



*Federal Network Security
Federal Interagency Technical Reference Architectures*

Domain Name System (DNS) Security Reference Architecture

Version 1.0

6/21/2011



Department of Homeland Security
National Cyber Security Division
Federal Network Security
Network & Infrastructure Security

Revision History

Date	Version	Description	Approved By
June 30, 2011	1.0	Final Version 1.0	Roberta G. Stempfley

Acknowledgements

This document is the product of a multi-agency collaborative initiative to provide guidance for the successful and secure implementation of Domain Name System (DNS) at Federal civilian agencies. Participants from several agencies have graciously volunteered their expertise; this document would not be possible without their selfless contributions.

Architecture Participants

Name	Agency
Paula Bailey	Department of Agriculture
Brian Kipper	Department of Homeland Security
Carl Beaudry	Department of Homeland Security
Earl Crane	Department of Homeland Security
Jim Rather	Department of Homeland Security
Richard Hudson	Department of Homeland Security
Robert Moore	Department of Homeland Security
Bill Lakner	Department of Labor
Ranny Reynolds	Department of the Treasury
James Boissonnault	Department of the Treasury (FMS)
Nnake Nweke	Federal Communications Commission
Peter Batista	Federal Communications Commission
Peter Cho	Federal Deposit Insurance Corporation
George Cartron	General Services Agency
Cathy Robertson	Internal Revenue Service
Timothy Morizot	Internal Revenue Service
Walter Lamar	National Institute of Health
Robert Toense	National Institute of Standards and Technology
Scott Rose	National Institute of Standards and Technology
Chi Kang	National Oceanic and Atmospheric Administration
Erwin Mascardo	National Oceanic and Atmospheric Administration
Sameka Prather	National Oceanic and Atmospheric Administration
Casey Deccio	Sandia National Laboratory
Donald Rudder	Tennessee Valley Authority
Brion Leary	U.S. Postal Service

Architecture Document Team Members

Name	Organization
Marilyn Rose	Department of Homeland Security (Project Leader)
Sean Donelan	Department of Homeland Security
Oscar Ahumada	Department of Homeland Security
Robert Moore	Touchstone Consulting Group
Eric Pratsch	Touchstone Consulting Group

Table of Contents

1	PURPOSE AND SCOPE	1
2	DNS ARCHITECTURAL COMPONENTS	2
1		2
2.1	NAME SERVER FUNCTIONAL TYPES	2
2.1.1	Authoritative Name Servers	2
2.1.2	Recursive Caching Name Server	2
2.2	NAME SERVER AUTHORITY	2
2.2.1	Primary Name Server	2
2.2.2	Secondary Name Server	2
2.3	NAME SERVER EXPOSURE	3
2.3.1	Public-Facing Name Server	3
2.3.2	Private Name Server	3
3	SECURITY PATTERNS	4
3.1	AUTHORITATIVE SERVER REQUIREMENTS	4
3.2	RECURSIVE CACHING SERVER REQUIREMENTS	5
4	SYSTEMIC THREATS & MITIGATIONS	7
5	DNS SECURITY CONFIGURATION	8
5.1	EXTERNAL AUTHORITATIVE SERVERS	8
5.2	RECURSIVE CACHING SERVERS	9
5.3	INTERNAL AUTHORITATIVE DNS SERVERS	10
6	IMPLEMENTATION CONSIDERATIONS	11
6.1	REMOTE VPN CLIENTS	11
6.2	DNS AND SECURITY POLICY	11
6.3	DNS OUTSOURCING	11
6.4	DNSSEC SIGNING	12
6.5	DNSSEC VALIDATION	13
	APPENDIX A: ACRONYMS – COMMON ABBREVIATIONS	15
	APPENDIX B: GLOSSARY – COMMON TERMS AND DEFINITIONS	17
	APPENDIX C: SELECTED EXISTING GUIDANCE	20
	LEGISLATION	20
	POLICIES, DIRECTIVES, REGULATIONS, AND MEMORANDA	20
	STANDARDS	20
	GUIDANCE	21

Index of Figures

FIGURE 1: DNS INFRASTRUCTURE MODEL	4
------------------------------------	---

Index of Tables

TABLE 1: DNS THREATS	7
TABLE 2: CONFIGURATION SUMMARY OF EXTERNAL AUTHORITATIVE SERVERS	8
TABLE 3: CONFIGURATION SUMMARY OF RECURSIVE CACHING SERVERS	9
TABLE 4: CONFIGURATION SUMMARY OF INTERNAL AUTHORITATIVE SERVERS	10
TABLE 5: IMPLEMENTING DNSSEC SIGNING	12
TABLE 6: IMPLEMENTING DNSSEC VALIDATION	13

1 Purpose and Scope

The overall purpose of the DNS Security Reference Architecture is to optimize and standardize the DNS currently in use by the Federal civilian government, and to improve the Federal government's security posture by reducing the threats against the DNS at Federal civilian agencies. This is not mandatory implementation guidance and will supplement - not repeat or replace - existing policies and standards. The document helps agencies comply with relevant Federal policies and offers best practices, which may be customized to unique Federal civilian agency requirements.

This document is a reference that provides insight and guidance for agencies implementing DNS and striving to comply with OMB M-08-23 *Securing the Federal Government's Domain Name System Infrastructure*. This document is descriptive in nature, recognizing that many organizations face unique challenges that do not lend themselves to a "one size fits all" solution. Unlike a Target Architecture, a Reference Architecture does not mandate specific solutions, but rather identifies a range of workable modular solutions.

