10th April 2023

2023-2030 Australian Cyber Security Strategy Development Discussion Paper Response

Lead author:
Chris Usserman - Director of Security Architecture
Infoblox Federal

Corresponding author:
Tim Hartman - Head of Solution Architecture
Infoblox Australia and New Zealand

Table of Contents

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054
+1.408.986.4000
www.infoblox.com

Summary

Infoblox, the leader in next generation Domain Name Systems Management and Security, thanks the Australian Government for the opportunity to provide our comments and recommendations to the 2023-2030 Cyber Security Strategy via this response.

First and foremost, Australia's Cyber Security Strategy paper succinctly captures challenges faced not only by the Commonwealth, but also highlights the similarities faced by other technologically advanced nations. For instance, both the United States and the United Kingdom continue to face challenges resulting from policy implementation, enforcement, and accountability. Many of these policies essentially become 'guidelines' when enforcement and accountability lack authority. Fortunately, the Commonwealth has the benefit of shared learnings from these experiences, both positive and negative.

We took note that of the organizations required to implement the 'Essential 8' as reported in the Australian Signals Directorate's (ASD) Cyber Posture Report to Parliament (2022), only 11% met Maturity Level 2, up from 4% in 2021. While this is a notable improvement, we've considered the cyber threat landscape's rapid capabilities advancement in recent years and applied those to the defined Maturity Levels. Many threat actors are opportunistic, leveraging "off-the-shelf" methods to gain access to random targets, with phishing and business email compromise being two of the most prolific access vectors as defined in Maturity Level 1. **However, the rate at which these threat actors are achieving and embracing methodologies as defined in Maturity Levels 2 and 3 is staggering compared to the rate at which enterprise networks are responding.** Therein lies both the problem and a potential solution, which is the scope of this paper–response and resilience.

The report also highlights that only 26% of eligible or mandated organizations leveraged the AUPDNS as of Dec 2022. AUPDNS is Australia's protective domain name system which employs RPZ (Response Policy Zones) to dynamically filter out malicious and suspicious domains, which according to a US National Security Agency cybersecurity study foils 92% of malware attacks. The 2022 report cites AUPDNS blocked more than 24 million domain requests; but without threat context or non-attributable target characterization, this number is largely meaningless.

The strategy paper focuses heavily on cybercrime as an isolated activity. However, for the past several years cybercrime and cyber espionage have converged. Reports have recently emerged where the North Korean government masquerade as financially motivated threat actors to further fund their espionage activities.

The discussion paper correctly highlights the continuing and accelerating evolution of the cyber threat landscape through the development of new technologies and iterations of proven technologies that both lower the barrier to entry by an individual, organized, or nation state threat actor, such as the

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054
+1.408.986.4000
www.infoblox.com

rapid development of AI at present. At the same time, these threat actors are massively expanding their compute and brute force capabilities through improvements in traditional CPU and GPU performance as well as the commercialisation and potential weaponization of Quantum computing over time.

Infoblox has chosen to respond to the following questions: **Question 1** provides our insight into how the Australian cyber security strategy compares and contrasts with other countries such as the United States and United Kingdom. **Question 2 Section B and D** offers our view on the Security and Critical Infrastructure Act, and the Cyber Security Act's effectiveness. **Question 10** provides a detailed look at effective threat blocking at scale using Domain Name Systems and Response Policy Zones and recommendations in detail, including device attribution and a means for the government agencies to not only detect but also respond appropriately and in a timely fashion. And finally **Question 20** provides feedback on measuring and managing progress of Australia's cyber resilience goals towards 2030.

Further consultation from Infoblox to the Commonwealth on any topics discussed in this response and broader policy concerning cyber resiliency is welcome and we would be very happy to facilitate.

QUESTION 1: What ideas would you like to see included in the Strategy to make Australia the most cyber secure nation in the world by 2030?

Against the above backdrop of both (1) short term adoption of appropriate controls and evolution thereof aligned to, or ahead of, global standards, and the (2) longer term view of the evolving threat landscape Infoblox proposes the following for inclusion.

As stated in the summary, adoption of the 'Essential 8' controls according to the Australian Signals Directorate's Cyber Posture Report to Parliament (2022) is "improved but remains low". The 'Essential 8' was established by the Australian Signals Directorate as a framework for improving an organisation's cybersecurity posture in response to the increasing number of and increasing sophistication of cyber threats facing organisations. In the short term it is imperative to drive national adoption of the 'Essential 8' across federal and state government departments, critical infrastructure, and businesses alike to create a culture of security.

