staffing for the pilot;

4 The physical locations of the pilot;

5 The expected costs of the pilot and of the proposed final implementation;

6 The number of any corresponding Capital Planning and Investment Control (CPIC) submission or Acquisition Approval Request (AAR);

7 The names, telephone numbers, and e-mail addresses of the pilot test or project leader and of the program manager in the business area for which this work is being done; and

8 The expected start and end dates of the pilot and of the entire project.

(c) Check the OCIO-maintained Web site to determine if a similar pilot is underway or has been completed. Facilitate an internal review of prior pilot tests that may provide the information needed to:

1 Move forward without initiating a new pilot; or

2 Incorporate experiences and knowledge from previous or current pilot tests into the newly proposed test.

(2) Ensure that tests follow Federal, USDA, and OCIO guidelines including the loan of equipment and services obtained without charge from vendors.

(3) Conduct pilots under realistic conditions or using modeling and simulation

technologies. Details, outcomes, and lessons learned shall be documented.

(4) Ensure that subject matter experts conduct pilots in order to ensure that the technologies are tested appropriately.

(5) Ensure that the pilot team updates the information on the OCIO Web site to include the findings of the pilot to include decisions regarding the "go" or "no-go" status of the entire project.

END

APPENDIX A

REFERENCES

National Federal Oversight Guidelines

Code of Federal Regulations, *CFR Title 41 - Public Contracts and Property Management, Subtitle C - Federal Property Management Regulations System, Chapter 101 - Federal Property Management Regulations;* Retrieved from: http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?sid=999e1ed5010643c50eb4c97f0b2b82ea&c=ecfr&tpl=/ecfrbrowse/Title41/41cfrv2_02.tpl#10100 on 04-21-2010.

Code of Federal Regulations, *CFR Title 41 - Public Contracts and Property Management, Subtitle C - Federal Property Management Regulations System, Chapter 102 - Federal Management Regulation;* Retrieved from: http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?sid=999e1ed5010643c50eb4c97f0b2b82ea&c=ecfr&tpl=/ecfrbrowse/Title41/41cfrv3_02.tpl on 04-21-2010.

Federal Register, *Executive Order 13011: Federal Information Technology,* July 16, 1996; Retrieved from: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=1996_register&docid=fr19jy96-133.pdf on 04-20-2010.

National Archives and Records Administration (NARA), General Records Schedule 12, Transmittal No. 8, Communications Records, §4 Telephone Use (Call Detail) Records, December 1988; Retrieved from http://www.archives.gov/records-mgmt/ardor/grs12.html on 04-20-2010.

US Congress, *Chief Financial Officers Act of 1990 (CFO Act)*, Public Law 101-576, Retrieved from: http://www.whitehouse.gov/omb/financial_ffs_ffmia/ on 04-21-2010.

US Congress, *Defense Authorization Act: The Government Information Security Reform Act: Public Law 106-398,* October 30, 2000; Retrieved from: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_cong_public_laws&docid=f:publ398.106.pdf on 04-21-2010.

US Congress, *Federal Acquisition Streamlining Act of 1994 (FASA), Public Law 103-355, October 13, 1994; Codified in Title 41 for civilian agencies.*

US Congress, *Federal Financial Management Improvement Act of 1996 (FFMIA), Public Law 104-208; Retrieved from: http://www.whitehouse.gov/omb/financial_ffs_ffmia/ and from: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=104_cong_public_laws&docid=f:publ208.104.pdf on 04-21-2010.*

US Congress, *Federal Manager's Financial Integrity Act of 1982 (FMFIA), September 8, 1982, Public Law 97-255; Retrieved from: http://www.whitehouse.gov/omb/financial_ffs_ffmia/ and from: http://www.whitehouse.gov/omb/financial/fmfia1982.aspx on 04-21-2010.*

US Congress, *Freedom of Information Act (FOIA), 5 U.S.C. §552*, Fall 1996; Retrieved from: http://www.justice.gov/oip/foia_updates/Vol_XVII_4/page2.htm on 04-21.2010.

US Congress, *Government Paperwork Elimination Act, 44 U.S.C. §3504*, October 21, 2003; Retrieved from: http://www.cio.gov/documents/paperwork_elimination_act.html on 04-21-2010.

US Congress, *Government Performance and Results Act of 1993*, Public Law 103-62, 1993; Retrieved from: https://www.acquisition.gov/sevensteps/library/PUBLICLAW103-62.pdf on 04-21-2010.

