infoblox

Horizon 2 Consultation Responses

Executive Summary

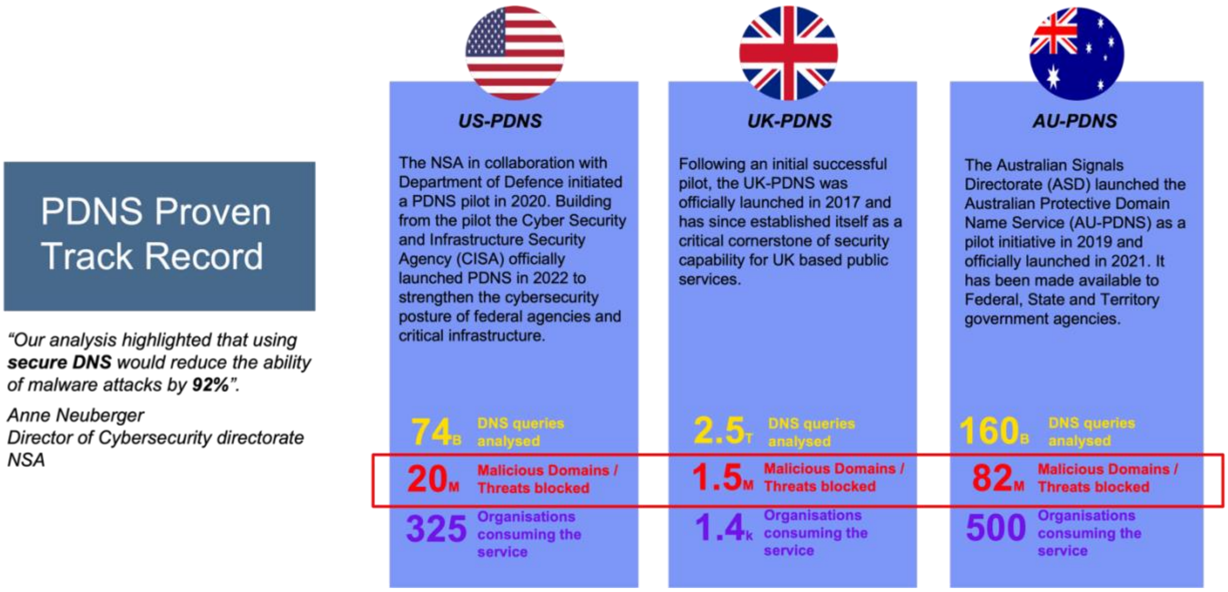
Infoblox welcomes the opportunity to contribute to Horizon 2. We support the Australian Government's objective of scaling cyber maturity across the whole economy and to strengthen the six "cyber shields" framework.

Infoblox, Inc. is a global company headquartered in the United States specializing in Domain Name System (DNS) management and security and related services such as Dynamic Host Configuration Protocol (DHCP) and Internet Protocol Address Management (IPAM).

Our products are used by government agencies and critical infrastructure organizations around the world, and over 90% of the Fortune 100 companies and 70% of the Fortune 500 companies.

Grounded in Infoblox's 25 years of expertise in DNS management and threat intelligence, this submission directly responds to the consultation's priority areas and provides Australian Government entities with proven, best-practice approaches to strengthening their defenses against an evolving cyber threat landscape.

The DNS is a foundational layer of the internet and an ideal control point for proactive cyber defense. Virtually every online activity begins with a DNS query, so security controls at the DNS layer can block threats before they reach users. DNS has been around for over 40 years. However, it is only in the last five years that we have seen widespread adoption of DNS-based security capabilities by governments. The reason for this rapid uptake has been the ability of DNS security controls to block threats at scale. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) reported that DNS security controls blocked nearly 700 million connection attempts from U.S. federal agencies to malicious domains in 2022-23.



