

Key Brief Number: SCC-01

**Home Affairs Portfolio
Department of Home Affairs
Budget Estimates Hearing – October 2022**

KEY BRIEF**Topic: Counter Terrorism – High Risk Terrorist Offenders****Responsible Deputy:** Andrew Kefford PSM, Social Cohesion and Citizenship Group**Key Points**

- The Commonwealth has a robust framework for managing High Risk Terrorist Offenders (HRTOs), including control orders, citizenship cessation, continuing detention, extended supervision and a presumption against bail and parole (sections 15AA (bail) and 19ALB (parole) of the *Crimes Act 1914*).
- The Commonwealth's HRTO Regime enables post-sentence orders, both Continued Detention Orders (CDOs) and Extended Supervision Orders (ESOs) for convicted terrorist offenders who pose the highest category of risk to the community if released.
- Commencing 1 July 2022, the Administrative Arrangements Order (AAO) transferred policy responsibility of Division 105A of the *Criminal Code*, which governs the HRTO Regime, to the Attorney-General's Department (AGD).
- The Department of Home Affairs has retained program management responsibility of the HRTO Regime, including responsibility for the negotiation of housing agreements and Federation Funding Agreements.

Key Statistics

- As at 23 September 2022, there are **54** convicted terrorist offenders serving periods of imprisonment who are eligible under the HRTO Regime.
- As at 23 September 2022, there are **26** people currently before the courts for terrorism offences, of these **23** have been charged with HRTO eligible offences.

If asked: what is the forward HRTO case load?

- Any case-specific HRTO questions should be directed to AGD.

If asked: Implementation of the HRTO Regime

- In August 2022, \$2.045 million was transferred to the AGD to administer HRTO functions in accordance with the AAO.
- The Department of Home Affairs has retained \$4.8 million to continue to build and sustain HRTO coordination capability in 2022-23. This includes supporting the management of post-sentence order applications and litigation, including appeals and reviews, case management and coordination, and the establishment of state-based HRTO teams (initially in Victoria and NSW).
 - Funding provision to jurisdictions for 2021-22 has been finalised with the Victorian and NSW Governments in accordance with the Federation Funding Agreement Framework.

 Released by Department of Home Affairs
under the Freedom of Information Act 1982

Key Brief Number: SCC-01

- Federation Funding Agreements for 2022-23 are currently being negotiated with the Victorian and NSW Governments.

If asked: how is the Department supporting States and Territories to implement the HRT0 Regime

- The Department has:
 - commenced a review of the HRT0 Regime Implementation Framework, which will be conducted in consultation with the states and territories to ensure implementation remains up to date and on track,
 - implemented overarching CDO Housing Agreements for NSW and Victoria to govern and fund accommodation and treatment of offenders subject to a CDOs within their jurisdiction, and
 - Housing Arrangements in place for the specific offenders on CDOs in Victoria and New South Wales
 - Home Affairs and Victoria have also finalised a final individual Housing Arrangement authorising the detention of s. 47F(1), superceding the interim Arrangement that was in place

If asked: will funding be available after 2022-23?

- The Department continues to work through Commonwealth budget processes to develop a sustainable funding model, in consultation with states and territories.

If asked: how much has the Department spent on legal fees for the HRT0 Regime?

- Questions relating to legal fees should be referred to Group Manager, Legal.

Consultation

- The Chief Statistician has cleared the statistics contained within this brief.
- The Chief Finance Officer has cleared financial data contained within this brief.
- Legal Group has reviewed this brief.
- The Attorney-General's Department was consulted in the development of this brief.

Additional Information

Offender statistics are current as at 23 September 2022.

Key Brief Number: SCC-02

**Home Affairs Portfolio
Department of Home Affairs
Budget Estimates Hearing – October 2022**

KEY BRIEF**Topic: Counter Terrorism – settings and listings****Responsible Deputy:** Andrew Kefford PSM, Social Cohesion and Citizenship Group**Key Points**

- The Department works with agencies, including ASIO and the AFP, and international partners to counter the potential appeal and proliferation of violent extremism.
 - Our social cohesion and countering violent extremism efforts will remain an important element in managing any increased risk of community radicalisation.
 - These efforts will continue to focus on the online environment, including working with industry to reduce the availability of violent extremist content online.
- The Department will continue efforts to limit the travel of terrorist sympathisers and fighters in support of terrorism, including through:
 - passport cancellations where criteria are met;
 - foreign incursions and recruitment offences; and
 - offences relating to membership, support for, or association with, terrorist organisations, such as Al-Qa’ida and Islamic State-Khorasan Province.

Australia’s ideologically motivated violent extremist threat

- Ideologically Motivated Violent Extremism (IMVE) remains a threat in Australia.
 - The primary concern is on lone actors and small cells, including those inspired by nationalist and racist ideologies.
- The Australian Government has put in place a number of targeted legislative measures to address the threat posed by IMVEs.
 - In 2021, the Government listed two nationalist and racist violent extremist groups – Sonnenkrieg Division and The Base – as terrorist organisations under Division 102 of the *Criminal Code Act 1995* (*Criminal Code*).
- The Department has implemented programs to engage with at risk communities and those who are considered vulnerable to extremist and/or ideological narratives.

Post Sentence Orders for High Risk Terrorist Offenders (HRTOs)

- The Attorney-General, in his capacity as AFP Minister, is responsible for the HRTO regime under Division 105A of the *Criminal Code*.
- The Independent National Security Legislation Monitor (INSLM) is currently undertaking a review into Division 105A of the Criminal Code that allows for HRTOs who still pose an unacceptable risk to the community to remain in prison at the end of their sentences.

OFFICIAL

Clearing Officer: Richard Feakes, First Assistant Secretary, Counter-Terrorism Coordination Centre

Listing terrorist organisations under Division 102 of the *Criminal Code*

- The listing process provides a mechanism for the Australian Government to identify terrorist organisations and sends a clear message that the Australian Government does not condone the use of terrorism to achieve political, religious or ideological objectives.
- Prior to 1 July 2022, the Minister for Home Affairs, as the then AFP Minister, was responsible for terrorist organisation listings under Division 102 of the Criminal Code.
 - The commencement of the Administrative Arrangements Order (AAO) on 1 July 2022 transferred responsibility for the Criminal Code to the Attorney-General in his capacity as AFP Minister.
 - The Department of Home Affairs retains policy responsibility for terrorist organisation listings and prepares advice to the AFP Minister on the listing, re-listing or de-listing of terrorist organisations.
- For an organisation to be listed as a terrorist organisation by the Governor-General, the Attorney-General, in his capacity as AFP Minister, must be satisfied on reasonable grounds that the organisation:
 - is directly or indirectly engaged in, preparing, planning, assisting in or fostering the doing of a terrorist act, or
 - advocates the doing of a terrorist act.
- Agencies also consider a range of non-legislative factors to prioritise organisations for consideration, including:
 - the organisation's links to Australia;
 - threats to Australian interests;
 - links to other terrorist groups;
 - listing by the United Nations or likeminded countries; and
 - the organisation's ideology and engagement in peace processes.

If asked: Is the Australian Government planning to list more organisations under the Criminal Code?


- It is the Government's longstanding practice not to comment on whether or not an organisation is being, or has been, considered for listing.
- The Department works with national security and law enforcement agencies to assess which listings are appropriate.

If asked: expanded listing of Hizballah

- Hizballah's External Security Organisation has been listed as a terrorist organisation under the Criminal Code since 2003.
- On the basis of legislative and non-legislative considerations, the Minister was satisfied that the previous listing of Hizballah's External Security Organisation should be expanded to the entirety of Hizballah.
- Regulations to list the entirety of Hizballah came into effect on 10 December 2021.
- The leader of the opposition was offered a briefing prior to the listing being made.

If asked: expanded listing of Hamas

- The paramilitary wing of Hamas, the Izz al-Din al-Qassam Brigades (Hamas Brigades), was first listed as a terrorist organisation on 5 November 2003 and most recently re-listed on 4 August 2021.
- On the basis of legislative and non-legislative considerations, the then-Minister (in their capacity as AFP Minister) was satisfied that the previous listing of the Hamas Brigades should be expanded to the entirety of Hamas.
 - o This followed the release of the PJCIS report in October 2021, recommending the Australian Government give consideration to extending the listing of Hamas' Izz al-Din al-Qassam Brigades as a terrorist organisation to the entirety of Hamas.
- Regulations to list the entirety of Hamas came into effect on 4 March 2022.
- Australia's listing of the entirety of Hamas brings it into line with the position taken by the US, UK and Canada.

Consultations. 33(a)(i)


Key Brief Number: SCC-03

**Home Affairs Portfolio
Department of Home Affairs
Budget Estimates Hearing – October 2022**

KEY BRIEF

Topic: ISIL-linked Australians in detention or internally displaced persons camps in Syria

Responsible Deputy: Andrew Kefford PSM, Social Cohesion and Citizenship

What has changed / Why is repatriation occurring

- The Australian Government is concerned for the welfare of Australian women and children in the internally displaced persons (IDP) camps in northeast Syria.
 - This issue raises complex personal, national security, diplomatic, and community safety considerations that need to be addressed.
- Safeguarding the Australian community remains the Government's primary consideration consistent with Australia's long-held position.
- s. 33(a)(i)

**Questions about Operations (even if public commentary)**

- I will not confirm details of operational activity in a public hearing
 - need to protect privacy of individuals,
 - need to preserve safety and security of officials – including for any future process.

Presence of Australian Officials in Syria

- I will not comment on operational activities by Australian officials to protect their safety, including for any future repatriation processes.

Consultation

- DFAT, ABF, AFP, AGD, ASIO, Defence, PM&C, Citizenship Integrity & Assurance, and National Security Legal have been consulted on the whole-of-government talking points used in this brief.

Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL

Clearing Officer: Andrew Kefford PSM, Commonwealth Counter-Terrorism Coordinator

**Home Affairs Portfolio
Department of Home Affairs
Budget Estimates Hearing – October 2022**

KEY BRIEF**Topic: Foreign Interference**

Responsible Deputy: Andrew Kefford PSM, Social Cohesion and Citizenship Group

Key Points

- Australia remains the target of sophisticated foreign interference by a range of states.
- Almost every sector of the community is a potential target for foreign interference.
- Australia's approach to countering foreign interference is country-agnostic and recognises the need for a whole-of-nation effort to raise the cost and reduce the benefit to foreign actors interfering in Australian society.
- The National Counter Foreign Interference Coordinator (NCFIC), supported by the Counter Foreign Interference Coordination Centre (CFICC), works across government and non-government sectors to strengthen arrangements to counter foreign interference.
- The Counter Foreign Interference (CFI) Taskforce, through the Australian Security Intelligence Organisation (ASIO) and the Australian Federal Police (AFP), leads operational activities.

