

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

DEPARTMENTAL REGULATION	NUMBER: DR 3300-001-I
SUBJECT: Internet	DATE: July 29, 2019
OPI: Office of the Chief Information Officer, Digital Infrastructure Services Center, Enterprise Network Services	EXPIRATION DATE: July 29, 2024

<u>Section</u>	<u>Page</u>
1. Purpose	1
2. Special Instructions/Cancellations	1
3. Background	2
4. Scope	2
5. Policy	2
6. Roles and Responsibilities	6
7. Penalties and Disciplinary Actions For Noncompliance	9
8. Policy Exceptions	10
9. Inquiries	10
APPENDIX A – Definitions	A-1
APPENDIX B - Acronyms and Abbreviations	B-1
APPENDIX C - Authorities and References	C-1

1. PURPOSE

This Departmental Regulation (DR) establishes policy for the management and use of the Internet in the United States Department of Agriculture (USDA).

2. SPECIAL INSTRUCTION/CANCELLATIONS

- a. This regulation supersedes DR 3300-001-I, *Internet*, dated March 23, 1999.
- b. The term “agency,” or “agencies and staff offices,” unless otherwise noted in this directive, will be considered to encompass the Mission Areas, agencies, and staff offices of USDA.

- c. Agencies and staff offices may supplement this DR when developing their internal operating procedures. Modifications to the intent or purpose of this DR are not allowed. If agencies or staff offices publish a supplement to this DR, one copy of each supplement shall be forwarded to the Office of the Chief Information Officer (OCIO), Enterprise Network Services (ENS), Telecommunications Infrastructure Management and Governance (TIMG) at ens.policy@ocio.usda.gov.

3. BACKGROUND

- a. The Internet is composed of a large number of interconnected worldwide networks ranging from intra-building local area networks (LAN) to global wide-area networks. Over the years, the Internet has expanded to include Government information, educational information systems, archives, and business resources. The USDA authorizes the use of the Internet to support Departmental, agency, and staff office missions.
- b. The Internet is an integral part of service delivery at USDA as high-speed networking technologies and developments have made it a desirable source for conducting research, disseminating information, and communicating. Access to the Internet is provided through the USDA Universal Telecommunications Network (UTN).

4. SCOPE

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

5. POLICY

USDA policy allows and encourages the use of Internet services to support Departmental, agency, and staff office missions. Users of the Internet shall adhere to the following policy regarding the content and management of Internet data and information.

- a. Appropriate Uses of the Internet
 - (1) The Internet may be used for, but is 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 Departmental mission, 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 Chief Information Officer (CIO) Council's [Recommended Executive Branch Model Policy/Guidance on "Limited Personal Use" of Government Office Equipment Including Information Technology](#) (*Limited Personal Use*), dated May 19, 1999, employees may use the Internet for personal matters on an occasional basis provided that there is no loss of employee productivity or interference with official employee duties.
- b. Inappropriate Uses of the Internet
- In accordance with the *Limited Personal Use* guidance, employees must not use the Internet:
- (1) To conduct activities that are illegal, inappropriate, or offensive 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, 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.

c. Proper Representation

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 equipment for non-Government purposes. If there is an expectation that such a personal use could be interpreted to represent an 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."

d. Privacy

USDA employees have no reasonable expectation of privacy regarding any communications involving, or data transiting or stored on, any Government telecommunications system. At any time, the Government may for any lawful government purpose monitor, intercept, search, and seize any communication, or data transiting or stored, on a Government telecommunications system. Any communications involving, or data transiting or stored, on any Government telecommunications system may be disclosed or used for any lawful government purpose. Use of Government telecommunications systems, including incidental and personal use, whether authorized or unauthorized, implies the employee's consent to monitoring, which is final and irrevocable. Employees may not rely on any statements or informal policies purporting to provide any expectation of privacy on Government telecommunications systems, whether oral or written, by any other official, except USDA's Chief Information Officer.

e. USDA UTN

- (1) The USDA UTN shall be used exclusively by USDA agencies and staff offices to connect to the Internet except in instances where a waiver to the use of the UTN has been granted by the ENS Director. Information about waivers is provided in Section 7 of this DR.
- (2) The USDA UTN shall use the most current General Services Administration (GSA) approved contract for circuits to connect to the Internet and to transport inter-Local Access and Transport Area (interLATA) data between USDA agencies and staff offices via the Internet.

f. Transition to Internet Protocol version 6 (IPv6)

