Submission to the Department of Home Affairs:

2023-2030 Australian Cyber Security Strategy

April 2023

.auDA

Table of Contents

Introduction

Who is auDA?

.au Domain Administration Ltd ("auDA") is the administrator of the .au country code Top Level Domain (ccTLD). The .au ccTLD includes the following namespaces: .au, com.au, net.au, org.au, asn.au, id.au, vic.au, nsw.au, qld.au, sa.au, tas.au, wa.au, nt.au, act.au, edu.au, gov.au.

auDA's role

As a critical part of the digital economy, auDA's role is to ensure the .au ccTLD remains stable, reliable and secure. Additionally, auDA performs the following functions:

- administers a licensing regime for .au domain names based in multi-stakeholder processes, including managing enquiries and maintaining an appropriate compliance and dispute resolution processes associated with the licensing rules
- licenses the .au registry operator and accredits and license registrars
- advocates for, and actively participates in, multi-stakeholder internet governance processes both domestically and internationally.

auDA's stakeholders

In performing its functions, auDA operates under a multi-stakeholder model, working closely with suppliers, business users, industry, civil society, consumers and the Australian Government.

It seeks to serve the interests of the internet community as a whole and takes a multi-stakeholder approach to internet governance, where all interested parties can have their say.

auDA is part of a global community of organisations in the domain name industry and engaged in internet governance. It plays an active role in representing .au at international fora, such as the Internet Corporation for Assigned Names and Numbers (ICANN) and the Asia Pacific Top Level Domain Association (apTLD).

auDA's advocacy principles

auDA's local and international advocacy is undertaken in accordance with the following key principles:

1. **Purpose driven** – we are a for purpose organisation. Our purpose is to:
    - administer a trusted .au domain for the benefit of all Australians
    - champion an open, free, secure and global internet.

Our purpose serves our vision, which is to unlock positive social and economic value for Australians through an open, free secure and global internet.

2. **Multi-stakeholder Approach** - We take a multi-stakeholder approach to our work, and we advocate for multi-stakeholder approaches to internet governance and policy matters. This involves us working closely with domain industry stakeholders, businesses, not-for-profit organisations, education and training providers, consumers, and Government entities to serve the interests of the internet community as a whole. This approach is founded on strong relationships locally and globally.
3. **Independence** - We are independent from government and from the corporate sector. This means we operate transparently and openly in the interests of all Australians.
4. **Leadership** – We seek to lead Australia's internet community to work better together on our shared work to actively advance an open, free, secure and global internet and positively influence policy and outcomes related to internet governance. We do this through quality policy advice and analysis, through research and information, and by sharing this insight with those can benefit from it. Partnership is integral to our way of working – we seek to work with others who support our vision and can help multiply our impact.
5. **Encouraging Innovation** – We support an innovative digital economy, and through our work we foster innovation across the technology sector, recognising its benefit to growing our digital economy and, in turn, benefitting all Australians. Legislative burden can negatively affect innovation in the technology sector, so we encourage the use of incentives and self-regulation where possible, and advocate for a consultative approach to regulation where it is needed.

In response to the Department of Home Affairs' Discussion Paper on the *2023-2030 Australian Cyber Security Strategy*, auDA is pleased to offer the below comment.

Submission

At auDA, upholding and preserving a reliable, resilient and secure Domain Name System (DNS) is our key priority in maintaining the integrity of the internet as the enabler of the digital ecosystem.

The DNS is essential for the continuous and stable operation of the internet, on which the digital economy and society depend. To this end, we provide comment on select matters raised in the Discussion Paper.

In response to the Department of Home Affairs' Discussion Paper on the *2023-2030 Australian Cyber Security Strategy* (the Discussion Paper), auDA is pleased to offer the below comment.

Background

Cyber security and resilience significantly contribute to the overall health and wellbeing of the digital ecosystem. Given the importance of the online world in the lives of Australians, their wellbeing is directly linked to the security and integrity of the digital ecosystem. Accordingly, cyber security should be considered a significant contributor to Australians' wellbeing, rather than an end in itself.

We note the Government's overarching premise that cybersecurity is a critical aspect of national security in the modern age. We agree that in the modern digital world cyber security is a prerequisite for national security. However, we moreover assert that cyber security should not be relegated as merely a national security goal, or considered a national security problem.

