

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

DEPARTMENTAL REGULATION	Number: 3300-025
SUBJECT: Secure Domain Name System	DATE: March 18, 2016
	OPI: Office of the Chief Information Officer, Enterprise Network Services

<u>Section</u>	<u>Page</u>
1. Purpose	1
2. Special Instructions/Cancellations	1
3. Policy	2
4. Compliance and Internal Controls	5
5. Roles and Responsibilities	7
6. Policy Exceptions	8
7. Inquiries	8
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 the minimum requirements for implementing Domain Name System (DNS) and Domain Name System Security Extensions (DNSSEC) services across all United States Department of Agriculture (USDA) networks.

2. SPECIAL INSTRUCTIONS/CANCELLATIONS

- a. This DR applies to USDA agencies, staff offices, employees, and contractors responsible for operating and managing DNS equipment and services.
- b. For any DNS standards not addressed in this policy, refer to the following guidance documents for additional direction and information: [Domain Name System \(DNS\) Security Reference Architecture, Version 1.0](#); [National Institute of Standards and Technology \(NIST\) Special Publication \(SP\) 800-81-2](#), *Secure Domain Name System*

(DNS) Deployment Guide; [NIST SP 800-57 Revision 1](#), *Recommendation for Key Management, Part 3: Application-Specific Key Management Guidance*; [Federal Information Processing Standards \(FIPS\) Publication \(PUB\) 140-2](#), *Security Requirements for Cryptographic Modules*; and [FIPS PUB 186-4](#), *Digital Signature Standard (DSS)*.

- c. This policy complies with the statutory responsibilities identified in the [Federal Information Security Modernization Act of 2014 \(FISMA\)](#), 44 U.S.C. § 3541, et seq.
- d. This policy adheres to the requirements established in the [Office of Management and Budget \(OMB\) Circular A-130, Appendix III](#), *Security of Federal Automated Information Resources* and [Appendix IV](#), *Analysis of Key Sections*.

3. POLICY

a. General Guidance

The following guidance applies to all DNS servers, including USDA enterprise DNS servers and agency and staff office administered DNS servers:

- (1) DNS servers shall meet all criteria defined in this policy and must be registered with the USDA Office of the Chief Information Officer (OCIO), Enterprise Network Services (ENS) Directorate and the Agriculture Security Operations Center (ASOC) in order to operate as a public facing name server.
- (2) The DNS roles of authoritative name server and recursive caching name server shall be separate. If these roles cannot be separate, an additional statement describing the configuration must be included with the information submitted for registration and USDA Chief Information Security Officer (CISO) authorization.
- (3) In order to comply with OMB, Department of Homeland Security (DHS), and NIST guidance, the USDA enterprise DNS solution shall:
 - (a) Conform with DHS's [Trusted Internet Connections Reference Architecture Document, Version 2.0](#) for DNS solutions;
 - (b) Provide a DNS service that can be offered to USDA agencies and staff offices; and
 - (c) Comply with relevant NIST, OMB, FIPS, and DHS standards, guidelines, and other processes and controls identified in this policy.

b. USDA Enterprise DNS Services

ENS shall implement, operate, and manage the USDA enterprise DNS solution. This solution shall fully interoperate (without errors) with the Trusted Internet Connections (TICs) and the USDA enterprise network.

c. Public Facing Authoritative Name Servers

Public facing authoritative name servers shall:

- (1) Prohibit recursive queries from external clients;
- (2) Implement DNSSEC signatures for authentication of zone data as mandated in [OMB Memorandum M-08-23](#), *Securing the Federal Government's Domain Name System Infrastructure*, and in accordance with NIST SP 800-81-2 and NIST SP 800-57 Revision 1 for zones classified as external in the context of [NIST SP 800-53 Revision 4](#), *Security and Privacy Controls for Federal Information Systems and Organizations*;
- (3) Provide DNS services via both Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6);
- (4) Log queries, access attempts, and provide appropriate audit information to ASOC Security Information and Event Management (SIEM) devices, as directed by the USDA CISO. These logs shall be transmitted using the system log (syslog) protocol, and as official records, be managed in accordance with Information Technology and Operations Management (ITOM)-11, ITOM-13, and ITOM-23 of the *United States Department of Agriculture Record Group 16 File Plan*;
- (5) Secure any zone data transferred between name servers using a secure method such as Transaction Signatures (TSIG), as discussed in NIST SP 800-81-2, or methods providing an equivalent or greater level of data security;
- (6) Use appropriate address match lists for split DNS views, if defined, to properly segment queries and zone definitions by relevant security contexts;
- (7) Be configured using the NIST SP 800-81-2 recommended configuration checklist as a guideline; and
- (8) Be registered with ENS and ASOC as an authorized USDA public facing authoritative server.