Protecting our Democratic institutions - elections

- The Australian Electoral Commission (AEC) is the Australian Government agency responsible for the integrity of federal elections.
- In 2018, the AEC established the Electoral Integrity Assurance Taskforce (EIAT) to safeguard the integrity of our elections from threats including foreign interference and disinformation.
 - The EIAT is led by the AEC and the Department of Finance and comprises federal government agencies — including Home Affairs, AFP and ASIO — that provide guidance and expertise on issues within Australia's electoral environment.
- Home Affairs supports the EIAT to identify and address adverse information events that may compromise electoral integrity.
 - The decision on whether the adverse information event does in fact compromise electoral integrity is a matter for the Australian Electoral Commissioner.
 - The CFI Taskforce is responsible for investigating and prosecuting foreign interference offences under Division 92 of the *Criminal Code Act 1995*.
- On 26 July 2022, the Australian Electoral Commissioner released a public media statement confirming that EIAT *"agencies did not identify any foreign interference, or any other interference, that compromised the delivery of the 2022 Federal Election"*.
- While no foreign interference has been discovered in any federal elections to date, we should not be complacent, as the electoral threat environment is rapidly changing.
- Home Affairs continues to work with state and territory electoral commissions through the EIAT to provide support for their upcoming elections.

Protecting our Democratic institutions – State, Territory and local

- Home Affairs is advancing national CFI efforts across the Commonwealth, and Australian states and territories through a network of state-based national partnerships teams.
 - These teams support and assist the development of resilience building measures in our state and territory Department of Premier and Cabinets, and Australia's local Governments and councils.

Safeguarding education and research from foreign interference

- The University Foreign Interference Taskforce (UFIT) is the primary mechanism for engagement on government-university CFI-related activities.
- November 2021 – the UFIT's *Guidelines to Counter Foreign Interference in the Australian University Sector* (the Guidelines) were released.
- The Guidelines:
 - Address on campus issues such as harassment, coercion, or intimidation of staff or students that can lead to self-censorship,
 - Support enhanced due diligence in the form of declaration of interest or disclosures from staff who are at risk of foreign interference, as well as clearer information on how to conduct due diligence assessments of research collaboration with foreign partners.
 - Focus on identifying an 'accountable authority' that is responsible for managing foreign interference risks.
 - Focus on communication, education and knowledge sharing to increase awareness internally.
- Universities are showing commitment to compliance, introducing measures to increase resilience to foreign interference, including:
 - improved cyber security practices
 - updated risk management policies;
 - research integrity training and awareness raising activities;
 - enhanced due diligence processes;
 - enhanced conflict of interest policies; and
 - nominated leadership roles responsible for implementing the Guidelines.
- Three working groups support implementation;:
 - Training Working Group to develop and implement materials to assist universities to implement the UFIT Guidelines.
 - Transnational Education Working Group to raise resilience for offshore higher education institutions.
 - Critical Technology Working Group to discuss forward work for the sector in relation to the *List of critical technologies in the national interest*.
- CFICC and other government agencies are working closely with the university sector

through the UFIT Steering Group to support implementation of the Guidelines.

Strengthening resilience to community interference

- The Commonwealth government, law enforcement and intelligence agencies, with jurisdictional law enforcement, work closely together to engage with, and support, communities concerned or affected by foreign interference.
- The Government maintains a range of policies and programs to strengthen Australia's social cohesion and build community resilience, including from foreign interference.
- The Department of Home Affairs' state-based counter foreign interference engagement officers meet with community groups to help strengthen resilience to foreign interference.
- Additionally, the Department of Home Affairs' network of Community Liaison Officers support the communication of official information to culturally and linguistically diverse communities, and provide a mechanism for community members to share information about their priorities and concerns.

Consultation

- Legal Group has reviewed this brief.

Key Brief Number: CISC-01

**Home Affairs Portfolio
Department of Home Affairs
Budget Estimates Hearing – October 2022**

KEY BRIEF**Topic:** Airport screening and processing delays**Responsible Deputy:** Hamish Hansford, Cyber and Infrastructure Security Centre**Key Points**

- Announced in 2018, all security controlled airports are required to introduce body scanners for domestic passengers and advanced X-ray technology by 31 December 2020.
 - 42 of 58 airports have completed the required upgrades.
 - Some airports have approved extension requests in place regarding the implementation of the enhanced security screening equipment.
 - The Department assesses all extension requests on a case-by-case basis.
- High volumes of passengers combined with shortages in airport staff have contributed to the long queues at some airports. Airports are actively recruiting to boost staffing numbers. The Department is working with airports and screening authorities by:
 - Providing flexibility in regulatory settings including in regards to who can perform non-screening roles to allow the surging of staff during peak travel times
 - Simplifying Aviation Screening Notices.
 - Working with airports to trial new security screening processes to identify possible procedural efficiencies.
- Recent media reports and high profile social media posts have expressed some individuals' concerns with security screening processes at Australian airports. Complaints were received from gender non-conforming passengers, women and people with special circumstances. In response to these reports:
 - On 24 July 2022, the Minister for Home Affairs wrote to the nine designated airports—Adelaide, Brisbane, Cairns, Canberra, Darwin, Gold Coast, Melbourne, Perth and Sydney—regarding the treatment of passengers while undergoing screening at airports. The letters addressed the recent media reports and reminded airport Chief Executive Officers that all travellers must be treated equally and with dignity and respect.
 - On 15 August 2022, the Department hosted the Strategic Aviation Security Meeting with senior representatives from designated airports and major airlines. An open dialogue between members canvassed ongoing challenges to aviation, including new screening technology, staffing and compliance.
 - From mid-July 2022, the Department issued several social media posts promoting the rights of passengers at screening points and explaining the process for screening. The posts clarified what passengers' rights are at the screening point, and providing answers to frequently asked questions, particularly regarding body scanners and frisk search at the screening point.
- The Department is continuing to review the requirements for providing consent for the conduct of frisk searches, and screening processes for transgender passengers and passengers with assistance animals.

OFFICIAL

Clearing Officer: Hamish Hansford, Group Manager, Cyber and Infrastructure Security Centre

Key Brief Number: CISC-01

- The Department is undertaking a number of lines of effort to ensure the screening process remains effective and respects the dignity of passengers. This includes:
 - Working with industry to share best practice, ensure technology is optimised and efficient processes are maintained. Two meetings of the screening working group have been held so far (18 May and 05 August 2022).
 - Reviewing Aviation Screening Notices—documents issued by the Secretary (or delegate) under the *Aviation Transport Security Act 2004* to each airport to specify the methods and techniques and equipment required to be followed for security screening. These documents will be updated through a co-design process with industry.
 - Engaging with international counterparts and airports to identify best practice technology that appropriately addresses the risks and threats posed.
 - Ensuring the Department has an easy-to-navigate reporting and feedback mechanism for the public to raise concerns with security screening practices, airports, service providers, and the CISC more broadly.

Recent security incidents:

- There have been a number of recent security incidents at Australian airports which involved errors in, or defective, aviation security screening.
 - 16 May 2022: person gained airside access to apron at Sydney Airport Terminal 3 by climbing temporary fencing. Individual has been charged and remanded in custody pending court proceedings.
 - 14 August 2022: an individual entered the landside area of Canberra Airport and fired shots at the windows located in the departures check-in area. The individual did not attempt to go through passenger screening and enter the sterile area of the airport.
 - 7 September 2022: passenger boarded flight from Sydney to Melbourne without being screened. All passengers and crew were treated as unscreened upon arrival in Melbourne, requiring AFP escort landside.
 - 11 October 2022: entry of unscreened person to sterile area at Melbourne airport and failure of screening equipment at Adelaide airport. Both incidents triggered spill of relevant terminals and for all people to be re-screened.
 - 11 October 2022: two persons gained access to sterile area without being screened at Gold Coast Airport.

Department's compliance posture:

- The Department assesses every reported or detected breach of legislation and adopts the approach most likely to promote the legislation's objectives, including encouraging voluntary compliance or taking enforcement action where appropriate.
 - Between 1 July 2022 and 4 October 2022, 11 infringements have been issued to individuals and corporations for breaches of transport security legislation.
- The Department has published a Cyber and Infrastructure Security Centre Compliance and Enforcement Strategy (at www.cisc.gov.au) outlining the key principles that underpin the Department's regulatory, compliance and enforcement approach.

Key Brief Number: SNR-02

**Home Affairs Portfolio
Department of Home Affairs
Budget Estimates Hearing – October 2022**

KEY BRIEF**Topic: Cyber Security****Responsible Deputy:** Marc Ablong PSM, Strategy & National Resilience Group**Key Points**

- Over the past two years the global cyber threat environment has intensified as more services and activities move online and new technologies emerge. Australia remains an attractive target for malicious actors and cybercriminals.
- Protecting Australia and Australians from cyber threats, while also ensuring a baseline level of cyber resilience across the economy is a key priority for the Government.
- The Government has appointed Australia's first dedicated Minister for Cyber Security to the Cabinet, providing an opportunity to enhance coordination across government on cyber policy, strategy and response mechanisms.
- The Department has established the position of Cyber Security Coordinator. Refer to **SB22-001054**.

2023-2030 Australian Cyber Strategy

- The Minister for Cyber Security, the Hon Clare O'Neil MP will be leading the development of a new Cyber Strategy, grounded in sovereign capability and developed in close consultation with industry. The Minister has stated the next strategy will focus on:
 - a secure economy and thriving cyber ecosystem;
 - a secure and resilient Critical Infrastructure and Government sector;
 - a sovereign and assured capability to counter cyber threats;
 - Australia's status as a global cyber leader.

If asked: Will initiatives under the Cyber Security Strategy 2020 be discontinued?

- Australia's Cyber Security Strategy 2020 invested \$1.67 billion over 10 years, delivering 47 programs (grouped under 19 thematic initiatives) across nine Commonwealth government agencies.
- The Government recognises the progress made under Australia's Cyber Security Strategy 2020, including initiatives are being implemented and adopted by industry, such as the Security of Critical Infrastructure Act 2018 reforms. Refer to **SB22-001054**.

If asked: What is the Government doing in response to the Optus data breach?

- Refer to SB22-001042.

OFFICIAL

Clearing Officer: Brendan Dowling, A/g Deputy Secretary Strategy and National Resilience

Key Brief Number: SNR-02*Cyber Security Best Practice Regulation Taskforce*

- On 13 July 2021, the Cyber Security Best Practice Regulation Taskforce (the Taskforce) commenced public consultation on options for regulatory reforms and voluntary incentives to strengthen cyber security across the Australian digital economy, including in the areas of smart devices.
- The Taskforce is preparing its final recommendations, which will provide Government with suite of possible reforms that could be implemented to uplift cyber security across the digital economy. Refer to **SB22-001054**.

Ransomware

- The Australian Government is currently considering policy and legislative reforms to strengthen Australia's capabilities to prevent and disrupt ransomware attacks. Refer to **SB22-000854**.

