NATIONAL ARCHIVES OF AUSTRALIA

Protecting Critical Infrastructure and Systems of National Significance: Submission to Department of Home Affairs

NATIONAL ARCHIVES OF AUSTRALIA

27 NOVEMBER 2020

RKS R1201062020

Contents

1. EXECUTIVE SUMMARY

About the National Archives

The National Archives of Australia (National Archives), established under the *Archives Act 1983*, provides leadership in best practice management of the official record of the Commonwealth and ensures that Australian Government information of enduring significance is secured, preserved and available to government agencies, researchers and the community. The National Archives:

- sets information management requirements for Australian Government agencies
- ensures the Australian Government creates and keeps records of its actions and decisions to demonstrate accountability to the community and evidence the integrity of the operations of the Australian Public Service
- authorises destruction of information assets with no ongoing value to government or community
- selects and preserves the most significant records of the Australian Government; and
- makes these records available to government and community as a national resource to enrich and inform how we live today, and into the future.

It provides advice and assurance that the Australian Government has access to authentic, reliable and usable Commonwealth records to enable evidence-based decisions, provide sound advice, develop good policy and deliver programs effectively and, to facilitate access to the archival resources of the Commonwealth.

Community members need to be confident that the information they share with government will be held securely, shared responsibly and made available as accurate proof of their entitlements when needed. Good information management is essential to building trust in the creation, collection and use of Australian government information as documentary heritage, to meet the outcomes required by government and community.

The National Archives understands that well-managed government records are foundational to the Australian Government's digital transformation and innovation agenda, to deliver world-leading digital services, as well as the future cultural identity and economic prosperity of the nation. It is a national resource for knowledge creation and sharing, which underpins the integrity of Australia's system of democracy, enabling trusted interactions between the community and a transparent, responsive and accountable government.

2. THE ROLE OF THE NATIONAL ARCHIVES IN INFORMATION MANAGEMENT

Accountability of government is underpinned by a records regime that upholds the rules of evidence. A chain of evidence is easily broken if entities fragment their records across various paper based and digital systems. As part of digital continuity, government entities are transitioning to entirely digital work processes, meaning complete records will be kept of business processes including authorisations and approvals.

End-to-end digital processes, operating in an information governance framework, will also ensure that records are enriched by metadata and assured by comprehensive and secure audit trails. The foundation upon which we can achieve this is digital continuity – a framework that ensures government data is authentic, accurate, complete and available for use but protected from abuse. Most importantly there is a need for reliable government records that are reusable now and in the future.

In 2011 our *Digital Transition Policy* mandated that high-value government information created in digital form be digitally maintained and accessible for as long as required. Subsequently, in 2015, we launched the *Digital Continuity 2020* (DC2020) Policy as a whole-of-government approach to information governance through the principles of data asset management, digital work processes and information interoperability. With the subsequent release of the Information Management Standard 2017, we have continued to drive the transition to mature digital information governance, work processes and information interoperability.

The results of our annual survey, Check-up PLUS, have shown that the DC2020 Policy has achieved significant progress in transitioning agencies' information management capability, as 81 per cent of agencies now manage most information digitally, up from 30 per cent in 2010. However, implementation is progressing at varying rates among agencies, one-third of which are not expected to adequately meet the requirements of the policy by December 2020. To address this continuing challenge, the National Archives has initiated the 'DC2020 – Agency Implementation Support Program' to assist those agencies identified as having lower information management maturity. A Check-up PLUS survey of all government agencies will be undertaken, reporting to the Minister and Prime Minister in 2021, setting out progress against the policy's objectives.

The National Archives has moved ahead in consultation with key information agencies, to finalise the new *Building trust in the public record: managing information and data for government and community policy*, to improve how Australian Government agencies create, collect, manage and use information assets (records, information and data). It will commence on 1 January 2021.

3. COMMENTS ON THE EXPOSURE DRAFT BILL

The National Archives supports this bill and the need to establish a positive security culture to protect the critical infrastructure and assets of most national significance. The cyber security threat is real and legislation to establish stronger accountability for the protection of our critical assets to safeguard Australia is urgent and important.

A number of the measures described in this bill could be applied to protect critical Australian government data assets. However, this needs to be supported by funding measures specifically targeted at improving and strengthening cyber security across the Australian Government. The National Archives supports the inclusion of the data storage and processing sector in the *Security of Critical Infrastructure Act 2018* but notes that the Bill deals with physical facilities and information technologies. The National Archives believes that the information that is managed by this infrastructure should be identified as an asset in its own right. It is the information, not the technology, that is of the greatest potential value to the community and to malevolent actors.

Throughout history, warfare has damaged and destroyed assets vital to nations' cultural heritage and national identity. While physical damage is often clear and immediate, cyberattacks targeting a nation's identity—its way of life, history, culture and memory— do not have the same physical visibility, but have the potential to cause more enduring and potentially irreparable harm.

In our increasingly digital world, it isn't difficult to imagine the types of cyberattacks we will be likely to face and the degree of impact on irreplaceable national identity assets.