Rather, the focus of the Strategy – and the overall conception of cyber security - should be on how to make Australians' digital lives more secure and enhance their confidence in the protection of their personal information. Australians' cyber security awareness and digital literacy must be improved, so that individuals and businesses can use the internet and technologies securely. In the context of developing a national Cyber Security Strategy, this is a difficult balance to strike, but it is a balance that we must get right.

At auDA, upholding and preserving a reliable, resilient and secure Domain Name System (DNS) is our key priority in maintaining the integrity of the internet as the enabler of the digital ecosystem. The DNS is essential for the continuous and stable operation of the internet, on which the digital economy and society depend. To this end, we provide comment on select matters raised in the Discussion Paper.

Addressing selected consultation questions

auDA suggestions for inclusion in the Strategy

Internet infrastructure security

Suggestion: The new Strategy should reinforce the importance of securing the underpinning infrastructure - the internet - given its centrality to modern digital economy and society. Support in the new Strategy of securing the internet, and of actions like the broader uplift of internet security standards such as Domain Name System Security Extensions (DNSSEC) could help improve overall security of Australia's digital environment. Several other jurisdictions (for example Singapore, European Union, United States) have included the security of the internet in their analogous strategies on this basis.

The Strategy should also reiterate the importance of data security and privacy as a prerequisite for the Digital Identity system. A minimalist approach to the collection and retention of personal information should be considered.

Background:

The Discussion paper emphasises the importance of Australians' internet access and connectivity.

auDA believes that the Strategy should also include and emphasise the importance of keeping the internet secure as the underlying infrastructure that enables and empowers the digital economy. In auDA's view, the full potential of the modern digital economy cannot be realised without Australians' ability to trust that our digital infrastructure is secure, even as the cyber threat landscape evolves.

The internet is a constant target for malicious attempts at disruption. At the same time, there is increased reliance on the core functions of the global and open internet, including the DNS. The DNS, as critical infrastructure, supports the operation of the internet. It is the backbone of the digital economy, with almost any activity on the internet relying on it. The vital role of the DNS in supporting the internet is evidenced by its classification as a critical asset in the ***Security of Critical Infrastructure Act 2018*** (SOCI Act).

As the DNS continues to evolve and expand, so does the need for uplifting Australia's cyber security posture.[1] auDA advocates for the uptake of well-established internet security standards and best practice for DNS, such as DNSSEC. The use of secure protocols such as DNSSEC is

[1] CSCRC and auDA (2022): Deciphering the DNS – What it is, how it works and why it's critical, November 2022, available at: Five takeaways: Deciphering the DNS with the Cyber Security CRC | auDA (accessed on 11 April 2023).

important to have a secure and stable internet infrastructure, underpinning the growing digital economy.

Emphasising the significance of internet infrastructure security in the Strategy would further raise awareness about secure internet protocols amongst Australians, and in turn foster greater adoption of internet security standards such as DNSSEC, lifting overall security of the internet.

Several other nations acknowledge the importance of the security of the internet infrastructure in their national cyber security strategies. For instance, in its Cybersecurity Strategy 2021, Singapore's government made minimising vulnerabilities in its internet architecture a strategic priority. It works with the Internet Service Providers to implement the DNSSEC protocol across local internet domains to augment the security of the internet, thereby preventing cyber threats affecting end-users.

The United States Cyber Security Strategy makes it a strategic aim to improve overall internet security and reduce cyber threats. As part of the Strategy, the U.S. Government is implementing new measures to detect and prevent cyberattacks, intending to reduce the number of attacks targeting the DNS, thereby enhancing internet users' trust in the digital world.

Likewise, the essentiality of the DNS, and specifically of Top Level Domain (TLD) operators is recognised in the European Union's ***Cyber Security Act***: "*The public core of the open internet, namely its main protocols and infrastructure, […] provides the essential functionality of the internet as a whole and underpins its normal operation. […] Public core of the open internet and the stability of its functioning, including, but not limited to, key protocols (in particular DNS[…], the operation of the domain name system (such as the operation of all top-level domains)[…].*"[2]

auDA would be pleased to provide further comment on the importance of internet infrastructure security to the Government, should it seek additional information. Through our stewardship of the .au domain, international collaboration with likeminded ccTLDs, participation in global and regional internet governance forums, and support of multi-stakeholder internet governance, we are well-placed to share insight into internet and DNS security.