Attribution

- Australia joined international partners to condemn malicious cyber activity on a number of occasions throughout 2022. Ongoing collaboration and joint attribution statements are critical to establishing and maintaining public cyber norms and governance expectations. Refer to **SB22-001054**.

Related documents

- **The Optus data breach** – refer to SB22-001042
- **The Optus data breach Question Time Brief** – refer to QB22-000255
- **Cyber Security Back Pocket Brief** – refer to SB22-001054
- **Cyber Security Question Time Brief** – refer to QB22-000167
- **Ransomware** – refer to SB22-000854
- **Labor wipes slate on cyber** – EC22-004897

Consultation

- Cyber & Infrastructure Security Centre

Key Brief Number: SNR-03

**Home Affairs Portfolio
Department of Home Affairs
Budget Estimates Hearing – October 2022**

KEY BRIEF**Topic: Critical Technology Visa Changes****Responsible Deputy:** Marc Ablong PSM, Strategy and National Resilience Group**Key Points***Overview*

- Enhanced visa screening protects Australia's world-class science and technology institutions from malicious activities.
 - University, industry and research sectors are key to our economic success and national security; however, some countries may seek to undermine Australia's interests through foreign interference.
 - Such activities can result in the transfer of knowledge or theft of intellectual property, undermining Australia's strategic and commercial advantages.
- The *Migration Amendment (Protecting Australia's Critical Technology) Regulations 2022* (the PACT Regulations) have established a new legislative framework in the *Migration Regulations 1994* to manage the risk of unwanted transfer of critical technologies. The framework comprises:
 - a Public Interest Criterion (PIC 4003B) by which an applicant can be refused a visa if there is an unreasonable risk of unwanted transfer of critical technology by the applicant;
 - a new condition for Subclass 500 (student) visa holders requiring approval from the Minister to undertake critical technology related studies in the postgraduate research sector; and
 - provision for the cancellation of a visa where the Minister is satisfied that there is an unreasonable risk of unwanted transfer of critical technology by the visa holder.
- On 1 July 2022, the PACT Regulations introduced PIC 4003B for Subclass 500 (Student) visa applications, the new visa condition for Subclass 500 (Student) visa holders, and related access to merits review where the Minister decides not to approve a student visa holder's request to undertake critical technology related study.
- The remaining amendments commenced on 6 October 2022. This includes the new cancellation provisions and extends the PIC to the below visa subclasses:
 - Subclass 186 (Employer Nomination Scheme (permanent) visa)
 - Subclass 187 (Regional Sponsored Migration Scheme (permanent) visa)
 - Subclass 189 (Skilled Independent (permanent) visa)
 - Subclass 858 (Distinguished Talent (permanent) visa)
 - Subclass 191 (Permanent Residence (Skilled Regional) visa)
 - Subclass 400 (Temporary Work (Short Stay Activity) visa)

OFFICIAL

Clearing Officer: Brendan Dowling, First Assistant Secretary, Cyber, Digital and Technology Policy

Key Brief Number: SNR-03

- Subclass 407 (Training)
- Subclass 408 (Temporary Activity)
- Subclass 476 (Recognised Skill Graduate)
- Subclass 482 (Temporary Skill Shortage)
- Subclass 485 (Temporary Graduate)
- Subclass 494 (Skilled Employer Sponsored Regional (Provisional) visa)
- The PACT Regulations are country-agnostic and are designed to mitigate the risks of unwanted knowledge transfer irrespective of the place of origin.

Status

- The visa screening framework is not yet operational, and has no effect on visa applicants or visa holders until the Minister for Home Affairs makes a legislative instrument to specify the kinds of technology that will be in scope as 'critical technology'.
- The Department of Home Affairs has, through structured and bilateral engagements, extensively consulted the higher education sector and technology industry peak bodies on the application of the PACT Regulations and a draft list of 'kinds of critical technologies'. The draft consultation list has been informed by the Department of the Prime Minister and Cabinet's *List of Critical Technologies in the National Interest*.

PIC4003(b) Weapons of Mass Destruction (WMD)

- The critical technology PIC 4003B is a separate screening process to the WMD PIC 4003(b). The Minister for Foreign Affairs, or her delegate, remains the responsible authority for making determinations under PIC 4003(b).

[Handling note: refer any queries on WMD-screening under PIC4003(b) to the Department of Foreign Affairs and Trade]

Key consultation dates

- First Assistant Secretary Cyber, Digital and Technology Policy Division briefed the Universities Foreign Interference Taskforce (UFIT) Steering Group and the UFIT Critical Technology Working Group on: 13 May 2022
- First Assistant Secretary Cyber, Digital and Technology Policy Division briefed the Universities Foreign Interference Taskforce (UFIT) Steering Group on 7 September 2022.
- Assistant Secretary Technology Policy Division has hosted a dedicated UFIT sub-working group and industry roundtable on the PACT Regulations on: 23 May 2022 and 08 August 2022.

Consultation

- Legal Group
- Immigration Programs Delivery
- Immigration Programs Assurance
- Counter Foreign Interference
- Strategic Powers Intelligence

Key Brief Number: SNR-04

Home Affairs Portfolio
Department of Home Affairs
Budget Estimates Hearing – October 2022

KEY BRIEF**Topic: Tik Tok****Responsible Deputy:** Marc Ablong PSM, National Resilience and Cyber Security**Key Points**

- The rise of social media and digital platforms has created new security and privacy challenges and risks. This underscores the importance of ensuring Australia's security and privacy settings remain fit for purpose in the digital age.
- On 4 September 2022, the Minister for Home Affairs requested the Department undertake a review of the security risks social media platforms present and the settings which govern them.
 - The security review will consider all options to address data security risks as they relate to social media platforms.
- The outcomes of the security review will be provided to the Minister in early 2023.
- The review is being undertaken in close consultation with key agencies including the Attorney-General's Department, the Department of the Prime Minister and Cabinet and partners from the National Intelligence Community.
- Data security concerns relating to non-social media platforms and applications will be considered as a part of the National Data Security Action Plan and the new Cyber Security Strategy currently under development.
 - **Refer to BPB - SB22-001052 – National Data Security Action Plan**

If Asked: OAIC

- The Department is aware that the Australian Information Commissioner is considering TikTok's data gathering practices in line with her office's regulatory action policy.
 - The Information Commissioner has noted that platforms must be sufficiently transparent about how they handle user's personal information and provide users with genuine choices.
- Any further questions should be directed to the OAIC.

If Asked: Data Harvesting and Surveillance by TikTok

- Social media and messaging apps typically collect extensive data as part of their business models.
 - The National Data Security Action Plan will consider the national security implications of the availability of vast data sets to the governments of non-likeminded countries. **Refer to BPB - SB22-001052 – National Data Security Action Plan**
 - Questions relating to the technical aspects of social media company data practices should be referred to the Australian Signals Directorate.
 - Questions relating to privacy should be referred to the Attorney-General's Department

OFFICIAL

Clearing Officer: Marc Ablong PSM, Deputy Secretary Strategy and National Resilience

Key Brief Number: SNR-04

If Asked: Public concern about the ability for foreign states to access Australian's personal information through social media

- Australians need to be mindful of the fact that they are sharing a lot of detailed information about themselves with apps that may not properly protect their information.
- It is important that all Australians take steps to inform themselves about what data an app may be accessing on their device and how it can be used online.
 - Australians can find updated guidance to better understand the privacy and security risks of social media platforms published on ASD's ACSC website, cyber.gov.au.
- The National Data Security Action Plan will consider the national security implications of the availability of vast data sets to the governments of non-likeminded countries. **Refer to BPB - SB22-001052 – National Data Security Action Plan**

If Asked: Mis/disinformation

- The Department is concerned about the effects of technological enablers and amplifiers across digital platforms, including persuasive technologies like algorithms.
- Disinformation, foreign interference and the promotion of divisive ideological narratives have been enabled and emboldened by lightly regulated digital platforms.

Background

- On 17 June 2022, BuzzFeed News reported that China-based employees of ByteDance had repeatedly access non-public data about US TikTok users following BuzzFeed's review of the leaked audio from more than 80 internal TikTok meetings.
 - This reporting resulted in broader coverage and strong public interest in TikTok's data governance practices.
- To date, the Department has consulted broadly across the Commonwealth and with international partners on this matter including the United States and United Kingdom.

Home Affairs engagement with TikTok since 1 June 2022.

- The Department of Home Affairs engages with a range of private sector organisations – including social media organisations in order to fulfil its broad range of functions.
- On 6 June 2022 the Minister for Home Affairs received a letter from TikTok's Director of Public Policy, Australia and New Zealand, Brent Thomas.
- On 21 July 2022 the Minister for Home Affairs received a letter from TikTok's Director of Public Policy, Australia and New Zealand, Brent Thomas.
- On 5 August, as part of ongoing engagement with social media companies, the Department sought to organise a meeting with ByteDance.
- On 9-10 August, the Department held an exercise with government, private sector and civil society organisations to prevent the spread of online terrorist and extremist content. TikTok representatives participated in this exercise.
- On 17 August the Department (Assistant Secretary Anstee) responded to Mr Thomas' first and second letter.

Key Brief Number: SNR-04

- On 5 September, a United States (US) based Home Affairs officer met with TikTok representatives in the US as part of ongoing engagement with social media companies.
- On 19 September, the Assistant Secretary Anstee received an email from Brent Thomas seeking a meeting. Assistant Secretary Anstee was on leave at the time.
- On 5 October, a US based Home Affairs officer met with Mr Thomas as part of ongoing engagement with social media companies in the US.
- On 7 October, Assistant Secretary Anstee responded to Mr Thomas' email to arrange a meeting.
- On 18 October, Assistant Secretary Anstee, Home Affairs officers, Mr Thomas and other TikTok Employees had a brief introductory phone call.
- On 21 October, Assistant Secretary Anstee attended a virtual meeting with Mr Thomas.

Consultation

- Digital Industry Strategic Policy; Cyber, Digital & Technology Policy.
- CFI Policy & Coordination; DS Social Cohesion & Citizenship.
- Counter-misinformation Comms & Insights; Social Cohesion & Multicultural Affairs.

