gai brodtmann

To Whom It May Concern

Thank you for the opportunity to provide input into the development of the Government's new critical infrastructure framework.

This submission recommends:

- Increasing the number of sectors covered in the framework
- Including institutions that protect our democracy
- Including institutions that preserve and share our national identity and story, and
- Enhancing the cyber resilience of government agencies, as a matter or urgency.

Given the focus and commitments in the 2020 Cyber Security Strategy,[i] this submission assumes reference will be made to cyber security and digital, information and operational technology in the framework and future regulation.

This point is made because the term cyber security did not appear in the *Security of Critical Infrastructure Act 2018*[ii].

Sectors

When compared to our Five Eyes partners, Australia is underdone in the number of sectors recognised as critical infrastructure.

The United States has 16 sectors[iii] 'whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.'

[redacted]

These are:

- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Financial Services
- Food and Agriculture
- Government Facilities
- Healthcare and Public Health
- Information Technology
- Nuclear Reactors, Materials and Waste
- Transportation Systems, and
- Water and Wastewater Systems.

The United Kingdom has 13 sectors[iv], which are classified as those 'facilities, systems, sites, information, people, networks and processes, necessary for a country to function and upon which daily life depends'.

These are:

- Chemicals
- Civil Nuclear
- Communications
- Defence
- Emergency Services

[redacted]

- Energy
- Finance
- Food
- Government
- Health
- Space
- Transport, and
- Water.

In contrast, Australia has just eight sectors[v] listed under the Trusted Information Sharing Network, the primary national mechanism for business-to-government information sharing and resilience-building initiatives to protect the critical infrastructure 'vital to Australia's social cohesion, economic prosperity and public safety'.

These are:

- Banking and Finance
- Communications
- Energy
- Food and Grocery
- Health
- Transport
- Water Services, and
- Commonwealth Government.

In keeping with the Five Eyes community and our 2018[vi] and 2020[vii] Five Country communique commitments, we need to increase the number of sectors classified as critical infrastructure in the new framework.

[redacted]

We need to separate out defence and the defence industrial base and include education, research and innovation, legal and professional services, mining and resources[viii], data and the Cloud[ix], emergency services, information technology and operational technology, chemicals, manufacturing, space[x], electoral systems and the institutions that preserve, protect and share our national identity.

The Government should also consider including State and Territory Government[xi].

Democracy

Our election systems and infrastructure are the very foundation of our democracy.

They underpin trust in the way we govern ourselves, and our values.

They are vital to the social wellbeing and cohesion of the nation.

Yet they are not yet recognised as critical infrastructure.

While voting in Australia is, in the main, paper-based[xii], our national, State, Territory and local voter registration databases are not.

Classifying our election systems as critical infrastructure would overlay the appropriate scrutiny and protections of these databases to assure the Australian people of the cyber resilience[xiii], and through it the security, of our democracy. This assurance is vitally important in a country where voting is compulsory, and in a world where election systems are increasingly under threat.

The US has acknowledged the importance of its election systems and infrastructure, even when it is voting is voluntary, by including it as a separate sub-sector[xiv] under the Government Facilities sector.

[redacted]

The sub-sector covers: 'a wide range of physical and electronic assets such as storage facilities, polling places, and centralized vote tabulations locations used to support the election process, and information and communications technology to include voter registration databases, voting machines, and other systems to manage the election process and report and display results on behalf of state and local governments.'

Australia has been a proud international advocate of democracy. If we are to maintain our global reputation, and the trust of the Australian people during these challenging times, we need to recognise the democratic systems that form the ballast to our way of life as the critical infrastructure they are.

National identity

National identity assets and institutions 'form the heart of who we are as a nation'[xv]. They are 'evidence of…our resources, our people, our culture, our way of life, our land, our freedom, our democracy'[xvi].

In her 2018 Australian Strategic Policy Institute paper *Identity Of A Nation*[xvii], Anne Lyons wrote:

'Keeping national identity assets safe and accessible is vital not only for chronicling Australia's past, but for supporting government transparency, accountability, the rights and entitlements of all Australians and our engagement with the rest of the world.'

'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— wouldn't have the same physical visibility, but have the potential to cause more enduring and potentially irreparable harm.'

[redacted]

The US also recognises national monuments and icons[xviii] as a critical infrastructure sub-sector under the Government Facilities sector. The sub-sector 'encompasses a diverse array of assets, networks, systems, and functions located throughout the United States'[xix]. Many monuments and icons are listed in either the National Register of Historic Places or the List of National Historic Landmarks.

As with our democratic systems, Australia should follow the US lead and recognise national identity assets in the new framework.

Government agencies

Both the 2020 Cyber Security Strategy[xx] and Industry Advisory Panel Report[xxi] acknowledged the need for government agencies to be the 'exemplar', 'to lead by example' so Australians 'have confidence that their data is safe' and systems and data are secure.

