DTA Digital Identity Legislation 2021

# SUBMISSION

AISA

AUSTRALIAN INFORMATION SECURITY ASSOCIATION

# EXECUTIVE SUMMARY

Australian Information Security Association (AISA) welcomes the request for submissions from the Australian Government's Digital Transformation Agency in relation to the Trusted Digital Identity Framework (TDIF) enforced by legislation as outlined in the Position Paper. As part of the consultation on Australia's Digital Identity legislation, the Australian Government recently sought feedback on the Digital Identity Legislation Position Paper. The purpose of the legislation is to establish permanent governance arrangements for the system. It will enshrine in law a range of privacy and consumer protections and enable the Digital Identity system to be used confidently across federal, state, territory, and local governments as well as the private sector.

AISA champions the development of a robust information security sector by building the capacity of professionals in Australia and advancing the cyber security and safety of the Australian public as well as businesses and governments in Australia. Established in 1999 as a nationally recognised and independent not-for-profit organisation and charity, AISA has become the recognised authority and industry body for information security, cyber security, and privacy in Australia. AISA caters to all domains of the information security industry with a particular focus on sharing expertise from the field at meetings, focus groups and networking opportunities around Australia.

AISA's vision is a world where all people, businesses and governments are educated about the risks and dangers of cyber-attack and data theft, and to enable them to take all reasonable precautions to protect themselves. AISA was created to provide leadership for the development, promotion, and improvement of our profession, and AISA's strategic plan calls for continued work in the areas of advocacy, diversity, education, and organisational excellence.

This response offered by AISA represents the collective views of over 7,000 cyber security and information technology professionals, allied professionals in industries such as the legal, regulatory, financial and prudential sector, as well as cyber and IT enthusiasts and students around Australia. AISA members are tasked with protecting and securing public and private sector organisations including national, state and local governments, ASX listed companies, large enterprises, NGO's as well as SME/SMBs across all industries, verticals and sectors.

AISA proactively works to achieve its mission along with its strategic partners. These include the Australian Cyber Security Centre (ACSC), AustCyber, Cyrise, the Risk Management Institute of Australia (RMIA), the Australian Strategic Policy Institute (ASPI), the Australian Institute of Company Directors (AICD), the Oceania Cyber Security Centre (OCSC), the Australian Security Industry Association Limited (ASIAL) as well as international partners such as $(ISC)^2$, ISACA, the Association of Information Security Professionals (AiSP) and over twenty five Universities and TAFEs across Australia.

It is AISA's hope that the Digital Transformation Agency will consider the responses to the Position Paper and incorporate recommendations included as part of a holistic drive by the Australian Government to help deliver a safer and more secure cyber world for the people of Australia, both now and well into the future.

# THE AISA VIEW OF THE POSITION PAPER

The Australian Information Security Association (AISA) is supportive of the process to seek consultation with industry and the broader community on the strategy to improving the DTA Trusted Digital Identity Legislation. AISA is supportive of the fundamental objective of the Trusted Digital Identity Framework (TDIF) to help Australians verify their identity in a safe and secure way when accessing government services online. In addition, providing a mechanism for individuals to voluntarily use their identity to access multiple services, thereby simplifying and minimising the need for disparate multiple identities when accessing government services.

It is important to recognise the introduction of a system that minimises the need for multiple identities can also be construed as the revival of the failed Australia Card and Access Card initiatives which have been wholly rejected by the Australian public. As per the Information Integrity Solutions Pty Ltd (IIS) submission, one of the reasons the TDIF is acceptable is that it does NOT REQUIRE a single identity. The individual can have multiple identities each of which is verified by different verifying parties.

This is absolutely critical for civil liberties, freedom, privacy and to avoid creating a single Digital God who has digital life and death power.