US Congress, *Information Technology Management Reform Act (ITMRA or the Clinger-Cohen Act of 1996, Public Law 104-106 (40 U.S.C. 1401(3)), also known as: Division E: Information Technology Management Reform Act);* Retrieved from: http://www.whitehouse.gov/omb/financial_ffs_ffmia/ from http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=104_cong_public_laws&docid=f:publ106.104.pdf and from http://www.cio.gov/Documents/it_management_reform_act_Feb_1996.html on 04-21-10.

US Congress, *Paperwork Reduction Act of 1995, 44 U.S.C. §3501 et seq.*, Retrieved from: http://www.archives.gov/federal-register/laws/paperwork-reduction/ on 04-21-2010.

US Congress, *Use of Government Property*, Code of Federal Regulations, 5 CFR Ch. XVI (1-1-09 Edition); Section 2635.704; Retrieved from: http://law.justia.com/us/cfr/title05/5-3.0.10.10.9.7.50.4.html and from: http://www.gpoaccess.gov/cfr/retrieve.html (Title 5, CFR Part 2635, Section 704) on 04-21-2010.

Federal Agency Guidelines

General Services Administration, *Federal Acquisition Policy Division, Federal Acquisition Regulation (FAR), subpart 13.303, Blanket Purchase Agreement;*. July 19, 2004; Retrieved from: https://www.acquisition.gov/far/html/Subpart%2013_3.html on 04-20-2010.

General Services Administration, Federal CIO Council, *Recommended Executive Branch Model Policy/Guidance On "Limited Personal Use" Of Government Office Equipment Including Information Technology;* Approved May 19, 1999; Retrieved from: http://www.cio.gov/Documents/limited_personaluse_memo_policy.pdf on 04-21-2010.

Office of Management and Budget, *OMB, Circular No. A-11, Preparation, Submission and Execution of Budget*; Last Revised July 21, 2010; Retrieved from: http://www.whitehouse.gov/omb/Circulars_a11_current_year_a11_toc/ on 08-11-2010.

Office of Management and Budget, *OMB Circular A-130, Revised, Transmittal Memorandum #4Memorandum for Heads of Executive Departments and Agencies: Management of Federal Information Resources;* November 28, 2000; Retrieved from: http://www.whitehouse.gov/omb/Circulars_a130_a130trans4/ on 04-20-2010.

USDA Guidelines

USDA, DR3080-001 (previously DR3040-002), *Records Management*; April 11, 2007; Retrieved from: http://www.ocio.usda.gov/directives/doc/DR3080-001.pdf on 04-20-2010.

USDA, DR3090-001, *Litigation Retention Policy for Documentary Materials including Electronically Stored Information*; May 28, 2008; Retrieved from: http://www.ocio.usda.gov/directives/doc/DR3090-001.pdf on 07-12-2010.

USDA, DR3300-001, *Telecommunications & Internet Services and Use*; March 23, 1999; Retrieved from: http://www.ocio.usda.gov/directives/doc/DR3300-001.pdf on 04-20-2010.

USDA, DM3500-000, *Cyber Security Manual Series 3500 et seq.*, July 15, 2004; Retrieved from: http://www.ocio.usda.gov/directives/doc/DM3500-000.pdf on 04-20-2010.

USDA, DR5001-1, *Acquisition, Workforce Training, Delegation and Tracking System*, Office of Procurement and Property Management; September 30, 2003; Retrieved from: http://www.ocio.usda.gov/directives/doc/DR5001-1final.pdf on 04-20-2010.

USDA, *Office of Procurement and Property Management (OPPM), Agriculture Acquisition Regulation Advisory (AGAR 58A), Prohibition on Using Purchase Cards or Convenience Checks to Acquire Telecommunications;* December 10, 2003; Retrieved from: http://www.dm.usda.gov/procurement/policy/advisories_x/AGARAD58A.PDF on 04-20-2010.

USDA, Agricultural Property Management Regulation, Chapter 110-36, *Disposition of Excess Personal Property, Supplementing Chapter 102 - Federal Management Regulation (FMR) Subchapter B - Personal Property Part 102-36 - Disposition of Excess Personal Property*; Retrieved from: http://www.dm.usda.gov/property/part10236.pdf on 04-21-2010.

USDA, Agricultural Property Management Regulations, Chapter 110-37, *Donation of Surplus Personal Property, Supplementing Chapter 102 - Federal Management Regulation (FMR) Subchapter B - Personal Property Part 102-37 - Donation of Surplus Personal Property;* Retrieved from: http://www.dm.usda.gov/property/part10237.pdf on 04-21-2010.