- (1) The Office of Management and Budget (OMB), Memorandum for Chief Information Officers of Executive Department and Agencies, [Transition to IPv6](#), dated September 28, 2010, specifies that the Federal Government must transition to IPv6 in order to:
 - (a) Enable the successful deployment and expansion of key Federal information technology (IT) modernization initiatives, such as Cloud Computing, Broadband, and SmartGrid, which rely on robust, scalable Internet networks;
 - (b) Reduce complexity and increase transparency of Internet services by eliminating the architectural need to rely on Network Address Translation (NAT) technologies;
 - (c) Enable ubiquitous security services for end-to-end network communications that will serve as the foundation for securing future Federal IT systems; and
 - (d) Enable the Internet to continue to operate efficiently through an integrated, well-engineered networking platform and accommodate the future expansion of Internet-based services.
- (2) The [Federal Acquisition Regulation](#) (FAR), 48 Code of Federal Regulations (CFR) Part 11.002 (g), sets the requirements for OMB's goal that Federal agencies include IPv6 compliance when buying networked IT products. In accordance with the OMB memorandum and FAR, all contracts that include the acquisition of IT using Internet Protocol (IP) must contain IPv6 contract clause language. This language can be found in USDA [Procurement Advisory 127](#), *Acquiring Information Technology - Recommended Language to Comply with Internet Protocol version 6 (IPv6)*.

g. Internet Protocol Addressing

- (1) To access the Internet via the USDA UTN, agencies and staff offices must use officially registered USDA IP addresses as explained in [DR 3300-001-M](#), *Internet Protocol (IP) Addresses*.
- (2) Official IP addresses uniquely distinguish each host or device connected to the network. The OCIO, ENS is the IP addressing and domain name registration authority for USDA.
- (3) Agencies and staff offices shall not connect a host or other device that uses IP and has an unregistered IP address to the Internet, the USDA UTN, or to any network connected to either of these networks.
- (4) Agencies and staff offices will modify their IP addressing plans to include the planned efficiencies and to bring all existing IP addresses in compliance with DR 3300-001-M.

h. Security

- (1) USDA connections to the internet allow many types of threat activities to be executed against the USDA IT infrastructure. Threat activities range from social threats such as phishing, spam, password guessing, visiting malware infected websites, exploitation of application vulnerabilities and misconfigurations, and data-malformation.
- (2) To defend USDA IT assets against the diverse types of weaknesses and threats, a series of cybersecurity policies are continually being created and updated. USDA cybersecurity policies can be found in the USDA [3500 to 3599 Series](#) cybersecurity directives.

- i. Pursuant to the authority vested in the *Inspector General Act of 1978*, [5 United States Code \(U.S.C.\) Appendix 3, Sections 1-12](#), the Office of the Inspector General is exempt from the provisions in this directive for mission-related activities only.

6. ROLES AND RESPONSIBILITIES

a. The USDA CIO will:

- (1) In accordance with the *Federal Information Technology Acquisition Reform Act* ([FITARA](#)) of December 19, 2014:
 - (a) Establish processes to regularly engage with program managers to evaluate IT resources supporting the strategic objectives of agency and staff offices;
 - (b) Define enterprise policy for the level of detail of planned expenditure reporting for all transactions that include IT resources;
 - (c) Define the development processes, milestones, review gates, and the overall policies for all capital planning, enterprise architecture (EA), project management, and reporting for IT resources;
 - (d) Approve any movement of funds for IT resources that require Congressional notification; and
 - (e) Conduct TechStat reviews, or use other applicable performance measurements to evaluate the use of IT resources.
- (2) Represent the USDA to the Federal CIO Council, GSA, and OMB regarding requests for exceptions to mandatory telecommunications services contracts;

- (3) Represent the USDA to oversight agencies, such as OMB, Government Accountability Office (GAO), Department of Homeland Security (DHS), Department of Commerce (DOC), and Federal Communications Commission (FCC) on telecommunications-related issues;
 - (4) Respond to oversight agencies with timely and accurate USDA telecommunications program and cost information;
 - (5) Serve as the USDA liaison with international, interLATA and intra-Local Access and Transport Area (intraLATA) telecommunications service providers; and
 - (6) Serve as the USDA representative to the Diplomatic Telecommunications Service Program Office (DTSPO).
- b. The ENS Director will:
- (1) Establish procedures for monitoring, measuring, and enforcing compliance with this DR;
 - (2) Oversee agency and staff office compliance with USDA Internet policies and procedures;
 - (3) Review security documentation to ensure that agency and staff office verification of security controls provided by private Internet Service Providers (ISP) is adequate;
 - (4) Maintain a database of approved private ISPs used by agencies and staff offices in lieu of the USDA Access Network;
 - (5) Perform vulnerability and risks assessments on agency and staff office network sites that connect to the USDA UTN;
 - (6) Process agency and staff office requests for IP network and subnetwork addresses and autonomous system;
 - (7) Refer all IP address service requests not received from an agency or staff office point-of-contact (POC) to the appropriate agency POC;
 - (8) Maintain a complete inventory of officially registered USDA IP network and subnetwork addresses used by agencies and staff offices;
 - (9) Operate the primary name server for the USDA UTN;
 - (10) Process agency and staff office requests for domain names and domain management and request the allocation of domain names from GSA in the order of request receipt;