## SPECIFIC AREAS OF CONCERN AND RECOMMENDATIONS

AISA has identified the following key areas of concern contained within the Exposure Draft:

- Ensuring that the use of Digital Identities created and managed through the TDIF system is voluntary, and alternatives continue to exist in perpetuity which are still “usable” and “accessible” by Australians and deliver the same level of access.
- Australians are not coerced to use TDIF systems.
- Genuine oversight and protection from surveillance by law enforcement and national security agencies. This includes but is not limited to legislations such as the Telecommunications and Other Legislation Amendment (TOLA) bill of 2020. This is vital to ensure trust between the Australian public and the Australian government is not eroded. A clear example of this oversight and form of trust abuse was demonstrated this year by law enforcement issuing warrants to access Western Australia’s COVID-19 contact tracing application (SafeWA). The societal benefit of the SafeWA app clearly outweighs law enforcement objectives and the same should be true for TDIF systems.
- Effective governance, oversight of the TDIF system, architecture, and continued evolution, use and adaption to prevent unintended consequences / blind spots due to legislative changes or scope creep that could lead to the erosion of public trust and confidence. This also includes preventing political influence in the body designated to provide oversight.
- Legislation should be structured to ensure the oversight authority has the resources to resolve multi-play / entity problems on behalf individual users, thereby shifting the burden from the individual to the oversight authority.

**Sections 5.3, 5.4.7, 6.4.1 and 6.4.5** – The bill should outline or be accompanied by statements indicating the funding provided to regulators to enforce and remediate issues. Lack of adequate and appropriate funding for the regulation and enforcement will result in legislation lacking the appropriate governance controls (e.g., fair and independent umpire).

**Sections 6.4.2** – The current structure and language used is vague and will ultimately lead to the watering down or abuse of appropriate independent oversight and governance and should be decoupled from Ministerial discretion. It would be more appropriate to create a consumer experience, privacy, and security

board with the composition of the board spelled out in the legislation. The board should function in a similar way to a commercial board with the power to veto decisions over TDIF rules and changes to accreditation rules as opposed to just an advisory board. It is also important for independence that the board has the power to report directly to Parliament. The appointment of the board should be individuals with suitable privacy, security, and customer experience backgrounds and who are not affiliated with large commercial entities. Ideally the board would be comprised of current or former privacy commissioners, state based Chief Information Security Officers as an example. The creation of an independent customer service commissioner would also be appropriate for inclusion as a board member.

**Sections 6.4.3** – The Oversight Authority be staffed by an Office separate from any Government Department (e.g., similar in function to the Office of the Australian Information Commissioner (OAIC)).

**Section 7.4.8** - All parties in the system be required to securely delete verification transaction data including meta-data and logs within a small number of days from the completion of the verification.

## ADDITIONAL AREAS OF CONCERN AND RECOMMENDATIONS

There are additional area of concern that should be addressed in the bill. The response submission from IIS, covers these additional concerns in more detail. Please refer to the appendix which also contains the IIS response.

## ABOUT THE LEAD AUTHOR

### Michael Trovato – AISA Board Director and Managing Director & Lead Security Advisor of IIS

**Mike Trovato** is a cyber security and technology risk advisor to boards, board risk committees, and executive management. He focuses on assisting key stakeholders with understanding the obligations and outcomes of effective privacy and cyber security. This includes solving an organisation's issues with respect to regulatory, industry, and company policy compliance and to protect what matters most in terms of availability, loss of value, regulatory sanctions, or brand and reputation impacts balanced with investment.

Mike is ICG's Global Cyber Practice Leader. Prior to joining IIS, he was the Founder and Managing Partner of Cyber Risk Advisors. Before then, he was Asia Pacific, Oceania and FSO Lead Partner EY Cyber Security; GM Technology Risk and Security for NAB Group; a Partner within Information Risk Management at KPMG in New York, and has held financial services industry roles at Salomon Brothers and MasterCard International.

Mike is a Graduate of the Australian Institute of Company Directors (GAICD), Member Australian Information Security Association (AISA), an AISA Board Member, ISACA Melbourne Chapter Board Member, and Member of National Standing Committee on Digital Trade.

Mike's professional credentials include being a Certified Information Systems Manager (CISM); Certified Data Privacy Solutions Engineer (CDPSE); Certified Information Systems Auditor (CISA); and PCI DSS Qualified Security Assessor (QSA). He is also a member of the International Association of Privacy Professionals (IAPP) and is an ICG Accredited Professional. He has an MBA, Accounting and Finance and BS, Management Science, Computer Science, and Psychology.

Mike is the co-author of **The New Governance of Data and Privacy: Moving from compliance to performance**, Australian Institute of Company Directors, November 2018.