Digital Identity and data minimisation

As noted in the Discussion Paper, the National Digital Identity system has significant relevance for the cyber security strategy and vice versa. As the Government considers the release of a final National Strategy for Identity Resilience later this year[3], the development and operationalising of a robust Digital Identity system should be approached as a multifaceted task that requires high

[2] Regulation (EU) 2019/881 ('EU Cybersecurity Act'), Recital 23, available at: EUR-Lex - 32019R0881 - EN - EUR-Lex (europa.eu) (accessed 12 April 2023).
[3] Department of Finance (2023): Data and Digital Ministers Meeting Communique, 24 February 2023, available at: data-and-digital-ministers-meeting-communique-240223.pdf (finance.gov.au) (accessed on 18 April 2023).

levels of data security and privacy to be incorporated into the Digital Identity system and its underlying digital wallet infrastructure.

Individuals' trust in the security of their own sensitive information held by Digital Identity wallets is a prerequisite for a successful implementation of the Digital Identity system. Consideration should be given to requiring inbuilt security by design measures into digital wallet solutions, especially since some of the data concerned stored in the wallet is particularly sensitive. Further, a minimalist approach to data collection and retention could serve as an additional data security layer. Once an individual's identity is verified, source documents should not be stored, and sensitive information should not be collected nor retained by default.

Streamlining cyber security laws and obligations [Q2(a) and (d), Q13(a)]

Suggestion: The Government should consolidate existing cyber security rules and laws to improve clarity of cyber security requirements. Any reform to or consolidation of existing reporting regimes should ensure that the distinct and important purposes of those regimes are carefully considered to ensure there are no resultant regulatory gaps.

If a Cyber Security Act was to be introduced, it should not be utilised to introduce new obligations or extend existing ones – unless they address pre-identified regulatory gaps.

Background:

Australia has multiple cybersecurity focused sector-specific laws or standards. Cyber security rules and requirements are developed in policy, regulatory, federal/state and departmental silos, resulting in duplication, dilution of efforts, and persistent legal uncertainty.[4]

By way of example, several mandatory reporting obligations exist for specific types of businesses. Those specific reporting obligations are spread across multiple pieces of legislation. This piecemeal regulatory environment is difficult to navigate for both public and private sector stakeholders and heightens the risk of end user confusion and the propensity for conflicting or overlapping rules. For example, current reporting requirements under various federal regulatory regimes include:

a) ***Security of Critical Infrastructure Act 2018*** (SOCI Act): under the SOCI Act, critical infrastructure asset owners and operators must report cyber security incidents having a "significant impact" within 12 hours of becoming aware of the incident, and other cyber security incidents having a "relevant impact" within 72 hours of becoming aware of the

[4] See e.g., Fair, Patrick (2020): Australian Cyber Security and Online Safety Infrastructure Chart, Deakin University, July 2020, available at PowerPoint Presentation (patrickfair.com) (accessed on 14 April 2028).

incident.[5]

b) In the financial services sector, the ***Prudential Standard CPS 234 on Information Security*** requires entities regulated by the Australian Prudential Regulation Authority (APRA) — including banks, insurers, and superannuation funds — to notify the regulator of material information security incidents within 72 hours. Entities must also notify APRA of material information security control weaknesses within 10 business days.[6]

c) Under the Notifiable Data Breaches (NDB) scheme, any organisation or agency the ***Privacy Act*** (1988)[7] – currently under review – covers, must notify affected individuals and the Office of the Australian Information Commissioner (OAIC)[8] when a data breach is likely to result in serious harm to an individual whose personal information is involved.

To add to the complexity, over the past year, several state-led cyber security strategies (see e.g. NSW Government Cyber Security Strategy; Victoria's Cyber Strategy - Mission Delivery Plan (2022-23)), and government portfolio-specific strategies (see e.g. Defence Cyber Security Strategy and 2022 Defence Information and Communications Technology Strategy) have also been released. These strategies and initiatives are not closely aligned or 'interlinked'.

The existence of distinct and overlapping requirements contained in legislation, regulation, strategies, plans and other guidance at federal, state and local government levels makes the cyber security landscape increasingly complex and has created ambiguity for public sector and private sector stakeholders.

