Afilias Australia Pty Ltd
Melbourne Central Tower
360 Elizabeth Street
Level 35, Suite 4
Melbourne, VIC
3000, Australia
T +1.215.706.5700
F +1.215.706.5701

Security Legislation Amendment (Critical Infrastructure) Bill
Submission

27 November 2020

To: The Department of Home Affairs

Subject: Afilias Australia Pty Ltd comments on the Exposure Draft Security Legislation Amendment (Critical Infrastructure) Bill 2020

In response to the Security Legislation Amendment (Critical Infrastructure) Bill, Afilias Australia Pty Ltd offers the below views.

Maintaining and protecting the essential services of Australia is a vital endeavour that is key to the safety and wellbeing of citizens, the government and to the success of the economy. The efforts by the Australian Government to define the full scope of services, mechanisms for increasing security and stability, and providing transparency deserve praise and recognition. The objectives are sound and the mechanisms to achieve them clearly articulated.

As the Registry Operator for the .au ccTLD, Afilias Australia Pty Ltd is aware of the important role the naming system plays in the security and stability of the internet's infrastructure in general and to Australia specifically. Accordingly, several oversight mechanisms are currently in place to ensure its security and maintain business continuity. These structural guardrails fulfill the goals of protecting the namespace without the need for further designation and Positive Security Obligations or Agency intervention during a cyber emergency that could add unnecessary burdens and costs.

Operation of the .au Domain Name System
The scope of work and performance requirements of the .au namespace are managed by .au Domain Administration Limited (auDA). The technical operation of the .au namespace is conducted by Afilias Pty Ltd via a contract awarded after a highly competitive global procurement process that prioritised experience delivering highly secure and stable registry services. The primary services provided by Afilias Australia Pty Ltd include:

- Core registry services of registering, maintaining, transferring and deleting domain names;
- Globally available DNS query system, generating and publishing the .au DNS zone file based on registered domain names;
- Providing registration data directory services (RDDS) (formerly referred to as WHOIS);
- ISO 22301 certified Business continuity services, (e.g. disaster plans, data escrow and drills); and
- Extensive reporting to auDA and registrars.

These services have respective performance requirements of the highest standards that are enforced by auDA. In our experience as Registry Operator of multiple country codes, we see auDA as a highly conscientious, diligent, and responsible steward of the .au ccTLD. They are actively engaged with us and the internet naming community. The team at auDA is professional and skilled; they understand the importance of the .au namespace and meticulously work to ensure it is available and resilient.

All aspects of Afilias' service delivery – from staff to networks to resolution – consider and address security challenges. Anticipating and mitigating threats is a core part of daily business. The actions we take include compliance with the Australian Signals Directorate's Essential Eight mitigation strategies and go beyond, in acknowledgement of the critical role of the .au namespace. For adequate context, several of Afilias Australia Pty Ltd's security practices and protocols are described below.

Afilias Australia Pty Ltd is certified in and follows strict security measures as defined by the ISO 27001 Information Security Management standard, to manage and support the .au ccTLD registry. As part of the established Security Management System, a risk management framework is defined to identify and manage physical and logical risks to the secure operation of the registry. To ensure resilience of the registry system, Afilias is certified in ISO 22301 Business Continuity Management System standard. Continuity drills are conducted twice a year to ensure a secure and timely setup of the registry in the secondary site in the event of a disaster at the primary location. Around 20 internal measurement audits are conducted to ensure compliance with the two ISO standards along with an annual third-party certification audit. Compliance with cyber security incident mitigation strategies as defined by ASD's Essential Eight is also ensured. In addition, Afilias has a MoU with CERT-Australia and ACSC to share and exchange information about threats to the .au ccTLD which includes:

- The distribution of information regarding specific security threats and vulnerabilities via the CERT-Australia Alert service;
- Information and advice relating to protection and mitigation strategies;
- Assistance with responding to and/or remediating security incidents;
- A guarantee by CERT-Australia that information is kept strictly confidential unless the registry has granted permission to share it with the ACSC to assist with investigations; and
- A highly confidential service for information sharing with "Traffic Light Protocol" classifications in place, indicating the level of sensitivity of specific information.

These extensive and well tested business continuity plans ensure rapid restoration of services without need for an Agency intervention during an emergency. This proposed requirement is therefore unnecessary for the .au namespace. In fact, international best practices demonstrate that intervention by a third party during an emergency would create more complications, decrease cohesion, and add more time to remediate the emergency.