Related Documents

- 15 July 2022 – ECC-003443 – Chinese Government can access TikTok data
- 19 July 2022 – ECC-003498 – TikTok and social Media Data collection a concern, says cyber minister
- 23 August 2022 – ECC-004189 – Media Article: Home Affairs minister Clare O'Neil's TikTok account has disappeared after her warning
- 5 September 2022 – ECC-004858 – O'Neil orders social media privacy review – Media article
- 5 September 2022 – ECC-004856 – Data-harvesting Review: Call to keep TikTok ban on table – Media article
- 6 September 2022 – ECC-004855 – Joint Media Release – Albanese Government putting Australian's online privacy at risk
- 11 October 2022 – ECC-005571 – Estimates – TikTok fear in suburbs
- 17 October 2022 – ECC-005710 – At TikTok, there is the chief and then there's the CEO
- 24 October 2022 – ECC22-0058843 – Estimates: Tik-ed off over Beijing spy risk – Media Article
- 25 October 2022 – ECC22-005926 – Estimates: Trump 'was right' on TikTok threat – Media Article

Released by Department of Home Affairs
under the Freedom of Information Act 1982

Key Brief Number: SNR-05

**Home Affairs Portfolio
Department of Home Affairs
Budget Estimates Hearing – October 2022**

KEY BRIEF

Topic: Big Technology (including AI, Critical Tech, Supply chain, security of social media)

Responsible Deputy: Marc Ablong PSM, Strategy and National Resilience Group

Key Points

- The Department of Home Affairs (the Department) is concerned about the effects of technological enablers and amplifiers across digital platforms, including persuasive technologies like algorithmic recommender systems, and anonymising and obscuring technologies like end-to-end encryption.
 - Whilst online connectivity can deliver benefits, these technologies intersect with, and enable, all types of online harms, including misinformation and disinformation, cybercrime, online child sexual abuse, money laundering and violent extremism.
- The Department is concerned that digital platforms are prioritising privacy to the detriment of national security.
 - Organised and dangerous criminals are increasingly utilising anonymising and oblivious technologies, such as end-to-end encryption, peer-to-peer networks, decentralised networks, cryptocurrencies and virtual private networks to avoid traditional law enforcement identification and investigation techniques.
 - The increasing normalisation of these technologies on digital platforms, including social media, is bringing Dark Web functionality to the mainstream.
- On 15 March 2022, the House Select Committee Inquiry into Social Media and Online Safety published their report into Social Media and Online Safety (the Report). Of the 26 recommendations, two specifically address the Department, with others recommending the Department be engaged.
 - **Recommendation 10:** That the Department of Infrastructure, Transport, Regional Development, Communications and the Arts (DITRDCA), in conjunction with the eSafety Commissioner and the Department of Home Affairs, examine the need for potential regulation of end-to-end encryption technology in the context of harm prevention; and
 - **Recommendation 13:** That the eSafety Commissioner, in conjunction with the Department of Infrastructure, Transport, Regional Development, Communications and the Arts and the Department of Home Affairs and other technical experts as necessary, conduct a review of the use of algorithms in digital platforms.
 - The Department has provided feedback on the consolidated Government response to the Report, led by DITRDCA.

Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL

Clearing Officer: Brendan Dowling, First Assistant Secretary, Cyber, Digital and Technology Policy

Page 1 of 2

SB22-000851

As at 13 October 2022

Key Brief Number: SNR-05

International Statement on End-to-End Encryption and Public Safety

- On 11 October 2020, the Australian Government (led by the Department), together with Five Country partners and the governments of India and Japan, signed the *International Statement: End-to-End Encryption and Public Safety*.
 - The statement highlights the severe impact end-to-end encryption would have on public safety if implemented. For example, the implications of messaging services “going dark”, precluding access to content to investigate serious crimes, such as terrorism, and online child sexual exploitation and abuse.
 - The Department has engaged closely with UK counterparts to pursue additional signatories to the International Statement and is hosting an event in conjunction with the UK Home Office on 26 October 2022 at the Australian High Commission, London, to commemorate the second anniversary of the Statement’s signing and welcome new signatory countries (Georgia, Singapore and Ecuador).

Critical Technology Supply Chain Principles

- On 15 November 2021, the Department released the Critical Technology Supply Chain Principles (the Principles).
- The Principles outline broad factors decision-makers across governments and organisations of all sizes are encouraged to consider when deciding to develop, procure, deploy or control critical technologies.
- The Principles are another step the Government is taking to help organisations securely adopt and benefit from critical technologies, and protect the supply of essential services all Australians rely on.
- There are ten Principles organised under the three pillars of security-by-design, transparency, and autonomy and integrity.
- The Department will conduct a review of the Principles’ efficacy 12 months post their release.

Securing government data

- The Department is currently developing Australia’s first National Data Security Action Plan in support of the Digital Economy Strategy. This will include a review of whether public sector data security policy settings remain appropriate.
- The Department is exploring options to both raise Commonwealth Government data security standards and increase data-sharing between jurisdictions.
- The Department is continuing to develop the Action Plan following initial consultation. This included a national roadshow, call for submissions and engagement with all state and territory governments.
- The Department will advise the Minister of its interim findings and recommendations in the coming weeks.
 - Handling note; refer to:
 - KIB SB22-000850 TikTok
 - BPB SB22-001052 National Data Security Action Plan

Related documents

- SB22-000850 TikTok
- SB22-001052 – National Data Security Action Plan

OFFICIAL

Clearing Officer: Brendan Dowling, First Assistant Secretary, Cyber, Digital and Technology Policy

OFFICIAL**Key Brief Number: SNR - 07**

**Home Affairs Portfolio
Department of Home Affairs
Budget Estimates Hearing – October 2022**

KEY BRIEF**Topic: Identity Matching Services Procurement****Responsible Deputy:** Marc Ablong PSM, Strategy and National Resilience**Key Points**

- The Department operates the Identity Matching Services (IDMS) which promotes privacy by strengthening the integrity and security of Australia's identity infrastructure – the identity management systems of government agencies that issue Australia's core identity documents such as driver licences and passports.
- The IDMS comprises the Document Verification Service, Face Matching Services, and the National Driver Licence Facial Recognition Solution which are currently managed by NTT Australia Digital Pty Ltd under two contracts which are due to expire on 30 December 2023.
- In line with the Commonwealth Procurement Rules an open approach to market was required to award the next contract for the provision of services. A request for tender was released on 27 January 2022 and closed on 21 March 2022.
 - The request for tender was for services currently being provided. The Department is not seeking to expand the existing services.
- The Department has identified a preferred tenderer and has successfully negotiated a contract. Subject to receiving authorisation from the Minister for Finance, the Department will enter into the new arrangement for an initial term of three years (commencing from 2023-24), with the discretion to extend of the contract for a further period or periods of up to four years (up to 2030-31).
- The Department has written to the Minister for Home Affairs and Cyber Security requesting she write to the Minister for Finance seeking authorisation under Rule 10 of the Interim Budget Process Operational Rules to enter a major commitment.

Related documents

- MS22-001550 – Major Commitment of Relevant Money – Provision of Managed Services for the Identity Matching Services.
- SB22-000708 – Identity Matching Services FAS Brief.

Consultation

- Finance Division has cleared financial information contained within this brief.
- Legal Group has cleared this brief.

OFFICIAL

Clearing Officer: Marc Ablong PSM, Deputy Secretary Strategy and National Resilience

Key Brief Number: SNR-08

**Home Affairs Portfolio
Department of Home Affairs
Budget Estimates Hearing – October 2022**

KEY BRIEF**Topic: Ransomware****Responsible Deputy:** Marc Ablong PSM, Strategy and National Resilience Group**Key Points**

- Ransomware continues to be one of the most prominent and destructive cyber threats facing all Australians, including governments, businesses and individuals.
 - Ransomware requires minimal technical expertise, is low cost and can have a significant impact on an organisation, potentially crippling its business functions.
 - The Australian Cyber Security Centre's (ACSC) Annual Cyber Threat Report 2020-21 – released on 15 September 2021 – shows that ransomware has grown in impact and remains one of the most disruptive threats to Australian organisations.
 - Research conducted by the Australian Institute of Criminology (AIC) has shown that almost five per cent of survey respondents had been subject to a ransomware attack but only one in five of those reported the attacks to the police or the ACSC.
 - The most effective defence to ransomware attacks is good cyber hygiene. Step-by-step guides and assistance are available at www.cyber.gov.au
- Hardening Australia's defences to prevent ransomware attacks is a key priority for the Minister for Cyber Security.
 - The Government will explore a suite of reforms to strengthen Australia's cyber resilience across the economy through its 2023-2030 Cyber Strategy.
 - These reforms will address a range of cyber threats including but not limited to ransomware, support the most vulnerable entities in Australia, including families and small businesses, to protect their data and have trust in a safe and secure digital environment.

Counter Ransomware Initiative

- The Australian Government continues to work collaboratively with international partners to address ransomware globally.
- On 13 and 14 October 2021, the Secretary of Home Affairs, Michael Pezzullo AO, represented Australia at the inaugural Counter Ransomware Initiative Summit, hosted by the United States White House National Security Committee. The inaugural Summit focused on accelerating cooperation to counter ransomware.
 - Australia leads the Counter Ransomware Initiative's Disruption Working Group, which has brought together the capabilities and expertise of 28 like-minded nations with the intent to affect long-term disruption of the ransomware ecosystem.
- On 31 October and 1 November 2022, Secretary Pezzullo will represent Australia at the next Counter Ransomware Initiative Summit in Washington DC.

OFFICIAL

Clearing Officer: Brendan Dowling. First Assistant Secretary, Cyber, Digital and Technology Policy

Key Brief Number: SNR-08

If asked – What can people do to protect themselves from ransomware?

- With ransomware, prevention is much better than the cure.
 - Investing in preventative cyber security measures, such as keeping regular offline backups of business critical data, patching known security vulnerabilities and cyber education, is more cost effective than the comparative costs incurred when attempting to recover from a ransomware incident.
- The ACSC has published the Ransomware Attacks Prevention and Protection Guide on cyber.gov.au for all Australians on how to mitigate ransomware threats.
- The Government urges victims to report ransomware incidents through cyber.gov.au.
 - Reporting cybercrime, including ransomware, assists law enforcement in being able to respond to specific incidents at the time of reporting and allows the ACSC to help prevent other organisations from becoming a victim, boosting Australia's collective cyber defences.
 - Reporting also helps the Australian Government to better understand the online threats impacting our community and helps build Australia's threat picture to assist the law enforcement response, so these criminals can be prosecuted to the full extent of the law.

If asked – What is the Government's response to the reintroduction of the Crimes Legislation Amendment (Ransomware Action Plan) Bill 2022? (EC22-005308)

- On 26 September 2022, the opposition introduced the Crimes Legislation Amendment (Ransomware Action Plan) Bill 2022 (the CLARAP Bill) into Parliament. This Bill proposes a number of criminal law reforms to ensure all aspects of the ransomware business model can be disrupted by law enforcement.
 - The CLARAP Bill was previously introduced into Parliament by the former Minister for Home Affairs on 17 February 2022, however the Bill lapsed due to Parliament's dissolution for the 2022 Federal Election.
- All questions regarding the reintroduction of the Crimes Legislation Amendment (Ransomware Action Plan) Bill, and the criminal justice elements of cyber should be referred to the Attorney-General's Department.

Related documents

EC22-005308 – Media Release – Labor needs to walk the walk on cyber security 'priority'

Consultation

- Cyber and Infrastructure Security Centre, Legal Group, Attorney-General's Department, Australian Signals Directorate, and the Australian Federal Police.