For example.

- Mandate implementation of 'Essential 8' controls at a national level.
- Define milestones of achievement and perhaps provide tax incentives to do so.

- Prioritise controls: identify which of the 'Essential 8' controls are most critical to the relevant organisation based on a risk assessment and prioritise their implementation.

- Phased approach: implement the controls in phases, focusing on the most critical controls first and gradually expanding to cover all requirements of ML2 and 3.

- Training and awareness: Ensure that staff are trained and aware of the 'Essential 8' controls and their importance. This will promote a culture of cybersecurity mindfulness and encourage employees to contribute to the organisation's success.

- Continuous monitoring and improvement: Regularly review progress and reassess priorities as the business changes and as implementation progresses. This will help ensure that the organisation's efforts remain aligned with the evolving risk landscape and compliance requirements.

While the 'Essential 8' provides a solid foundation for cybersecurity, it is not as comprehensive as the NIST SP800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organisations. A gap analysis between 'Essential 8' and NIST Special Publication 800-53 may highlight further areas for consideration:

- Risk Management and Governance: Developing a comprehensive ***living*** cyber risk management program, including risk assessments, risk mitigation strategies, and communication of risks to relevant stakeholders.

- Incident response and recovery: Establishing a robust incident response plan that includes clear roles and responsibilities, communication protocols, and a recovery plan to restore operations during and after a security incident. Test this plan regularly.

- Vendor and supply chain management: Assessing the security of third-party vendors and implementing both internal controls and compliance standards to manage supply chain risks.

- Identity and access management: Implementing more advanced controls such as Multi Factor Authentication (MFA) and privilege management for critical systems and users. While government entities may already embrace MFA, are regulated entities as compliant?

- Continuous monitoring: Evaluate the US Cybersecurity and Infrastructure Security Agency's Continuous Diagnostics and Mitigations program and adopt their most successful components; there are some functions it does well, but leaves many gaps in visibility, particularly with respect to victim attribution that the Commonwealth may wish to address.

QUESTION 2: What legislative or regulatory reforms should the Government pursue to: enhance cyber resilience across the digital economy?

SECTION B: Is further reform to the Security of Critical Infrastructure Act required? Should this extend beyond the existing definitions of 'critical assets' so that customer data and 'systems' are included in this definition?

Infoblox has reviewed documentation pertaining to SOCI Act 2018, the (Critical Infrastructure Protection Act (CIPA)) 2022 revisions and supporting references. In our assessment of SOCI 2018, Section 5 already defines an asset class that includes data and systems, though it doesn't inherently specify a differentiation between company owned data and customer data. Our interpretation is that the current definition adequately covers all data categorizations, and that Section 9 builds upon those definitions to incorporate critical assets.

However, the existing legislation and reference materials don't clearly stipulate nested dependencies within the base or expanded critical asset classes. For instance, a responsible entity performing fuel distribution relies heavily on both the physical distribution mechanisms (e.g., fuel trucks, pipeline, seaports) but also a computer network containing data and supervisory control systems. In this example, there are multiple critical sub-classes of assets that all contribute to the relative health of an asset class. Every critical sector as defined by the Commonwealth is either a producer or consumer of at least one other critical sector asset class, yet the focus for that asset class is centred on its primary role/function (e.g., fuel distribution).

The U.S. experienced this first hand during the ransomware attack on the Colonial Pipeline. While the company's fuel distribution systems were intact, the ransomware attack disrupted the company's billing and accounting systems contained within the administrative network. As a result, Colonial suspended distribution operations throughout their 5,500-mile pipeline from 6-12 May 2021 disrupting fuel availability to petrol stations, airports, and other downstream distributors ultimately affecting millions of people and other critical infrastructure sectors across most of the eastern U.S. Their decision caused additional unintended consequences with social, economic, and public safety concerns. The President declared a State of Emergency on 9 May, and a $4M+ ransom was paid to regain control of Colonial's network. In the aftermath, it was determined that regulators (auditors) only focused on the physical distribution systems and direct-connect computing systems (i.e., SCADA) as critical assets, not the corporate administrative networks.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054
+1.408.986.4000
www.infoblox.com

Another direct example per the CIPA and the Critical Infrastructure Risk Management Plan identify 'critical domain name systems (DNS)' as requiring enhanced protections. However, per the SOCI 2018 definitions, only an 'Australian DNS' is specified, but not DNS systems owned and operated by other critical sector entities. DNS and other critical component systems such as central data storage servers owned and/or operated by the regulated entity should also be afforded greater protections.