These are agencies that hold sensitive and personal data on every Australian and information[xxii] across a range of economic, commercial, policy or regulatory, national security, program and service delivery and corporate activities. They should, therefore, be the benchmark against which others measure themselves.

Unfortunately, multiple Australian National Audit Office cyber resilience reports[xxiii], over many years, have found that just 29% of audited government entities comply with mandatory cybersecurity standards—even after the Bureau of Meteorology, Department of Parliamentary Services,[xxiv] Australian Bureau of Statistics [xxv]and Australian National University[xxvi] incidents.

[redacted]

To ensure the cyber resilience of our government agencies, the Joint Committee on Public Accounts and Audit's recommendations of 2017 [xxvii] should be fully implemented, by mandating that every entity[xxviii]:

- Complies with cyber resilience standards[xxix] and the Internet Gateway Reduction Program, and
- Completes the annual Australian Signals Directorate cybersecurity survey.

The framework should also:

- Include compliance with cyber resilience standards in the performance agreements of entity heads, with hard and fast deadlines
- Mandate the appointment of Chief Information Security Officers in every government entity and university
- Require training on cyber security hygiene for parliamentarians and their staff and volunteers and appoint dedicated cyber security officers in electorate offices, along the lines of the first-aid officer or fire warden
- Introduce a data management strategy
- Make it a contractual requirement for suppliers to government entities and critical infrastructure, especially in the national security sector, to meet a specified cyber hygiene standard – noting the 2020 Cyber Security Strategy
- Review the maturity of the cyber insurance market and assess the suitability of cyber insurance as a mandatory requirement for contracting to government agencies, in line with existing requirements for public liability and professional indemnity insurance
- Ensure the Australian Cyber Security Centre provides guidance on, and continuously vets and reports on, technologies being installed in government entities – noting the 2020 Cyber Security Strategy, and
- Establish a National Cabinet cyber security sub-committee.

[redacted]

gai brodtmann

As more and more government services move online, the Australian people are entitled to know their information is being managed and stored according to best-practice standards and processes.

I look forward to seeing the new framework and regulatory response. Please feel free to contact me via my email address if you have any queries.

Yours sincerely

[redacted]

Gai Brodtmann

Former Member for Canberra
Former Shadow Assistant Minister for Cyber Security and Defence

16 September 2020

[redacted]

References

[i] https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf

[ii] https://www.legislation.gov.au/Details/C2018A00029/Download

[iii] https://www.cisa.gov/critical-infrastructure-sectors

[iv] https://www.cpni.gov.uk/critical-national-infrastructure-0

[v] https://cicentre.gov.au/tisn/groups/tsg

[vi] https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/security-coordination/five-country-ministerial-2018

[vii] https://www.justice.gov/opa/pr/virtual-five-country-ministerial-meeting-joint-communiqu

[viii] https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf

[ix] https://www.homeaffairs.gov.au/reports-and-pubs/files/protecting-critical-infrastructure-systems-consultation-paper.pdf

[x] https://www.homeaffairs.gov.au/reports-and-pubs/files/protecting-critical-infrastructure-systems-consultation-paper.pdf

[xi] https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf

[xii] https://www.abc.net.au/news/2020-08-23/canberra-early-voting-to-dominate-act-election-result/12583474?nw=0

[xiii] https://www.anao.gov.au/sites/default/files/ANAO_Report_2017-2018_25a.pdf

[xiv] https://www.cisa.gov/government-facilities-sector

[xv] https://www.aspi.org.au/report/identity-nation

[xvi] https://www.aspi.org.au/report/identity-nation

[xvii] https://www.aspi.org.au/report/identity-nation

[xviii] https://www.cisa.gov/government-facilities-sector

[xix] https://www.cisa.gov/government-facilities-sector

[xx] https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf

[xxi] https://www.homeaffairs.gov.au/cyber-security-subsite/files/2020-cyber-security-strategy-iap-report.pdf

[xxii] https://www.anao.gov.au/work/performance-audit/cyber-resilience-government-business-enterprises-and-corporate-commonwealth-entities

[xxiii] https://www.anao.gov.au/work/performance-audit/cyber-resilience-government-business-enterprises-and-corporate-commonwealth-entities

[xxiv] https://www.canberratimes.com.au/story/6395537/parliament-hackers-stole-small-amountof-data/

[xxv] https://theconversation.com/did-the-census-really-suffer-a-denial-of-service-attack-63755

[xxvi] https://www.abc.net.au/news/2019-06-04/anu-data-hack-bank-records-personal-information/11176788

[xxvii] https://parlinfo.aph.gov.au/parlInfo/download/committees/reportjnt/024076/toc_pdf/Report467CybersecurityCompliance.pdf;fileType%3Dapplication%2Fpdf

[xxviii] https://www.anao.gov.au/work/performance-audit/cyber-resilience-government-business-enterprises-and-corporate-commonwealth-entities

[xxix] https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-ism-mapping

[redacted]