State of Nevada

Information Security Committee

Standard

Document ID	Title	Revision	Effective Date	Page
S.5.06.02	Domain Name System (DNS)	F	01/09/2023	1 of 4

1.0 PURPOSE

The purpose of this standard is to establish the minimum requirements for Domain Name System (DNS) servers, services, and settings that are to be used by State agencies utilizing any State network.

2.0 SCOPE

This standard applies to all state agencies and authorized users meeting the criteria identified in the State Information Security Program Policy, Section 1.2, Scope and Applicability.

3.0 EFFECTIVE DATES

This standard becomes effective at the time of approval of the State Chief Information Officer (CIO).

4.0 RESPONSIBILITIES

The agency head and appointed Information Security Officer (ISO) have the responsibility to ensure the implementation of and compliance with this standard.

5.0 RELATED DOCUMENTS

State Information Security Program Policy, 100

6.0 STANDARD

To ensure appropriate and verified communications in the State of Nevada's DNS infrastructure, EITS manages multiple enterprise DNS servers to provide DNS resolution services.

6.1 INTERNAL DNS

A. All agency DNS domain and network segment information must be reliably and accurately resolvable by the State Domain Name System (DNS) servers.

B. If an agency maintains agency DNS servers, agency DNS servers are the authoritative source of forward and reverse DNS lookups for all agency-assigned subnets.

   i. If an agency does not maintain their own DNS servers, agency technology assets will either utilize the State enterprise DNS servers for DNS services or utilize EITS-hosted DNS servers provided on behalf of the agency.

C. Agencies must formally authorize DNS servers to be used as Authorized External Forwarders (AEF). Agency AEFs will be the only nodes permitted to forward DNS requests to the Internet.

D. To support the use of secure DNS services, agencies with AEFs are required to administer their own DNS security policies. Those policies must be approved by the agency head.

E. Agencies will provide EITS with a list of the agency's DNS servers and IP subnets used for their technology assets to ensure enterprise DNS queries communicate only to

agency-authorized DNS servers. If changes to any agency DNS server addresses occur, agencies must notify the EITS Helpdesk as soon as possible (ASAP) to maintain stable DNS resolution communications between the enterprise and agency.

F. Agencies must allow bi-directional communication for DNS queries to and from all State enterprise DNS servers. Agencies should contact the EITS Help Desk to obtain the appropriate IP addresses for these servers if needed.

G. Agencies must use Fully Qualified Domain Names (FQDN) for all server and application connectivity.

H. DNS suffixes are not required on the STATE domain, or child domains of the STATE domain. However, if agencies choose to utilize DNS suffixes, agency technology assets should have their DNS suffix search list configured to point to the following domains in the order listed: 1) The agency's domain 2) "state.nv.us" 3) "nv.gov"

6.2 **EXTERNAL DNS**

A. All Public Service Zone (PSZ) or Demilitarized Zone (DMZ) technology assets requiring internet DNS need to use the PSZ enterprise DNS servers as specified by EITS. Agencies should contact the EITS Help Desk to obtain the appropriate IP addresses for these servers if needed.

B. Agencies may manage their external DNS records under the following provisions:

i. Agencies will be given access to a tool/platform provided by EITS. The tool will be limited to the agency's domain. This tool must be used for management of the records.

ii. Activity in the tool will be logged. Logs will be available to the agency either directly through the tool or through a direct request to EITS.

iii. Agencies shall not modify or delete records used to provide EITS-hosted services without consultation and written approval from EITS.

iv. Agencies shall not create, modify, or delete external DNS records in a manner inconsistent with this or any other applicable security standard.

C. Third parties may be given SPF records in the under the following provisions:

i. The request for a third-party SPF record must come from the ISO, head of IT, or agency head of a sponsoring state agency. The sponsoring agency will be responsible for any activity related to the record, and ensuring the third party follows State policy and standards.

ii. Third party SPF and MX records will be restricted to agency-specific subdomains of the "info.nv.gov" and "alerts.nv.gov" domains. The sponsoring agency shall add their agency domain to the record (i.e. "admin.info.nv.gov" or "dps.alerts.nv.gov").

1. "alerts.nv.gov" shall be used for low-frequency, high-importance communications from agencies sent via third-party email services.

2. "info.nv.gov" shall be used for higher frequency, lower importance communications from agencies sent via third-party email services.

iii. SPF records will be entered into the DNS and managed by EITS.

6.3 DNS RECORD RESPONSIBILITY

EITS reserves the right to view, add, modify, or delete DNS records on all EITS-hosted or EITS-managed DNS systems as needed to support EITS-hosted services, ensure compliance with state security standards, or to meet any other legitimate business needs as defined by the State.

7.0 DEFINITIONS

Authoritative External Forwarders (AEF): DNS Servers managed at the agency level that can forward DNS requests to the Internet.

Domain Name System (DNS): The DNS is a critical network infrastructure component, enabling the communication of State computers and other devices within the State networks.

Sender Policy Framework (SPF): An SPF record is a type of DNS record that lists all the servers authorized to send emails from a particular domain.

Technology Assets: As defined in CIS Controls v7.1, the term "Technology Assets" (also referred to therein as "Hardware Technology Assets" or "Hardware Assets") collectively refers to equipment and devices that have the potential to store or process information, whether connected to the network or not.

8.0 RESOURCES

Center for Internet Security (CIS), CIS Controls v7.1 Guide

9.0 EXCEPTIONS

Requests for exception to the requirements of this Information Security Standard must be documented, provided to the Office of Information Security (OIS), and approved by the State Chief Information Security Officer (CISO).

Approved By

Title	Signature	Approval Date
State Information Security Committee	Approved by Committee	11/17/2022
State Chief Information Security Officer (CISO)	Signature on File	01/09/2023
State Chief Information Officer (CIO)	Signature on File	01/09/2023

State of Nevada

Information Security Committee

Standard

Document History

Revision	Effective Date	Change
A	7/25/2013	Initial release
B	8/31/2017	Biennial review and update
C	3/28/2018	Revisions to address Authorized External Forwarders
D	12/26/2018	Renumbering (137 to S.5.06.02) and compliance to ADA standards
E	12/31/2020	Biennial review for alignment with CIS Controls v7.1, Implementation Group 1 (IG1)
F	01/09//2023	Added provisions for third-party SPF records and agency management of external DNS, general language cleanup