Protective DNS statistics across AUKUS governments – source:

As Australia moves to Horizon 2 of the Cyber Strategy, Infoblox believes that DNS security controls should be applied at a similar scale to protect Small and Medium Businesses (SMBs), not-for-profits and wider industry from the rising costs of cyber-crime. The success of the Australian government Protective DNS (PDNS) service highlights the value of DNS as a cyber security control. Standardizing Protective DNS across the broader economy is an opportunity to vastly improve the scale and efficacy of malware and fraud prevention.

The value of Protective DNS services extends well beyond blocking known threats at scale. Protective DNS infrastructure also generates rich, machine-readable threat intelligence that can proactively identify and disrupt malicious activity. By analyzing DNS traffic patterns, governments and operators can uncover the DNS "backbone" of criminal enterprises that rely on thousands of domains to host malware, deliver scams, and orchestrate fraud. For example, research into the Vextrio "Viper" network found it controls more than 70,000 malicious domains used by dozens of affiliate operators to distribute malware and launch large-scale fraud campaigns, often evading traditional endpoint or email-based defenses (see Krebs on Security, July 2023). This demonstrates how DNS-based exploitation tactics are being deployed at industrial scale. Leveraging DNS-derived intelligence is therefore essential to detect, attribute, and block these kinds of systemic threats.

This approach directly supports directive 003-2024 in the July 2024 Protective Security Policy Framework (PSPF), which requires agencies to share cyber threat information with the Australian Signals Directorate (ASD). In the case of DNS-generated threat intelligence, the sharing of

Protective DNS logs and DNS queries blocked due to their association with malicious activity, provides automated and actionable machine-readable threat intelligence. It also provides the Australian Signals Directorate (ASD) with the opportunity to understand the threat actor landscape based on the DNS footprint of the threat actors.

The value of PDNS has been made clear by its widespread adoption in key global economies and the increasing incorporation of DNS controls into a range of compliance regimes. On January 16, 2025, the White House issued an Executive Order mandating encrypted DNS protocols to ensure the confidentiality and integrity of DNS traffic. Similarly, in April 2025, the National Institute of Standards and Technology (NIST) released a draft update to NIST Special Publication 800-81: *the Secure DNS Deployment Guide*, highlighting three pillars of secure DNS practices and defining DNS-based resilience. This includes not only Protective DNS but recommendations for securing critical DNS infrastructure and ensuring the integrity of the DNS. Finally, the European Union's NIS2 technical implementation guidance includes secure DNS best practices that mirror NIST SP 800-81. NIS2 technical requirements call for Protective DNS, dedicated DNS servers to ensure resiliency, and maintaining DNS/DHCP logging for incident response.

The DNS system itself is both a systemic risk but also a highly scalable platform for threat mitigation on a national scale. Based on the empirical evidence of the value of PDNS as a security control that works on a macro scale and the rapid policy uptake of it in allied and partner jurisdictions like the U.S. and EU, Infoblox recommends the Department of Home Affairs consider incorporating similar Secure DNS requirements as central feature Australian cyber-security policy under Horizon 2.

Shield 1 — Strong businesses and citizens

Recommended Actions:

1. **Promote Secure DNS Best Practices and DNSSEC:** Beyond network-level protective services, businesses and citizens should be guided toward secure DNS configurations as part of basic cyber hygiene. The Government’s cyber awareness messaging (which the Horizon 2 paper seeks to consolidate) should include simple, actionable advice such as: “Use a reputable DNS resolver with security filtering,” and “Ensure your domain names have DNSSEC enabled.” DNSSEC (DNS Security Extensions) is critical for preventing DNS hijacking and ensuring the authenticity of DNS answers. Currently, few commercial hosting providers turn

on DNSSEC by default, leaving many Australian business domains vulnerable. We recommend a focused effort to increase DNSSEC uptake that Government takes the lead by mandating DNSSEC on all .gov.au domains and validating DNSSEC on government resolvers) and include DNSSEC status in cyber security best-practice checklists. By implementing DNSSEC on their principal domains, organizations guard against attackers redirecting customers to fake websites– a simple step that protects brand trust and citizens from fraud. In addition, the Government should encourage use of encrypted DNS protocols (DNS over HTTPS/TLS) in tandem with protective filtering. Encrypted DNS helps protect citizens' queries from eavesdropping and clear guidance can help users balance privacy and security.

