1. PURPOSE

This Departmental Regulation (DR) establishes the United States Department of Agriculture (USDA) policy for planning and managing USDA’s wireless networks and devices that use USDA wireless networks.

2. SPECIAL INSTRUCTIONS/CANCELLATIONS

a. This DR replaces Departmental Manual (DM) 3300-005, Policies for Planning and Managing Wireless Technologies in USDA, dated November 10, 2010.

b. This DR will be in effect until it is superseded or expires.

c. The term “wireless network” encompasses any network that uses the Institute of Electrical and Electronics Engineers Standards Association (IEEE-SA) 802.11.
Standards, such as Wireless Local Area Networks (WLAN) or Wireless Fidelity (Wi-Fi).

d. All Mission Areas, agencies, and staff offices will align their policies and procedures with this DR within 6 months of the publication date.

e. All Mission Areas, agencies, and staff offices may supplement this DR when developing their internal guidance. Modifications to the intent or purpose of this DR are not allowed. If Mission Areas, agencies, and staff offices publish internal guidance that supplements this DR, one copy of each supplement will be forwarded to the Office of the Chief Information Officer (OCIO), Digital Infrastructure Services Center (DISC), Enterprise Network Services (ENS), Telecommunications Infrastructure Management and Governance (TIMG) at ens.policy@usda.gov.

3. SCOPE

a. This DR applies to USDA wireless networks and devices (e.g., laptops) that use USDA wireless networks.

b. This DR excludes wireless devices (e.g., cellular phones) that are provisioned for use on a third-party cellular network.

c. This DR applies to all USDA Mission Areas, agencies, staff offices, employees, contractors, data centers, cooperative partners, and others working for, or on behalf of, the USDA.

4. BACKGROUND

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. As this practice continues, the Department loses visibility and control of wireless technologies. Thus, a policy is needed to ensure that there is a more strategic, centralized management of wireless technologies.

5. POLICY

a. Mission Areas, agencies, and staff offices are required to receive approval from the USDA Chief Information Officer (CIO) prior to the purchase of any wireless networking technologies regardless of the dollar amount. These purchases include
all software and equipment for the implementation of new wireless networks as well as upgrades or changes to existing wireless networks. Mission Area, agency, and staff office approval requests for wireless networks will describe business and security requirements, include a cost trade-off analysis between the proposed wireless network and a hardwired network with equivalent capabilities, and provide total anticipated costs for each.

b. Mission Areas, agencies, and staff offices 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 or staff office enterprise architecture (EA). Mission Area, agencies, and staff offices will ensure technical personnel are adequately trained to oversee the planning, development, implementation, and management of wireless networks in order to be compliant with the **USDA Quality of Service (QoS)/Class of Service (CoS) Standard** (eAuthentication access required).

c. All Internet Protocol (IP) based data transmission (e.g., email) to and from Government networks will be registered with USDA Domain Name System (DNS) servers and routed through the USDA secure internet gateways. Agencies and staff offices will 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 will be analyzed by Mission Area, agency, or staff office telecommunications subject matter experts (SME) to:

1. Ensure that networks are secure and engineered in a manner that maintains high QoS to USDA customers;

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

3. Determine corrective actions that address excessive, infrequent, or non-usage of Government-issued devices.

d. USDA OCIO will establish enterprise contracts or place task orders through General Services Administration (GSA) contracts for wireless technologies. Mission Areas, agencies, and staff offices will limit wireless device purchases to those technologies that are available through GSA contracts approved by the USDA CIO. Mission Areas, agencies, and staff offices will appoint Telecommunications Mission Area Control Officers (TMACO) to place orders for all wireless technologies.

e. USDA OCIO will facilitate the Departmental adoption of next generation wireless technologies and eliminate redundant Mission Area, agency, or staff office pilot tests of wireless networks. Mission Areas, agencies, and staff offices will follow OCIO procedures for conducting and coordinating pilot tests and share test results with each other through the OCIO established processes.
f. Appropriate Uses of USDA Wireless Technologies

(1) USDA wireless networks and devices may be used for, but are not limited to, the following purposes:

(a) The communication and exchange of data between State and local governments, private sector organizations, and educational and research institutions, both in the United States and abroad;

(b) The development of internet-based projects;

(c) Interactive sharing of information without compromising USDA secured data;

(d) The exchange of any non-sensitive data between USDA entities in support of Mission Area, agency, and staff office missions, or other official purposes; and

(e) The distribution and collection of information related to official program delivery that is in compliance with Federal and Departmental guidelines.

