Identity Digital Australia

Melbourne Central Tower
360 Elizabeth Street
Level 12
Melbourne, VIC 3000
Australia

Response to 2023-2030 Australian Cyber Security Strategy Discussion Paper

Identity Digital Australia

Identity Digital Australia Pty Ltd is the registry operator and services provider for .au domain names and our head office is in Melbourne, Victoria. We work closely with .au Domain Administration (auDA, the administrator of Australia's .au top level domain) and our registrar partners to ensure that the .au Domain Name System (DNS) maintains high standards of security, reliability and interoperability. The .au domain has been deemed part of Australia's suite of critical infrastructure, given the centrality of the .au DNS to Australia's digital economy and society.

Identity Digital Australia is a subsidiary of Identity Digital Inc. Identity Digital simplifies and connects the online world with domain names and related technologies to empower people to build, market, and own their authentic digital identities. With the world's largest portfolio of over 450 Top Level Domains (TLDs) under management such as .photography, .studio, .live, .technology, and .restaurant, Identity Digital supports more than 25 million domains on its innovative registry services platform. In addition, Identity Digital enables customers to discover, register, support and use high-quality domain names with its registrar, Name.com. Identity Digital is a global organisation with approximately 250 employees.

Domain Name Infrastructure and Cyber Security

Domain names are memorable addresses on the Internet. Each day, millions of Australians access information on email and website addresses with extensions like .com.au, .au, .org, or .com.

Identity Digital and auDA collaborate closely to establish and enforce security measures[1] to protect .au users from criminal exploits like phishing or spam. These measures have made .au names among the safest in the world. However, criminals and even some nation states are working hard to find vulnerabilities in critical national infrastructure such as the DNS, to both eavesdrop on and disrupt the flow of information, commerce, civil society and academia.

[1] https://www.auda.org.au/blog/keeping-au-secure

Identity Digital Australia

Melbourne Central Tower
360 Elizabeth Street
Level 12
Melbourne, VIC 3000
Australia

Discussion Paper Questions

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?

> **Identity Digital Response:** The Digital Lives of Australians 2022 report[2] reveals that 98% of Australians feel that the Internet provides value to their lives and 61% of working Australians say they could not do their job without the Internet. Many Cyber Security discussions do not recognise sufficiently that the security of the Internet is a distributed responsibility, where many stakeholders must take action. As a distributed system with no central point of control, the Internet requires collaboration between companies, non-profits, governments and individuals to maintain and continuously improve its security and trustworthiness. Australia should work nationally and internationally to ensure that a cohesive and single Internet root remains at the core of how the domain name system works, beating back proposals from other nation states to fragment or build a private Internet (e.g., China and Russia).
>
> As an Organisational Member of The Internet Society, Identity Digital endorses their paper 'Major Initiatives In Cyber Security [3]: This paper sets out core Internet infrastructure examples where many parties work together to create 'collaborative security'. Examples include:
>
> **Routing Infrastructure**: The routing system that interconnects the Internet's tens of thousands of networks needs a secure foundation in order to ensure 100% reliability.
> **DNS Infrastructure**: The DNS translates human-friendly names into Internet addresses. A scalable and trustworthy DNS is essential to maintain confidence in the Internet.
> **Time Infrastructure**: Accurate and synchronised time information is needed both within the Internet's cryptographic foundation and in many business applications, such as equities trading.
> **Data Communications Security**: Encryption of Internet communications would significantly enhance the privacy of personal and business data.
> **Identity**: The proliferation of different accounts and passwords creates security and trust problems across the Internet. Identity services help users to carry a single identity with them.

---

2 https://assets.auda.org.au/a/2022-11/auda_digital_lives_of_australians_2022_research_report_171122.pdf?VersionId=1O_bi31mYof0ybFTABWaRJstNSfw.36y

3 https://www.internetsociety.org/wp-content/uploads/2020/01/Major-Initiatives-in-Cybersecurity-Infographic_20191218-Final-EN.pdf

Identity Digital Australia

Melbourne Central Tower
360 Elizabeth Street
Level 12
Melbourne, VIC 3000
Australia

We suggest that The Strategy should focus not only on end-user technologies but also on the core infrastructure that underpins the Internet, as outlined above. The Strategy could encompass the goals of working both nationally and internationally in a multi-stakeholder collaboration with like-minded governments, relevant Australian government departments, technologists (such as the Internet Engineering Task Force), Domain Registries (such as Identity Digital), the private sector, consumer advocates and standards bodies to create cyber security standards and norms that improve security and trustworthiness whilst maintaining availability to all.

