DNS Security Battle Card

		DNS Server Role (Trust Sector)			
		Recursive	Internal authoritative	External authoritative	External hosted DNS
Control scope	Deployment	o Deploy dedicated and redundant recursive DNS servers to process client DNS queries o For moderate to large networks, deploy forwarder DNS servers near client populations and a set of more powerful recursive servers near Internet connections	o Deploy dedicated and redundant authoritative DNS servers to process internal client DNS queries o Deploy a hidden master to protect against authoritative poisoning	o Deploy dedicated authoritative DNS servers to process DNS queries for your namespace from the Internet o Deploy a hidden master to protect against authoritative poisoning o Configure anycast addressing across multiple external DNS servers o Consider use of an external DNS hosting provider to supplement capacity and as a DDoS defensive measure	o Consider use of self-managed DNS servers and/or multiple external DNS hosting providers to supplement capacity and as a DDoS defensive measure
	Routing controls	o Prevent externally spoofed query packets by configuring router/firewall IP address filtering using reverse path forwarding o Permit outbound DNS queries only from authorized recursive servers. o Block inbound DNS queries from the Internet (permit only to external authoritative DNS servers) o Prevent administrative access except from the "management" (i.e., internal) IP address space	o Prevent externally spoofed query packets by configuring router/firewall IP address filtering using reverse path forwarding o Block inbound DNS queries from the Internet (permit only to external authoritative DNS servers) o Prevent administrative access except from the "management" (i.e., internal) IP address space	o Prevent externally spoofed query packets by configuring router/firewall IP address filtering using reverse path forwarding o Block inbound DNS queries from the Internet (permit only to external authoritative DNS servers) o Prevent administrative access except from the "management" (i.e., internal) IP address space	o Block inbound DNS queries from the Internet (permit only to external authoritative DNS servers if you've deployed them)
	Server controls	o Apply physical security controls (maintain inventory, harden operating system, constrain physical server access, audit server room access logs, control server movement, monitor environmentals) o Apply server access controls (change default vendor login IDs/passwords, define logins as necessary with least privilege, secure remote access, audit access logs) o Monitor security dispatches, prudently apply patches for operating system/kernel as well as DNS vendor software	o Apply physical security controls (maintain inventory, harden operating system, constrain physical server access, audit server room access logs, control server movement, monitor environmentals) o Apply server access controls (change default vendor login IDs/passwords, define logins as necessary with least privilege, secure remote access, audit access logs) o Monitor security dispatches, prudently apply patches for operating system/kernel as well as DNS vendor software	o Apply physical security controls (maintain inventory, harden operating system, constrain physical server access, audit server room access logs, control server movement, monitor environmentals) o Apply server access controls (change default vendor login IDs/passwords, define logins as necessary with least privilege, secure remote access, audit access logs) o Monitor security dispatches, prudently apply patches for operating system/kernel as well as DNS vendor software	o Assign service access controls (change default vendor login IDs/passwords, define logins as necessary with least privilege, secure remote access, audit access logs)
	DNS controls	o Allow recursive queries only from lower tier forwarder DNS servers (local recursive servers) and/or internal clients using your allocated internal (e.g. private, ULA) address space. o Allow query access to cache to lower tier forwarders and/or internal clients o Allow recursion, queries and access to cache only on the server interface possessing the internal IP address. This will help prevent spoofed queries received on other server interfaces (e.g., DMZ-facing). o Configure dnsCrypt or DNS cookies to protect the client-recursive server link o Disallow dynamic updates and zone transfers o Inhibit exposure to the server implementation to the extent possible o Define query rate limits o Configure DNSSEC validation o Configure DNS firewall o Monitor queries and responses for anomaly identification, tunneling detection and query auditing	o Disallow recursive queries o Sign zone transfers between the master and slave servers o Allow notify's and zone transfers only among the master and slaves o For the hidden master, allow queries only from the slaves' IP addresses o Inhibit exposure to the server implementation to the extent possible o Configure inbound rate limiting to protect against DDoS attacks; consider anycast deployment as well o Consider implementation of DNS cookies o Protect authoritative data from attack and sign with DNSSEC o Monitor queries and responses for anomaly detection and auditing	o Disallow recursive queries o Sign zone transfers between the master and slave servers o Allow notify's and zone transfers only among the master and slaves o For the hidden master, allow queries only from the slaves' IP addresses o Inhibit exposure to the server implementation to the extent possible o Configure response rate limiting to protect against reflector attacks o Protect authoritative data from attack and consider signing with DNSSEC o Monitor queries and responses for anomaly detection and auditing o Query/audit your namespace periodically to detect unauthorized changes	o Protect authoritative data from attack and sign with DNSSEC o Monitor queries and responses for anomaly detection and auditing o Query/audit your namespace periodically to detect unauthorized changes in your delegation or resource record information