If the Government decided to develop a Cyber Security Act, a comprehensive assessment of existing relevant legislation and regulation should be conducted to prevent duplication, overlaps and unnecessary regulatory and compliance burden. Such an Act ought to consider the issues raised in recent and ongoing consultations (i.e., Privacy Act Review Report, Digital Identity regime, and other data policy related matters). The focus should be on consolidating and streamline existing rules and laws to improve clarity of cyber security requirements, and to resolve the gaps and inconsistencies in current legislation and regulatory frameworks.

Question 13(a) proposes a single reporting portal for all cyber incidents, harmonising existing requirements to report separately to multiple regulators. Clarification on how such a portal would function, and in particular, how different reporting requirements (e.g. SOCI Act

[5] CISC (2023): Security of Critical Infrastructure Act 2028 – General Guidance for Critical Infrastructure Assets, February 2023, available at: SOCI Obligations Factsheet (cisc.gov.au) (accessed on 4 April 2023).
[6] APRA (2029): Prudential Standards CPS 234 – Information Security, July 2029, available at: cps_234_july_2019_for_public_release.pdf (apra.gov.au) (accessed on 4 April 2023).
[7] Attorney-General's Department (2023): Privacy Act Review Report, 16 February 2023, available at: Privacy Act Review Report | Attorney-General's Department (ag.gov.au) (accessed on 4 April 2023)
[8] OAIC (2023): Data breach preparation and response, available at: https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/preventing-preparing-for-and-responding-to-data-breaches/data-breach-preparation-and-response (accessed on 4 April 2023).

requirements) and obligations (e.g. those anchored in the NDB scheme) are considered, would be helpful. If a single reporting portal was introduced, the portal should be designed to ensure the reporting requirements for each regime are incorporated.

In February 2023, the Department of Home Affairs announced the establishment of a Cyber Security Coordinator to direct cyber security work across Government, support a streamlined cyber breach response and help Australians to manage the consequences of any cyber security incidents.[9] A 'one-stop-shop' for all cyber incidents would improve efforts to identify the root cause of those incidents and coordinate whole-of-government responses to data breaches.

Effective coordination of policy and regulatory frameworks by Government should be a priority. auDA considers the Tech Policy Design Centre's (TPDC) Tech Policy and Regulation Coordination (TPRC) Model sets out good practice and could be used to enhance regulatory coherence.[10]

Reform to the Security of Critical Infrastructure Act [Q2(b)]

Suggestion: Prior to considering further changes to the SOCI Act, the Government should allow time for critical infrastructure operators to have fully adopted, assessed, and evaluated recent amendments. Making additional amendments prematurely could lead to unintended consequences.

The Government should also await potential changes to the Privacy Act before making further amendments to the SOCI Act.

Background:

As an operator of critical infrastructure assets, auDA is subject to SOCI Act obligations. Given the criticality of the DNS to the functionality of the internet, auDA complies with ISO 27001 and engages an independent party to undertake annual audits of its own security. auDA also helps to ensure Australia's DNS remains secure by requiring all accredited registrars to adhere to ISO 27001 and adopt the Australian Signal Directorate's Essential Eight.[11]

Question 2(b) of the Discussion Paper requests feedback on whether further reform to the SOCI Act is required. auDA notes that amendments to the SOCI Act have been made only recently and an independent review of the operations, effectiveness and implications of the Act is yet to be conducted.[12] Additional substantial amendments at this time would likely be premature.

---

[9] See Clare O'Neil's MP speech at the Australian Information Security Association's (AISA) Australian Cyber Conference 2023, 22 March 2023, available at: Clare O'Neil MP > Australian Information Security Association's (AISA) Australian Cyber Conference 2023 (clareoneil.com.au) (accessed on 16 April 2023)

[10] See TPDC (2023): Cultivating Coordination – Research Report, available at TPDC_Cultivating_Coordination_2_20230221.pdf (techpolicydesign.au) (accessed on 14 April 2023).

[11] auDA (2021): Registrar Accreditation, available at: Registrar Accreditation | auDA (accessed on 12 April 2023).

[12] See section 60A (Independent Review) of the *Security Legislation Amendment Act 2022* (Critical Infrastructure Protection).