d. Public Facing Recursive Caching Servers

Public facing recursive caching servers shall:

- (1) Restrict recursive queries to internal clients only;
- (2) Attempt DNSSEC validation for all queried names;
- (3) Provide DNS services via both IPv4 and IPv6;
- (4) Log queries, access attempts, and provide appropriate audit information to ASOC SIEM devices, as directed by the USDA CISO. The logs should be transmitted in syslog format and be retained by the owner of the system for a minimum of 30 days;
- (5) Provide DNS filtering or security controls such as DNS blackholing, DNS blacklisting, DNS firewall services, or other controls as deemed appropriate by the USDA CISO;
- (6) Be configured using the NIST SP 800-81-2 recommended configuration checklist as a guideline;
- (7) Be registered with ENS and ASOC as authorized USDA public facing recursive caching resolvers; and
- (8) Not host authoritative zones, except for the following:
 - (a) Locally hosted zones as recommended in the Internet Engineering Task Force (IETF) [Locally Served DNS Zones](#), or when necessary to achieve the goals or objectives defined in the IETF [Special-Use Domain Names](#);
 - (b) Zones hosted in a split view configuration if required by multiple security contexts; and
 - (c) Zones necessary to implement a security control as required in section 3d(5).

e. Internal or Private Servers

Internal or private servers shall:

- (1) Restrict access to internal queries only;
- (2) Forward all unresolvable queries to an authorized public facing recursive caching resolver or to an enterprise internal authoritative server;
- (3) Attempt DNSSEC validation for external names and for internal names where appropriate;
- (4) Provide DNS services on both IPv4 and IPv6 where possible, as directed by OMB mandates and other USDA directives;

- (5) Electronically log queries to create an audit trail between the original client query and the resolved DNS response, as directed by the agency or staff office Chief Information Officers (CIOs) or the USDA CISO; and
 - (6) Be configured using the NIST SP 800-81-2 recommended configuration checklist as a guideline.
- f. External or Commercial DNS Servers

DNS services provided to USDA by external, commercial, or other non-USDA sources shall meet the requirements of this policy. External servers hosting public facing USDA zones must be approved by the USDA CISO as authorized USDA public facing servers and must be included on the authorized USDA DNS server list maintained by ENS.
- g. External or Public Facing Domains

DNS domains or zones that are external or public facing only shall be hosted on DNS servers that are policy compliant and are authorized USDA public facing servers that meet the requirements identified in section 3c.

4. COMPLIANCE AND INTERNAL CONTROLS

In order to ensure that the requirements of policy statements defined in section 3 are met, the following internal controls shall be used:

- a. Measures to Ensure DNSSEC Compliance
 - (1) The ENS Director shall review the weekly DHS National Cybersecurity Assessment and Technical Services (NCATS) report detailing issues found with USDA second level non-DNSSEC compliant domains.
 - (2) Upon determining that a DNS domain is noncompliant through a review of the weekly NCATS report or by other means, ENS shall correct all subdomains hosted on the enterprise DNS. Agencies and staff offices shall correct any noncompliant domains that they host. ENS shall advise and assist agencies and staff offices in correcting their noncompliant domains.
 - (3) Agency or staff office domains that remain noncompliant after 45 days following notification shall require the domain owner to either move the domain to a server where it can become DNSSEC compliant, or pursue steps in section 6 to obtain a temporary policy exception waiver until the issue can be corrected.

b. Measures to Track USDA Public Facing Servers

- (1) The ENS Director shall compile and maintain a list of DNS servers that are authorized by the USDA CISO as policy compliant USDA public facing DNS servers. The data collected to populate the DNS server list not only serves as an indicator of the level of compliance, but also provides valuable operational data for interactions between the enterprise DNS servers and other authorized DNS servers.
- (2) In order to ensure continued validity of the authorized server list, the ENS Director shall coordinate, quarterly, with the ENS or agency technical point of contact (POC) or administrative POC, as appropriate, to verify the information is correct for a random sample of servers from the list.
- (3) ASOC shall continuously monitor inbound and outbound DNS traffic at the USDA network perimeter and identify servers that are sending or receiving DNS queries or answers to or from external destinations.
- (4) At the discretion of the USDA CISO, DNS servers not present on the authorized public facing server list may be blocked at the USDA perimeter firewall and be prevented from sending or receiving DNS messages.