Finally, Section 12P of SOCI 2018 provides examples of responding to a cyber security incident, but only very briefly provides three objectives: prevention, mitigation, and recovery. The section does not mention 'resilience' as an objective, nor does it address requirements for external reporting, community-based information sharing, or references to other legal precedence or authorities for said activities.

QUESTION 2. SECTION D: Should Australia consider a Cyber Security Act, and what should this include?

In short, yes. The challenge with formalizing regulation pertaining to many sectors is that those sectors often experience technological advancements that expand beyond the current state of the art. As a result, governments around the world are often chasing technology with considerations regarding potential legislation. Case in point–the 2022 amendment didn't even consider the implications and impact ChatGPT has already had in the 30 days prior to this document's submission. The SOCI 2018 Act, CIPA and the CIRMP each provide a solid baseline, while the 2022 amendment furthers the cyber security component, including the Enhanced Cyber Security Obligations Framework. However, there's not a clear distinction as to whether these acts pertain to [my] entity, nor which components/addendums/attachments apply. In fact, the Enhanced Cyber Security Obligations Framework only applies to a subset of critical infrastructure entities declared as 'systems of national significance' but should definitely be considered for the broader critical infrastructure sectors.

A Cyber Security Act separate from other methods of critical sector business impact is imperative since a single cyber-attack could negatively affect each and every critical infrastructure sector at the same time. No other regularly occurring event [hazard] could cause such catastrophic disruption across the Commonwealth. The Act should further the establishment of public/private partnerships within the critical infrastructure sector communities of interest wherein sensitive data may be shared for awareness and action while keeping with sensitive information protection standards. This must be a bi-directional partnership where the government shares classified information where feasible and community members share non-attributable 'victimology' data and relevant information pertaining to cyber-attacks whether successful or not.

infoblox.

Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, we provide real-time visibility and control over who and what connects to your network, so your organization runs faster and stops threats earlier.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054
+1.408.986.4000
www.infoblox.com

QUESTION 10: What best practice models are available for automated threat-blocking at scale?

The answer to this question requires an explanation for two distinct components: why the current models aren't enough, and that a next generation solution depends upon the community served. The U.S. National Security Agency's Cybersecurity Directorate conducted a study, cited in June 2020, that stated their '*analysis highlighted that using secure DNS would reduce the ability for 92% of malware attacks … from a command and control perspective, deploying malware on a given network.*' Every operational network uses DNS, even if that network never touches the internet.

Traditionally, DNS servers have only existed for one main purpose–to translate between human-readable domain names (i.e., 'australia.gov.au') and their IP addresses; australia.gov.au is '13[.]107.226.40'. One of the most popular enterprise-grade DNS servers comes bundled as a free add-on component to the primary function—domain authentication. While the DNS service itself does just one function (address translation), it was never intended, designed, or enabled to support a protective DNS capability until the server edition published in 2019–consisting only of base RPZ support. Unfortunately, many organizations don't routinely upgrade their critical servers as frequently as the Security community would like. Even then, RPZs are only a first step to preventing DNS exploitation.

The Australian, United Kingdom and United States governments have all operated a protective DNS (PDNS) capability for multiple years, with each technology going through multiple advancements to address certain limitations while also attempting to keep up with threat actor techniques.

Current Model Limitations

In December 2020, the world became aware of a supply chain attack that affected hundreds of high-profile customers of Solarwinds. The initial attack into Solarwinds was determined to have happened in October 2019 with subsequent downstream victims infected beginning in March 2020. From March until early December, the nation-state threat actor operated with impunity across their victim base. In Congressional hearings that followed, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) was questioned why their PDNS solution, Einstein 3 Advanced (E3A), didn't catch this threat despite massive investments. A August 2020 Government Accountability Office report estimated $10 Billion dollars has been spent over the program's lifecycle as of the time of reporting.

In retrospect, the attack was quite simple. E3A leveraged both commercial and classified indicators of compromise (IoC), otherwise known as 'threat feeds' or 'block lists' to block outbound DNS queries sent from agency gateways to the internet. Only E3A stood in the middle, and it leveraged these block lists to determine whether a DNS query/connection request should be honoured or if it should be blocked. These block lists required a cyber threat intelligence generating organization with credibility

(i.e. ACSC, ASD, *Infoblox*) to observe and apply a determination that the internet domain was "bad", and add it to a threat feed. The command and control domain used by the nation-state actor was registered in July 2018 and remained in good standing until a [victim] cyber security firm detected the breach in their own network. E3A didn't have the ability to analyse DNS traffic beyond reputation-based threat feeds.

