State of Nevada

Information Security Committee

Standard

Document ID	Title	Revision	Effective Date	Page
S.5.06.02	Domain Name System (DNS)	D	4/05/2018	1 of 3

1.0 PURPOSE

DNS (Domain Name System) is an important component to the communication of State computers and other devices within the State of Nevada's networks. All agency DNS domain and network segment information must be reliably and accurately resolvable by the servers of the State of Nevada DNS System. The purpose of this standard is to establish the requirements for DNS systems and settings that are to be used by State agencies utilizing any State of Nevada network.

2.0 SCOPE

This standard applies to any entity, regardless of physical location, that operates, manages, or uses SilverNet services or equipment.

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, Section 5.6 System-to-System Interconnection

6.0 STANDARD

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

6.1 Agency DNS servers are the authoritative source of forward and reverse DNS lookups for all agency-assigned subnets, unless an agency does not maintain their own DNS servers. If an agency does not maintain their own DNS servers, systems such as desktops, laptops, servers, tablets, network devices, etc. need to utilize the State enterprise servers NS2 (preferred) and NS4 (alternate).

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

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

6.4 Agencies will provide EITS with a list of the agency's DNS servers and IP subnets used for their systems to ensure enterprise DNS queries communicate only to agency-authorized DNS servers. If changes to agency any DNS server addresses occur, please notify EITS

Helpdesk ASAP to maintain stable DNS resolution communications between the enterprise and agency.

6.5 Agencies must allow bi-directional communication for DNS queries to and from enterprise DNS servers NS1, NS2 NS3 and NS4. Contact the EITS Helpdesk to obtain the appropriate IP addresses for these servers if needed.

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

6.7 DNS suffixes are not required on the STATE domain, or child domains of the STATE domain. However, if agencies choose to utilize DNS suffixes, all systems such as desktops, laptops, servers, tablets, network devices, etc., 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"

6.8 All Public Service Zone (PSZ) or Demilitarized Zone (DMZ) systems requiring internet DNS need to use the PSZ enterprise DNS servers EDGENS1 (preferred) and EDGENS2 (alternate). Contact the EITS Helpdesk to obtain the appropriate IP addresses for these servers if needed.

7.0 DEFINITIONS

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

State agency: Any State of Nevada Government entity (Department, Division, Board, Commission, Committee, etc.).

Systems: Mainframes, servers, PC's, laptops, tablets, printers, scanners, and other computing devices that have configurable DNS settings and that are connected to the State of Nevada's networks.

8.0 RESOURCES

N/A

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).

State of Nevada

Information Security Committee

Standard

Approved By

Title	Signature	Approval Date
State Information Security Committee	Approved by Committee	3/28/2018
State Chief Information Security Officer (CISO)	Signature on File	4/02/2018
State Chief Information Officer (CIO)	Signature on File	4/05/2018

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.