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

a. What is the appropriate mechanism for reforms to improve mandatory operational cyber security standards across the economy (e.g. legislation, regulation, or further regulatory guidance)?
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?
c. Should the obligations of company directors specifically address cyber security risks and consequences?
d. Should Australia consider a Cyber Security Act, and what should this include?
e. How should Government seek to monitor the regulatory burden on businesses as a result of legal obligations to cyber security, and are there opportunities to streamline existing regulatory frameworks?
f. Should the Government prohibit the payment of ransoms and extortion demands by cyber criminals by:
(a) victims of cybercrime; and/or
(b) insurers? If so, under what circumstances?
i. What impact would a strict prohibition of payment of ransoms and extortion demands by cyber criminals have on victims of cybercrime, companies and insurers?
g. Should Government clarify its position with respect to payment or nonpayment of ransoms by companies, and the circumstances in which this may constitute a breach of Australian law?

Identity Digital Response: We opine on the areas that align with our expertise:

Identity Digital Australia

Melbourne Central Tower
360 Elizabeth Street
Level 12
Melbourne, VIC 3000
Australia

Regulation: Many governments worldwide seem to view regulation as a significant response mechanism to combat Cybercrime. Individual regulations may have good intent, but multiple policies add complexity for businesses that need to comply with all regulations in the context of a global Internet, and this complexity introduces its challenges to cybersecurity and data protection, not always improving them. Policies must be creative in increasing protection while decreasing regulatory complexity.

Technology moves at a very rapid pace, and almost always outstrips the ability of regulation to fully deter crime. Government must work collaboratively with the many stakeholders who are necessary to make the Internet secure, in addition to appropriate regulatory measures that safeguard the nation without reducing Australia's competitiveness on the global stage.

Response to cyber criminals: In our experience, it is exceedingly difficult to arrive at a single rule or law that addresses the variety of situations that result in ransoms and extortion demands. We further note that some companies or professions tend not to report incidents resulting in ransom or extortion *if the impact is not visible to the outside world*.

3. How can Australia, working with our neighbours, build our regional cyber resilience and better respond to cyber incidents?

Identity Digital Response: As outlined in our response to question 1, Identity Digital believes that multi-stakeholder collaboration is the key to building regional cyber resilience and better responses to cyber incidents. As an international company with extensive operations in the Asia Pacific region and around the world, we are already working collaboratively with partners such as auDA. Specific areas where the Australian government could facilitate or encourage collaborative multi-stakeholder work in the Asia Pacific region include:

- **DNS Ring of Defense**: Provisioning both DNS servers and root server instances in the Pacific Islands and Australia's northern and western neighbours to help insulate Australia with an "outer ring" of cyber defenses. This could provide early warning in addition to capacity to absorb/repel attacks.
- **Failover services**: Establishing an EBERO (Emergency Back End Registry Operator) capability by leveraging Australian and regional resources with the technical, operational, people and financial resources to quickly step in and

Identity Digital Australia

Melbourne Central Tower
360 Elizabeth Street
Level 12
Melbourne, VIC 3000
Australia

provide failover service to regional TLD operators requiring assistance. Protecting vulnerable island nations will make Australia safer.

- **DNSSEC adoption**: Wide adoption of DNSSEC by registrars and registrants would substantially improve the security of transactions involving domain names.
- **Regional CERT:** Coordinating a group of regional cyber-security leaders to form a region-focused Computer Emergency Response Team dedicated to information sharing to enhance protection across the region.
- **Education**: A comprehensive curriculum introduced at an early stage, focusing on cyber hygiene and identity protection.
- **Tabletop Exercises**: Helping organisations and businesses and governments understand the value of tabletop exercises and scenario planning.
- **Cyber Risk Plan**: Educating organisations, businesses and governments on the relevance and importance of creating a Cyber Risk Plan that provides a roadmap for responses to various cyber threats.

4. What opportunities exist for Australia to elevate its existing international bilateral and multilateral partnerships from a cyber security perspective?

Identity Digital Response: Regulators should continue to focus attention on supporting a global multi-stakeholder collaborative model of Internet governance and cyber security rather than a multilateral one. The ideas provided in our answer to Question 3 would also help.