The intent is to enable agencies to leverage existing capabilities and technologies when implementing DNS in evolving Enterprise Architectures and to achieve compliance with the National Strategy for Trusted Identities in Cyberspace (NSTIC) in the context of their respective missions, programs, and initiatives. NSTIC calls for the development of interoperable technology standards and policies — an "Identity Ecosystem" — where individuals, organizations, and underlying infrastructure — such as routers and servers — can be authoritatively authenticated. DNSSEC is a critical enabling technology for NSTIC.

This document is intended for use by Federal civilian agencies. The information in this document is based upon collaboration with multiple agencies, the definitions and requirements in the Federal Information Security Management Act (FISMA), National Institute of Standards and Technology (NIST) guidance and standards, TIC Reference Architecture v2, and Office of Management and Budget (OMB) Memoranda.

2 DNS Architectural Components

DNS is a globally distributed database accessed using a simple query/response protocol. The DNS protocol resolves human readable domain names (e.g., “www.agency.gov”) to an Internet Protocol (IP) address and is often the first step in any network communication. An agency’s DNS is a key component of its network infrastructure. Therefore it is vital that the DNS infrastructure is responsive, robust, and secure so that it can meet its two primary business purposes: (1) allow agency personnel to reach the Internet; and (2) allow the general public to reach the agency’s public-facing web services.

2.1 Name Server Functional Types

For the purposes of this Architecture, DNS components can be divided into two broad functional categories: components that maintain and distribute domain names for clients (Authoritative Name Servers), and components that request domain names from servers (Recursive Caching Name Servers).

2.1.1 Authoritative Name Servers

Authoritative servers maintain a portion of the global DNS database for an enterprise (referred to as its **zone**, as an example, ‘agency.gov’). The authoritative servers for the respective zones are able to provide any resolution within its portion of the name space (e.g. *.agency.gov) or issue an error message such as NXDOMAIN (not able to resolve the requested name to an IP address).

2.1.2 Recursive Caching Name Server

A **recursive caching server** (or “caching resolver server”) performs DNS resolution on behalf of clients (“stub” clients without the ability to do a full DNS query.) It then stores the responses in a cache for the benefit of all the stub clients it services.

2.2 Name Server Authority

Authoritative servers are further divided into two categories: **primary** (or “master”) and **secondary** (or “slave”).

2.2.1 Primary Name Server

A **primary** name server loads its information from a locally maintained file or database.

2.2.2 Secondary Name Server

A secondary name server is an authoritative name server which obtains the zone information that it serves from a primary name server instead of a locally maintained database. This is usually accomplished within the DNS protocol by means of a **zone transfer**. A zone transfer is a special type of DNS query and response that transfers the contents of a zone database in a single

transaction and is often done over TCP rather than UDP (as traditional query/response transactions). Some DNS implementations do not use zone transfers to replicate zone information; instead these use some other data replication services to perform a functionally equivalent task. Regardless of what protocol is used, a name server is secondary if it obtains its zone information from another server.

2.3 Name Server Exposure

Authoritative servers are classified according to the following exposure levels: public-facing or private.

2.3.1 Public-Facing Name Server

An authoritative name server is “public-facing” if it responds to DNS queries from an external network. It is usually located in an agency’s DMZ but may reside elsewhere. An authoritative server’s zone information includes the addresses of all externally facing services (e.g. web, mail, etc.). Public-facing name servers should always be authoritative because public-facing recursive caching servers are more vulnerable to cache poisoning attacks and can be used as reflectors for distributed denial of service (DDoS) attacks.