(2) In accordance with the Federal CIO Council’s Recommended Executive Branch Model Policy/Guidance on "Limited Personal Use" of Government Office Equipment Including Information Technology (Limited Personal Use), May 19, 1999, employees may use Government wireless devices for personal matters on an occasional basis provided that there is no loss of employee productivity or interference with official employee duties.

g. Inappropriate Uses of USDA Wireless Technologies

In accordance with the Limited Personal Use guidance, employees will not use USDA wireless networks and devices:

(1) To conduct illegal, inappropriate, or offensive activities to fellow employees or the public. Such activities include, but are 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;

(2) To create, download, view, store, copy, or transmit sexually explicit or sexually oriented materials;

(3) To create, download, view, store, copy, or transmit materials related to illegal gambling, illegal weapons, terrorist activities, and any other illegal activities or activities otherwise prohibited;
(4) To conduct activities that could cause congestion, delay, or disruption of service to any Government system or equipment. For example, greeting cards, video, or other large file attachments can degrade the performance of the entire network;

(5) For commercial purposes or in support of “for-profit” activities or other outside employment or business activity (e.g., consulting for pay or sales of goods and services);

(6) To engage in any outside fundraising activity, endorse any product or service, participate in any lobbying activity, or engage in any prohibited partisan political activity;

(7) To post Departmental information to external newsgroups, bulletin boards, or other public forums without authority; and

(8) To conduct activities that could generate more than a minimal expense to the Government.

h. Proper Representation

(1) In accordance with the Limited Personal Use, it is the responsibility of employees to ensure 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 an expectation that such a personal use could be interpreted to represent a Mission Area, agency, or staff office, 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.”

(2) It is the responsibility of employees not to use or wear any official Government logos, trademarks, seals, or insignias while displaying, portraying, or posting any acts that would be detrimental to the Government, including any State, local, or federally illegal activities, or any of the previously mentioned prohibited activities.

i. Privacy

USDA employees will use Government wireless networks and devices with the understanding that such use serves as consent to monitoring of any type of use, including incidental and personal uses, whether authorized or unauthorized. In addition, access of such systems is not anonymous. For example, for each use of the internet over Government systems, these systems may capture information transmitted, received, or stored on the system.

6. ROLES AND RESPONSIBILITIES

a. The USDA CIO will:
(1) Provide leadership to Mission Area, agency, and staff office programs for the integration of wireless technologies into the existing USDA infrastructure;

(2) Set the priorities for USDA wireless programs, projects, and activities based on Departmentwide business requirements and available resources;

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

(4) Represent the USDA to oversight agencies on wireless technologies-related issues;

(5) Serve as the USDA representative to the Diplomatic Telecommunications Service Program Office (DTSPO);

(6) Respond to oversight agencies, such as Office of Management and Budget (OMB), Government Accountability Office (GAO), Department of Homeland Security (DHS), Department of Commerce (DOC), and Federal Communications Commission (FCC), with timely and accurate USDA telecommunications program and cost information; and

(7) Perform management and oversight responsibilities in accordance with the Federal Information Technology Acquisition Reform Act (FITARA), Public Law (P.L.) 113-291, as applicable to this directive.

b. The ENS Director will:

(1) Establish policies and procedures for the management of wireless technologies throughout USDA;

(2) Oversee Mission Area, agency, and staff office compliance with USDA wireless technologies policies and procedures;

(3) Manage USDA wireless technologies in accordance with prescribed laws, regulations, standards, and related USDA 3300 Series telecommunications directives;

(4) Grant technical approval for acquisition of new wireless technologies when the analysis of the request indicates that this is the best approach for USDA;

(5) Review and render a decision for Mission Area, agency, and staff office policy waiver requests;

(6) Maintain an electronic file of approved waivers;

(7) Work with Mission Areas, agencies, and staff offices to eliminate redundant
or unused wireless technologies;

(8) Include wireless technology requirements and initiatives as part of the telecommunications planning process;

(9) Use GSA and USDA mandated programs when Mission Area, agency, and staff office requirements can be met cost effectively; and

(10) Maintain inventories of USDA wireless networks and devices to the extent necessary to:

   (a) Ensure that there are adequate and appropriate wireless networks and devices to support the Mission Area, agency, and staff office mission;

   (b) Ensure accountability for USDA wireless networks and devices; and

   (c) Meet Departmental and Federal requests for periodic or special inventory reports.

c. Mission Area Assistant CIOs and Agency and Staff Office Information Technology (IT) Directors will:

   (1) Ensure Mission Area, agency, and staff office personnel comply with this directive;

   (2) Ensure Mission Area, agency, and staff office internal directives conform to this DR’s stated requirements;

   (3) Lead the cost-effective implementation of programmatic applications of wireless technologies;

   (4) Establish cooperative or collaborative programs with other Mission Areas, agencies, and staff offices to promote the cost-effective adoption of wireless technologies throughout USDA;

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

   (6) Adhere to Federal and USDA wireless strategies, policies, standards, and best practices;

