



Strengthening Cybersecurity Through NSA's Protective Domain Name Service

Last updated: September 2024

In today's rapidly evolving digital landscape, cybersecurity has become a top concern for businesses worldwide. As part of our commitment to ensuring the security of the data entrusted to us by our customers and the resiliency of our operations, we would like to **introduce you** to a valuable resource provided by the National Security Agency (NSA) Cyber Collaboration Center (CCC) that can enhance the security of your company's online presence.

NSA Protective Domain Name Service (PDNS)

What is NSA PDNS?

NSA PDNS is designed to safeguard against a wide range of cyber threats, particularly those targeting Domain Name Systems (DNS). It combines commercial cyber threat feeds with NSA's unique insights to filter external DNS queries and block known malicious or suspicious website traffic, mitigating nation-state malware, spear phishing, botnets, and more.

While implementing NSA PDNS or a similar DNS capability is entirely voluntary, it is a significant step toward fortifying your cybersecurity posture and ensuring the safety of your digital assets. We encourage you to explore the benefits of this or a similar service and consider integrating or supplementing it into your own cybersecurity strategy.

How to get more information?

DoD contractors can get started with NSA PDNS or learn more about other cybersecurity services offered by NSA CCC, by visiting their [website](#), contacting DIB_Defense@cyber.nsa.gov, or filling out a contact request form provided [here](#).

We value the partnership we share and believe that proactive collaboration is key to safeguarding our businesses against cyber threats.