2. **Continue Uplifting Small Businesses and NFPs with Scalable Services:** Small and medium businesses and not-for-profits face unique challenges – they often lack dedicated IT security staff and can be overwhelmed by complex guidance. Horizon 2 rightly focuses on uplifting cyber standards for SMBs and encouraging uptake of resources like the Small Business Cyber Resilience service and "Cyber Wardens" training programs. We submit that scalable, managed security services like protective DNS are among the most impactful supports for this sector. Government should partner with industry associations and Managed Service Providers to bundle secure DNS, email filtering, and other basics into easy packages for SMBs consumption. One example would be the delivery of a DNS Domain Monitoring service. Many smaller organizations fall victim to threat actors who hijack or impersonate legitimate domains via registration of "lookalike" domains. Two thirds of phishing campaigns leverage "lookalikes." but it is unrealistic to expect each SMB or non-profit to manage this risk. A government supported service would have the benefits of scale and centralized expertise to help smaller organizations mitigate these risks and would remove cost and complexity barriers, allowing even the smallest firms to immediately improve their defenses against phishing, malware and online scams. By reducing the effort and expertise required to deploy protections, we can empower small businesses and nonprofits to actively defend themselves and their customers online. This aligns with the Strategy's intent to encourage SMBs to use available cyber resources and will make the economy more resilient.

3. **Secure DNS Adoption Services:** To drive policy to outcomes and to supplement the value of managed services and centralized Protective DNS services, provision should be made to enable smaller organizations to secure their existing DNS infrastructure. A Secure DNS adoption program that provides free education and assessment tools can facilitate these organizations to apply basic cyber hygiene for DNS. In partnership with vendors and system

integrators, a program can enable these organizations to deploy a secure by design infrastructure that can also seamlessly integrate with other government or MSSP services. This includes implementation of DNS query logging and integration with security operations tools such as SIEM's.

Shield 3 — World-class threat sharing and blocking

Recommended Actions:

1. **Scale Up Threat Intelligence Exchange Mechanisms:** Infoblox recommends the Government invest in trusted platforms and partnerships that make sharing easier and safer. This could involve expanding the Joint Cyber Security Centers (JCSCs) as hubs for threat information exchange at the state/regional level, with dedicated programs to onboard SMBs and local governments into intel sharing circles.

   Creating new Information Sharing and Analysis Centers (ISACs) for under-represented sectors is another priority. We suggest sectors like local government, healthcare, and the not-for-profit community would greatly benefit from their own threat-sharing forums, given they increasingly face cyber threats but often lack tailored intelligence. Government can kick-start these ISACs by convening stakeholders, providing baseline funding, and offering automated threat feed services to participants.

   Importantly, Australia should also leverage existing international ISACs where possible to avoid building overly insular or cost-heavy models, while recognizing that the Australian regulatory landscape and sectoral risk profile remain unique and will require tailored approaches. By normalizing real-time intel exchange with global partners – whether through machine-readable feed– Australia can ensure that a threat seen by one is quickly known to all. The faster threat insights circulate, the faster Australia can block attacks nation-wide.

2. **Improve Readiness for Cyber Crises Through Sharing and Exercises:** The world-class threat sharing and blocking shield must also extend to how major cyber incidents or conflicts are handled. We recommend clarifying and exercising the roles of government and industry in such scenarios, as the consultation paper probes. A critical activity is joint cyber incident exercises that simulate large-scale attacks to practice coordinated response. **These could be**

conducted under Australia's National Cyber Exercise Program, ensuring alignment with existing national preparedness frameworks and avoiding ad hoc or duplicative drills.