OFFICIAL**Key Brief Number: SNR-09**

Home Affairs Portfolio
Department of Home Affairs
Budget Estimates Hearing – October 2022

KEY BRIEF**Topic: Optus Data Breach**

Responsible Deputy: Marc Ablong PSM, Strategy and National Resilience Group

Key Points

[N.b. this is a fast changing issue and this brief will need to be updated prior to the Estimates hearings.]

- On 21 September 2022, Optus reported a compromise of its network to the Australian Signals Directorate's Australian Cyber Security Centre (ACSC).
 - The ACSC informed the Department of Home Affairs and the office of the Minister for Home Affairs.
- On 22 September 2022, Optus released a statement stating it had experienced a data breach involving millions of its current and former customers' personally identifiable information.
 - This information includes the names, dates of birth, phone numbers and email addresses of as many as 9.8 million customers. For a sub-set of customers, it also includes their address and information about the credentials used to prove their identity.
- On 22 September 2022, the Department of Home Affairs (Home Affairs) held a call with Minister O'Neil to discuss the scope of the compromise and responses.
- On 24 September 2022, Home Affairs with the Department of the Prime Minister and Cabinet held a meeting with the Attorney-General's Department; the Australian Signals Directorate; the Office of the Australian Information Commissioner; the Department of Industry, Science and Resources; Treasury, and the Australian Prudential Regulatory Authority to discuss the protection of customers affected by the data breach.
- On 24 September, Home Affairs held call with the Optus Vice President, Regulatory and Public Affairs.
- On 24 September, Home Affairs and the Australian Signals Directorate held multiple calls with Minister O'Neil on response options and operational matters.
- On 26 September 2022, Minister O'Neil held a teleconference with the Optus CEO.
- On 26 September 2022, the Australian Federal Police (AFP) launched Operation HURRICANE to investigate the criminal aspects of the breach.
- On 27 September 2022, 10,000 records were released with a threat to continue to release data over the next four days until a \$1m payment is made.
- From 27 September 2022, Home Affairs and the Australian Signals Directorate held meetings with all states and territories to share information and coordinate a response,

OFFICIAL

Clearing Officer: Marc Ablong PSM, Deputy Secretary Strategy and National Resilience

including on protecting Optus customers whose state or territory identity documents were exposed.

- From 27 September 2022, Home Affairs and the Department of the Prime Minister and Cabinet held regular meetings with a range of Commonwealth agencies to coordinate responses, including on protecting Australians identity information and preventing identity fraud.
- The Government has worked on all possible options to protect Optus' customers, investigate subsequent criminal use of exposed credentials, and to prevent similar incidents in the future.
- The Department of Home Affairs (the Department) response to the Optus data breach includes:
 - Establishing a Commonwealth Credential Protection Register to help stop compromised identities from being used fraudulently.
 - The Register will prevent some compromised identity credentials from being verified through the Document Verification Service.
 - The Document Verification Service is used by some government agencies and businesses, such as banks, to verify an individual's identity online.
 - This will prevent credentials that are included on the Register from being used fraudulently. Rightful owners will also not be able to use them online to verify their identity.
 - As at 14 October, the Register includes around 100,000 Australian Passports.
 - Working with Commonwealth, state and territory agencies to obtain data on exposed credentials that, through the Commonwealth Credential Protection Register, can be used to prevent identity theft and fraud.
 - The Department is seeking only the minimum data required to identify an exposed credential, to avoid unnecessary collection of personal information.
 - Working with the Australian Cyber Security Centre, the Office of the Australian Information Commissioner and the Australian Federal Police.
 - Coordinating whole-of-government advice for affected Optus customers, which has been placed on relevant government websites.
- The Minister for Immigration, Citizenship and Multicultural Affairs has written to Optus seeking Optus' agreement to cover the cost to departmental clients of replacing credentials, where those clients were affected by the data breach.
- To avoid giving scammers and perpetrators information that could be used to target departmental clients, we do not intend to confirm whether credentials issued by the Department were exposed.
- The Department is working with key communities to ensure they are aware of the heightened risk of scams and identity crime in the wake of the Optus data breach.

- The Department is considering regulatory levers available under the *Telecommunications Act 1997* and *Security of Critical Infrastructure Act 2018* to ascertain Optus' level of compliance with their obligations as a licenced carrier.

If asked – is the Department of Home Affairs contacting affected Optus customers?

- Optus is responsible for contacting its clients.
- Where the Department becomes aware that a credential it issued has been exposed, it will also seek to contact the affected client.

If asked - What is the government doing to keep our data safe?

- The Government is taking an all vectors approach to cyber and data security.
- The Government's new Cyber Security Strategy will build whole-of-nation resilience against these types of attacks and ensure our networks and devices are protected against malicious actors.
 - The Department is developing Australia's first National Data Security Action Plan, which will map the nation's data security settings and provide measures to strengthen consistency and resilience against data security threats.
 - The Digital Transformation Agency, with the Department of Home Affairs, the Australian Taxation Office and Services Australia, is working on expanding the use of secure digital identities so that companies can meet their customer identification requirements while collecting less personally identifiable information. This will reduce the damage inflicted by these types of incidents.
 - The Attorney-General's Department is reviewing the *Privacy Act 1988* to ensure that Australia's privacy laws are fit-for-purpose in the digital age and that they accord with community expectations in light of the rise of digital platforms and other technological changes.
 - On 26 October, the Australian Government introduced the Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022 including amendments to significantly increase penalties for repeated or serious privacy breaches.
- The Australian Government works with industry to take action and address the possible consequences and harm relating to a serious data breach.
- Under the Notifiable Data Breaches scheme, entities regulated by the *Privacy Act 1988* (Cth) must notify affected individuals and the OAIC when a data breach is likely to result in serious harm to an individual whose personal information is involved.
- The Government provides funding to IDCARE, a not-for-profit organisation providing identity support services. IDCARE is a not-for-profit agency that helps Australians to reduce the harm they experience from the compromise and misuse of their identity information.
- Under section 313 of the *Telecommunications Act 1997*, Optus and other telecommunications carriers must do their best to protect their networks and facilities from unauthorised access and interference.

- The Department regularly engages with Optus both formally and informally regarding their regulatory obligations.

If asked: Why was the National Coordination Mechanism activated in response to Medibank cyber attack, but not the Optus data breach?

- Responsible agencies can convene at short notice to ensure coordinated, timely government action in response to any nationally significant event, including cyber incidents.
 - That is what has happened in response to both the Optus and Medibank incidents and is a normal function of Government.
- In both cases, while the vehicles have been different, the Australian Government's actions have been synchronised, coordinated and responsive.
 - This includes regular engagement with Optus, including through an Optus-Australian Government working group.
 - In both cases, Home Affairs and the Australian Cyber Security Centre have also coordinated with state and territory agencies on cyber security and identity security issues.

Consultation

Internal

Cyber and Infrastructure Security Centre, National Emergency Management Agency, Disputes and Corporate Law, Media Operations.

External

Australian Signals Directorate, Australian Competition and Consumer Commission, eSafety Commission, Australian Federal Police, Australian Prudential Regulation Authority, Australian Securities and Investment Commission, Department of Health, Department of the Prime Minister and Cabinet, Services Australia, Attorney-General's Department, Australian Taxation Office, Treasury, Australian Transaction Reports and Analysis Centre, Digital Transformation Agency, Department of Foreign Affairs and Trade, Office of National Intelligence, Department of Defence.

Attachments:

Attachment A – Chronology of events

Attachment B – 27 September 2022 Media Release - Statement on Optus data breach

Authorising Officer	Contact Officer
Marc Ablong PSM Deputy Secretary Strategy and National Resilience Group Department of Home Affairs ____/____/2022 Ph: s. 22(1)(a)(ii)	Brendan Dowling First Assistant Secretary Cyber, Digital and Technology Policy Division Department of Home Affairs ____/____/2022 Ph: s. 22(1)(a)(ii)

OPTUS DATA SECURITY BREACH

Current as at 27 October 2022

CHRONOLOGY

- 21 September 2022, Optus reported a compromise of its network and data breach to the Australian Signals Directorate's Australian Cyber Security Centre (ACSC).
- 21 September 2022, Home Affairs informed of cyber incident through a Cyber Incident Report.
- 22 September 2022, Home Affairs informed of data breach in the Department's role as an Optus customer.
- 22 September 2022, Home Affairs emailed to Optus Account Director seeking additional information.
- 22 September 2022, Home Affairs call with Minister's Office notifying of regulatory actions underway post the mandatory cyber incident report.
- 22 September 2022, Home Affairs call with Minister O'Neil.
- 22 September 2022, Optus released a media statement on their website, advising of the cyber incident and the associated actions taken to investigate and remediate.
- 22 September 2022, Office of the Australian Information Commissioner (OAIC) released a statement advising of the Optus data breach and providing advice about how Australians can respond to, and protect themselves from, its impacts.
- 23 September 2022, Home Affairs email to Optus Account Director confirming that departmental data, such as staff who have a departmental issued Optus mobile phone, was not compromised.
- 24 September 2022, Home Affairs email to Minister's office with draft action direction correspondence and Whole of Government paper on data exchange.
- 24 September 2022, multiple Home Affairs and ASD calls with Minister O'Neil.
- 24 September 2022, Home Affairs email to Minister O'Neil regarding the *Security of Critical Infrastructure Act 2018*.
- 24 September 2022, Interdepartmental Committee (IDC): Optus Data Breach meeting, led by PM&C, with attendees from across government to discuss response and data sharing.
- 24 September 2022, Home Affairs call with Optus Vice President, Regulatory and Public Affairs.
- 25 September 2022, IDC: Optus Data Breach meeting, led by PM&C, with attendees from across government to discuss response and data sharing.
- 25 September 2022, Home Affairs email to Minister O'Neil and Minister's Office on information disclosure and protection.
- 25 September 2022, multiple Home Affairs and ASD calls with Minister O'Neil.

OFFICIAL

Clearing Officer: Marc Ablong PSM, Deputy Secretary Strategy and National Resilience

- 26 September 2022, Minister O'Neil held a teleconference with the Optus CEO Kelly Bayer Rosmarin.
- 26 September 2022, the Australian Federal Police (AFP) launched Operation HURRICANE to investigate the criminal aspects of the breach.
- 26 September 2022, Minister O'Neil discussed the Optus data breach with Rafael Epstein on ABC Radio Melbourne.
- 26 September 2022, Minister O'Neil discussed the Optus data breach with Laura Tingle on the ABC's 7.30 report.
- 26 September 2022, Minister O'Neil was quoted in the *Australian Financial Review* article 'Optus hack brings data law revamp':
 - 'One significant question is whether the cybersecurity requirements we place on large telecommunications providers in this country are fit for purpose. I also note that in other jurisdictions, a data breach of this size will result in fines amounting to hundreds of millions of dollars'.
- 27 September 2022, 10,000 records were released with a threat to continue to release data over the next four days until a \$1m payment is made.
- 27 September 2022, National Cyber Security Committee (NCSC) meeting regarding National Operations Sub Committee (NOSC) & Optus with attendees from states and territories.
- 27 September 2022, IDC: Optus Data Breach meeting, led by PM&C, with attendees from across government.
- 27 September 2022, NCSC meeting, regarding NOSC and Optus, led by Defence, with attendees from Home Affairs, ACSC and states and territories.
- 27 September 2022, Minister O'Neil released a statement on the Optus data breach.
- 28 September 2022, Minister O'Neil held a teleconference with the Optus CEO.
- 28 September 2022, Home Affairs meeting with state and territory road and transport agencies to discuss the Optus data breach and possible remediation activities to protect identity information.
- 28 September 2022, Multiple IDC: Optus Data Breach meetings, led by PM&C with attendees from across government including on data sharing and identity protection.
- 28 September 2022, Minister O'Neil discussed the Optus data breach with Dimity Clancey on A Current Affair.
- 28 September 2022, the Minister for Foreign Affairs contacted Optus requesting that it cover the cost of replacement passports.
- 28 September 2022, the Prime Minister confirmed that Optus had agreed to cover the cost of replacement passports.
- 28 September 2022, Optus made a further mandatory cyber incident report about a separate issue.