Therefore, auDA recommends that the Government allows time for critical infrastructure operators to have fully adopted, assessed, and evaluated the recent changes. This process is vital to ensuring that any new amendments to the SOCI Act requirements and obligations are based on evidence, are consistent and complementary to existing policies, and address a genuine and clearly identified gap. Further, noting the ongoing review of the Privacy Act, auDA suggests the Government awaits potential changes to privacy laws before considering making further amendments to the SOCI Act.

With respect to the proposed extension of the definition of 'critical assets', auDA notes that the definition of 'asset' under the SOCI Act is already broad. The SOCI Act defines an asset as a system, network, facility, computer, computer device, computer program, computer data, premises, and any other thing.[13] 'Systems' and 'customer data' appear to be already captured by the existing definition (e.g., under 'systems' and/or 'any other thing'). This raises the question of what practical implications with respect to the granted ministerial powers the extension of the current definition would have. auDA suggests the Government provides sufficient clarification on the intent and practical consequences of such amendments.

Specific cyber security obligations of company directors [Q2(c)]

Suggestion: Cyber risk should be treated as high-priority business risk by boards and executives. The Cyber Security Governance Principles developed jointly by the Australian Institute of Company Directors and the Cyber Security Cooperative Research Centre provide a comprehensive practical framework for effective board oversight of cyber security.

Background:

As an owner of critical infrastructure assets, auDA requires its board directors to comply with the legal obligations under the SOCI Act. auDA also requires board directors and staff members across all levels to conduct monthly cyber security trainings.

It is our understanding that under Section 180 of the ***Corporations Act*** (2001), directors are already required to consider cyber security related issues within the duty to act with reasonable care and diligence. Given the severity of most recent cyber incidents, auDA reiterates that cyber risk must be treated as high-priority business risk by boards and executives.

auDA notes that the Australian Institute of Company Directors (AICD), in collaboration with the Cyber Security Cooperative Research Centre (CSCRC), recently published the Cyber Security Governance Principles. The Principles are a practical framework for effective board oversight of cyber security across five key areas, including building a cyber-resilient culture, and preparing

[13] See *Security of Critical Infrastructure Act* 2018, Division 2, Section 9, available at: Security of Critical Infrastructure Act 2018 (legislation.gov.au)

and responding to a significant cyber incident. They included practical examples and case studies and serve as guidelines for directors.

Build cyber resilience in the Asia-Pacific region [Q3]

Suggestion: The Government should utilise forums such as the Asia Pacific Regional Internet Governance Forum (APrIGF) to build stronger alliances and strengthen regional cyber resilience. Adopting the multi-stakeholder approach, the APrIGF event provides a platform for discussion and collaboration to advance internet governance development in the Asia Pacific region.

auDA considers it important that the Government continues to fund regional cyber capacity building through engaging with Computer Emergency Response Teams and Law Enforcement Agencies.

The Government should also continue to support and fund the Department of Foreign Affairs and Trade's Cyber and Critical Tech Cooperation Program.

Background:

In August 2023, auDA will host the Asia Pacific Regional Internet Governance Forum (APrIGF), one of the key regional initiatives on Internet governance. Adopting the multi-stakeholder approach as its core principle, the APrIGF event provides a platform for discussion exchange and collaboration at a regional level to advance internet governance development in the Asia Pacific region.

Bringing together representatives from the Asia Pacific internet community, including Government officials, civil society representatives, industry leaders, technical experts and academics, the APrIGF will focus on emerging technologies and drive discussions on whether the Asia Pacific is ready for the next phase of the internet.

The APrIGF provides an opportunity for the Australian Government and others to strengthen collaboration, support capacity building initiatives in the Asia-Pacific region. It also provides an opportunity to work more closely with our regional neighbours to build strong networks and share information on emerging technologies and related topics such as security-by-design principles and data privacy.

auDA would welcome Government's participation in the APrIGF and its support in bringing the Asia Pacific internet community together. Building stronger alliances with Asia Pacific counterparts would help to better position Australia in the global policy debate about emerging technologies and cyber security.

In this context, auDA acknowledges the importance of the work of the Asia Pacific Network Information Centre (APNIC), the regional internet registry for the Asia Pacific region, and the Asia Pacific Top Level Domain Association (APTLD), an association for ccTLD (country-code Top Level Domain) registries in Asia Pacific region. Through their diverse activities and capacity building in

the region, both organisations support the maintenance of an open, globally connected and secure internet.

auDA recommends the Government continues to fund regional cyber capacity building through engaging with Computer Emergency Response Teams (CERTs) and Law Enforcement Agencies (LEAs). Further, the Government should consider strengthening information sharing networks to detect and prevent (and respond to and recover from) cyber-attacks a strategic priority. auDA also recommends it continues to support and fund the Department of Foreign Affairs and Trade's Cyber and Critical Tech Cooperation Program.