5. How should Australia better contribute to international standards-setting processes in relation to cyber security, and shape laws, norms and standards that uphold responsible state behaviour in cyberspace?

Identity Digital Response: Regulators should work with international standards bodies such as the Internet Engineering Task Force (IETF) and the Internet Corporation for Assigned Names and Numbers (ICANN) to strengthen cyber security standards.

7. What can government do to improve information sharing with industry on cyber threats?

Identity Digital Response: Information sharing between the government and industry is critical to ensuring that organisations are able to respond in a timely manner to emerging threats based on information and intelligence. The ability for private industry to share their discoveries and insights is also vital as no company is an island in the cyber defense arena. They also help overcome obstacles to the sharing of knowledge and creativity to address one of the world's most pressing challenges. These 'Cyber Commons' facilitate two-way exchanges of information. Examples of this in other nations

Identity Digital Australia

Melbourne Central Tower
360 Elizabeth Street
Level 12
Melbourne, VIC 3000
Australia

that have been successful are CiSP in the United Kingdom, and in the United States there are multiple vehicles in which the sharing occurs. These include the NSA.

A properly functioning Cyber Commons could include the following elements:

- Provide publicly accessible tools that gives every involved organisation a simple and standardised way to share data, and allow others to use the data for learning in a responsible manner
- Work closely with major institutions and governments to create, adopt and implement protected data sharing and threat monitoring
- Build a Cyber Commons Secure Network, a secure community initiative that increases the quality and frequency of shared knowledge worldwide
- Produce a Cyber Commons Summit, a regular event held at least annually to invite security researchers, technologists, policymakers and other experts to share best practices and new countermeasures

Cybersecurity Collaboration Center for the defence industrial base, CISA's Automated Indicator Sharing for critical infrastructure, and the National Cyber-Forensics and Training Alliance for wider industry and law enforcement along with Information Sharing and Analysis Centers for various industries.

One key element for government sharing that is changing relates to reducing over-classification of information; what is known is not as sensitive as how an agency knows it. Private industry can benefit from the knowledge gleaned from confidential sources and should be able to receive it as long as sources and methods are protected.

8. During a cyber incident, would an explicit obligation of confidentiality upon the Australian Signals Directorate (ASD) Australian Cyber Security Centre (ACSC) improve engagement with organisations that experience a cyber incident so as to allow information to be shared between the organisation and ASD/ACSC without the concern that this will be shared with regulators?

Identity Digital Response: We believe that responsible information sharing is essential for a more secure and resilient DNS infrastructure. While confidentiality is an important element, a far more critical need is the establishment of trusted networks and a safe Cyber Commons where organisations can legally share information without fear of compromise, punishment or reputational harm.

11. Does Australia require a tailored approach to uplifting cyber skills beyond the Government's broader STEM agenda?

Identity Digital Response: Nations around the globe have sought ways to address the gap in skilled cyber security practitioners by expanding STEM education. While Australia's National STEM School Education Strategy focuses on partnerships and other

Identity Digital Australia

Melbourne Central Tower
360 Elizabeth Street
Level 12
Melbourne, VIC 3000
Australia

practical measures, the gap in this methodology is that cyber security is a particular skill set, both technically and intellectually. Learning about technology, be it coding, infrastructure management, or next-generation topics like Blockchain and AI, does not guide young minds implicitly towards secure coding, hardened infrastructure deployment and resiliency, and secure, ethical AI applications. Additional resources, particularly in later stages of education after introducing students to STEM and general cyber security hygiene, in the model of CISA's NICCS Cybersecurity for Students provides the guide rails necessary to set future cyber security professionals on that path.

19. How should the Strategy evolve to address the cyber security of emerging technologies and promote security by design in new technologies?

Identity Digital Response: Emerging technologies like Blockchain, Artificial Intelligence and Identity-based Security are the new frontier for security vulnerabilities.

The Strategy should recognise these technologies, and provide incentives for prompt disclosure of cyber threats. It should also focus on the identification of inherent risks in emerging technologies and education and awareness building for unsuspecting users about those risks.

A Cyber Commons where threats and vulnerabilities can be shared responsibly and where credible organisations and individuals can discuss counter measures could be a viable solution that scales and adapts to emerging technologies.