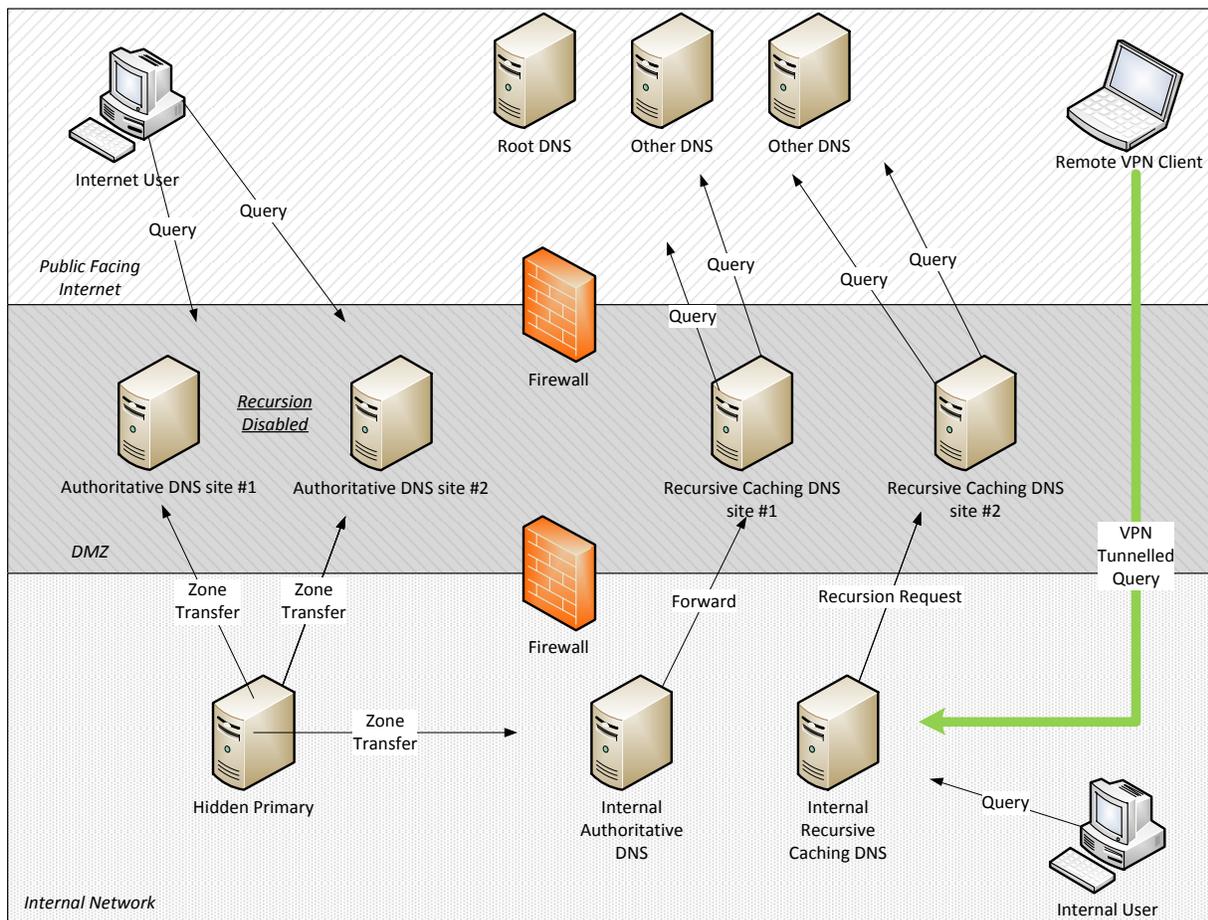
2.3.2 Private Name Server

A name server is private if it does not respond to DNS queries from an external network. Private name servers are positioned inside firewalls as close to internal users as is practical. Private name servers may be authoritative for internal zones or purely recursive caching servers that obtain DNS records from public facing servers.

3 Security Patterns

When planning the DNS infrastructure for an agency, DNS architects should take the respective roles of each name server type into consideration and separate the systems performing each task. Each role has specific usage and security concerns that should be addressed when designing the DNS for the agency. The agency will set up one set of systems for the authoritative service (the left side of Figure 1) and another to provide recursive service for clients within the agency (the right side of Figure 1).

Figure 1: DNS Infrastructure Model



3.1 Authoritative Server Requirements

The basic requirements for an agency’s authoritative DNS service are data integrity and high availability in the face of any potential network disruption (intentional or unintentional). A Denial of Service (DoS) attack or network segment break could take the entire agency off line if all of the agency’s authoritative servers are located on the same LAN segment. These requirements are met by separating the internal and external authoritative servers (based on the clients they will respond to and the zone information they contain) and dispersing both groups of authoritative servers across different network segments and geographic locations (if possible).

The authoritative servers for the agency should be broken down into two sets: One set to host internal zone data (internal mail servers, application servers, etc.) that resides on the internal network and only responds to other internal hosts, and another set to host externally facing servers that are located on the agency's "demilitarized zone" (DMZ) or Service Network and responds to queries from the external Internet.

Both sets of servers should have all other unnecessary network services uninstalled. Additionally, the authoritative servers located in the DMZ should sit behind the agency's external facing firewall for further protection and only permit allowed necessary ports/protocols.

To ensure the integrity of zone data, DNS administrators should deploy the DNS Security Extensions (DNSSEC) with their zone data. DNSSEC provides source authentication and integrity protection for DNS data through the use of digital signatures. To ensure the integrity of the process, the generation of these digital signatures should be done as close to the authentic data source as possible, with the signed zone then transferred to the hidden primary (for external zones) and internal authoritative zones. More information on how to plan and deploy DNSSEC can be found in NIST SP 800-81r1.

Network administrators should consider using a hidden primary name server for the external DNS authoritative servers. Hidden primary servers make the maintenance of DNSSEC trust relationships much easier in large and complex implementations. A hidden primary is a DNS server that does not appear in the zone data itself as one of the name server records for the zone and yet is the primary server for the zone. The hidden primary is often located behind a firewall and cannot be queried from the external Internet and does not serve zone information to regular users. Its sole function is to host the zone and perform zone transfers to a collection of secondary servers which, in turn are available on the DMZ.

3.2 Recursive Caching Server Requirements

The dedicated recursive servers should also be located within the DMZ. These limited recursive servers should be the only DNS servers allowed to query outside of the agency to retrieve the name resolution.

The dedicated recursive servers should have their access control list tightened to only allow queries from the internal recursive servers. These servers *should not* be accessible from the outside (e.g. through the usage of firewall) as they can be used by attackers as a reflector to launch DDoS attacks. DNS resolution should also be restricted by name as well as IP address.

The dedicated recursive servers should not be used by stub client (resolvers) directly, but through a forwarder. These dedicated recursive servers are also referenced as **forwarders** (or **DNS proxy**), as in other DNS servers forward their queries to these servers to further aggregate the cache. Forwarders also limit the number of DNS servers that are allowed to go out to the Internet to contact external DNS servers. The internal DNS servers (either authoritative or

recursive) that are located in the internal network should accept queries only from the internal hosts.

Usually, these internal recursive DNS servers will be configured to **forward** queries to the dedicated recursive servers located in the DMZ. Normally, the internal DNS servers can be configured to allow full recursion, however, it is recommended that the internal DNS servers only forward and not be allowed to query directly against the root or external DNS servers. For example, when the internal DNS servers cannot resolve entries (e.g. www.website.com), the recursion request is forwarded to the dedicated recursive servers located in the DMZ. The recursive servers will perform the recursion and return the results back to the internal DNS server.