   (7) Align wireless technology planning, acquisition, design, integration, and management plans with the current USDA Information Technology Strategic Plan, USDA EA, USDA standards and Departmental directives, and Federal guidelines promulgated by Office of Science and Technology Policy (OSTP), OMB, National Telecommunications and Information Administration (NTIA), Federal CIO
Council, DHS, National Institute of Standards and Technology (NIST), FCC, and other Federal organizations that manage wireless technologies;

(8) Assess, design, implement, manage, and maintain a wireless network architecture that is compatible and fully integrated with the Universal Telecommunications Network (UTN);

(9) Provide guidance to end users on the appropriate and secure use of Government wireless technologies;

(10) Obtain waivers and approvals from the ENS Director when agency and staff office requirements cannot be met through mandated programs;

(11) Assign TMACOs to select required wireless technology from GSA Program follow-on contracts for the Mission Areas, agencies, and staff offices. More information on this topic can be found in DR 3300-020, *Telecommunications Mission Area Control Officer Roles and Responsibilities*;

(12) Include wireless technology requirements and initiatives as part of the telecommunications planning process;

(13) Provide the TMACO’s name and contact information to the USDA CIO; and

(14) Maintain Mission Area, agency, and staff office inventories of USDA wireless networks and devices to the extent necessary to:

   a. Ensure that adequate and appropriate wireless networks and devices support the Mission Area, agency, or staff office mission;

   b. Ensure accountability for USDA wireless networks and devices; and

   c. Meet Departmental and Federal requests for periodic or quarterly inventory reports.

d. TMACOs will perform their roles and responsibilities as provided in DR 3300-020.

7. COMPLIANCE

a. **DR 4070-735-001**, *Employee Responsibilities and Conduct*, Section 16 sets forth USDA’s policies, procedures, and standards on employee responsibilities and conduct relative to the use of computers and telecommunications equipment. DR 4070-735-001, Section 21, states that a violation of any of the responsibilities and conduct standards contained in this directive may be cause for disciplinary or adverse action; and

b. Such disciplinary or adverse action will be effected in accordance with applicable law and regulations such as Office of Personnel Management (OPM) regulations, OMB
regulations, and the *Standards of Ethical Conduct for Employees of the Executive Branch*.

8. POLICY EXCEPTIONS

a. All USDA Mission Areas, agencies, and staff offices are required to conform to this policy. If a specific policy requirement cannot be met as explicitly stated, Mission Areas, agencies, and staff offices may submit a waiver request to the ENS Director for review and determination. Submit the waiver request to ens.policy@usda.gov. The waiver request will explain the reason for the request, identify compensating controls and actions that meet the intent of the policy, and identify how the compensating controls and actions provide a similar or greater level of defense or compliance than the policy requirement.

b. Waivers to stipulations of this directive that have been granted approval by the ENS Director and that are associated with a NIST *Special Publication (SP) 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations*, control will be recorded and tracked as a Plan of Action and Milestones (POA&M) item in the USDA *Federal Information Security Modernization Act of 2014 (FISMA), 44 United States Code (U.S.C.) Section 3551*, data management and reporting tool.

c. Waivers will expire at the end of the fiscal year or 6 months from the date of approval, whichever is longer. Unless otherwise specified, Mission Areas, agencies, and staff offices will review and renew approved policy waivers every fiscal year.

9. INQUIRIES

Questions and comments concerning the requirements of this regulation should be directed to OCIO, DISC, ENS, TIMG at ens.policy@usda.gov.