The cornerstone of our security practices and protocols is the Afilias Risk Management Framework. A Risk Log is managed based on security reviews of software development and operations, continuity drills, and analysis of audits. All operational incidents, including any degradation in service, are subject to an impact analysis for sharing with and reporting to auDA. With our global footprint, privacy regulations present unique risks. A privacy impact assessment is used to identify and manage the risks associated with the principles of data

localisation, data minimisation, and limiting data access to ensure the security and stability of all data in the management of the .au namespace. Each of these actions ensure our daily operations are anticipating and considering threats to the .au namespace and that we work diligently with auDA to be responsible stewards.

The operation of the DNS for the .au namespace by Afilias Australia Pty Ltd follows very stringent security measures. Much of the basis of our security posture follows directly from the guidance provided by the "Essential Eight" from the Australian Cyber Security Centre[i], including:

- The use of multi-factor authentication for access to any online asset;
- We ensure that access to any DNS asset is only possible via a small set of secured systems, known as "jump boxes";
- We follow a rigorous patching schedule for both operating systems and applications; and
- We ensure that access to all DNS assets is further restricted to the dedicated DNS team.

In addition to the Essential Eight guidelines, Afilias Australia Pty Ltd has advanced processes in place to ensure the integrity of the Australian DNS. Only data and applications which are required to run the DNS are located on any individual asset, to minimise information leakage in the event of an incident. Assets are maintained using configuration automation, which ensures that environments have a consistent setup with minimal chance for manual error. The DNS is only loosely coupled to registry systems, with a clear and distinct handoff mechanism of DNS data, which further minimises the chance of attack penetration through the asset.

DNS Security Extensions (DNSSEC) have been deployed throughout all .au zones managed by Afilias Australia Pty Ltd. All DNSSEC operations are performed on dedicated systems, segmented away to a secure network. Cryptographic material is sequestered to a set of hardware-based High Security Modules, which are locked in secure data centres, and are tamper resistant. All DNSSEC keys utilise the SHA-256 algorithm.

While auDA is the official sponsor of the .au namespace, ICANN, as the Act notes, also plays a role in the stability of the .au ccTLD. While there is no contractual relationship, auDA and Afilias are actively involved in the ICANN community and have used their defined standards and protocols as a basis for establishing requirements for the .au ccTLD that mirror the largest global gTLDs. Further, it is an acknowledgement of the single internet and the importance of operating in a manner that ensures stability and would in no way fragment the internet. Being a strong part of this fabric is important for the stability of the .au ccTLD.

Additional efforts are also taken to ensure the .au namespace is highly secure and stable. These activities include, but are not limited to:

- Active participation in the development of internet standards, e.g. IETF;
- Demonstrating leadership in norms and best practices for organisations, e.g., IGF, APWG, M3AWG;
- Close collaboration with law enforcement, domestically and internationally;

- Coordination with other naming and numbering organisations to stabilise DNS operations, e.g., DNS OARC, APNIC;
- A partnership with CERT-Australia in the management and mitigation of security incidents; and
- Cooperation with both the ACSC and JCSC to protect against, identify and respond to ongoing threats in .au.

Each of these measures as defined above ensures the .au ccTLD is at the cutting edge of technology, informed of the latest threats, and implementing the relevant norms and best practices.

With our contractual commitments, strong oversight by auDA, and the performance record of the .au domain, further regulatory requirements are unnecessary currently. The processes, requirements, and actions in place today to secure the .au namespace exceed those of most other ccTLDs. This business model is proven and efficient. The wholesale cost of domain registration, the price to the retail sales channel, is among the lowest in the world for a level of service that rivals the world's best managed TLDs (who charge 50-600% more per domain). Additional administrative requirements that would come with activating the Positive Security Obligation would add no additional security benefit for the .au namespace, while significantly increasing the cost of delivering the service, and adding time-consuming distractions.

Recommendation

Australia is reaping the benefits of a highly secure and stable .au namespace at a very affordable price. The spirit and intent of Critical Infrastructure designation is already captured in the management and oversight of the .au ccTLD today. The Government is well-advised to continue its path to keep the Positive Security Obligation dormant for the .au namespace.

[i] https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-explained