As stated previously, threat actor capability acceleration far exceeds security control compliance implementation. Quality DNS-focused threat feeds are absolutely required, at a minimum, but have not been sufficient at addressing even moderately capable threat actors for quite a few years. Consider threat feeds as equivalent to antivirus signature updates; those antivirus signatures are derived from the previous observation of malicious software that's been subsequently shared to a broader audience. However, it's now generally rare an antivirus solution catches an infected file when threat actors are routinely employing more advanced exploitation methods, including obfuscation and 0-day attacks.

As such, a PDNS capability must be resilient to both known and unknown threats that not only act on response policy zone (RPZ)-enabled threat feeds, but also are able to detect DNS tunnelling and covert communications techniques. The National Institutes of Health report cited 80% of malware leverages DNS for C2. An attack-resilient PDNS solution should also detect anomalous behaviours in DNS packet headers and related traffic, signatures associated with exploitation techniques across DNS sessions, in both the outbound query and the inbound response, and most importantly–alert and stop it in the quickest time possible. The Commonwealth's recent ITSM update (Control: ISM-1782, Rev 1, Dec-22) regarding use of RPZs across government networks is a great first step.

For governmental agencies, AUPDNS serves to protect agency communications enroute to the internet. There are several limitations to an 'edge' solution such as AUPDNS that limit the ability to detect, prevent, contain, mitigate, and recover from various DNS-based exploitation.

First, they don't have visibility into the events happening on "local" enterprises wholly within an organization. Many forms of malware often run rampant within a local enterprise moving laterally to discover more of an organization's "crown jewels", obtain additional credentials, and/or conduct more destructive attacks (i.e., ransomware). Second, should AUPDNS detect malicious activity within an organization, the analysts don't have any network-based intelligence/attribution to identify the source of the infection aside from which organization it came from, nor do they have visibility or understand how widespread the attack is.

However, the AUPDNS analysts can see how many organizations within its protection base are infected with the same type of attack. Refer to Figure 1, denoting the threats facing public and private enterprises today. Without a PDNS solution to detect malicious activity across internal networks, threats leveraging DNS may only be detected once they leave the enterprise with the assumption that

AUPDNS actually detects the activity as the last line of defence. According to the ASD's report to Parliament, only 2% of organizations participate in the Cyber Threat Intelligence Sharing (CTIS) platform.