It is recommended that DNS query logging be implemented on the recursive name servers closest to the resolving client. This can be done directly in some DNS implementations as well as by a dedicated network Security Information and Event Manager (SIEM).

For small agencies, one or two recursive servers may be enough. Larger agencies may need several recursive servers and may want to consider having a larger agency-wide aggregate cache (i.e. forwarder) to provide faster response time for users and provide a single gateway for any monitoring by intrusion detection systems (IDS) or similar systems. Separate departments within an agency would have their own recursive server that would forward its queries to the aggregate cache, which would then build an agency-wide cache of responses.

Agencies that perform DNSSEC validation of responses have additional configuration options to consider when setting up recursive systems. At this time, most stub clients (i.e., desktop and laptop systems) do not perform DNSSEC validation, and must rely on a validating recursive server. Therefore, it is important to perform validation as close to the end system as possible to minimize any potential hijack of the response. This risk can be further minimized by the use of IPsec or similar security measures (e.g., DNS transaction signatures; TSIG) for communication between end systems and the validating recursive server.

Administrators also need to configure DNSSEC public keys as trust anchors for one or more zones to enable validation. These trust anchors should be chosen based on a designated security policy. The public key for the root zone should be chosen as one trust anchor, as well as any other zones that the agency wishes to maintain independently.

There are automated protocols and tools to keep trust anchors up-to-date, but initial configuration requires human action. The administrator needs to first identify and obtain the desired trust anchors to install on the validating recursive servers and then establish and monitor a process to perform regular key maintenance. Even though the end nodes may not request DNSSEC validation, DNSSEC validation-enabled recursive servers will perform the chain-of-trust checks starting with available loaded trust anchors. If there is a misconfiguration (e.g. mismatching keys), then the validation will fail, and then subsequent name resolution will fail as well. DNSSEC validation should be enabled with proper operational protocols in place when and if an external site has misconfigured DNSSEC which causes validation to fail for queries to those sites.

4 Systemic Threats & Mitigations

General DNS threats can be categorized into two categories and several sub-categories as discussed in NIST Special Publication 800-81r1: *Secure Domain Name System (DNS) Deployment Guide*. Threats to the **DNS Hosting Environment** include threats to the host platform, the DNS software and the DNS data contents. Threats to **DNS transactions** include threats to DNS queries and responses, threats to zone transfers, threats to dynamic updates and DNSNOTIFY threats. Several checklists are set forth in the NIST publication listing specific mitigation techniques.

Close attention should be paid to the operational context in which DNS servers operate. Not only must they be protected by firewalls and other inherited controls, but DNS server logs should be actively monitored by an integrated security information and event management infrastructure and considered critical information assets by incident response staff.

Table 1: DNS Threats

Threat	Description	Impact
Denial of Service (DoS)	DoS can be initiated intentionally either malicious attacker or unintentionally by a valid user/system. The effect is that the DNS services are overloaded with requests and not able to handle valid requests. DoS can also result when DNS data is incorrectly modified (either maliciously or unintentionally) thus not allowing connectivity to those services.	DoS can make the DNS service unavailable for both authoritative or recursive servers, compromising the availability of the DNS servers.
Cache Poisoning	DNS client is redirected to different set of IP addresses for valid names. The user is not aware that the traffic isn't being directed to the "correct" servers.	Sensitive information such as password can be captured by the attackers, compromising the confidentiality of scores of users.
Compromised Zone transfer data	Zone transfers the full zone from the primary to the secondary. If the transfer isn't secure, the transfer data will be compromised.	The full set of data may be available to malicious attackers, compromising the integrity of the zone information.
Unauthorized Updates	For DNS servers supporting Dynamic DNS Updates (DDNS), the client can issue DDNS update to automatically update the particular zone with data.	Malicious attacker can leverage DDNS to make unauthorized updates against the zone, thus compromising the integrity of the DNS response.

5 DNS Security Configuration

Based upon the concepts developed in previous sections, the following is a brief description of the security capabilities that should be utilized for DNS. These are not new requirements but highlights of existing NIST guidance and standards set forth in NIST Special Publications 800-53, 800-53A, 800-41, 800-81r1 and subsequent publications, federal laws, standards, and guidelines. Industry best practice guidelines are also considered.

5.1 External Authoritative Servers

Table 2: Configuration Summary of External Authoritative Servers

Recommendation	Description	Key Benefits
Use dedicated external name servers	Disable recursion since the name servers should not be performing any recursion.	Eliminate cache poisoning.
Disperse name servers	Name servers should be spread across multiple switches and sites to minimize the impact of outages. Larger sites may use wide-area routing protocol strategies, such as Anycast, to balance query loads across many geographically dispersed servers.	Increase availability Site resiliency.
Utilize DNS resolution blocking and logging	BIND 9.3 is an example with capabilities such as allow query list, recursion allowed list, etc.	Tighten security control.
Turn off all services except for DNS	Remove any unnecessary software / services running from the external DNS authoritative servers.	Minimize DoS. Minimize impact of security vulnerabilities of other services.
Restrict access to DNS ports to outside users	Use a Firewall system to further prevent access to the servers.	Minimize DoS. Increase defense depth.
Use hidden primary	Place the primary server that is hidden (no NS record) inside the firewall. All changes on the zones are made on the primary and transferred.	Minimize configuration errors leading to DoS. Eliminate DoS targeting primary servers for zones.
Use authenticated zone transfers	For each secondary server, use a unique Transaction SIGNature (TSIG) key or some other means to authenticate zone transfers (e.g. IPSec).	Compromised Zone transfer data.
Disable DDNS	External DNS servers do not allow DDNS.	Eliminate Unauthorized DNS updates.
Enable DNSSEC to	DNSSEC provides integrity of the records	Minimize cache

sign zones	by signing each record set with the private key and publishing the public key via DNSSEC record. DNSSEC validating servers can then use the public key stored in the DNSSEC record to decrypt the signature to validate the integrity of the DNSSEC record(s).	poisoning.
------------	--	------------

