Domain Name System (DNS)

What is it?

Domain Name System (DNS) is the fundamental backbone of the internet.

The DNS allows us to search the internet with words, instead of long, hard-to-remember numbers.

Every domain name on the internet relies on the DNS to help people find a website and receive their email.

- For example, GoDaddy.com's IP address is 208.109.192.70
  - — User enters GoDaddy.com (domain name) in a browser.
  - — DNS converts the domain name to an IP address and finds the route to that server.
  - — Website is displayed on the user's computer.

Why Is it important?

Understanding DNS is important as it is a common reason for many interactions with our customers. If a customer's DNS is set up incorrectly, then visitors won't be able to find their website and customers won't be able to get their email.

You will interact with DNS often in many different ways. For example, when you work with US Locality domains, you may find that the label or domain name is set up in the DNS only.

DNS Security Extensions (DNSSEC)

What is it?

DNSSEC, short for **Domain Name System Security Extensions**, is a technology upgrade that **protects against attacks by digitally 'signing' data with keys so you can be assured it is valid**. Within our Registry platform, agents may assist customers by securing domain names with these keys.

How does it work?

DNSSEC services protect against threats to the Domain Name System (DNS), including cache poisoning (see next page).

- In order to eliminate the threat from the internet, DNSSEC must be deployed at each step in a DNS route, from root zone to final domain name (e.g., www.example.co).
- Note that **DNSSEC does not encrypt data**. Instead, it attests to the validity of the address of the site you visit.

DNSSEC provides:

- origin authentication of DNS data
- data integrity
- authenticated denial of existence

For additional information on DNSSEC, review this video:

- DNSSEC Overview

DNSSEC and Cache Poisoning

What is it?

The simplest form of **cache poisoning**, also known as a **man-in-the-middle attack**, is **sending fake "answers" to a user's DNS server**.

- DNS servers constantly send out questions ("What's the IP address of www.example.co?") and receiving answers ("www.example.co is at 209.237.229.14").
- The servers don't authenticate the source of the answers.

With DNSSEC, the server sends back an authenticated answer ensuring the user that the website viewed is the actual website requested and that a potential security vulnerability is not being exploited.