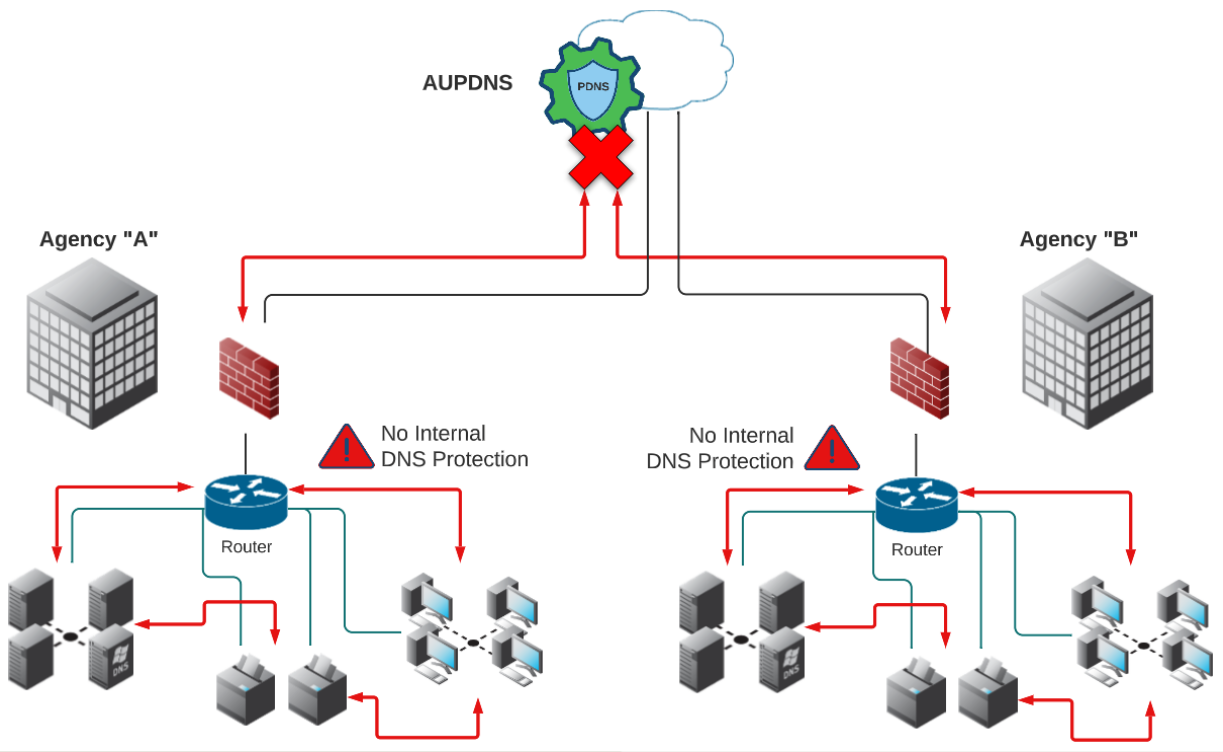

Figure 1, Lateral movement within enterprise networks

The U.S. and the U.K. PDNS systems (contracted commercial offerings), as well as many commercial PDNS products have one massive fault–they're open DNS resolvers. Today, any private entity or individual may utilize the freely available services that do both DNS and threat blocking. For example, a private individual may point their home router to use a freely available PDNS product that blocks threats based on the provider's threat feeds. The individual doesn't have configuration control nor access to detected threat activity (logs). However, should the individual or a business choose to subscribe, they are provided additional configuration controls, including the use of their own threat feeds, and access to log data. The U.S. and the U.K. systems supporting both public and private organizations leverage these types of services, and threat actors know it. The new U.S. PDNS solution leverages one of these freely available products but added data lake and custom configuration controls for federal agencies. Therein lies the problem: the same detection engine being used to protect the U.S. federal government is also being used globally by other paying customers, private individuals, and yes–even threat actors. Threat actors, including several prominent ransomware groups have been

identified leveraging freely available online security tools to develop and test against before they field new capabilities.

To be clear, the AUPDNS service is effective, but like the U.S. and the U.K. systems, may require a significant overhaul. AUPDNS's capabilities should be assessed and strengthened (where appropriate) to accommodate not only the reputational threat feeds, but also analysing the behavioural and signature components of DNS activity to identify covert communications channels that are already frequently employed by threat actors conducting cyber crime and/or cyber espionage. Mandiant just published a report on APT43, a prolific threat actor operating on behalf of the North Korean regime that Mandiant has observed engaging in cybercrime to fund their espionage operations.

Automated, Scalable Threat Blocking

Many public and private organizations around the world have begun to expand beyond defence-in-depth towards truly embracing a Zero Trust model, as defined by NIST more than ten years ago. At the heart of a Zero Trust Architecture (ZTA) is the notion that 'data' is the crown jewel. When you consider an organization's data resides in the cloud, on servers, and endpoints, ZTA takes a stance that information security controls should start where the data is, not just at the edge. According to the aforementioned ASD report to Parliament, only 2% of organizations are participating in the Cyber Threat Intelligence Sharing platform. The models that follow provide a mechanism for ***automatically sharing threat indicators*** detected locally as well as broadly across communities and sectors of interest.

So, how would the Commonwealth establish an automated threat blocking capability that operates at the scale of the state and its citizens? By leveraging successful components from different models, the U.S. and the U.K. established, the Commonwealth could realize a drastically more secure environment throughout the whole of Australia. The first served community is the Federal and Territorial governments, the second supporting critical infrastructure entities, and the third would support smaller businesses and/or private citizens.

A. Protecting the Federal and Territorial governments.

If you apply the NSA's guidance on PDNS, a sound Zero Trust architecture, and a continuous diagnostics, monitoring, and reporting methodology, the ACSC could have broad visibility not just across organizations, but also the ability to provide the protected organizations with actionable alerts. Since ~92% of malware can be stopped by a PDNS solution, each governmental organization should implement an internal robust protective DNS solution capable of applying threat feeds in RPZ format and the ability to detect known and unknown threats with behavioural and signature-based detection. This localized solution would automatically identify and prevent threats at the first attempts to