c. Delegations for Public Facing Zones

- (1) Section 3g specifies that all public facing or “external” zones be hosted on an authorized public facing server. All public facing zones or subdomains delegated from the enterprise USDA DNS servers to another DNS server shall be hosted on an authorized USDA public facing server.
- (2) The ENS Director shall validate annually or at the Key Signing Key (KSK) update interval, whichever is more frequent, that public facing subdomains are delegated to servers that are on the authorized USDA public facing server list.
- (3) Zones delegated to servers not present on the authorized USDA public facing server list shall either be moved to an authorized server or agencies shall pursue steps identified in section 6 to obtain a temporary policy exception waiver until the identified issue can be corrected.

d. Other Controls

The ENS Director and USDA CISO may implement additional monitoring tools or controls, or conduct network access tests, to further validate compliance with elements in this policy. Continued failure to meet the requirements of this policy may result in affected servers being removed from the authorized server list or loss of access through the USDA perimeter firewall.

5. ROLES AND RESPONSIBILITIES

- a. The USDA CIO shall provide oversight to promote and ensure agency and staff office compliance with this policy.
- b. The USDA CISO shall:
 - (1) Issue access control policy for data and system access, and ensure compliance through assessment and authorization concurrency reviews;
 - (2) Define audit log and security control specifications as referenced in sections 3c(4), 3d(4), 3d(5), and 3e(5), and coordinate such guidance with agency and staff offices;
 - (3) Enforce DNS policy for the USDA through the use of compliance reviews, automated tools, or other appropriate methodologies;
 - (4) Review and respond to requests for waivers to this policy;
 - (5) Authorize use of USDA public facing name servers; and
 - (6) Determine whether DNS servers not on the authorized server list shall be allowed through the USDA perimeter firewall.
- c. The ENS Director shall:
 - (1) Provide oversight for the implementation and operation of the USDA enterprise DNS;
 - (2) Work with agencies and staff offices to provide support, guidance, and delegated DNS services on the enterprise platform;
 - (3) Develop and provide a DNS service to and for the agencies and staff offices in order to facilitate consolidation of agency and staff office DNS services on the enterprise DNS;
 - (4) Compile and maintain a current list of authorized public facing name servers. This list shall be reviewed and updated quarterly or at DNSSEC KSK rollover periods, whichever is more frequent;
 - (5) Ensure any DNS server hosting a public facing zone delegated from the USDA enterprise DNS is a public facing server authorized by the USDA CISO;
 - (6) Review the weekly DHS NCATS report, which details issues found with USDA second level non-DNSSEC compliant domains;
 - (7) Issue guidance for DNS access control and configuration;

- (8) Provide technical assistance and support on DNS and DNSSEC configurations to the agency or staff office POC implementing this policy;
 - (9) Maintain a current copy of the DNS authorized server list; and
 - (10) Maintain all necessary documentation provided by agency and staff offices for public facing server registration.
- d. Agency and Staff Office CIOs shall:
- (1) Implement, comply with, and maintain this policy within their respective agency or staff office; and
 - (2) Provide all necessary documentation to the ENS Director and USDA CISO for public facing server registration.

6. POLICY EXCEPTIONS

- a. All USDA agencies and staff offices are required to conform to this policy. In the event that a policy requirement cannot be met as explicitly stated, the agency or staff office CIO must submit a waiver request to the USDA CISO.
- b. 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 comparable or greater level of defense or compliance than required by the policy. Agency and staff office CIOs will submit all policy waiver requests to the USDA CISO for review and decision.
- c. Approved waivers from the USDA CISO must be associated with a NIST control that is recorded and tracked as a Plan of Action and Milestones (POA&M) item in the USDA's FISMA data management and reporting tool. Waivers will expire at the end of the fiscal year or six 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.

7. INQUIRIES

Questions and comments concerning the requirements of this regulation should be directed to OCIO-ENS, Telecommunications Management & Governance (TMG) at ens.policy@ocio.usda.gov.