5.2 Recursive Caching Servers

Table 3: Configuration Summary of Recursive Caching Servers

Recommendation	Description	Key Benefits
Use dedicated recursive servers	No authoritative zones will be “hosted” on the recursive servers.	Isolate name server functions.
Disperse name servers	Name servers should be spread across multiple switches and sites to minimize the impact of outages.	Increase availability. Site resiliency.
Place recursive servers at the DMZ	These become “DNS” Proxy servers as many organizations do not allow DNS traffic to go directly from the internal network to the “outside”. By leveraging forwarding, the DNS proxy (recursive) servers will fetch the name resolution and return it back to the original resolver.	Maintain tighter security boundary.
Restrict access to internal users	The DNS traffic will always originate from recursive servers, and never from outside TO the recursive servers. We lock down these servers from being ‘reachable’ from outside world.	Minimize DoS Eliminate our servers being hijacked by attackers to perform DoS against others.
Restrict access to legitimate domains	Recursive DNS servers can be configured to disallow and/or log attempts to resolve certain domains. This can be done either in place of or as part of an integrated Data Loss Prevention (DLP) solution.	Increase site security/Minimize threats to internal hosts.
Define recursion-list	Although recursion is enabled, the recursion-allowed list should be tightly set so that only a small set of systems can send queries to the recursive server.	Minimize DoS. Eliminate our servers being hijacked by attackers to perform DoS against others.
Define query-list	This is similar to the recursion allowed list. Only a small set of IP’s should be allowed to query these servers.	Tighter control. Minimize DoS vectors.
Enable DNSSEC Validation	Once DNSSEC is deployed more widely, DNSSEC validation takes advantage of	Eliminate cache poisoning.

	the signed zones by validating not only the chain of trust (root servers and down) but also the validity of each record.	
--	--	--

5.3 Internal Authoritative DNS servers

Table 4: Configuration Summary of Internal Authoritative Servers

Recommendation	Description	Key Benefits
Set up DNS forwarding	The internal authoritative servers should only forward DNS queries to the dedicated recursive servers. These should not be allowed to recurse or query outside.	Isolate name server functions. Maintain tighter security boundary.
Disperse name servers	Name servers should be spread across multiple switches and sites to minimize the impact of outages.	Increase availability. Site resiliency.
Define query-list	This is similar to the recursion allowed list. Only the internal clients should be listed on the query list.	Tighter control. Minimize DoS.
Block Access from Outside	The internal name servers should not be reachable from the outside world.	Minimize DoS.
Use “hidden” primary name server	Although hidden primary isn’t as important as it is for external name servers, it still adds value by minimize the impact of misconfigured primary servers on the secondary servers.	Minimize configuration errors leading to DoS.
Evaluate DNSSEC	Most organizations are not yet ready for DNSSEC for internal zones. The agency should at least evaluate what needs to be done, what hurdles need to be overcome to implement DNSSEC. By evaluating its readiness, the agency can make the necessary steps to move toward them.	Eliminate cache poisoning. Maintain DNS integrity.

6 Implementation Considerations

The following sections provide implementation considerations for VPN clients, security policy, outsourcing, and DNSSEC signing and validation. In addition to the considerations listed here for DNSSEC signing and validation, the Federal CIO Council publication on *Considerations for Federal Agency Implementation of DNS Security Extensions and Email Authentication* may provide further information to agencies when implementing DNSSEC.

6.1 Remote VPN Clients

Administrators need to provide one or more recursive servers for remote users connecting back to the agency's network via a VPN. Mobile users may not be able to trust the recursive server provided by the remote network. Also, the remote network's recursive server(s) may not perform DNSSEC validation and if validation is performed, mobile users will not know what trust anchors are used. Mobile users should have a means to connect back to the home agency's network and use one of the trusted recursive servers (or a special recursive server for VPN users).

6.2 DNS and Security Policy

Under FISMA, critical information technology resources are configured and evaluated as parts of General Support Systems (GSS's) and applications, both major and minor with differing respective configuration and auditing guidance. Because DNS affects every existing GSS, often in multifaceted ways, changes to DNS will have repercussions to those existing systems. It is therefore recommended that agencies consider establishing DNS as a separate GSS under FISMA rules. This makes it much easier to evaluate the effect of major changes (such as implementing DNSSEC) on other critical infrastructure elements prior to ratifying changes.

Because DNS is involved in virtually every network transaction, DNS servers should be characterized as both highly critical and highly sensitive under FISMA guidance.

6.3 DNS Outsourcing

Agencies may choose to outsource all or part of their DNS infrastructure. The reasons for doing so are that trusted third parties may be better able to provide the security, geographical dispersion and high-availability safeguards than an internal network data center. There also may be cost considerations.

