The Domain Name System (DNS) provides a critical service for the Internet. The DNS acts as an online directory, translating easy-to-remember domain names (e.g., govtech.com) into an IP address (e.g., 52.44.42.61). Unfortunately, traditional DNS lookups are inherently insecure. While website owners can mitigate these security vulnerabilities, few state governments have taken the necessary steps to do so.

Although Internet users routinely rely on the DNS, most are unaware of its importance because DNS lookups run imperceptibly in the background. After a user enters a website domain name in a browser, his or her computer sends out a request for the relevant record from a DNS server that recursively queries other DNS servers until it finally finds one that gives an authoritative answer. However, the original DNS specifications do not require the servers to authenticate the responses they receive or verify that they are correct. As a result, attackers can exploit these weaknesses in the DNS system to hijack users' connections and redirect them to malicious sites that may steal their passwords or expose them to malware.

While security researchers identified these security weaknesses in the DNS in the early 1990s, it was not until 1997 that network engineers created the first draft of DNS
security extensions, or DNSSEC. DNSSEC is a technical standard for the Internet that adds cryptographic signatures to DNS records to create a chain of trust, so that users can be confident that they have received a valid response and they are not being subjected to a man-in-the-middle attack. This chain of trust has extended all the way to the root zone, the part of the DNS that contains all of the top-level domains, since July 15, 2010.

It has taken some time to implement DNSSEC. The federal government deployed the system to the .gov top-level domain name in January 2009 and mandated that all agencies implement DNSSEC on their domains by December of the same year. In September 2010, 36 percent of federal agency domains had properly implemented DNSSEC. As of last year, 90 percent of popular federal government websites had properly enabled DNSSEC, and the National Institute of Standards and Technology tracks more than 800 federal domains that have properly signed DNS records.

However, a forthcoming study from the Information Technology and Innovation Foundation has found that state governments have been much slower at adopting DNSSEC. In 2010, only three states — Idaho, Vermont and Virginia — had implemented DNSSEC on at least one of its domains. Not much has changed. Today, only nine states have implemented the standard on at least one of their primary government website domains. A few — including Kentucky, Massachusetts, Minnesota, New Jersey, Vermont and Virginia — had implemented it on most, but not all, of their domains. And only one state, Idaho, had implemented DNSSEC on all its domains. The vast majority of states have not implemented it at all.

It is not entirely clear why more state governments have not made DNSSEC a greater priority. While implementation can raise some technical challenges, the widespread adoption in federal government shows these hurdles can be overcome. More likely, the lack of adoption reflects the fact that DNSSEC is an investment in security for users rather than government agencies. Many government security investments — network firewalls, two-factor authentication, intrusion detection systems — focus on making the government itself more secure from attacks. While DNSSEC certainly benefits government users too, the primary beneficiaries are average citizens who can access government services more securely because DNSSEC validates that they are being directed to the correct site and are not caught in a man-in-the-middle attack.

Given that it has been more than two decades since security researchers identified vulnerabilities in the DNS, states have no excuse for further delaying implementation of DNSSEC, and they should move expeditiously to implement it on all state government domains.