leverage DNS from an infected host containing the threat from moving laterally across the enterprise or communicating with threat actor infrastructure on the internet. Moreover, the organization's Security Operations (SecOps) team can be immediately informed of the communications attempt, while automated playbooks are enacted across the security technology ecosystem to prevent further threat actor activity. The SecOps team would have full network attribution down to the source that instigated the DNS queries, threat context providing information about why the DNS activity is bad, and the ability to automate response processes to further contain the threat while providing maximum resilience for the enterprise. Each organization shall share with ACSC cyber threat indicators observed within their environment, but not required to share details pertaining to the extent of impact unless otherwise mandated. This would permit ACSC to have broad government visibility into targeted and broad-spectrum attacks while still protecting the reporting agency's reputation. The AUPDNS solution has the distinction of being the last line of defence by leveraging potentially classified threat feeds or other detection capabilities to detect any other anomalous activity that may "get through'' an organization's Zero Trust defences. See Figure 2.

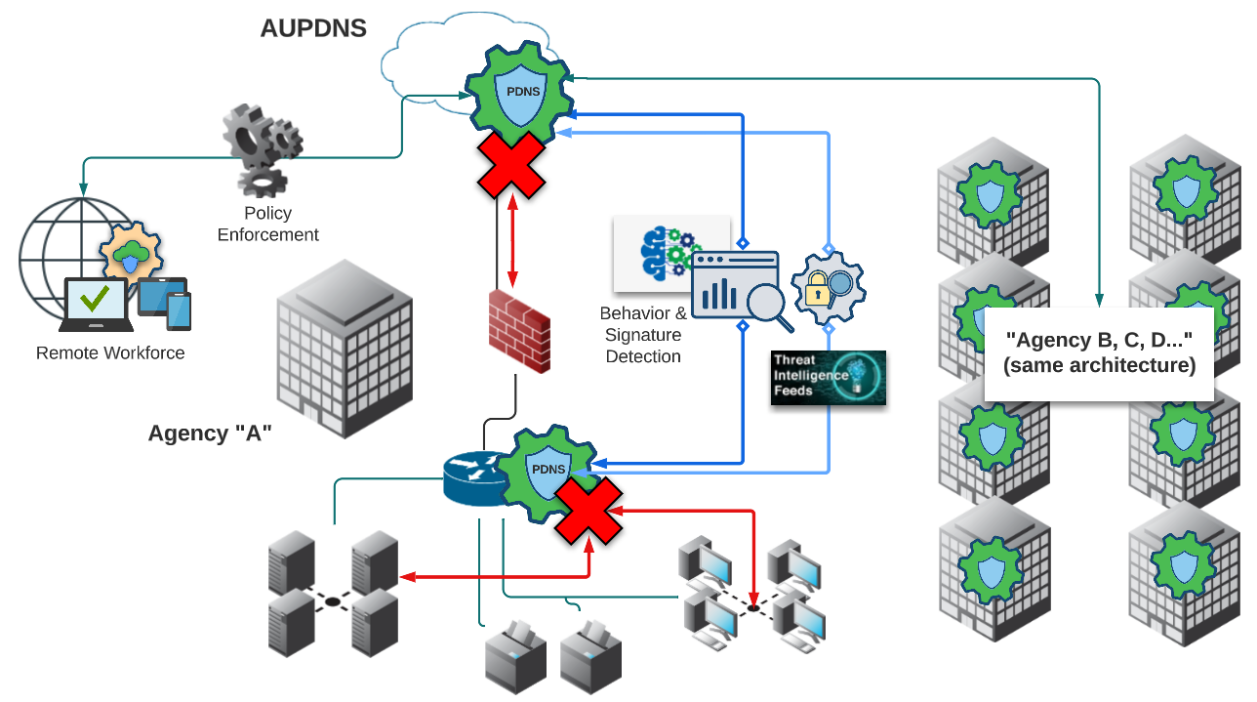

Figure 2, PDNS deployed in a Zero Trust model.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054
+1.408.986.4000
www.infoblox.com

B. Protecting Critical Infrastructure Entities

The NSA implemented a PDNS program supporting up to 1,000 defence industrial companies across the United States that either directly or indirectly conduct business with the Department of Defence. While the intention was noble, implementation has been challenging since all DNS traffic from a protected company would now flow through the NSA's system. There are two potential strategies for Australia: the Commonwealth could establish a separate AUPDNS service IP address for any registered critical infrastructure entity; or the Commonwealth could contract with a trusted third party capable of meeting the Commonwealth's PDNS requirements. The challenge for ACSC–do they want to just provide security protection without organizational alerting and feedback on detected activity…or would they prefer the entity can self-manage security feeds and policy configurations while sharing valuable threat intelligence back to ACSC?