Outsourcing DNS infrastructure, however, does present drawbacks. Not only can it complicate remote administration, but it may subject the agency to security attacks leveled at the outsourced organization. It may also make it difficult to monitor recursive servers close to internal users. The nature of DNS also makes a hybrid solution possible where part of the DNS is hosted internally and the external facing DNS is hosted either all or in part by a trusted third party.

It is therefore recommended that agencies consider both the costs and benefit of an outsourced approach when designing their DNS architecture.

6.4 DNSSEC Signing

Secure DNS architecture is complex and difficult to implement. Network administrators should consider multiple facets of DNSSEC when planning an implementation. The following is a set of implementation recommendations with corresponding issues for administrators to consider for a successful implementation of DNSSEC.

The DNSSEC signing is mandated through OMB Mandate M-08-23, *Securing the Federal Government's Domain Name System Infrastructure*. The DNSSEC signing is only mandated for the external DNS zones and not for internal DNS zones. A first task for the administrator is to evaluate the current external name server.

The following are some questions that should be answered about the existing implementation prior to implementing DNSSEC signing.

Table 5: Implementing DNSSEC Signing

Questions	Steps to Resolve
Can our current external name servers support DNSSEC?	<p>Check the current versions and confirm that the DNSSEC signing is supported. The primary server must supporting DNSSEC signing while the secondary/slave only needs to support DNSSEC records.</p> <p>Review different options to deploy DNSSEC. If your current DNS environment cannot support DNSSEC, review the options (e.g. upgrade, replace, or outsource).</p>
Will our Firewall configuration support DNSSEC?	<p>DNSSEC records are larger than the typical DNS records. DNSSEC packets can be as big as 4096 bytes and sometimes TCP is used as a transport instead of UDP.</p> <p>For DNS servers sitting behind the FW, the setting for packet must be reviewed and tested. Firewalls should be set to allow DNS traffic to use both TCP and UDP on port 53.</p>
What exactly are our available DNSSEC capabilities?	<p>The encryption level and the NSEC3 capability should be reviewed carefully before signing the zone. Once the zone is signed with particular encryption level and/or NSEC3, changing the setting requires a set process of resigning zone data, which can be difficult.</p> <p>Review the various signing options and select the ones that meet the requirements.</p>
Can we automate DNSSEC	DNSSEC adds layer of administration that requires

administration?	considerable amount of time to do day-to-day functions such as adding or updating a DNS record. Consider automated scripts or automated tools to streamline the signing of the records as well as zone/key signing key roll-over process.
What do we do with the DNSSEC private key?	As with any PKI related products, the private key that signs the records must be maintained in a secure place. Once the key is compromised, all records must be unsigned and resigned with a different key. Develop methods to secure the private key. Identify and minimize who will have the access to the key.
How do we roll-over DNSSEC Keys?	While the KSK (key signing key) rollover is 1 year (recommended), the ZSK (zone signing key) is recommended to roll-over every month. Rolling over ZSK will be a considerable effort if done manually. Automate the zsk roll-over process by either scripting or implementing an automated tool.
How do I test DNSSEC signing?	Before signing your production zones, a pilot zone can and should be signed first to confirm the functionality. Visit http://www.dnsops.gov/ and participate in the pilot program.

6.5 DNSSEC Validation

DNSSEC validation is not covered under the current OMB Mandate M-08-23, *Securing the Federal Government's Domain Name System Infrastructure*. However, it should be considered as part of the DNSSEC implementation.

Table 6: Implementing DNSSEC Validation

Questions	Steps to Resolve
How do we set the Root Trust-Anchor?	Chain-of-anchor must be set manually (and out-of-band). The IANA website (https://www.iana.org/dnssec/) publishes the root zone DNSSEC trust anchor. Document and test the steps to load the trust anchor from the website into your recursive servers.
How do we avoid DNSSEC validation problems?	When other agencies make a DNSSEC configuration errors such as letting signatures expire or mismatching the DS and DNSKEY records, the result will be that your DNSSEC validation enabled servers will not able to resolve anything from the other agencies DNS server. Define a protocol on what will be done if and when misconfiguration or DNS attack is identified.
How will DNSSEC affect Recursive Server	DNSSEC validation will require additional processing power on your recursive servers. Obtain performance baseline

performance?	before validation is turned on and compare the performance metrics after the validation is enabled.
--------------	---

APPENDIX A: Acronyms – Common Abbreviations

ACL - Access Control List

BIND - Berkeley Internet Name Domain

CIO - Chief Information Officer

DDNS - Dynamic Domain Name System

DDoS - Distributed Denial of Service

DMZ – De-Militarized Zone

DNS - Domain Name System

DNSSEC - Domain Name System Security Extensions

DoS - Denial of Service

FIPS - Federal Information Processing Standards

FISMA - Federal Information Security Management Act

FW – Firewall

GSA - General Services Administration

IDPS - Intrusion Detection and Prevention Systems

IDS - Intrusion Detection System

IPS – Intrusion Prevention System

IP - Internet Protocol

ITILoB - Information Technology Infrastructure Line of Business

KSK - Key Signing Key

LAN - Local Area Network

NIST - National Institute of Standards and Technology

NSEC3 - Next Secure

NSTIC – National Strategy for Trusted Identities in Cyberspace

OMB - Office of Management and Budget

PKI - Public Key Infrastructure

RR – Resource Record

TCP - Transmission Control Protocol

TIC - Trusted Internet Connections

TSIG - Transaction Signature

UDP - User Datagram Protocol

VPN - Virtual Private Network

WG - Working Group

ZSK - Zone Signing Key

APPENDIX B: Glossary – Common Terms and Definitions

Authoritative Server: A server that knows the content of a DNS zone from local knowledge, and thus can answer queries about that zone without needing to query other servers.