- (11) In accordance with [DR 3150-001](#), *Internet Domain Name Policy*, and [DR 3300-025](#), *Secure Domain Name System*, manage and maintain the Domain Name System (DNS) for USDA, including a complete inventory of officially registered domain names used by USDA agencies and staff offices;
 - (12) Manage the DNS for any agency or staff office that requests a specific domain name but does not manage its own DNS;
 - (13) Monitor usage of the Internet and maintain usage statistics;
 - (14) Ensure USDA Internet access is protected by a firewall that meets requirements specified in [DR 3140-001](#), *USDA Information Systems Security Policy*.
 - (15) Manage USDA telecommunications services, equipment, and facilities in accordance with prescribed laws, regulations, standards, and related USDA [3300 Series](#) telecommunications directives;
 - (16) Review and render a decision for agency and staff office policy waiver requests;
 - (17) Maintain an electronic file of approved waivers;
 - (18) Work with agencies and staff offices to eliminate redundant or unused services and equipment;
 - (19) Include telecommunications requirements and initiatives as part of the telecommunications planning process;
 - (20) Use GSA and USDA mandated acquisition programs when agency and staff office requirements can be met cost-effectively;
 - (21) Maintain inventories of USDA telecommunications resources to the extent necessary to:
 - (a) Ensure adequate and appropriate telecommunications resources to support the agency and staff office mission;
 - (b) Ensure accountability for USDA telecommunications property; and
 - (c) Meet Departmental and Governmental requests for periodic or special inventory reports.
- c. Mission Area Assistant CIOs and Agency and Staff Office IT Directors will:
- (1) Ensure agency and staff office personnel comply with this directive;

- (2) Ensure agency and staff office internal directives conform to this DR's stated requirements;
 - (3) Provide guidance to end users on the appropriate and secure use of Government systems-interfacing telecommunications equipment;
 - (4) Include telecommunications requirements and initiatives as part of the telecommunications planning process;
 - (5) Use enterprise telecommunications or regional contracts for Continental United States (CONUS) and Outside the Continental United States (OCNUS) telecommunications services;
 - (6) Establish controls for the strict management and oversight of all non-standard options in telecommunications services contracts for which the Government will be billed to avoid potential telecommunications fraud and abuse;
 - (7) Assign a Telecommunications Mission Area Control Officer (TMACO) to select required telecommunications service from GSA Program contracts for the agency or staff office. More information on this topic can be found in [DR 3300-020](#), *Telecommunications Mission Area Control Officer Roles and Responsibilities*;
 - (8) Obtain waivers and approvals from the ENS Director when agency and staff office requirements cannot be met through mandated programs; and
 - (9) Provide the TMACO's name and contact information to the DTSP and USDA CIO.
- d. The roles and responsibilities for TMACOs are provided in DR 3300-020.

7. PENALTIES AND DISCIPLINARY ACTIONS FOR NONCOMPLIANCE

- a. [DR 4070-735-001](#), *Employee Responsibilities and Conduct*, Section 16, October 4, 2007, 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:
 1. A violation of any of the responsibilities and conduct standards contained in this directive may be cause for disciplinary or adverse action; and
 2. Disciplinary or adverse action shall be effected in accordance with applicable law and regulations.
- b. Such disciplinary or adverse action shall 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 Federal Employees of the Executive Branch](#).