Information sharing between government and industry [Q7]

Suggestion: To improve threat information sharing with industry, the Government should ensure that the information is:
- specific and comprehensive (e.g. targeted towards critical infrastructure sectors)
- shared securely and confidentially (if required) and in a timely and ongoing manner
- shared bi-directionally for Government and industry to develop mutual threat understanding
- effectively leveraged to support organisations in developing actionable threat mitigation measures.

Background:

auDA frequently engages in several information sharing initiatives. auDA believes that information sharing between Government and industry can be improved through the following measures:

- **Sharing of specific information**: due to the severity, magnitude and sophistication of most recent attacks, generic threat intelligence is often of limited value to organisations (e.g. critical infrastructure operators). Specific threat information would be more effective in helping organisations implement mitigation measures.

- **Forming subject-specific partnerships**: Government should consider forming additional targeted partnerships with industry to improve information sharing. Such partnerships could be tiered in a way that specific "groups" (e.g. SMEs, critical infrastructure operators, etc.) are established to inform and share with Government threat data and insights specific to their sector. Most importantly, information-sharing between industry and Government should be bidirectional, not one-directional.

- **Assuring confidentiality and security of shared information**: clarification on the confidentiality and security of shared information (e.g. through the use of encryption and other security measures) would be beneficial and help to build trust between Government and industry.

Assistance for small businesses [Q15(a)]

Suggestion: Small businesses hold increasingly large volumes of Australians' personal information. Nevertheless, most of them have insufficient cyber protection in place.

auDA recommends Government encourages and incentivises small businesses to implement targeted measures such as delivering staff trainings, adopting cyber security standards (e.g. ISO 27001) and conducting cyber security exercises and controls testing to improve their cyber resilience.

The Government should consolidate existing cyber security guidance material and checklists and make them more engaging and accessible to often time-poor small businesses.

Background:

Small businesses hold increasingly large volumes of Australians' personal information. Further, many small (and medium-sized) businesses play an integral role in the supply chains of critical infrastructure operators, the defence industry, and Governments entities. This makes small businesses attractive targets for malicious actors.

auDA's Digital Lives research found that less than half of the small businesses surveyed feel very confident with processes to protect their online security. Only around one in five small businesses have a cyber security policy and formal training or management review processes in place. Many small businesses feel "reluctant" to increase spending on security measures. Such findings are concerning and reiterate the need to build awareness among small businesses. The successful uplifting of cyber resilience and hygiene across the entire economy, requires measures to make small businesses more cyber secure.

auDA recommends that Government should consider incentivising and/or encouraging small businesses to adopt measures such as:

- providing regular cyber awareness trainings for all staff members,
- implementing common cyber security standards such as ISO 27001, and
- conducting cyber security exercises on a regular basis to test cyber security controls and mechanisms, and ensure that cyber defence responses are robust.

Cyber security is not a set and forget exercise. Like physical security, it must be maintained, updated as technology and the threat environment evolve, and security standards change.

auDA notes that several guides and checklists have been produced to help small businesses increase their cyber security:

- Australian Competition and Consumer Commission (ACCC) and ScamWatch: Protect your small business
- Australian Cyber Security Centre (ACSC): Small Business Cyber Security Guide

- Australian Small Business and Family Enterprise Ombudsman (ASBFEO): Cyber Security Checklist
- Australian Tax Office (ATO): Top cyber security tips for businesses
- CPA Australia: Cyber Security Tips for Small Business

The Government should consider consolidating existing resources and look at ways the information can be more engaging and accessible to the often time poor SME owner.

Promote security by design in new technologies [Q19]

Suggestion: Considering the exponential increase in Internet of Things (IoT) devices, we recommend the Government considers measures to make such devices secure-by-design. Existing internationally recognised standards (ESTI EN 303 645 (Cyber Security for Consumer Internet of Things) should be considered to encourage vendors and manufacturers to enhance data security, software update, and password control requirements.