If the Commonwealth chose to identify a third-party to provide a PDNS security solution, ACSC could provide a "black box" threat feed that takes highest priority (first block) over any entity-specified or derived threat feeds. This would ensure the entities are maximally protected with government-furnished threat feeds while extending alerts and configuration control to the protected entities. Since each entity would have access to their own alerts, they can quickly take action to contain the threat, better manage organizational risk, and maintain continuity of operations. Infoblox recommends ACSC also be alerted to malicious activity aiding in correlating threat activity across entities, sectors, and the government. Refer to Figure 3 as a depiction of the service model.

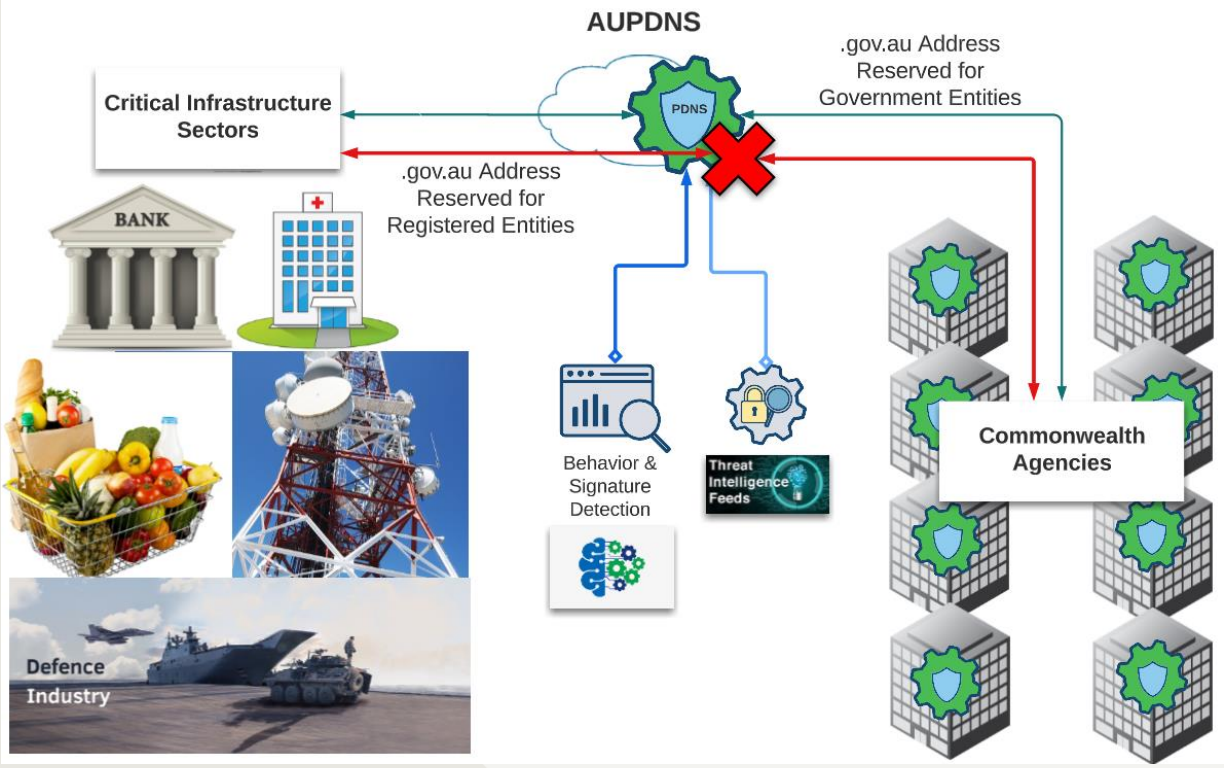

Figure 3, Combined protection for government and critical infrastructure

C. Protecting Private Citizens

Suggest the Commonwealth partner with the leading, if not all, telecommunications providers in Australia to support a PDNS offering to their clients in an opt-in fashion (no additional cost to the client). Responsible entities within the Commonwealth (i.e., ACSC) would provide a curated threat feed in conjunction with commercially available DNS-focused threat feeds to the partner telecommunications companies for immediate application. ACSC's responsibility for verifying threat feed accuracy ensures that only the most critical/dangerous threats would be actioned. This model protects against perceived government "overreach" and privacy implications, while still blocking the most critical threats.