USDA, *Information Technology Capital Planning and Investment Control Guide for the Fiscal Year 2011 Budget*; at 3, Executive Summary; at 14, §2.3, Process; at 16-17, §2.3.3, Develop Concept; at 17, §2.3.4, Develop Preliminary Business Case; at 18, §2.3.8, Make Final Investment Decisions; and at 21, §3.3.4, Develop Major Investment Supporting Materials; Retrieved from: http://www.ocio.usda.gov/cpic/doc/CPIC_Guide_for_FY2011_Budget_Year_Main.pdf on 04-20-2010.

US Department of Agriculture (USDA), Office of the Chief Financial Officer (OCFO), *Quick Guide: Proper Use of Budget Object Codes for Personal Property: Effective FY2006;* December 2005; Retrieved from: http://www.usda.gov/ocfo/acctpol/pdf/propbocg.pdf on 04-20-2010.

NOTE: The references in this Appendix reflect the current guidance as of the writing of this policy. Agencies must employ the most current guidance available.

APPENDIX B

LIMITED PERSONAL USE POLICY

General Services Administration Office of Governmentwide Policy

June 07, 1999

MEMORANDUM TO: Chief Information Officers All Agencies

FROM: G. Martin Wagner /s/ 06-07-1999 Associate Administrator

SUBJECT: Model "Limited Personal Use Policy" of Government Equipment

Attached is the "Recommended Executive Branch Model Policy/Guidance on "Limited Personal Use" of Government Office Equipment including Information Technology".

General Services Administration is distributing this model policy to Government agencies to ensure the issues raised in the policy are considered and addressed within Government organizations. This model policy has been developed by the Federal Chief Information Officers (CIO) Council, and was approved at their May 19, 1999, meeting after it was coordinated with the ethics, legal, procurement and human resources communities in Government as well as representatives from the Legislative Branch. The policy has been well reviewed and includes many components that may not be present in current agency policies.

While adopting the policy as written is not required, it provides a model for agencies to consider when addressing the issues contained in it.

If additional information is needed you may contact Keith Thurston at keith.thurston@gsa.gov.

RECOMMENDED EXECUTIVE BRANCH MODEL POLICY/GUIDANCE ON

"LIMITED PERSONAL USE" OF GOVERNMENT OFFICE EQUIPMENT

INCLUDING INFORMATION TECHNOLOGY

Federal CIO Council
General Services Administration
contact: keith.thurston@gsa.gov
Approved - May 19, 1999

RECOMMENDED EXECUTIVE BRANCH MODEL POLICY/GUIDANCE ON "LIMITED PERSONAL USE" OF GOVERNMENT OFFICE EQUIPMENT INCLUDING INFORMATION TECHNOLOGY

I. PURPOSE

This document provides general recommended policy, or a model, for assisting agencies or departments in defining acceptable use conditions for Executive Branch employee personal use of Government office equipment including information technology. This model provides a backdrop of conditions for an agency or department to consider when developing a personal use policy for Government office equipment. This model makes use of material already implemented in various agencies or departments personal use policies and can be implemented unless superseded by any other applicable law or regulation..

II. BACKGROUND

The Executive Branch of the Federal Government serves the American people through hundreds of thousands of employees located in offices across the nation. Increasingly, the Government is called upon to deliver more and better services to a growing population that continues to expect ever-increasing improvements in service delivery. Much of this productivity increase has come about through the use of modern information technology such as computers, facsimile machines, and the Internet. This technology has raised new opportunities for its use by employees to live their lives more efficiently in balance with the overriding imperative that American taxpayers receive the maximum benefit for their tax dollars.

This policy establishes new privileges and additional responsibilities for employees in the Executive Branch of the Federal Government. It recognizes these employees as responsible individuals who are the key to making government more responsive to its citizens. It allows employees to use government office equipment for non-government purposes when such use involves minimal additional expense to the government, is performed on the employee's non-work time, does not interfere with the mission or operations of a department or agency and does not violate the Standards of Ethical Conduct for Employees of the Executive Branch.

Taxpayers have the right to depend on their Government to manage their tax dollars wisely and effectively. Public confidence in the productiveness of government is increased when members of the public are confident that their

government is well managed and assets are used appropriately. The relationship between the Executive Branch and the employees who administer the functions of the Government is one based on trust. Consequently, employees are expected to follow rules and regulations and to be responsible for their own personal and professional conduct. The Standards of Conduct states "Employees shall put forth honest effort in the performance of their duties" (Section 2635.101 (b)(5)).

Executive Branch employees should be provided with a professional supportive work environment. They should be given the tools needed to effectively carry out their assigned responsibilities. Allowing limited personal use of these tools helps enhance the quality of the workplace and helps the Government to retain highly qualified and skilled workers.