IoT security should be considered as a collective responsibility. Government should encourage manufacturers and consumers to take joint responsibility for the cyber security of IoT devices.

Background:

While an increasing number of smart devices are connected to the internet, security and resilience are not sufficiently built in by design, leading to insufficient cyber security.

As stated by Minister O'Neil at the Sydney Dialogue event on 4 April 2023[14], poorly secured IoT devices and services can become entry points for cyber-attacks, compromising sensitive information, weaponisation, and threatening the security of Australian users.

auDA recommend the Government should consider measures to make internet-connected things in Australia secure-by-design, resilient to cyber incidents, and quickly patched when vulnerabilities are discovered.[15] This is particularly important as Australians' reliance on IoT devices increases. Globally, the number of smart IoT devices connected to the internet is forecast to grow to more than 29 billion by 2030 (from 9.7 billion in 2020).[16]

[14] Minister Clare O'Neil (2023): Sydney Dialogue Speech, Australian Strategic Policy Institute, 4 April 2023, available at: Clare O'Neil MP > Sydney Dialogue - Speech (clareoneil.com.au) (accessed on 11 April 2023).
[15] See also comments provided by the CSCRC, ACCC, AustCyber and OAIC to the Department of Home Affairs consultation on "Strengthening Australia's cyber security regulations and incentives", August 2021, submissions available at: Strengthening Australia's cyber security regulations and incentives (homeaffairs.gov.au) (accessed on 11 April).
[16] Statista (2022): Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2021, with forecasts from 2022 to 2030, November 2022, available at: IoT connected devices worldwide 2019-2030 | Statista (accessed on 21 March 2023).

In an effort to make IoT devices more secure, the Government should consider existing internationally recognised standards such as ESTI EN 303 645 (Cyber Security for Consumer Internet of Things). Some of the baseline requirements in the standard are:

- No universal default passwords
- Implement a means to manage reports of vulnerabilities
- Keep software updated
- Ensure that personal data is secure

auDA notes that other sector submissions have discussed the concept of a certification and labelling scheme in this area. auDA notes these submissions with interest but auDA does not have a position on this matter. For example, auDA notes that the IoT Alliance proposes a consumer-informed, market driven, industry-led certification and labelling scheme supported by Government.[17] Such schemes have already been implemented in other jurisdictions: the Cyber Security Agency of Singapore (CSA) has launched a Cyber Security Labelling Scheme (CLS) for consumer smart devices, and Germany has introduced the IT Security Label to enhance digital consumer protection.

If Australia was to adopt a CLS, it is important to ascertain that the scheme is interoperable with other internationally recognised schemes and standards. Labelling should be consistent with those used by other major markets. Further, a labelling scheme must be accessible and simple to understand for consumers.

IoT security should be considered as a collective responsibility. Manufacturers of IoT smart devices should not be solely responsible for the security of those devices. Consumers have to be made more aware of security risks in IoT (see our comment on "**Uplifting cyber skills**"). Malicious actors will only stand no chance if manufacturers and consumers take joint responsibility for the cyber security of IoT devices. Adopting a whole-of-nation approach, all stakeholders must be involved in creating and leveraging the Internet of *secure* Things ecosystem.

Conclusion

auDA recommends the Government in its 2023-2030 Australian Cyber Security Strategy addresses the importance of maintaining the security and integrity of the internet as the enabler of Australia's digital economy.

[17] IoT Alliance Australian (2021): Response to Strengthening Australia's Cyber Security Regulations and Incentives Discussion Paper, August 2021, available at: Response to Strengthening Australia's Cyber Security Regulations and Incentives Discussion Paper (iot.org.au) (accessed on 14 April 2023).

Considering the long-term horizon of the Strategy (2023-2030) in the context of the dynamic and fast-changing cyber security environment, auDA recommends Government sets out key milestones and clearly measurable goals to assess performance of the Strategy, and allow for amendments, if and where required.

Should the Department of Home Affairs or Government wish to consult further on incentives or other mechanisms to improve Australia's cyber-security, auDA would welcome the opportunity to provide input.

If you would like to discuss our submission, please contact auDA's Internet Governance and Policy Director, Jordan Carter [redacted]

.au Domain Administration Ltd
www.auda.org.au

PO Box 18315
Melbourne VIC 3001
info@auda.org.au