Berkeley Internet Name Domain (BIND): BIND is the most commonly used implementation of the Domain Name System (DNS) protocols. BIND provides a robust and stable platform on top of which organizations can build distributed computing systems with the knowledge that those systems are fully compliant with published DNS standards.

Cache: A component that transparently stores data so that future requests for that data can be served without contacting the original host.

Cache Poisoning: A malicious attack that compromises the integrity of DNS by redirecting the domain to a different IP address.

Demilitarized Zone (DMZ): The DMZ (or Service Network) is a perimeter network segment that enforces the internal network information assurance policy for external information exchange.

Denial of Service (DoS): Intentionally or unintentionally overloading a computer resource to make a service unavailable.

DNS Security Capabilities: Requirements that cover industry best practice security measures for DNS

Domain Name System (DNS): DNS is a hierarchical, distributed database for any resource connected to the Internet or private network that translates readable domain names to IP addresses.

Domain Name System Security Extensions (DNSSEC): DNSSEC is a suite of specifications that provides origin authentication, authenticated denial of existence, and data integrity to DNS clients (resolvers). DNSSEC was designed to prevent cache poisoning and does not provide services for availability or confidentiality.

Intrusion Detection: The process of monitoring the events occurring in a computer system or network and analyzing them for signs of potential incidents.

Intrusion Detection and Prevention System (IDS/IPS or IDPS): Identifies potential incidents, logging information about them, attempting to stop them, and reporting them to security administrators.

Intrusion Prevention: The process of performing intrusion detection and attempting to stop detected potential incidents.

Listed Server: An Authoritative Server for which there is an NS resource record (RR) in the zone.

Name Server (NS): Provides responses to name resolution queries. An authoritative name server for a zone provides responses to name resolution queries for resources for that zone, using the Resource Records (RRs) in its own zone file.

NSEC3: The purpose of an NSEC (Next Secure) record is to prove that no records exist between two different points. NSEC3 records use hashes to prevent queries from reporting what records do exist.

NSTIC: The National Strategy for Trusted Identities in Cyberspace is a White House initiative to work collaboratively with the private sector, advocacy groups, public sector agencies, and other organizations to improve the privacy, security, and convenience of sensitive online transactions.

Primary Server: An authoritative server for which the zone information is locally configured. A Primary Server is also known as a Master Server.

Public Facing Name: A name server which responds to queries from external networks.

Private Name Server: A name server which does not respond to queries from external networks.

Recursive Caching Name Server: A server that combines both caching and recursive functions in the same Name Server. These servers store DNS query results for a period of time (caching), and also implement the recursive algorithm necessary to resolve a given name starting with the DNS root through to the authoritative name servers of the queried domain. The combination of these two functions in one name server is not mandatory; the functions can be implemented independently in servers for special purposes

Recursion: A method of defining functions (or protocols) in which the function being defined is applied within its own definition.

Resolver: A client of the DNS which seeks information contained in a zone using the DNS protocols.

Resource Records (RRs): RRs are the basic data elements in the domain name system. RRs translate Domain Names to IP addresses. When sent over an IP network, RRs use the common format specified in RFC 1035 (NAME, TYPE, CLASS, TTL, RDLENGTH, and RDATA).

Secondary Server: An authoritative server that obtains information about a zone from a Primary Server via a zone transfer mechanism. A Secondary Server is also known as a Slave Server.

Server: An implementation of the DNS protocols able to provide answers to queries. Answers may be from information known by the server, or information obtained from another server.

Stealth Server: An authoritative server, usually a secondary server, which is not a Listed Server.

Transaction Signatures: Transaction signatures provide a means of authenticating queries between servers, including updates to a Dynamic DNS database. TSIG uses shared secret keys and one-way hashing to provide a cryptographically secure means of identifying each endpoint of a connection as being allowed to make or respond to a DNS update.

Transmission Control Protocol (TCP): TCP provides reliable, ordered delivery of a stream of bytes on an Internet Protocol (IP) network from a program on one computer to another program on another computer. TCP, along with UDP, are the two core Network Protocols in the Internet Protocol Suite.

User Datagram Protocol (UDP): UDP allows computer applications to send messages (datagrams) to other hosts on an Internet Protocol (IP) network without requiring prior communications to set up special transmission channels or data paths. UDP provides an unreliable service and datagrams may arrive out of order, appear duplicated, or go missing without notice. UDP assumes that error checking and correction is either not necessary or performed in the application, avoiding the overhead of such processing at the network interface level. UDP, along with TCP, are the two core Network Protocols in the Internet Protocol Suite.

Zone: A DNS zone is a portion of the global DNS namespace for which administrative responsibility has been delegated.

Zone Transfer: A DNS function used to replicate DNS databases across other DNS servers.

APPENDIX C: Selected Existing Guidance

The origin for this initiative is OMB M-08-23. The following OMB Memoranda impact this Reference Architecture:

- OMB M-08-23: *Securing the Federal Government's Domain Name System Infrastructure*

A comprehensive list of applicable legislation, policies, directives, regulations, memoranda, standards, and guidelines can be found in the following:

LEGISLATION

E-Government Act [includes FISMA] (P.L. 107-347), December 2002.

POLICIES, DIRECTIVES, REGULATIONS, AND MEMORANDA

National Security Presidential Directive (NSPD) 54, *Cyber Security and Monitoring*, 8 January 2008. Also known as HSPD-23.