8. POLICY EXCEPTIONS

- a. All USDA agencies and staff offices are required to conform to this policy. In the event that a specific policy requirement cannot be met as explicitly stated, agencies and staff offices may submit a waiver request to the ENS Director. The waiver request shall explain the reason for the request, identify compensating controls/actions that meet the intent of the policy, and identify how the compensating controls/actions provide a similar or greater level of defense or compliance than the policy requirement.
- b. Mission Area Assistant CIOs and Agency and Staff Office IT Directors shall address all policy waiver request memoranda to the ENS Director, and submit the waiver request to ens.policy@ocio.usda.gov for review and determination.
- c. Waivers to stipulations of this directive that have been granted approval by the ENS Director and that are associated with a National Institute of Standards and Technology (NIST) [Special Publication \(SP\) 800-53 Revision 4](#), April 2013, control shall 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) data management and reporting tool.
- d. Waivers will expire at the end of the fiscal year or 6 months from the date of approval, whichever is longer. Unless otherwise specified, agencies and staff offices shall 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, ENS, TIMG at ens.policy@ocio.usda.gov.

-END-

APPENDIX A

DEFINITIONS

- a. Continental United States (CONUS). The 48 contiguous United States and the District of Columbia. ([Federal Travel Regulation](#), 41 Code of Federal Regulations (CFR) 300, as amended, July 29, 2015)
- b. Domain. A set of subjects, their information objects, and a common security policy. (NIST, Interagency or Internal Report [\(IR\) 7298 Revision 2](#), *Glossary of Key Information Security Terms*, May 2013)
- c. Domain Name System (DNS). DNS services are used by a Cloud Service Provider (CSP) to run DNS servers for networking ([DR 3650-001](#), *Cloud Computing*, September 9, 2015)
- d. 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. (NIST, IR 7298 Revision 2)
- e. 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, peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services and related resources. (OMB, [M-15-14](#), *Management and Oversight of Federal Information Technology*, June 10, 2015)
- f. InterLATA. A telecommunications transmission between two or more locations that are in different Local Access and Transport Areas. (Federal Communications Commission, [Consumer Guides](#))
- g. Internet. The Internet is the single, interconnected, worldwide system of commercial, governmental, educational, and other computer networks that share (a) the protocol suite specified by the Internet Architecture Board (IAB), and (b) the name and address spaces managed by the Internet Corporation for Assigned Names and Numbers (ICANN). (NIST, IR 7298 Revision 2)Internet Protocol (IP). Standard protocol for

transmission of data from source to destinations in packet-switched communications networks and interconnected systems of such networks. (NIST, IR 7298 Revision 2)

- h. Internet Protocol (IP) Address. A numeric address allocated to identify nodes on a Transmission Control Protocol (TCP)/IP network. These addresses can be statistically of dynamically allocated. The current addressing scheme on the Internet is known as Internet Protocol version 4 (IPv4) and IPv6. ([Departmental Manual 3595-001](#), USDA Cyber Security Manual Series 3500 Appendix A Glossary, May 16, 2005)
- i. IntraLATA. A telecommunications transmission between two or more locations that are in the same Local Access and Transport Areas. (Federal Communications Commission, [Consumer Guides](#))
- j. Non-Foreign Area. The states of Alaska and Hawaii, the Commonwealths of Puerto Rico and the Northern Mariana Islands, Guam, the U.S. Virgin Islands, and the territories and possessions of the United States (excludes the former Trust Territories of the Pacific Islands, which are considered foreign areas for the purposes of the *Federal Travel Regulation*). (Federal Travel Regulation)
- k. Outside the Continental United States (OCONUS). See Non-Foreign Area.
- l. TechStat. TechStat is a face-to-face, evidence-based review of an IT program with OMB and agency leadership . TechStat sessions enable the government to turnaround, halt, or terminate IT investments that do not produce dividends for the American people. (The White House, U.S. CIO, [25 Point Implementation Plan to Reform Federal Information Technology Management](#), December 9, 2010)
- m. Telecommunications. Preparation, transmission, communication, or related processing of information (writing, images, sounds, or other data) by electrical, electromagnetic, electromechanical, electro-optical, or electronic means. (NIST, IR 7298 Revision 2)
- n. Telecommunications Services. The services and solutions that deliver or augment communications between users up to and including interstate and international communications. Telecommunications services refer to communications services or solutions specified as a discrete offering or set of capabilities. ([DR 3300-020](#), *Telecommunications Mission Area Control Officer Roles and Responsibilities*, October 13, 2016)
- o. USDA Universal Telecommunications Network (UTN). The USDA UTN is a logical scalable network that coexists with other logical networks and will serve the Internet access component for a USDA Enterprise Network. USDA access to the Internet gateway is in the Washington, DC, metropolitan area and Fort Collins, CO. A USDA Enterprise Network will be owned, managed, and operated by the USDA use applicable GSA contact circuitry for all InterLATA transport of data, including email, applications enabled by email, and data exchange.