- 29 September 2022, multiple IDCs: Optus Data Breach meetings, led by PM&C, with attendees from across government.
- 29 September 2022, Home Affairs discussion regarding impact on departmental services provided by Optus.
- 29 September 2022, Optus Service Performance Management Forum Meeting, with members from Home Affairs and Optus Account team, to discuss the importance of this issue for the government and Optus' official communications.
- 29 September 2022, call between Home Affairs and Optus State Director, Federal Government to ensure Home Affairs is receiving appropriate information.
- 30 September 2022, IDC: Optus Data Breach meeting, led by PM&C, with attendees from across government.
- 30 September 2022, NCSC situation update, led by Defence, with attendees from across government.
- 30 September 2022, Home Affairs meeting with state and territory road and transport agencies to discuss the Optus data breach and possible remediation activities.
- 30 September 2022, IDC: Optus Data Breach meeting, led by PM&C, with attendees from across government.
- 30 September 2022, multiple CISC, OAIC, ACMA and ACCC meetings to coordinate the approach, alignment and coordination to Optus.
- 1 October 2022, multiple IDCs: Optus Data Breach meetings with attendees from across government.
- 2 October 2022, Minister O'Neil held a teleconference with Optus CEO Kelly Bayer Rosmarin.
- 2 October 2022, Minister O'Neil made a public statement on the Optus data breach with the Minister for Government Services.
- 3 October 2022, Minister held a teleconference with Optus CEO Kelly Bayer Rosmarin.
- 3 October 2022, Optus commissioned an independent external review of the data breach.
- 4 October 2022, IDC: Optus Data Breach meeting, led by PM&C, with attendees from across government.
- 4 October 2022, Home Affairs meeting with state and territory road and transport agencies to discuss the Optus data breach and possible remediation activities.
- 4 October 2022, Minister O'Neil held a teleconference with the Optus CEO Kelly Bayer Rosmarin.
- 4 October 2022, Optus provided the Australian Government with the detailed information of customers who had Medicare cards, or other government credentials, exposed.
- 5 October 2022, Home Affairs meeting with IDCARE to discuss funding for Optus-related support activities.

- 5 October 2022, IDC: Optus Data Breach meeting, led by PM&C, with attendees from across government.
- 5 October 2022, Minister's Office meeting with Home Affairs Cyber Policy and Strategy Branch.
- 5 October 2022, email to Optus Account Director to confirm dates of the data breach and formal notification to Home Affairs.
- 6 October 2022, IDC: Optus Data Breach meeting, led by PM&C, with attendees from across government.
- 6 October 2022, Legislation Data Breach Working Group meeting, led by AGD, with attendees from across government.
- 6 October 2022, email to Optus Account Director to confirm that the only data stored in Optus' enterprise systems is Home Affairs' staff names and work email addresses.
- 6 October 2022, Home Affairs brief to the Minister's Office. Brief advised:
 - the establishment of a coordination group with state and territory road transport agencies to identify effective options for responses to compromised driver licences, and
 - working to establish a Commonwealth Credential Protection Register to prevent the fraudulent use of identity credentials.
- 7 October 2022, Home Affairs wrote to Optus requesting voluntary disclosure of information as authorised by section 86E of the *Crimes Act 1914*.
- 7 October 2022, Optus-Australian Government Data Breach Working Group, led by AGD, with attendees from across government.
- 7 October 2022, Home Affairs meeting with state and territory road and transport agencies to discuss the Optus data breach and possible remediation activities.
- 7 October 2022, Minister O'Neil wrote to the Prime Minister requesting that options be explored for a regarding a review of the Optus data breach.
- 10 October 2022, Home Affairs meeting with the Victorian Government to discuss the protection of compromised Victorian drive licenses, the use of the Credential Protection Register and the implementation of mandatory driver licence card numbers.
- 11 October 2022, Home Affairs meeting with state and territory road and transport agencies to discuss the Optus data breach and possible remediation activities.
- 11 October 2022, the OAIC and the Australian Communications and Media Authority (ACMA) both announced that they would commence investigations under their respective regulatory frameworks into the personal information handling practices of Optus in regard to the data breach.
- 12 October 2022, Optus-Australian Government Data Breach Working Group, led by AGD, with attendees from across government.

- 12 October 2022, Home Affairs meeting with all Gateway Service Providers of the Document Verification Service.
- 12 October 2022, call between Home Affairs and Optus Senior Director advising of Optus' engagement with federal and state government, along with engagement with Deloitte to investigate and develop a report which will include learnings to be shared.
- 13 October 2022, Home Affairs meeting with state and territory road and transport agencies to discuss the Optus data breach and possible remediation activities.
- 13 October 2022, Home Affairs Secretary wrote to state and territory road transport agencies regarding the creation of a Commonwealth Credential Protection Register.
- 14 October 2022, Optus-Australian Government Data Breach Working Group, led by AGD, with attendees from whole of government.
- 14 October 2022, Home Affairs convened a meeting of all government users and document issuers of the Document Verification Service to provide information regarding the response to the Optus Data Breach.
- 17 October 2022, Home Affairs hosted representatives from ID Support NSW to discuss identity remediation and recovery support and the Optus response.
- 18 October 2022, IDC: Optus Data Breach meeting, led by PM&C, with attendees from across government.
- 18 October 2022, Home Affairs meeting to address the departmental response for visa holders who had their foreign passport compromised in the Optus data breach.
- 18 October 2022, Home Affairs meeting with state and territory road and transport agencies to discuss the Optus data breach and possible remediation activities.
- 18 October 2022, Home Affairs meeting with representatives from ID Support NSW to discuss identity remediation and recovery support and the Optus response.
- 19 October 2022, Home Affairs met with Services Australia to discuss identity security, protection of credentials and identity, remediation and recovery activities and the response to the Optus data breach.
- 19 October 2022, Home Affairs met with ACMA to discuss the ramifications of the Optus data breach, the scope of the compromised documents and what mitigations Home Affairs is putting in place through the Identity Matching Services.
- 19 October 2022, Optus Vendor Relationship Review Meeting, with members from Home Affairs and Optus Account Team to discuss the data breach and Optus' engagement across government and with private enterprise. Home Affairs noted that Optus' learnings should be shared broadly with other service providers.
- 19 October 2022, Minister O'Neil wrote to Minister Shorten regarding the creation of a Commonwealth Credential Protection Register.
- 20 October 2022, Home Affairs meeting with state and territory road and transport agencies to discuss the Optus data breach and possible remediation activities.

- 20 October 2022, Minister O'Neil discussed the Optus data breach with Sabra Lane on ABC radio.
- 21 October 2022, Optus-Australian Government Data Breach Working Group, led by AGD, with attendees from across government.
- 21 October 2022, Minister O'Neil held a teleconference with Optus CEO Kelly Bayer Rosmarin.
- 22 October 2022, Minister O'Neil was quoted in *The Australian* article 'Hacked firms to be hit for millions':
 - 'We need to do better as a country... We're in the order of five years behind where we need to be on our cyber laws and our policies and our approaches'.
- 25 October 2022, Home Affairs meeting with state and territory road and transport agencies to discuss the Optus data breach and possible remediation activities.
- 25 October 2022, Minister O'Neil was quoted in *Campaspe News* article 'Medibank hack bigger than first thought'.
 - Minister O'Neil said she had been in constant contact with the health insurer and insisted her government had provided the necessary resources to tackle the breach.
 - 'The latest advice from Medibank is deeply concerning ... the government recognises that this incident is very stressful for affected Australians'.
 - 'The toughest and smartest people in the government are working directly with Medibank to try to ensure that this horrendous criminal act does not turn into what could be irreparable harm to some Australian citizens'.
- 25 October 2022, Minister O'Neil discussed the Optus data breach on ABC Radio:
 - 'The government is taking this and other recent data breaches seriously, Combined with *Optus*, this is an enormous wake up call for the country here, cybercriminals are the thugs of the 21st century...'
- 26 October 2022, Home Affairs meeting with New Zealand to discuss the protection of compromised New Zealand passports through the Credential Protection Register.
- 26 October 2022, Home Affairs meeting on a departmental response for visa holders who had their foreign passport compromised.
- 26 October 2022, Minister O'Neil was mentioned in *The Australian* article 'Hack attack: Nearly \$6m for Optus probe'.
 - The Minister said the money [an additional \$5.5 million for the Office of Australian Information Commissioner] was 'part of fulfilling the government's election commitment to combat scams and online fraud'.
- 26 October 2022, Minister O'Neil was mentioned in *The Australian* article 'Fast track for nation's data shield'.
 - Minister O'Neil said the government was extremely concerned about the attack, given the personal nature of the stolen health data, and the damage could be "irreparable".

- Minister O’Neil said ‘Australians who are struggling with mental health conditions, drug and alcohol addiction, with diseases that carry some shame or embarrassment, they are entitled to keep that information private and confidential’.
- 26 October 2022, Minister O’Neil was mentioned in *The Chronicle* article ‘Federal Budget 2022: Millions of dollars to combat and investigate cyber attacks’.
 - Minister O’Neil said it was all about responding to challenges from threats and keeping Australians safe.
- 27 October 2022, NCSC meeting, led by Defence, with attendees from across government.
- 28 October 2022, Optus-Australian Government Data Breach Working Group, led by AGD, with attendees from across government.

