Government Protective DNS Module

In an era where digital threats continuously evolve, the US Federal Government stands at the forefront, needing fortified digital barriers more than ever. Recognizing the nuances and complexities of federal operations, the iboss Government Protective DNS Module is the gold standard in cybersecurity.

Developed in line with the rigorous standards and guidelines set by agencies such as the NSA and CISA, this solution offers a multi-pronged approach, ensuring every DNS query is meticulously screened for threats. With features like DNS Rate Limiting and comprehensive DNS security, iboss ensures the highest levels of protection and compliance for the government's digital assets.

The Government Protective DNS Module makes it easy for Government Agencies to integrate with CISA's Protective DNS and provides. The iboss Zero Trust SSE provides each Government Agency unique and dedicated IP addresses that are needed when connecting to CISA's Protective DNS offering. The iboss platform also encrypts and logs all DNS queries to help agencies quickly and easily meet the requirements from OMB

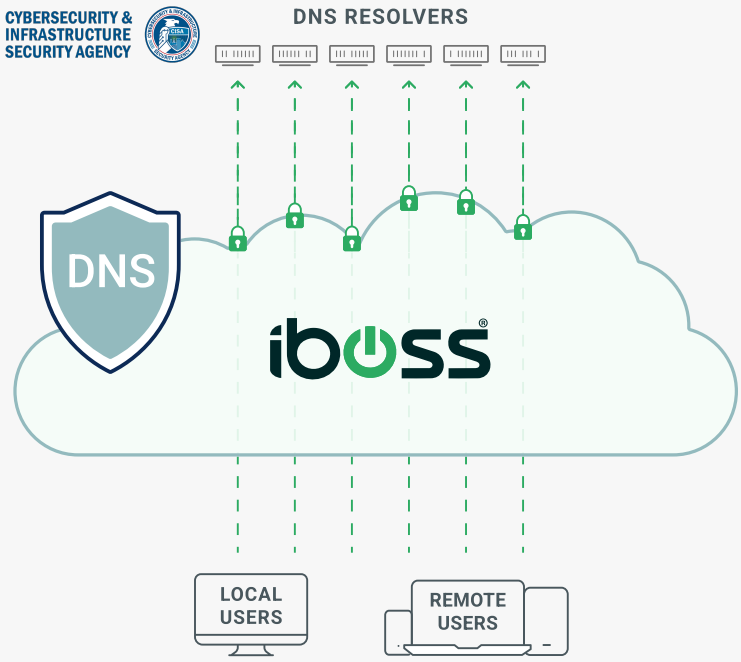
M-21-31 and M-22-09. This includes encrypting DNS from remote workers and encrypting and forwarding DNS from systems without these capabilities. The iboss Zero Trust SSE is the fastest and easiest way for Government Agencies to integrate with CISA and meet DNS requirements.

BENEFITS

- Built to easily meet government DNS requirements in OMB M-21-31 and M-22-09, ensuring complete compliance.
- Advanced Threat Detection and DNS Rate Limiting to detect and thwart threats like DNS tunneling and phishing attempts.
- Forwards logs to SIEMs in real-time, meeting OMB logging requirements.
- Encrypts DNS queries, including from remote workers, and centrally captures, secures and logs to meet OMB requirements.
- Provides the necessary per-agency dedicated IP addresses needed to integrate with CISA's Protective DNS resolvers.
- Forwards all DNS queries to CISA's Protective DNS Resolvers for all infrastructure and agency workers, regardless of location.

Government Protective DNS Module

Government agencies can now deploy encrypted DNS across all devices and integrate with CISA's Protective DNS service with ease. The Government Protective DNS Module helps Government agencies easily meet the encrypted DNS security and logging requirements of OMB M-21-31 and M-22-09. The iboss platform provides the necessary unique per-agency IP Addresses required by CISA to integrate with CISA's Protective DNS.



Ordering Information

SKU: Government Protective DNS Module

Required Package: Zero Trust Advanced or Higher

HOW IT WORKS

- **Provide CISA with iboss provided and Agency Dedicated IP Addresses:** The iboss Zero Trust SSE provides unique IP Addresses that will forward DNS queries to CISA's PDNS. Provide the iboss IP Addresses into CISA's PDNS service.
- **Configure iboss to forward DNS to CISA:** Enter the IP Addresses of CISA's PDNS resolvers into the iboss platform. The iboss platform will forward all DNS queries to CISA.
- **Install iboss Agents:** Deploy iboss Cloud Connector agents on government devices, ensuring DNS requests are encrypted and secure, even outside federal networks.
- **Forward DNS from OT/IoT to iboss:** iboss will provide protection for the DNS queries and forward them to CISA's PDNS resolvers.
- **Agency-Wide Protection:** All DNS queries will be redirected through iboss, which applies security and logs the request, then forwards to CISA PDNS meeting OMB M-21-31 and M-22-09 DNS requirements.