Homeland Security Presidential Directive (HSPD) 23, *Computer Network Monitoring and Cyber-security*, 8 January, 2008. Also known as NSPD-54.

Office of Management and Budget (OMB) Memorandum M-05-22, *Transition Planning for Internet Protocol Version 6 (IPv6)*, 2 August 2005.

Office of Management and Budget (OMB) Memorandum M-07-06, *Validating and Monitoring Agency Issuance of Personal Identity Verification Credentials*, 11 January 2007.

Office of Management and Budget (OMB) Memorandum M-08-05, *The Trusted Internet Connection initiative (TIC)*, November 2007.

National Security Telecommunications And Information Systems Security Committee NTTISSP 101, *National Policy on Securing Voice Communications*, 14 September 1999.

STANDARDS

Homeland Security Presidential Directive 7, *Critical Infrastructure Identification, Prioritization, and Protection*, December 2003.

Office of Management and Budget Memorandum M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, October 2001.

General Services Administration (GSA), Public Buildings Service (PBS), *Facilities Standards (P100)*, 2009.

Federal Information Processing Standard (FIPS) Publication 140-2, *Security Requirements for Cryptographic Module*, 3 December 2002.

Federal Information Processing Standard (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.

Federal Information Processing Standard (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006.

Federal Information Processing Standard (FIPS) Publication 201-1, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, March 2006.

IEEE 802.1X: IEEE Standard for port-based Network Access Control (PNAC).

GUIDANCE

Federal CIO Council, *Considerations for Federal Agency Implementation of DNS Security Extensions and Email Authentication*, June 2011.

NIST's Information Technology Laboratory, ITL Security Bulletins, *An Introduction to Secure Telephone Terminals - ITL Security Bulletin*, March 1992.

National Institute of Standards and Technology Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook*, October 1995.

National Institute of Standards and Technology Special Publication 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, September 1996.

National Institute of Standards and Technology Special Publication 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006.

National Institute of Standards and Technology Special Publication 800-29, *A Comparison of the Security Requirements for Cryptographic Modules in FIPS 140-1 and FIPS 140-2*, June 2001.

National Institute of Standards and Technology Special Publication 800-34, Revision 1, *Contingency Planning Guide for Information Technology Systems*, May 2010.

National Institute of Standards and Technology Special Publication 800-35, *Guide to Information Technology Security Services*, October 2003.

National Institute of Standards and Technology Special Publication 800-39 *Managing Information Security Risk: Organization, Mission, and Information System View*, March 2011.

National Institute of Standards and Technology Special Publication 800-41, Revision 1, *Guidelines on Firewalls and Firewall Policy*, September 2009.

National Institute of Standards and Technology Special Publication 800-44, Version 2, *Guidelines on Securing Public Web Servers*, September 2007.

National Institute of Standards and Technology Special Publication 800-45, Version 2, *Guidelines on Electronic Mail Security*, February 2007.

National Institute of Standards and Technology Special Publication 800-46, Revision 1, *Guide to Enterprise Telework and Remote Access Security*, June 2009.

National Institute of Standards and Technology Special Publication 800-47, *Security Guide for Interconnecting Information Technology Systems*, August 2002.

National Institute of Standards and Technology Special Publication 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009.

National Institute of Standards and Technology Special Publication 800-53A, Revision 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans*, June 2010.

National Institute of Standards and Technology Special Publication 800-57 (Revised), *Recommendation for Key Management*, March 2007.

National Institute of Standards and Technology Special Publication 800-61, Revision 1, *Computer Security Incident Handling Guide*, March 2008.

National Institute of Standards and Technology Special Publication 800-73-3, *Interfaces for Personal Identity Verification*, February 2010.

National Institute of Standards and Technology Special Publication 800-76-1, *Biometric Data Specification for Personal Identity Verification*, January 2007.

National Institute of Standards and Technology Special Publication 800-78-3, *Cryptographic Algorithms and Key Sizes for Personal Identification Verification (PIV)*, December 2010.

National Institute of Standards and Technology Special Publication 800-81, Revision 1, *Secure Domain Name System (DNS) Deployment Guide*, April 2010.

National Institute of Standards and Technology Special Publication 800-86, *Guide to Integrating Forensic Techniques into Incident Response*, August 2006.

National Institute of Standards and Technology Special Publication 800-92, *Guide to Computer Security Log Management*, September 2006.

National Institute of Standards and Technology Special Publication 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS)*, February 2007.

National Institute of Standards and Technology Special Publication 800-100, *Information Security Handbook: A Guide for Managers*, October 2006.

National Institute of Standards and Technology Special Publication 800-113, *Guide to SSL VPNs*, July 2008.

National Institute of Standards and Technology Special Publication 800-114, *User's Guide to Securing External Devices for Telework and Remote Access*, November 2007.

National Institute of Standards and Technology Special Publication 800-123, *Guide to General Server Security*, July 2008.

Office of Management and Budget Memoranda, M-08-16, *Guidance for Trusted Internet Connection Statement of Capability Form (SOC)*, 4 April 2008.

Office of Management and Budget Memoranda, M-08-26, *Transition from FTS 2001 to NETWORX*, 28 August, 2008.

Office of Management and Budget Memoranda, M-08-27, *Guidance for Trusted Internet Connection (TIC) Compliance*, 20 September 2008.

Office of Management and Budget Memoranda, M-09-32 *Update on the Trusted Internet Connections Initiative*, 17 September 2009.