During these drills, the mechanisms for intelligence sharing and threat blocking should be tested: e.g., how quickly can ACSC push out an emergency blocking rule via DNS to all telecom providers? Who has authority to take decisive actions like sinkholing a malicious domain at the .au registry level if needed? These questions should be addressed in Horizon 2 planning, with the goal that both government and industry participants feel "better prepared to respond in a cyber conflict or crisis". The outcome of this programmatic approach will be a clearly defined playbook for collaborative cyber defense, where threat intelligence flows unimpeded and pre-agreed blocking actions can mitigate an attack's impact. Encouraging businesses to adopt vulnerability disclosure policies – potentially through incentives or recognition – will cultivate more intelligence about weaknesses before adversaries exploit them.

Shield 4 – Protected Critical Infrastructure

Recommended Actions:

1. **Expand and Scale Protective DNS across all critical sectors:** The Government should expand the Australian Protective DNS (AUPDNS) program beyond government agencies to cover operators of critical infrastructure (energy, finance, health, telecom, etc.). PDNS can automatically block domain-based threats (phishing, malware, C2) *before* they reach critical systems. By onboarding critical infrastructure entities to a national PDNS, starting with those entities designated as Systems of National Significance, Australia can prevent high-impact attacks (like ransomware or supply chain intrusions) at scale. This not only protects the target institutions but also reduces cascading effects across the economy. Infoblox recommends making PDNS enrollment a baseline expectation in critical infrastructure sectors, with Government facilitating easy adoption (e.g. via managed service offerings or public-private partnerships). This will ensure that even organizations with limited security staff benefit from world-class threat blocking and intelligence.

2. **Incorporate DNS security into critical infrastructure standards:** We urge the Government to embed **Secure DNS requirements** into the SOCI Act rules and other relevant security standards for critical infrastructure. This means requiring that essential service providers follow DNS hardening best practices – for example, using dedicated, redundant DNS servers

with DDoS protection, enabling DNSSEC on their domains, and logging DNS/DHCP activity for threat monitoring. As previously stated, both NIST and NIS2 frameworks highlight these measures as pillars of resilient infrastructure. Ensuring authentic and reliable DNS resolution is especially crucial for critical services; NIS2 places particular emphasis on DNSSEC to guarantee the integrity of DNS data for vital operations. We recommend Australia mirror these expectations. For instance, regulators could require all critical infrastructure operators to implement DNSSEC on their internet-facing domains (and the Government should lead by example by mandating DNSSEC across *.gov.au*). Likewise, requiring robust DNS redundancy (e.g. secondary DNS services or anycast networks) will improve availability and resistance to attacks. The DNS system is both a potential point of failure and a powerful mitigator of threats – it must be governed with the same rigor as other security controls. Adopting these measures in our critical infrastructure standards will raise the baseline and close gaps before adversaries exploit them.

We recommend any Secure DNS requirements mirror those of the NIS2 technical requirements and cite NIST Special Publication 800-81r3, which would align and harmonize Australian requirements with those of other global economies:

> "DNS security practices:
> - deploying DNS security extensions (DNSSEC),
> - deploying protective DNS, wherever technically feasible, to provide additional network-wide security capabilities,
> - encrypting DNS traffic, both internal and external, wherever feasible,
> - deploying dedicated DNS servers to reduce attack surface and
> - following all technical guidance on ensuring that DNS deployments and the DNS protocol are as secure and resilient as possible."

3. We further recommend that **DNS security logs, DHCP log data, and IP address management log data should be included in requirements for incident response and reporting:** "DNS security log data" refers to records generated by a network security system that capture details about DNS requests, particularly those flagged as potentially malicious. DNS security logs provide insights into suspicious network activity like malware attempts or phishing domains, enabling administrators to investigate threats based on the queried domains and related information.