A cyberattack targeting national identity assets has the potential to cause major disruption and collective psychological damage. Such an attack would almost certainly lead to the further erosion of public trust in Australia's democratic institutions and our reputation internationally. Our vitally important national identity assets are not adequately protected, and a long-term plan to protect them is lacking. The damage that their loss would cause makes them a tempting target for the next wave of cyber-enabled political and foreign interference.

National and state government archives play the role of 'impartial witnesses', identifying and holding this information and holding the government to account under the rule of law and in the 'court' of history. Many other institutions have additional holdings that collectively form our national identity assets. We need to trust that these impartial witnesses can identify, keep and preserve this evidence. This is a matter of national security and is at the heart of our society. The biggest impact from an attack on national identity assets would be the resulting corrosion of trust in public institutions. As foreign interference in other countries' elections has demonstrated, the erosion of trust is more corrosive to democracy than the win or loss of any particular candidate. Attacks on truth and trust affect individuals and nations and, while just one breach can erode trust, a concerted campaign can do much more.

We note recommendations provided by Anne Lyons, Fellow – Professional Development of the Australian Strategic Policy Institute , on this issue, in the report Identity of a nation – Protecting the digital evidence of who we are. We suggest this matter should be addressed either in this Bill or a complementary Bill with policy relevance, outlined as follows:

1. Australia's national identity and high-value data and information, the destruction or corruption of which would have a serious impact on our sovereignty, should be recognised as part of our critical infrastructure framework.

2. The Trusted Information Sharing Network should examine existing coverage of vulnerabilities and establish a dedicated forum on that data and information.

3. The Australian Government should explore a legislative response to managing and evaluating that data on a coherent national basis.

4. National security agencies should engage with the National Archives to undertake a risk assessment of the archives' digital national identity assets and jointly develop proposals to defend them from future attack.

5. The National Archives use its legislated powers to prescribe what government information and data constitutes national identity assets and set mandatory management and governance standards to ensure, protect and maintain their long-term integrity and reliability of those assets.

6. The Australian Productivity Commission should explore the value of digital national identity assets to Australia, defining the parameters to be considered in identifying and valuing them and the cost should they be destroyed or manipulated, or should trust in their authenticity and reliability be eroded.

7. The Australian Government, through the Department of Finance, should investigate and provide guidance and standards for agencies to assess the value of their information and data assets.

8. The Australian Government, through the Department of Finance, should develop a tool to assist organisations to assess the value of their data and digital information, to assist in developing strong business cases for protection.

9. A new funding model for memory institutions should be explored by Australian governments to help protect digital national identity material.

10. Digital preservation principles should be built into information security requirements, such as those in the Australian Government's Information security manual.

11. The Digital Transformation Agency, in conjunction with CSIRO's Data 61, should explore the use of blockchain technology to track, record and ensure the provenance of national identity and high-value data.

12. The Australian Cyber Security Centre (ACSC) should produce a 'state of the nation' report on cybersecurity health and readiness.

13. All public, private and community sector organisations holding national identity assets should be encouraged to publicly report their annual cyber resilience status.

14. The Australian National Audit Office, in conjunction with the ACSC, should explore the creation of an authenticity audit, so that internal and external auditors can assess digital assets on a scheduled, regular basis, employing a standardised methodology.

15. All Australian governments should better coordinate their information, data and related cyber policy agencies and strengthen information governance as the overarching requirement, incorporating all elements of information management, security, privacy and data management

3.1. Critical data

We note that the Bill considers a 'critical data storage or processing asset' as being owned by an external-to-government entity that provides services on a commercial basis. As such it appears to exclude data assets held within government systems. These data assets would be significant and potentially of the greatest value. We further note that the proposed definition of 'business critical data' appears too narrow to capture a wide range of information of critical importance. For example, records that provide citizens with evidence of rights and entitlements, such as immigration records or defence service records. Commonwealth Government agencies hold many other records vital for the operation of civil society.

The National Archives, as the archival resources of the Commonwealth and Commonwealth memory, notes that our collections are the primary source of data storage of data and information that is critical to national identity and memory. As the spirit of this draft Bill recognises, we place significant importance in investing in ICT and Cyber-resilience capability, as we develop our 5th Generation Digital Archive as a secure end-to-end digital repository for government information held by the National Archives.

This approach is designed to realise a reskilled and digitally competent workforce, the development and delivery of a new 5th Generation Digital Archive with an end-to-end Integrated Archival Management System (IAMS), with enhanced digital preservation capability, secure storage and a digital access platform, which will:

- improve the security (including against cyber-threats), information governance and management of records, information and data
- create efficiencies and cost savings for government through improved digitisation, earlier sentencing and disposal, and preservation of at-risk collections
- deliver better services and improved access to the national archival collection for the Australian public, researchers, as well as use by creative and data industries; and
- enable capability and capacity building, and knowledge sharing in our region.

4. RECOMMENDATIONS

Our recommendations specific to this Bill are as follows:

1. Information assets should be included as critical resources.
2. Data storage and systems owned by government should be included within the scope of the Bill.
3. The definition of ‘business critical data’ should be expanded to include records supporting citizen rights and entitlements as well as other information required for the effective operation of civil society.