Submission of the .au Domain Administration Ltd (auDA) to the Australian Government's Cyber Security Review

About auDA

.au Domain Administration Ltd (auDA) is the industry self-regulatory, not-for-profit manager of Australia's ".au" country code Top Level Domain (ccTLD). As part of this role, auDA:

- develops, reviews and enforces policy frameworks;
- oversees the management of critical technical infrastructure (such as nameservers) to ensure the stable and secure operation of the .au namespace;
- facilitates the promotion of competition, fair-trading and consumer protection in .au; and
- participates actively in international fora related to our technical and policy mandate.

auDA is not an agency of government, however was formally endorsed to perform its current functions by the Minister for Communications (on behalf of the Commonwealth of Australia) in 2000.

Introduction

The Domain Name System (DNS) is a distributed system that facilitates the translation of Internet Protocol (IP addresses) to Internet domain names. It is critical for the stability and integrity of the model that every Internet-connected device or network has a unique identifier and that every translation that occurs is accurate.

The global mechanism for managing the DNS is decentralised. While it is coordinated by the Internet Corporation for Assigned Names and Numbers (ICANN), each country or territory manages its own national country code – the role auDA performs for .au.

The physical and operational security of the servers that host the .au top level domain (TLD) and subsequent second level domains like com.au and gov.au (2LDs), as well as the communications between the .au registry and global and local DNS industry participants, are absolutely critical. With so much of Australia's communications, commerce and entertainment relying on the stability of the Internet, auDA takes its role in maintaining this element of critical infrastructure very seriously. It is why we have existing networks and relationships with law enforcement and why we actively participate in a range of fora that address cyber security issues.

Given the above context, auDA welcomes the opportunity to provide input to the Australian Government's cyber security review and looks forward to participating further as the review proceeds.

General questions

There are three broad areas that PM&C is seeking views from all organisations consulted.

- *Roles and responsibilities, in particular the Australian Government's, in cyber security.*
  - *Do current roles and responsibilities for cyber security in Australia need clarifying and/or updating?*
  - *Do they reflect your views on the Australian Government's role and responsibilities and that of your organisation/institution?*

auDA's interaction with the Australian Government in relation to cyber security and our administration of the .au DNS is through the following channels:

- the Department of Communications, for liaison on general Internet policy matters at a domestic and international level
- the Australian Government Information Management Office (AGIMO) within the Department of Finance, for the management of the gov.au domain space
- CERT Australia within the Attorney-General's Department, for liaison and cooperation on cyber security incidents involving .au domain names.

We believe that the roles and responsibilities of each of these parties are clear to all involved however may not be well understood by those in the broader cyber security ecosystem. auDA believes that the role of government should be to maintain existing relationships and to facilitate greater awareness and more effective networking across relevant stakeholders.

- *Challenges and opportunities.*
  - *What is the key challenge Australia faces in cyber security? What is the key challenge being faced by your organisation in cyber security?*
  - *What are opportunities for Australia in cyber security? Are we taking advantage of these?*

The key challenge facing Australia (and other economies) in cyber security is not a single threat or incident, but rather the rapid growth in scale, complexity and sophistication of "cyber adversaries". Our mechanisms for response and mitigation must be equally sophisticated and capable of rapid change. This is why auDA advocates the maintenance of strong private and public sector partnerships and a role for government in facilitating robust networks for collaboration and communication.

From auDA's perspective, the .au DNS is a piece of critical national infrastructure, and as such, it is a key target for cyber security attacks. The two most significant types of possible attack are:

- denial of service (DOS) or distributed denial of service (DDOS) attack on the .au primary and/or secondary nameservers, the aim being to cause severe degradation or failure of the .au DNS (.au domain names would cease to work)
- hacking of the registry database, the aim being to access domain name records for the purpose of hijacking or redirecting .au domain names.

auDA and the 2LD registry operator, AusRegistry, are constantly taking action to mitigate these risks and have critical incident response and disaster recovery plans in place to deal with cyber attacks on the .au DNS infrastructure and registry. However, one of the key challenges we face is the ability to access sufficient bandwidth to be able to absorb the volume of traffic in a sustained DDOS attack, so as to minimise the impact on the .au DNS and its users.

We note that high profile gov.au domain names are likely to be a target for cyber security attacks, due to the potential to cause serious impact on users and political embarrassment for the Government. We believe it is important for AGIMO and government agencies to ensure they have taken appropriate measures to manage the risks of cyber security attacks targeting gov.au domain names.

- *Identifying the most important 'missing piece' of cyber security in Australia.*
  - *What would you change about existing methods of approaching / managing cyber security, and why?*

From auDA's perspective, the 'missing piece' is a lack of clarity over the role and responsibilities of the Australian Cyber Security Centre (ACSC) and its interaction with other organisations in this area (acknowledging that the ACSC has only been in operation for less than 6 months).