-END-
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CFR</td>
<td>Code of Federal Regulations</td>
</tr>
<tr>
<td>CIO</td>
<td>Chief Information Officer</td>
</tr>
<tr>
<td>CoS</td>
<td>Class of Service</td>
</tr>
<tr>
<td>DHS</td>
<td>Department of Homeland Security</td>
</tr>
<tr>
<td>DISC</td>
<td>Digital Infrastructure Services Center</td>
</tr>
<tr>
<td>DM</td>
<td>Departmental Manual</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name System</td>
</tr>
<tr>
<td>DOC</td>
<td>Department of Commerce</td>
</tr>
<tr>
<td>DR</td>
<td>Departmental Regulation</td>
</tr>
<tr>
<td>DTSPO</td>
<td>Diplomatic Telecommunications Service Program Office</td>
</tr>
<tr>
<td>EA</td>
<td>Enterprise Architecture</td>
</tr>
<tr>
<td>ENS</td>
<td>Enterprise Network Services</td>
</tr>
<tr>
<td>FCC</td>
<td>Federal Communications Commission</td>
</tr>
<tr>
<td>FISMA</td>
<td>Federal Information Security Modernization Act</td>
</tr>
<tr>
<td>FITARA</td>
<td>Federal Information Technology Acquisition Reform Act</td>
</tr>
<tr>
<td>GAO</td>
<td>Government Accountability Office</td>
</tr>
<tr>
<td>GSA</td>
<td>General Services Administration</td>
</tr>
<tr>
<td>IEEE-SA</td>
<td>Institute of Electrical and Electronics Engineer – Standards Association</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>MAC</td>
<td>Media Access Control</td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technology</td>
</tr>
<tr>
<td>NTIA</td>
<td>National Telecommunications and Information Administration</td>
</tr>
<tr>
<td>OCIO</td>
<td>Office of the Chief Information Officer</td>
</tr>
<tr>
<td>OMB</td>
<td>Office of Management and Budget</td>
</tr>
<tr>
<td>OPM</td>
<td>Office of Personnel Management</td>
</tr>
<tr>
<td>OSTP</td>
<td>Office of Science and Technology Policy</td>
</tr>
<tr>
<td>P.L.</td>
<td>Public Law</td>
</tr>
<tr>
<td>POA&amp;M</td>
<td>Plan of Action and Milestones</td>
</tr>
<tr>
<td>QoS</td>
<td>Quality of Service</td>
</tr>
<tr>
<td>SME</td>
<td>Subject Matter Expert</td>
</tr>
<tr>
<td>SP</td>
<td>Special Publication</td>
</tr>
<tr>
<td>TIMG</td>
<td>Telecommunications Infrastructure Management and Governance</td>
</tr>
<tr>
<td>TMACO</td>
<td>Telecommunications Mission Area Control Officer</td>
</tr>
<tr>
<td>USDA</td>
<td>United States Department of Agriculture</td>
</tr>
<tr>
<td>UTN</td>
<td>Universal Telecommunications Network</td>
</tr>
<tr>
<td>Wi-Fi</td>
<td>Wireless Fidelity</td>
</tr>
<tr>
<td>WLAN</td>
<td>Wireless Local Area Network</td>
</tr>
</tbody>
</table>
APPENDIX B

DEFINITIONS

a. **Domain Name System (DNS) Server.** Any computer registered to join the DNS. A DNS server runs special purpose networking software, features an internet protocol (IP) address, and contains a database of network names and addresses for other internet hosts. DNS servers can be configured to perform as an authoritative name server, a recursive caching server, or both (Source: USDA, DR 3300-025, Secure Domain Name System, March 18, 2016)

b. **Enterprise Architecture (EA).** The description of an enterprise’s entire set of information systems: how they are configured, how they are integrated, how they interface to the external environment at the enterprise’s boundary, how they are operated to support the enterprise mission, and how they contribute to the enterprise’s overall security posture. (Source: NIST, Information Technology Laboratory, Computer Security Resource Center, Glossary)

c. **Gateway.** An intermediate system (interface, relay) that attaches to two (or more) computer networks that have similar functions but dissimilar implementations and that enables either one-way or two-way communication between the networks. (Source: NIST, Information Technology Laboratory, Computer Security Resource Center, Glossary)

d. **Information Technology (IT).** Any services or equipment, or interconnected system(s) or subsystem(s) of equipment, that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the Agency where such services or equipment are used by an Agency, if used by the Agency directly or if used by a contractor under a contract with the Agency, that requires either use of the services or equipment or requires use of the services or equipment to a significant extent in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including provisioned services such as cloud computing and support services that support any point of the lifecycle of the equipment or service), and related resources. The term “information technology” does not include any equipment that is acquired by a contractor incidental to a contract that does not require use of the equipment. (Source: OMB, M-15-14, Management and Oversight of Federal Information Technology, June 10, 2015)

e. **Telecommunications.** The preparation, transmission, communication, or related processing of information (writing, images, sounds, or other data) by electrical, electromagnetic, electromechanical, electro-optical, or electronic means. (Source:
f. **Wireless Technologies.** Technologies that permits the transfer of information between separated points without physical connection. Note: Currently wireless technologies use infrared, acoustic, radio frequency, and optical. (Source: NIST, Information Technology Laboratory, Computer Security Resource Center, *Glossary*)
APPENDIX C

AUTHORITIES AND REFERENCES


*Federal Travel Regulation*, 41 Code of Federal Regulations (CFR) 300, July 1, 2018

IEEE-SA, *802.11 Standards*

NIST, Information Technology Laboratory, Computer Security Resource Center, *Glossary*


USDA, *3300 Series* Telecommunications Directives

USDA, *DR 3300-020, Telecommunications Mission Area Control Officer Roles and Responsibilities*, July 12, 2019

USDA, *DR 3300-025, Secure Domain Name System*, March 18, 2016

USDA, *DR 4070-735-001, Employee Responsibilities and Conduct* (October 4, 2007)

USDA, *Quality of Service (QoS)/Class of Service (CoS) Standard, Version 1.0, January 10, 2012*

USDA, *USDA Information Technology Strategic Plan 2014-2018*