APPENDIX B

ACRONYMS AND ABBREVIATIONS

CFR	Code of Federal Regulations
CIO	Chief Information Officer
CONUS	Continental United States
CSP	Cloud Service Provider
DOC	Department of Commerce
DHS	Department of Homeland Security
DNS	Domain Name System
DR	Departmental Regulation
DTSP0	Diplomatic Telecommunications Service Program Office
EA	Enterprise Architecture
ENS	Enterprise Network Services
FAR	Federal Acquisition Regulation
FCC	Federal Communications Commission
FISMA	Federal Information Security Modernization Act
FITARA	Federal Information Technology Acquisition Reform Act
GAO	Government Accountability Office
GSA	General Services Administration
IAB	Internet Architecture Board
ICANN	Internet Corporation for Assigned Names and Numbers
interLATA	Inter-Local Access and Transport
intraLATA	Intra-Local Access and Transport
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISP	Internet Service Provider
IR	Interagency or Internal Report
IT	Information Technology
LAN	Local Area Network
NAT	Network Address Translation
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OCONUS	Outside the Continental United States
OMB	Office of Management and Budget
OPM	Office of Personnel Management
P.L.	Public Law
POA&M	Plan of Action and Milestones
POC	Point-of-Contact
SP	Special Publication
TCP	Transmission Control Protocol
TMACO	Telecommunications Mission Area Control Officer
TIMG	Telecommunications Infrastructure Management and Governance

U.S.C.	United States Code
USDA	United States Department of Agriculture
UTN	Universal Telecommunications Network

APPENDIX C

AUTHORITIES AND REFERENCES

[*E-Government Act of 2002*](#), 44 U.S.C. §3501 (2017)

[*Federal Acquisition Regulation*](#) (FAR), 48 CFR § 11, et seq. (2018)

Federal CIO Council, [*Recommended Executive Branch Model Policy/Guidance on "Limited Personal Use" of Government Office Equipment Including Information Technology*](#), May 19, 1999

Federal Communications Commission, [*Consumer Guides*](#)

Federal Information Security Modernization Act of 2014 ([*FISMA 2014*](#)), 44 U.S.C. §3551, et seq., December 18, 2014 (2017)

Federal Information Technology Acquisition Reform Act ([*FITARA*](#)), Public Law (P.L.) 113-291, Title VIII, Subtitle D, §831-837, December 19, 2014

[*Federal Travel Regulation*](#), 41 CFR 300, as amended (2018)

Inspector General Act of 1978, [5 U.S.C., Appendix 3, Sections 1-12](#), et seq.

NIST, [*IR 7298 Revision 2*](#), *Glossary of Key Information Security Terms*, May 2013

NIST, [*SP 800-53 Revision 4*](#), *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013

Office of Government Ethics, [*Standards of Ethical Conduct for Employees of the Executive Branch*](#), November 18, 2016, Effective January 1, 2017

OMB, [*M-15-14*](#), *Management and Oversight of Federal Information Technology*, June 10, 2015

OMB, Memorandum for Chief Information Officers of Executive Departments and Agencies, [*Transition to IPv6*](#), September 28, 2010

The White House, U.S. CIO, [*25 Point Implementation Plan to Reform Federal Information Technology Management*](#), December 9, 2010

USDA, Office of Contracting and Procurement, [*Procurement Advisory 127*](#), *Acquiring Information Technology - Recommended Language to Comply with Internet Protocol version 6 (IPv6)*, November 7, 2016

USDA, [Departmental Manual 3595-001](#), *USDA Cyber Security Manual Series 3500 Appendix A Glossary*, May 16, 2005

USDA, [DR 3140-001](#), *USDA Information Systems Security Policy*, May 15, 1996

USDA, [DR 3150-001](#), *Internet Domain Name Policy*, December 5, 2006

USDA, [DR 3300-001-M](#), *Internet Protocol (IP) Addresses*, March 23, 1999

USDA, [DR 3300-020](#), *Telecommunications Mission Area Control Officer Roles and Responsibilities*, October 13, 2016

USDA, [DR 3300-025](#), *Secure Domain Name System*, March 18, 2016

USDA, [DR 3650-001](#), *Cloud Computing*, September 9, 2015

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

USDA, [3300 Series](#) Telecommunications Directives

USDA, [3500 to 3599 Series](#) Cybersecurity Directives