In the event of a cyber incident, mapping a SOC alert to a device can be a difficult and time-consuming process, especially because some asset metadata such as IP address, network location and ownership are often *dynamic*. Most cyber-attacks begin with an IP address, yet in common organizational IP management schemes, the same IP address may often be reassigned to a different device and/or owner. Mapping an IP address to the compromised asset, specifically at the time of the attack, requires tracking key attributable metadata (network location, IP address, ownership, and data classification) on a real-time basis, together with a history of its allocation to each asset and resource. Organizations that are equipped with detailed DNS security logs, DHCP logs, and IP address management logs, mapped to relevant threat indicators, are better placed to track a threat actor as it moves across a compromised network, and to take swift action to remediate that threat.

4. **Strengthen threat intelligence sharing with critical infrastructure operators:** Protective DNS not only blocks threats but also produces high-quality, machine-readable threat data (e.g. queries to malicious domains) that can be shared in near-real-time. We recommend building formal channels to share DNS-derived threat intelligence between industry and government, specifically tailored to critical infrastructure needs. Horizon 2 initiatives for *"developing playbooks to guide incident responses"* should include protocols for rapid DNS-based action: for example, if a new malware campaign targeting the energy sector is observed, ACSC could swiftly push a blocking rule via PDNS or work with domain registries to sinkhole malicious domains. Joint cyber exercises for critical sectors should test this mechanism. By leveraging DNS intelligence, critical infrastructure defenders gain early warning of attacks (like detection of domain hijack attempts or malware beaconing) and can respond in a coordinated way. The faster threat insights circulate, the faster Australia can block attacks nation-wide, especially for those sectors that keep our country running.

Shield 5 – Sovereign Capabilities

Recommended Actions:

1. **Continue Education Capacity Building University Partnerships:** as part of the Horizon 2 initiative, it is critical to address the education, skills and awareness gap. Developing the necessary cyber capacity and resourcing requires investment in education and development of DNS-literate talent, which typically crosses over between traditional network management and network security roles. Infoblox believes that there is a good opportunity

for the private sector, including vendors like Infoblox, to partner with University institutions to develop DNS security curriculums that can ensure a steady flow of talent. That talent can help support scaling and expanding initiatives such as the ASD Protective DNS as well as facilitate adoption programs. Infoblox has had discussions with education institutions such as the University of Queensland and strongly believes there is scope to both build capacity and initiate research partnerships to enable Australia to become a leader in DNS Security research and threat intelligence.

Shield 6 - Resilient Region and Global Leadership

Infoblox supports Shield 6's objective for Australia to strengthen regional cyber resilience and partnerships, and Infoblox is committed to supporting Australia's efforts to uplift cyber defenses in under-served economies.

Recommended Actions:

1. **Continue investment in cyber capacity across Southeast Asia and the Pacific Islands through the SEA-PAC Cyber Program:** SEA-PAC plays a vital role in building cyber capacity across Southeast Asia and the Pacific Islands, funding a wide range of initiatives to support regional partners. A Protective DNS service, aligned with global best practices and national frameworks such as Cyber Essentials, would offer a high-impact solution to enhance regional resilience and bolster Australia's security leadership.

Conclusion

Infoblox appreciates the opportunity to contribute to Horizon 2 and strongly supports the Government's objectives. By embedding Protective DNS, Secure DNS practices, and DNS-based intelligence sharing into Horizon 2, Australia can raise its baseline protections for citizens and small businesses, improve preparedness for major incidents, and strengthen the resilience of critical infrastructure.

Drawing on global best practice and the demonstrated success of Protective DNS programs in allied nations, we encourage the Department of Home Affairs to adopt Secure DNS as a central feature of Horizon 2. This will not only align Australia with international standards but also deliver scalable, cost-effective protection against the evolving threat landscape. Infoblox looks forward to partnering with Government and industry stakeholders to ensure DNS security plays its full role in protecting Australians online and advancing national security.

For more information contact:

[redacted]

[redacted]

[redacted]

www.infoblox.com