There are two possible approaches: 1, in return for added security protection, the end clients must acknowledge that non-attributable information would be shared with the ACSC if attempted communications are observed with internet destinations contained within the threat feeds; or 2, in accordance with the Surveillance Legislation Amendment (Identify and Disrupt) Act 2021 and its predecessor, the Surveillance Devices Act 2004, as well as relevant Privacy legislation, the

Commonwealth may be *within its right* to arbitrarily act to protect its citizens. In other instances, the Commonwealth *may choose to do nothing* in an effort to further investigate crimes against the State (often measured as 'Intelligence Gain/Loss').

In either instance, Infoblox recommends the Commonwealth ***not block*** threats identified through behavioural or signature-based detection. As with open internet resolvers and free DNS security services, opening a service to a broad swath of Australian public that detects ***and blocks*** these types of DNS activities dramatically increases the adversary's ability to conduct test-refine-test-attack methods. Instead, the telecommunications partners should provide automated reporting of said activities. It's worth noting that there are legitimate applications which leverage DNS tunnelling for business operations, including some airline apps and antivirus signature updates.

QUESTION 20: How should the government measure its impact in uplifting national cyber resilience?

A. Essential 8 and AUPDNS adoption

The current accurate measure of both 'Essential 8' controls and AUPDNS uptake among Government departments, Critical Infrastructure, and Australian business is the Australian Signals Directorate's Cyber Posture Report to Parliament (2022) as outlined in the summary above. This is a great first step but flawed in that the report is produced annually and for the better part self-reported with little or no recourse if not adopted.

The recent announcements by the Minister for Home Affairs to conduct exercises to test and better prepare for potential cyber-attacks of critical services is a great initiative. Scaling this out to include similar "self-service" checks for individuals and businesses along the lines of the exercise-in-a-box initiative already in place are an excellent vehicle to drive awareness and compliance to at minimum a base level of protection.

Depending on the size and scope of the business, measurement and reporting should be continuous, and "self service" or third party verified by accredited Australian owned and operated cyber security services companies wherever appropriate and reported to the ACSC or ASD as a statement of record.

B. AUPDNS best practice

As discussed in detail in our response to Question 10 above concerning automated threat blocking at scale using Protective Domain Name Systems. The Commonwealth's recent ITSM update (Control: ISM-1782, Rev 1, Dec-22) regarding use of RPZs across government networks is a great first step to improve protection against known and unknown malicious domains before a network flow is established. It cannot be overstated how critical the uptake of this is both in terms of technology and in terms of the percentage of government departments, critical infrastructure and businesses is, as well as subsequent participation in the Government's Cyber Threat Intelligence Sharing Platform, of which current uptake is as low as 2% according to the previously mentioned ASD report to Parliament.

To reiterate. The U.S. National Security Agency's Cybersecurity Directorate conducted a study, cited in June 2020, that stated their '*analysis highlighted that using secure DNS would reduce the ability for 92% of malware attacks … from a command and control perspective, deploying malware on a given network.*'

A good example here is the impact the WannaCry outbreak had on the National Health Service in the United Kingdom in 2017. A Protective DNS service with the ability to detect and block before a network flow is established, as well as report on, and in the best designed case, for Government Agencies to respond by attributing the outbreak to a device or devices would dramatically reduce the likelihood of an outbreak as per the NSA findings and proof of PDNS effectiveness.

For the Australian Commonwealth to reach an enviable cyber security position by 2030 we recommend a detailed requirements study as outlined in our response to Question 10, unlocking the reasons why AUPDNS adoption is much lower than expected, and an unacceptable risk today.

As mentioned in the summary, Infoblox is available for further consultation to the Commonwealth on any topics discussed in this response and broader policy concerning cyber resiliency.

Thank you.

Chris Usserman & Tim Hartman on behalf of Infoblox.

About Infoblox

Infoblox is the leader in next generation Domain Name Systems management and security at scale. More than 12,000 customers, including over 70 percent of the Fortune 500, rely on Infoblox to scale, simplify and secure their hybrid networks to meet the modern challenges of a cloud-first world. The Infoblox Cyber Intelligence Unit creates, aggregates and curates information on threats to provide actionable intelligence that is high quality, timely and reliable. Threat information from Infoblox minimises false positives, so you can be confident in what you are blocking, while ensuring unified security policy across the entire security infrastructure. Infoblox Federal is a cleared US contractor supporting the US government, FIVE EYES partners, and public sector entities.

infoblox.

Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, we provide real-time visibility and control over who and what connects to your network, so your organization runs faster and stops threats earlier.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054
+1.408.986.4000
www.infoblox.com