## Malcolm Crompton AM – Founder & Lead Privacy Advisor of IIS

**Malcolm Crompton** is the Lead Privacy Advisor and was the founder and first Managing Director of Information Integrity Solutions Pty Ltd (IIS), a global consultancy based in Asia Pacific, specialising in data protection and privacy strategies. IIS assists companies increase business value and customer trust, and assists governments meet the high standards expected of them in the handling of personal information.

As Australia's Privacy Commissioner from 1999 to 2004, Malcolm led the implementation of the nation's private sector privacy law. He hosted the 25th International Conference of Data Protection and Privacy Commissioners in Sydney in 2003.

Malcolm was the founding President of the International Association of Privacy Professionals Australia New Zealand (iappANZ), an affiliate of the International Association of Privacy Professionals (IAPP). He served as a Director of iappANZ until 2016. He was a Director of IAPP from 2007 to 2011 and is an IAPP Certified Information Privacy Professional.

Through IIS, Malcolm has advised a wide range of industry sectors. He has also consulted to the Asia-Pacific Economic Cooperation forum (APEC) regularly on implementation of the APEC privacy framework and to the Organisation for Economic Cooperation and Development (OECD).

Malcolm is a Director of Bellberry Limited, a private not-for-profit company which provides privacy and health ethics advisory services. Malcolm is a member of the NSW Data Analytics Centre Advisory Board and the NSW Government's Information and Privacy Committee. He is also a Fellow of the Australian Institute of Company Directors and member of the International Association of Privacy Professionals (IAPP). He chaired the board of PRAXIS Australia Ltd, a private not-for-profit company that promotes the conduct of ethical research involving human participants, for the first five years through its start-up phase until 2019.

Between 1996 and 1999, Malcolm was Manager of Government Affairs for AMP Ltd. In the previous 20 years, he held senior executive positions in the Federal Department of Finance, served as both a superannuation scheme trustee and scheme founder and worked in the Transport and Health portfolios. He has degrees in Chemistry and Economics.

Malcolm was made a Member of the Order of Australia in the 2016 Queen's Birthday Honours for significant service to public administration, particularly to data protection, privacy, and identity management, and to the community. Malcolm received the 2012 Privacy Leadership Award in Washington DC from the IAPP in recognition of his global reputation and expertise in privacy. He received the inaugural Chancellor's Medal for distinguished contribution to the Australian National University in 2004.

Malcolm is a co-author of **The New Governance of Data and Privacy: Moving from compliance to performance**, Australian Institute of Company Directors, November 2018.

## ABOUT CONTRIBUTING AUTHORS

### Damien Manuel – AISA Board Director and Industry Professor / Director of Deakin's Centre for Cyber Security Research and Innovation (CSRI)

**Damien Manuel** is the Industry Professor and Director of Deakin's Centre for Cyber Security Research & Innovation and is the Chairperson of the Australian Information Security Association (AISA), a not-for profit organisation which aims to improve Cyber Security in Australia at a Government, Industry and Community level.

In his former role as the Chief Information Security Officer (CISO) for Symantec Australia and New Zealand, Damien worked with senior executives in the region to align security architectures to industry best practices. Damien also worked as a senior information security governance manager and later as an enterprise IT and security risk manager at National Australia Bank (NAB), where he was responsible for managing the bank's information security standard globally. He also held senior roles at RSA, Telstra, Ericsson and Melbourne IT and was on the board of the Oceania Cyber Security Centre (OCSC).

Damien is currently on CompTIA's Executive Advisory Committee in the USA, the Victorian Ombudsman's Audit and Risk Committee, the board of RSA Australia, the chair of Standards Australia's Standards development committee for cyber security and privacy and helps mentor entrepreneurs through CyRise, Australia's only cyber security startup accelerator.

Damien has supported CompTIA for over 18 years through the development of CompTIA Server+, CompTIA Network+, CompTIA Security+ and the CompTIA Advanced Security Practitioner certification. Damien's passion for making a difference motivated him to establish Information Technology community resource centres to improve literacy and skills in impoverished and disadvantaged communities in Kenya, Laos, Uganda and Cambodia.

Underpinning his over 25 years of experience is a diverse educational grounding ranging from the highest security, audit and governance certifications complemented by an Executive MBA with an international business focus. Damien also has a background in genetic engineering and is passionate about science. He has spoken on a number of podcasts (including with Dr Karl), conference keynotes internationally and locally, radio and TV appearances.