At a more general level, auDA observes that over the last few years, various policy and operational functions with respect to cyber security appear to have shifted between the Attorney General's Department, PM&C and other agencies. In our view, this is not an optimal situation for maintaining the stability and reliability of trust networks between government and stakeholders.

Specific questions

We also seek your views on a number of specific areas within the scope of the Review.

- *Cyber security in the Australian economy.*
  - *How do you anticipate yours cyber security focus will change over the next five and ten years?*
  - *What does the 'cyber landscape' look like in 2025—what are the opportunities and risks?*

auDA believes that the risk of cyber attacks on the .au DNS is ever-present and likely to remain that way over the next five and ten years. This is based on knowledge gleaned from our international counterparts about their experiences in dealing with cyber attacks, as well as our dealings with the IT industry and cyber security agencies in Australia and overseas.

Accordingly, our focus is on continuing to improve the security and resilience of our technical infrastructure and our operational processes. Along with the work we are doing within our own organisation, we are also committed to improving the security practices of .au registrars through our Information Security Standard (ISS) compliance and audit program (see below).

- *International engagement*
  - *Where are the risks and opportunities for Australia engaging internationally on cyber security?*

We consider it vitally important that Australia engages internationally on cyber security, in both the public and private sectors.

auDA is an active participant in the Internet Corporation for Assigned Names and Numbers (ICANN), the Internet Engineering Task Force (IETF), the Internet Governance Forum (IGF) and regional fora such as the Asia-Pacific Top Level Domain Association (APTLD). Cyber security issues are discussed at all of these fora to varying degrees.

auDA also maintains strong relationships with our international counterparts in order to share information and best practice, and offer practical assistance in the event of a cyber security incident.

- *Partnerships and information sharing.*
  - *What are your views on cyber security information sharing between governments and private sector?*
  - *What mechanisms need to be in place now in Australia that are not currently accessible / available?*

auDA supports the sharing of cyber security information between relevant government agencies and private sector organisations, and we would welcome more clarity on the mechanisms by which this can be achieved. As mentioned previously, clear communication and effective trust networks are absolutely critical to the efficiency of Australia's response to cyber threats and the Australian Government has a key role to play in this regard.

- *Legislation, standards, guidelines and privacy issues.*
  - *What are your views on baseline standards and/or guidelines for cyber security?*
  - *What is the right balance between standards/regulation and self-determination?*

auDA is committed to following security best practice in DNS administration. At the end of 2014, we implemented Domain Name System Security Extensions (DNSSEC), a security extension that facilitates the digital signing of Internet communications, helping to ensure the integrity and authenticity of transmitted data. The .au TLD and all .au 2LDs except gov.au have now been signed, and .au registrants in the signed zones have the choice to deploy DNSSEC for their own domain names.

In 2013, we introduced the auDA Information Security Standard (ISS) for .au registrars, to encourage and assist registrars to manage and improve the security and resiliency of their own businesses, and to protect .au registrants, and the overall integrity and stability of the .au DNS. Compliance with the ISS is mandatory. auDA developed the ISS in the absence of any existing industry-specific standard or guideline (although it is based on ISO 27001, which is the internationally recognised baseline standard for information security management).

At a more general level, auDA believes that the development of technical standards is absolutely essential for the stable operation of the Internet and, by association, for the battle against cyber crime. However, the terms "standards" and "regulation" should not be used interchangeably. Standards are often developed in a collaborative environment whereas regulations or legislation may not be. While standards provide a shared understanding, regulations may serve to limit the scope and agility of a cyber security response. As such, auDA believes regulations must be kept to the minimum-possible level that still allows appropriate coordination.

- *Cyber security research, development and innovation.*
  - *How can Government better support thought leadership on cyber security to drive innovation and practical outcomes in cyberspace for the Australian economy?*

auDA has no specific comment in response to this question, though notes our earlier observation that the government should play a visible role in coordinating cyber security efforts. This would necessarily support thought leadership and deliver practical outcomes.

- *Cyber security skills and cyber literacy.*
  - *What specific cyber security skills are in shortage within your organisation, and more broadly, what are the skills you see in demand within client organisations?*
  - *How could Government and industry work together better to address the skills shortage?*
  - *Do you undertake community engagement programs on cyber security in order to improve the Australian community's awareness and understanding of the importance of cyber security?*

We believe that auDA has a role to play in raising awareness and understanding of cyber security issues within our own industry, which we do in a number of ways:

- the introduction of the ISS for registrars and the provision of associated security training and resources
- the ‘Security and Online Safety’ award category of the Australia and New Zealand Internet Awards (ANZIAs), which we run each year in conjunction with InternetNZ
- cyber security-related panel sessions and workshops at the Australian Internet Governance Forum (auIGF), which we host each year
- regular attendance and participation by senior auDA staff at relevant conferences and events, such as the ACSC Conference.