Federal Budget 2019-20 analysis:

Cyber Security & Privacy

Cyber wins over Privacy in the 2019-20 Budget

Who's responsible ?

The Hon Peter Dutton, Member for Dickson Queensland and Federal Minister for Home Affairs.

The Department of Home Affairs (DHA) is the Australian Government's lead agency for cybercrime and identity security policy and includes the following operational agencies:

- Australian Border Force (ABF)
- Australian Criminal Intelligence Commission (ACIC)
- Australian Federal Police (AFP)
- Australian Institute of Criminology (AIC)
- Australian Security Intelligence Organisation (ASIO)
- Australian Transaction Reports and Analysis Centre (AUSTRAC)

The Department of Defence (DoD) through the Australian Signals Directorate (ASD) also makes a significant contribution to Australia's national cyber security capability.

The 2019-20 Budget papers for the Home Affairs portfolio state… "the portfolio is countering the growth in cybercrime by strengthening our legislative framework, governance arrangements and whole-of-nation policy settings".

"The co-location of Home Affairs' cyber staff with operational and technical colleagues in the Australian Cyber Security Centre allows greater collaboration to build Australia's resilience to cybercrime, particularly through the development of a new National Plan to Combat Cybercrime".

Cyber Security - What was in the Budget?

- **$571.4** million over five years (from 2018-19) to for the **AFP** and **ASIO** "to strengthen capacity to meet the Governments national security objectives", which include "managing cyber security strategy, policy and coordination to make **Australia a cyber-resilient nation**".
- The AFP will receive the bulk of this funding - $512.8 million – and ASIO will receive $58.6 million in 2019-20 "to sustain current operations and undertake preliminary work to further enhance its future operations." (BP2, P113)
- **ASD**'s 2019-20 expenditure for "**cyber security and offensive cyber operations**" is included in its annual allocation of **$833.2** million. (DoD PBS, P167)

Cyber Uplift

- An unpublished (nfp) allocation has been made across "various agencies" for **Cyber Uplift** – to enhance whole-of-government cyber security arrangement including support for the 2019 Federal election, and to "mitigate potential cyber threats through enhanced monitoring and response capabilities. This includes the creation of **cyber "Sprint Teams**" within the Australian Cyber Security Centre" and a **Cyber Security Response Fund**. (BP2, P66)
- AIIA members will need to wait to after the 2019 Federal Election to see whether any of this funding will be used to update the Cyber Security Strategy 2016.

Election 2019

- The Australian Electoral Commission (AEC) will receive **$10.8** million from 2019-20, with the funds previously provisioned for use in 2021-22 to roll out **enhanced polling place technology**.

- A short-term **Security Operations Centre** (SOC) capability[1] was established in March 2019 by the **AEC** to provide "a live alerting system for significant events" in preparation for the 2019 Federal elections.

Cyber Security Strategy, Skills and Small Business

- The Department of Industry, Innovation and Science (DIIS) tranches of **$2.0** million and **$8.75** million for implementation of **Australia's Cyber Security Strategy**. (BP1.11, P39-42)
- **DIIS** also has an increased 2019-20 target to provide **2900 grants** under its Cyber Security Small Business Program, more than a 10 fold increase from 2018-19. (BP1.11 P51)
- Under the Government's Delivering Skills for Today and Tomorrow package a pilot of **Skills Organisations** will develop **training packages** for **high demand skills**, including in information and communications technology, healthcare, **cyber security** and aged and disability care. These organisations will foster closer links with industry.
- The Department of Education and Training (DET) will receive **$488,000** (building on $479,000 in 2018-19) to support training of "specialised cyber security professionals" through its **Academic Centres of Cyber Security Excellence** (ACCSE) in Australian universities program. (BP1.5, P61)
- A further $156 million Cyber security package was announced by the Prime Minister on 29 April 2019. $40 million will go towards hiring more military cyber specialists in the ADF over four years. $40 will go towards setting up a "countering foreign cyber criminals" capacity within the existing Australian Cyber Security Centre (ACSC) which will work with the Australian Federal Police against organised crime. $26 million will be given to ACSC to expand its assistance to the community. Some of the money will go to Questacon, to educate teachers and increase student interest in science, technology, engineering and maths, or STEM with the aim to train 1000 primary school teachers.

What about Privacy?

The Attorney-General's Department holds broad responsibility for privacy and information access.

Given the Australian public's and media's scrutiny of the Government's digital performance, specifically regarding trusted data custodianship, there are surprisingly few "privacy" initiatives in listed 2019-20 Federal budget.

- The Office of the Australian Information Commissioner (OAIC) will receive **$25.1** million over three years to facilitate timely response to privacy complaints and support stronger action in relation to social media and other online platform privacy breaches. (BP2, P69)
- $18.0 million was provided in 2018-19 for three years to support a range of small business services, including **data privacy**, through the Department of Jobs and Small Business Australian Small Business Advisory Services (ASBAS) Digital Solutions program. (Building Stronger Regional Communities 2019-20, P259)

Links

- Australia's Cyber Security Strategy 2016
- AIIA Pre-Budget Submission to Treasury 2019
- Australian Government 2019-2020 Budget Papers
- Treasurer's Budget Address
- For an excellent overview of Federal Government Digitalisation and a background on national cybersecurity initiatives AIIA highly recommend the following references produced by the Parliamentary Library's Cyber and Digital Research Group:
- Public sector digital transformation: a quick guide,
- Cybersecurity, cybercrime and cybersafety: a quick guide to key internet links

Related media articles

- AIIA raises concern over rushed digital legislation
- AIIA voices concern over two critical pieces of rushed digital legislation
- Hastily written tech laws threaten online privacy and security

[1] iTnews April 18 2019