-END-

APPENDIX A

DEFINITIONS

- a. Authoritative Name Server. An authoritative name server defines and originates DNS resource records and is considered public facing if it responds to DNS queries from an external network.
- b. DNS Blackholing. An anti-spam technique in which an Internet service provider blocks packets coming from a certain domain or address. Blackholing of specific domains can prevent certain types of malware and denial of service attacks.
- c. DNS Blacklisting. A security practice or procedure in which DNS requests for malicious DNS names can be blocked, redirected, or dedicated to a security logging device.
- d. 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.
- e. DNS Zone. A DNS zone is the contiguous portion of the DNS domain name space over which a DNS server has authority. A zone is a portion of a namespace and not a domain. A DNS zone can contain one or more contiguous domains. A DNS server can be authoritative for multiple DNS zones. A non-contiguous namespace cannot be a DNS zone.
- f. DNS Zone Data. The zone file contains information about various resources in that zone. The information about each resource is represented in a record called a Resource Record (RR). Because a zone may contain several domains and several types of resources within each domain, the format of each RR contains fields for making this identification. The RR consists of the following major fields: domain or resource name, time to live in seconds, class, type of resource, and information about the resource.
- g. Internal or Private Server. A name server that does not respond to DNS queries from the external network. Private name servers are positioned inside firewalls as close to internal users as is practical.
- h. Recursive Caching Server. A recursive caching name server is a server that does not originate or host any authoritative zones, but is dedicated to issuing queries to other name servers in order to resolve mappings defined by other name servers. A recursive caching server is considered public facing if it generates DNS queries to and receives responses from an external network.

- i. Systems Log (Syslog) Protocol. Syslog protocol is used to convey event notification messages. This protocol utilizes a layered architecture, which allows the use of any number of transport protocols for transmission of syslog messages. It also provides a message format that allows vendor-specific extensions to be provided in a structured way.

Further definitions regarding roles of servers and their related functions can be found in the DHS publication, [Domain Name System \(DNS\) Security Reference Architecture](#).

APPENDIX B

ACRONYMS AND ABBREVIATIONS

ASOC	Agriculture Security Operations Center
CIO	Chief Information Officer
CISO	Chief Information Security Officer
DHS	Department of Homeland Security
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DR	Departmental Regulation
DSS	Digital Signature Standard
ENS	Enterprise Network Services
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ITOM	Information Technology and Operations Management
KSK	Key Signing Key
NCATS	National Cybersecurity Assessment and Technical Services
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
POA&M	Plan of Action & Milestones
POC	Point of Contact
PUB	Publication
RR	Resource Record
SIEM	Security Information and Event Management
SP	Special Publication
Syslog	System Log
TIC	Trusted Internet Connection
TMG	Telecommunications Management & Governance
TSIG	Transaction Signature
USDA	United States Department of Agriculture

APPENDIX C

AUTHORITIES AND REFERENCES

DHS, [*Domain Name System \(DNS\) Security Reference Architecture, Version 1.0*](#), June 21, 2011

DHS, [*Trusted Internet Connections Reference Architecture Document, Version 2.0*](#), October 1, 2013

[*Federal Information Security Modernization Act of 2014 \(FISMA\)*](#), 44 U.S.C. § 3541, et seq.

[*FIPS PUB 140-2*](#), *Security Requirements for Cryptographic Modules*, May 25, 2001

[*FIPS PUB 186-4*](#), *Digital Signature Standard (DSS)*, June 2013

IETF Request for Comments 6303, [*Locally Served DNS Zones*](#), July 2011

IETF Request for Comments 6761, [*Special-Use Domain Names*](#), February 2013

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

[*NIST SP 800-57 Revision 1*](#), *Recommendation for Key Management, Part 3: Application-Specific Key Management Guidance*, January 2015

[*NIST SP 800-81-2*](#), *Secure Domain Name System (DNS) Deployment Guide*, September 2013

[*OMB Circular A-130, Appendix III*](#), *Security of Federal Automated Information Resources*, November 2000

[*OMB Circular A-130, Appendix IV*](#), *Analysis of Key Sections*, November 2000

[*OMB Memorandum M-08-23*](#), *Securing the Federal Government's Domain Name System Infrastructure*, August 22, 2008

United States Department of Agriculture Record Group 16 File Plan, April 7, 2014