This policy does not supersede any other applicable law or higher level agency directive or policy guidance.

III. AUTHORITY

Generally, Federal employees may use Government office equipment for authorized purposes only. As set forth below, limited personal use of the government office equipment by employees during non-work time is considered to be an "authorized use" of Government property. Authority for this policy is cited as 5 U.S.C. sec 301 which provides that the head of an executive department or military department may prescribe regulations for the use of its property; and Executive Order 13011, Federal Information Technology, section 3(a)(1), which delineates the responsibilities of the Chief Information Office (CIO) council in providing recommendations to agency heads relating to the management and use of information technology resources.

IV. GENERAL POLICY

Federal employees are permitted limited use of government office equipment for personal needs if the use does not interfere with official business and involves minimal additional expense to the Government. This limited personal use of government office equipment should take place during the employee's non-work time. This privilege to use Government office equipment for non-government purposes may be revoked or limited at any time by appropriate Federal agency or department officials.

Agency officials may apply this policy to contractor personnel, interns, and other non-government employees through incorporation by reference in contracts or memorandums of agreement as conditions for using Government office equipment and space.

This policy in no way limits agency personnel in the use of Government office equipment including information technology for official activities.

A. DEFINITIONS

1. **Privilege** means, in the context of this policy, that the Executive Branch of the Federal Government is extending the opportunity to its employees to use government property for personal use in an effort to create a more supportive work environment. However, this policy does not create right to use government office equipment for non-government purposes. Nor does the privilege extend to modifying such equipment, including loading personal software or making configuration changes.

2. **Government office equipment including information technology** includes but is not limited to: personal computers and related peripheral equipment and software, library resources, telephones, facsimile machines, photocopiers, office supplies, Internet connectivity and access to internet services, and E-mail. This list is provided to show examples of office equipment as envisioned by this policy. Executive Branch managers may include additional types of office equipment.

3. **Minimal additional expense** means that employee's personal use of government office equipment is limited to those situations where the government is already providing equipment or services and the employee's use of such equipment or services will not result in any additional expense to the government or the use will result in only normal wear and tear or the use of small amounts of electricity, ink, toner or paper. Examples of minimal additional expenses include, making a few photocopies, using a computer printer to printout a few pages of material, making occasional brief personal phone calls (within agency policy and 41 CFR 101-35.201), infrequently sending personal E-mail messages, or limited use of the Internet for personal reasons.

4. **Employee non-work time** means times when the employee is not otherwise expected to be addressing official business. Employees may for example - use government office equipment during their own off-duty hours such as before or after a workday (subject to local office hours), lunch periods, authorized breaks, or weekends or holidays (if their duty station is normally available at such times).

5. **Personal use** means activity that is conducted for purposes other than accomplishing official or otherwise authorized activity. Executive Branch employees are specifically prohibited from using government office equipment to maintain or support a personal private business. Examples of this prohibition include employees using a government computer and Internet connection to run a travel business or investment service. The ban on using government office equipment to support a personal private business also includes employees using government office equipment to assist relatives, friends, or other persons in such activities. Employees may, however, make limited use under this policy of government office equipment to check their Thrift Savings Plan or other personal investments, or to seek employment, or communicate with a volunteer charity organization (examples).

6. **Information technology** means 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.

B. Specific Provisions on Use of Equipment and Services

Employees are authorized limited personal use of Government office equipment. This personal use must not result in loss of employee productivity or interference with official duties. Moreover, such use should incur only minimal *(1) additional expense to the Government in areas such as:

* Communications infrastructure costs; e.g., telephone charges, telecommunications traffic, etc.;
* Use of consumables in limited amounts ; e.g., paper, ink, toner, etc.;
* General wear and tear on equipment;
* Data storage on storage devices;
* Transmission impacts with moderate E-mail message sizes such as emails with small attachments.

(*(1)Minimal additional expense may be defined further in any specific agency directive that implements this policy.)

C. Inappropriate Personal Uses

Employees are expected to conduct themselves professionally in the workplace and to refrain from using government office equipment for activities that are inappropriate. Misuse or inappropriate personal use of government office equipment includes:

*Any personal use that could cause congestion, delay, or disruption of service to any government system or equipment. For example, greeting cards, video, sound or other large file attachments can degrade the performance of the entire network.

"Push" technology on the Internet and other continuous data streams would also degrade the performance of the entire network and be an inappropriate use.

* Using the Government systems as a staging ground or platform to gain unauthorized access to other systems.

* The creation, copying, transmission, or retransmission of chain letters or other unauthorized mass mailings regardless of the subject matter.

* Using government office equipment for activities that are illegal, inappropriate, or offensive to fellow employees or the public. Such activities include, but is not limited to: hate

speech, or material that ridicules others on the basis of race, creed, religion, color, sex, disability, national origin, or sexual orientation.

* The creation, download, viewing, storage, copying, or transmission of sexually explicit or sexually oriented materials;

* The creation, download, viewing, storage, copying, or transmission of materials related to illegal gambling, illegal weapons, terrorist activities, and any other illegal activities or activities otherwise prohibited, etc.

* Use for commercial purposes or in support of "for-profit" activities or in support of other outside employment or business activity (e.g. consulting for pay, sales or administration of business transactions, sale of goods or services).

* Engaging in any outside fund-raising activity, endorsing any product or service, participating in any lobbying activity, or engaging in any prohibited partisan political activity.

* Use for posting agency information to external newsgroups, bulletin boards or other public forums without authority. This includes any use that could create the perception that the communication was made in one's official capacity as a Federal Government employee, unless appropriate Agency approval has been obtained or uses at odds with the agencies mission or positions.

* Any use that could generate more than minimal additional expense to the government.

* The unauthorized acquisition, use, reproduction, transmission, or distribution of any controlled information including computer software and data, that includes privacy information, copyrighted, trade marked or material with other intellectual property rights (beyond fair use), proprietary data, or export controlled software or data.

D. Proper Representation

It is the responsibility of employees to ensure that they are not giving the false impression that they are acting in an official capacity when they are using government office equipment for non-government purposes. If there is expectation that such a personal use could be interpreted to represent an agency, then an adequate disclaimer must be used. One acceptable disclaimer is –"*The contents of this message are mine personally and do not reflect any position of the Government or my agency."*

The Standards of Conduct states - "…an employee shall not use or permit the use of his Government position or title or any authority associated with his public office in a manner that could reasonably be construed to imply that his agency or the Government sanctions or endorses his personal activities…" (Section 2635.702(a)).

E. Access Management

Employees have no inherent right to use government office equipment. Therefore, all Agencies will establish appropriate controls to ensure that the equipment is used appropriately.

F. Privacy Expectations

Executive Branch employees do not have a right, nor should they have an expectation, of privacy while using any Government office equipment at anytime, including accessing the Internet, using E-mail. To the extent that employees wish that their private activities remain private, they should avoid using an Agency or department's office equipment such as their computer, the Internet, or E-mail. By using Government office equipment, executive branch employee simply their consent to disclosing the contents of any files or information maintained or pass-through Government office equipment.

By using this office equipment, consent to monitoring and recording is implied with or without cause, including (but not limited to) accessing the Internet, using E-mail. Any use of government communications resources is made with the understanding that such use is generally not secure, is not private, and is not anonymous.

System managers do employ monitoring tools to detect improper use. Electronic communications may be disclosed within an agency or department to employees who have a need to know in the performance of their duties. Agency officials, such as system managers and supervisors, may access any electronic communications.

G. Sanctions for Misuse

Unauthorized or improper use of Government office equipment could result in loss of use or limitations on use of equipment, disciplinary or adverse actions criminal penalties and/or employees being held financially liable for the cost of improper use.

H. Agency Implementation and Use

This policy is intended to be a model policy/guidance for the Executive Branch. Therefore, each Agency must assess its individual needs and responsibilities as they relate to mission, security, budget, workload, public contact, etc. in determining the extent to which this policy is established and implemented.

I. Agency Labor Relations Responsibilities

Agencies should involved their unions early – before adopting and complete any labor relations obligations for bargaining, where appropriate. The labor-management relations

partnerships should be consulted during the agency consideration of adopting this policy. It should be indicated, if appropriate, that the policy does not apply to union representatives when fulfilling their official capacity for the union. Agencies should consult their collective bargaining agreements for the procedures and rules that apply to the union's use of equipment and technology under those conditions. However, when union representatives are not engaged in their union representation responsibilities, this policy does apply.

- - - - - - - -

Related Authorities

5 CFR 2635 – Standards of Ethical Conduct for Employees of the Executive Branch

Part 1 of Executive Order 12674 – Implementing Standards of Ethical Conduct for Employees of the Executive Branch -

5 CFR 301 – Departmental Regulations

41 CFR 101-35. 201 -TELECOMMUNICATIONS MANAGEMENT POLICY

Retrieved from: http://www.cio.gov/Documents/limited_personaluse_memo_policy.pdf on 04-21-2010.