MEDIA ARTICLES

<u>Date</u>	<u>Outlet</u>	<u>Reporting</u>
24 October 2022	The Mandarin	It is anticipated that the government will tip even more money into cyber response in the Budget following the Optus and Medibank Private incidents, as well as boosting resources for the OAIC and ACCC. Fines skyrocket under new data breach crackdown laws
23 October 2022	The Guardian	The Department of Home Affairs had blocked the passport numbers of those affected from being used in the federal Document Verification System (DVS). Optus data breach: customers yet to be reimbursed for passport replacements
15 October 2022	ABC News	MyDeal.com.au, a subsidiary of the Woolworths Group, has announced that data was exposed when its customer relationship management system was accessed by a "compromised user credential". Woolworths MyDeal becomes latest target of cyber attack. What information was leaked and what can you do if you're affected?
14 October 2022	Nine News	The AFP are scrambling to ensure the safety of some of its secret agents and operations exposed in a massive cyberhack of Colombian government files. AFP concerned for safety of anti-drug agents exposed by data hack
13 October 2022	ABC News	Medibank Private says it has been hit by a cyberattack. The company said ‘unusual activity’ had been detected on its network, but there was not evidence that sensitive data had been accessed. Health insurer Medibank Private hit by cyber attack

13 October 2022	itNews	The Department of Home Affairs boss Michael Pezzullo has suggested the Optus breach, while driving much discussion about cybersecurity policy, isn't necessarily a good model for policy debates. Home Affairs: Optus breach is not a model for policy debate
11 October 2022	Sydney Morning Herald	The OAIC and the ACMA announced co-ordinated investigations to investigate whether Optus needed to keep extensive data on millions of its customers and understand how it was stored. OAIC launches investigation into telco
11 October 2022	Australian Financial Review	Experts who advise big companies on their data strategies say they are seeing a post-Optus surge in inquiries from executives who don't even understand existing rules, while tech chiefs at both Commonwealth Bank and ASX said companies had to review and ensure they were using data for valid reasons. Optus breach: Corporate Australia expects tough privacy laws, rushes to check data hoards
11 October 2022	ABC News	Optus customers who signed up using international identification say they feel abandoned by the company, and are unsure whether they need to replace documents or who will cover the cost. International students, visa holders feel 'abandoned' by company
7 October 2022	Daily Telegraph	An Australian law firm has formally started legal action against telco giant Optus to seek compensation for the millions of customers who had their personal information stolen in last month's cyberattack. Aussie law firm Maurice Blackburn files action against telco
6 October 2022	IDCARE	On 6 October 2022, IDCARE has responded to over 15,000 community engagements and the other cases involving identity compromise and misuse to result from scams, cybercrimes and identity theft have more than doubled. Optus DB response
6 October 2022	ABC News	Operation Guardian the AFP investigation set up after 10,200 customer records were published online following the Optus cyberattack has arrested and charged a 19-year-old Sydney man. The AFP announce the first arrest linked to the Optus data breach.
6 October 2022	ABC News	The federal government has released planned changes to telecommunications laws following the Optus data breach,

		which affected nearly 10 million customers and former customers. Government strengthens powers for telcos to share affected data following Optus hack
4 October 2022	IDCARE	IDCARE had captured 121 alleged misuse / exploitation cases from community contacts. Optus DB response
3 October 2022	Optus	Optus commissions independent external review of cyberattack. Cyberattack Support
3 October 2022	OPTUS	Optus updates to customers. Cyberattack Support
3 October 2022	Daily Telegraph	Optus has informed current and former customers whether their driver licence and card numbers were exposed in the cyberattack - but has again come under fire over its poor communication and ongoing confusion. Problem with Victorian driver licence number text notification
2 October 2022	Optus	Optus Update on Medicare card and Driver Licence numbers. Cyberattack Support
30 Sep 2022	AGD	Attorney- General's Department release a statement regarding Optus data breach. Optus data breach Attorney-General's Department
29 Sep 2022	ABC News	Professor Asha Rao, Associate Dean of Mathematical Sciences at RMIT University, says Australia needs new laws to prohibit companies from engaging in unnecessary data harvesting. Too much data collection means we're more at risk of having personal details stolen, expert say
28 September 2022	Optus	Optus update on Medicare ID Number. Cyberattack Support
28 September 2022	Maurice Blackburn Lawyers	Maurice Blackburn investigates second legal claim over yet another Optus customer data breach. Maurice Blackburn investigates second legal claim over yet another Optus customer data breach
28 September 2022	The Guardian	Australians residing in New South Wales, Victoria, Queensland and South Australia who were affected by the data breach, will be able to change their driver's licence numbers and receive new cards. Optus is expected to bear the multimillion dollar cost of this changeover.

		Optus data breach: Australians will be able to change their driver's licence with telco to pay.
27 September 2022	Twitter	Chris O'Keefe, Political Reporter for 9News claims that victims are now receiving text messages from hackers demanding \$2000AUD be paid into a CBA bank account, with threats their data will be sold for "fraudulent activity within 2 days." Chris O'Keefe: Victims are now receiving text messages from hackers.
27 September 2022	ABC News	An online account that claims to be behind the Optus data breach says it has deleted its only copy of customers' information and it no longer cares about a ransom. Online account claiming to be behind data leak apologises, drops ransom threat.
27 September 2022	The Sydney Morning Herald	Fresh laws to constrain the use of facial recognition technology used by retailers, police and schools - are a step closer to reality after the Optus breach. New laws to tackle hackers head-on.
27 September 2022	The West Australian	Anthony Albanese says companies will be forced to notify banks faster when they experience cyberattacks, after describing the hacking of the country's second-biggest telecoms firm as a "a huge wake-up call" for the corporate sector. Albanese puts banks on notice as AFP joins Optus hack probe.
27 September 2022	Australian Financial Review	The focus of the disastrous Optus data breach has shifted from the company's campus in Sydney's Macquarie Park to the Canberra office of Home Affairs and Cyber Security Minister Clare O'Neil. Optus breach needs federal response.
27 September 2022	Australian Financial Review	Companies may face multimillion dollar fines for failing to protect customer data from hackers, as Home Affairs Minister Clare O'Neil rebuked Optus over its data breach that has affected almost 10 million Australians. Labor scolds Optus, flags stricter laws.
26 September 2022	Optus	On 26 September 2022, 'OptusData' modified their original post, and published a data set comprising 10,000 rows of ex-filtrated data, as a result of Optus' failure to meet the ransom demands. The actor added that they will continue to post 10,000 rows of data each day, until the ransom is paid. Cyberattack Support

26 September 2022	The Canberra Times	Slater and Gordon is investigating a potential class action against Optus on behalf of current and former customers who have been affected. Optus: Class action under consideration for customers.
26 September 2022	7 News	Optus has announced it would offer 12 months of free credit monitoring from a credit reporting agency Equifax for their “most affected” current and former customers. Telco to offer credit monitoring program amid fears hack could lead to identity theft.
26 September 2022	ABC News	Home Affairs Minister said today that the massive breach of Optus customer data should not have happened, and urged the company to offer free services to monitor customer accounts for fraud. Home affairs minister points finger at Optus, saying hack should not have happened.
25 September 2022	The Age	News of the Optus cybersecurity attack is shocking. The millions of customers potentially impacted by the breach is mind-boggling. But the real startling question is how a breach of this magnitude is still occurring in 2022. No, Optus doesn't need to keep your sensitive information for so long.
25 September 2022	Mercury	A person claiming to be the evil genius responsible for the Optus data breach is demanding \$1.5 million in ransom money from the telco giant. Optus data breach: Hacker demands \$1.5 million ransom, customer info leaked on dark web.
25 September 2022	7NEWS	Optus customers whose passport or driver's licence numbers were stolen in a massive data breach are being contacted, amid warnings that scammers will try to profit from the cyberattack. Optus issues fresh warning as \$1.5m ransom threat is investigated: 'Do not click'.
25 September 2022	ABC News	The Home Affairs Minister is soon expected to announce several new security measures following the massive Optus data breach that saw hackers steal the personal details of up to 9.8 million Australians. Federal government to unveil new security measures following massive Optus data breach.
24 September 2022	9news	Optus said today the attack could trigger illegitimate offers to sell customer details online as a user on a data breach forum has claimed two files containing sensitive customer information will be sold if a \$1.53 million ransom is not paid within a week. Optus cyber attack investigation amid alleged ransom threat.

24 September 2022	SBS News	Optus has admitted it is likely that criminals will make claims capitalising financially on the leak, after the company announced it was a victim of a major cyberattack, but says it won't comment on the veracity of the claims its customer data is being sold online. Federal police monitoring reports of stolen Optus data being sold on the dark web.
24 September 2022	Guardian	Attorney general Mark Dreyfus has been briefed by the privacy commissioner about hack and is seeking 'urgent' meeting with telco. AFP investigates \$1m ransom demand posted online for allegedly hacked Optus data.
23 September 2022	Australian Cyber Security Magazine	A threat actor registered an account on popular forum Breach Forums as 'OptusData'. This actor had no prior history on Breach Forums under that username, or any other repositories frequently monitored by IDCARE analysts. Optus Customer Data Posted on Dark Web as Hacker Demands \$1 million
23 September 2022	ABC News	Anonymous senior Optus figurehead offers confidential insights into the early findings of the investigation. Breach likely down to human error. 'Human error' emerges as factor in Optus hack affecting millions of Australians.
23 September 2022	The Guardian	Peter Dutton criticises Government's handling of Optus breach and emphasises the need for Ministers to provide information and assurances to the public. Australia news live: Dutton reiterates support for national anti-corruption commission; stranded whale rescue operation continues.
23 September 2022	Newcastle Herald	Senator Sarah Henderson has urged Labor to deliver tougher online privacy and data protection laws and to adopt the Coalition's Online Privacy Bill. Laws questioned after Optus cyber attack.
22 September 2022	Optus	Optus notifies customers of cyberattack compromising customer information. Optus indicated that approximately 9.8 million records containing customer data was exfiltrated but did not indicate corporate systems had been impacted by an encryption (indicative of a ransomware attack). Optus notifies customers of cyberattack compromising customer information

21 September 2022	Cyberknow	Optus suffered a cyberattack. Up to 11.2 million past and present Optus, customers are likely impacted. Optus Data Breach Timeline
-------------------------	-----------	---

OFFICIAL**Key Brief Number: SNR-10**

**Home Affairs Portfolio
Department of Home Affairs
Budget Estimates Hearing – October 2022**

KEY BRIEF**Topic: Medibank Data Breach****Responsible Deputy:** Marc Ablong PSM, Strategy and National Resilience Group**Key Points**

[N.b. this is a fast changing issue and this brief will need to be updated prior to the Estimates hearings.]

- On 12 October 2022, Medibank Private Limited (Medibank Private) reported to the Australian Signals Directorate's Australian Cyber Security Centre (ACSC) that it was experiencing a cyber security incident.
- On 12 October 2022, a Hot Issues Brief advising of the incident was prepared by the Australian Cyber Security Centre and shared with the Department and the office of the Minister for Home Affairs.
- 13 October 2022, Minister O'Neil's Office held a teleconference with Medibank Private CEO.
- On 13 October 2022, Medibank Private publicly reported it had identified unusual activity on its network but that there was no evidence any sensitive data had been accessed.
- On 19 October 2022, Medibank Private released a statement advising it had received messages from a group that wished to negotiate regarding their alleged removal of customer data.
- On 19 October 2022, Minister O'Neil released a statement on the Medibank cyber incident noting that:
 - 'A significant cyber security incident has occurred within Medibank. The facts are continuing to be established'.
 - 'I have spoken with the CEO of Medibank, David Koczkar, and the heads of Australian Signals Directorate (ASD) and the Australian Federal Police (AFP).
- On 20 October 2022, Medibank Private released a statement advising that it had been contacted by a criminal claiming to have stolen data. The criminal provided a sample of records for 100 policies which Medibank Private believe came from its ahm and international student systems.
- On 20 October 2022, the AFP launched Operation PALLIDUS to investigate the Medibank Private data breach.

Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL

- On 22 October 2022, the National Coordination Mechanism was activated to bring together agencies across the Government on all possible response options and support to people affected. National Coordination Mechanism meetings were held on 23, 25 and 27 October.
- On 25 October 2022, Medibank Private released a public announcement stating that they had received additional files from the criminal including a further 1,000 AHM policy records (which include personal and health claims data).
- On 26 October 2022, Medibank Private released a statement advising that the data breach was wider than originally thought, with the criminal having access to all international student customer, AHM and Medibank Private customers' personal data, and significant amounts of health claims data.
- The data includes names and addresses, dates of birth, Medicare card numbers, policy numbers, phone numbers, and some personal health and claims data.
 - The criminal claims to have stolen other information, including data related to credit card security, which has not yet been verified by Medibank Private's investigations.
 - Services Australia advises that Medicare card numbers, by themselves, cannot be used for identity misuse and there is no need to replace Medicare cards.
- Medibank Private has announced:
 - That it has begun making direct contact with affected customers.
 - That it is taking steps to remediate the exploited vulnerability and assess other networks as necessary.
 - A support package for affected customers including
 - a hardship package providing financial support for uniquely vulnerable customers
 - access to mental health and wellbeing support
 - access to identity monitoring services
 - reimbursement of fees for re-issue of fully compromised identity documents
- The Australian Signals Directorate's Australian Cyber Security Centre (ACSC) is providing cyber security advice and technical assistance, and continues to work with Medibank Private to assess the extent of the incident.
- The government is looking at all possible options to protect Medibank Private customers, investigate subsequent criminal use of exposed credentials, and to prevent similar incidents in the future.
 - Medibank Private is receiving ongoing technical advice and assistance from Australian Government agencies, including the Australian Signals Directorate (ASD) and the AFP.

- The AFP has launched Operation PALLIDUS to investigate the Medibank Private data breach.
- The OAIC has been notified of the breach in accordance with the Notifiable Data Breaches scheme and is working with Medibank Private to ensure they are complying with the requirements of the Notifiable Data Breaches scheme and providing advice on how Australians can respond and protect themselves from further harm.
- Services Australia and the Department of Health and Aged Care (Health) have been in contact with Medibank Private to understand the implications for privately insured customers, and support Medibank Private's strategy for communication with affected customers.
- Services Australia has put in place additional security measures on the first dataset and the second dataset to protect customer information. It is important to note that people cannot access a person's Medicare details with just a Medicare card number.
- On 22 September 2022, in response to the Optus data breach, the Department of Home Affairs (the Department) established a Commonwealth Credential Protection Register (the Register) to help stop compromised identities from being used fraudulently. Where it is applicable, the Register will be used for documents compromised in the Medibank breach.
 - The Register will prevent some compromised identity credentials from being verified through the Document Verification Service.
 - The Document Verification Service is used by some government agencies and businesses, such as banks, to verify an individual's identity online.
 - This will prevent credentials that are included on the Register from being used fraudulently. Rightful owners will also not be able to use them online to verify their identity.

If asked – is the Department of Home Affairs contacting affected Medibank Private customers?

- Medibank Private is responsible for contacting its affected customers and has begun making contact with them.

If asked – What is the government doing to keep our data safe?

- The Government is taking an all vectors approach to cyber and data security.
- The Government's new Cyber Strategy will build whole-of-nation resilience against these types of attacks and ensure our networks and devices are protected against malicious actors.
 - The Department is developing Australia's first National Data Security Action Plan, which will map the nation's data security settings and provide measures to strengthen consistency and resilience against data security threats.
 - The Digital Transformation Agency, with the Department, the Australian Taxation Office and Services Australia, is working to expand the use of secure digital identities. Companies can use secure digital identities to meet their customer identification

requirements while collecting less personally identifiable information. This will reduce the damage inflicted by these types of incidents.

- The Attorney-General's Department is reviewing the *Privacy Act 1988* to ensure that Australia's privacy laws are fit-for-purpose in the digital age and that they accord with community expectations in light of the rise of digital platforms and other technological changes.
- On 26 October, the Australian Government introduced the Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022 including amendments to significantly increase penalties for repeated or serious privacy breaches.
- In the October 2022 Budget, the Government announced additional funding of \$2.0 million in 2022-23 for IDCARE as part of the Government's commitment to fighting online scams. IDCARE is a not-for-profit agency that helps Australians to reduce the harm they experience from the compromise and misuse of their identity information.
 - This is on top of \$6.1 million over four years under the *Cyber Security Strategy 2020*.
- In January 2021 and prior to the Optus data breach, the Department engaged IDCARE under a four year \$6.1 million contract to provide counselling and support services to Australian victims of identity theft and cyber-crime as part of *Australia's Cyber Security Strategy 2020*.

If asked: Why was the National Coordination Mechanism used to respond to the Medibank cyber incident, but not to the Optus data breach?

- The response to the Optus data breach involved:
 - a Commonwealth Inter-Departmental Committee led by the Department of the Prime Minister and Cabinet;
 - the inter-jurisdictional National Cyber Security Committee led by the Australian Cyber Security Centre; and
 - regular engagement with Optus, including through an Optus-Australian Government working group.
- This enabled a coordinated response to the Optus data breach.

Related documents

- SB22-001042 – Optus data breach
- SB22-001194 – back pocket brief – Optus and Medibank data breaches
- EC22-005955 – Media article, 26 October 2022 – Fast track for nation's data shield (The Australian)

Consultation

Internal

Cyber and Infrastructure Security Centre, National Emergency Management Agency,
Disputes and Corporate Law, Media Operations.

External

Australian Signals Directorate, Australian Competition and Consumer Commission, eSafety
Commission, Australian Federal Police, Australian Prudential Regulation Authority,
Australian Securities and Investment Commission, Department of Health, Department of the
Prime Minister and Cabinet, Services Australia, Attorney-General's Department, Australian
Taxation Office, Treasury, Australian Transaction Reports and Analysis Centre, Digital
Transformation Agency, Department of Foreign Affairs and Trade, Office of National
Intelligence, Department of Defence.

Attachments:

Attachment A – Chronology of events

Attachment B – 19 October 2022 Media Release - Statement on Medibank cyber incident

Attachment C – 20 October 2022 Media Release - Press Conference

Attachment D – 25 October 2022 Media Release - Medibank cyber incident

Authorising Officer	Contact Officer
Brendan Dowling First Assistant Secretary Cyber, Digital and Technology Policy Division Department of Home Affairs ____ / ____ /2022 Ph: s. 22(1)(a)(ii)	Kavita Kewal Assistant Secretary Identity and Biometrics Policy and Strategy Branch Cyber, Digital and Technology Policy Division Department of Home Affairs ____ / ____ /2022 Ph: s. 22(1)(a)(ii)

ATTACHMENT A

MEDIBANK DATA SECURITY BREACH

Current as at 27 October 2022

CHRONOLOGY

- 12 October 2022, Medibank Private reported to the Australian Signals Directorate's Australian Cyber Security Centre (ACSC) that it was experiencing a cyber security incident..
- 13 October 2022, Minister's Office held a teleconference with Medibank Private CEO David Koczkar.
 - Following this meeting, Medibank Private sent the office a copy of their ASX release dated 13 October 2022.
- 13 October 2022, Medibank Private released a statement advising that they had detected unusual activity on their network. Medibank Private advised that:
 - There was no evidence that any sensitive data, including customer data, had been accessed.
 - It would be isolating and removing access to some customer-facing systems to reduce the likelihood of damage to systems or data loss.
- 14 October 2022, Home Affairs meeting with Medibank Private CEO David Koczkar.
- 14 October 2022, Medibank Private advised it had begun the process of communicating to its customers about the incident with around 2.8 million emails sent to Medibank Private and AHM customers.
 - Medibank Private also advised that while their investigation was ongoing, at this stage there was no evidence that its customer data has been accessed.
- 17 October 2022, Home Affairs discussion with Medibank representative Meghan Telford.
- 19 October 2022, Home Affairs meeting with Medibank Private CEO David Koczkar.
- 19 October 2022, Minister O'Neil held a teleconference with Medibank Private CEO David Koczkar.
- 19 October 2022, Medibank Private released a statement advising it had received messages from a group that wishes to negotiate regarding their alleged removal of customer data.
 - Medibank Private is undertaking urgent work to establish if the claim is true, although based on their ongoing forensic investigation they are treating the matter seriously at this time.
 - Medibank Private advised that their systems had not been encrypted by ransomware, which means usual activities for customers continues. Medibank

Released by Department of Home Affairs
under the Freedom of Information Act 1982

Private also advised that its ongoing response to safeguard its networks and systems may cause necessary temporary disruptions to its services.

- 19 October 2022, Minister O’Neil released a statement on the Medibank cyber incident.
 - ‘A significant cyber security incident has occurred within Medibank. The facts are continuing to be established’.
 - ‘I have spoken with the CEO of Medibank, David Koczkar, and the heads of Australian Signals Directorate (ASD) and AFP.
- 20 October 2022, Minister O’Neil call with Minister Butler, Health and Aged Care and Government Agencies to discuss operational and policy responses.
- 20 October 2022, Minister O’Neil call with ASD, Home Affairs and AFP to discuss whole-of-government coordination of response and law enforcement engagement with Medicare.
- 20 October 2022, Minister O’Neil held a teleconference with Medibank Private CEO David Koczkar.
- 20 October 2022, Interdepartmental Committee meeting (IDC), led by Home Affairs with cross government agencies to discuss risk and response to identity fraud and health implications.
- 20 October 2022, Home Affairs-led meeting with Medibank Private CEO, Treasury, Services Australia, Health, AFP, ACSC, OAIC, AGD and APRA to update on developments in scope of data.
- 20 October 2022, Medibank Private released a statement advising that it had been contacted by a criminal claiming to have stolen 200GB of data.
 - The criminal has provided a sample of records for 100 policies which Medibank Private believes has come from its AHM and international student systems.
 - The data includes first names and surnames, addresses, dates of birth, Medicare card numbers, policy numbers, phone numbers, and some claims data.
 - The claims data includes the location of where a customer received medical services and codes relating to their diagnosis and procedures.
 - The criminal claims to have stolen other information, including data related to credit card security, which has not yet been verified by Medibank Private’s investigations.
 - Medibank Private is continuing to work closely with government departments and organisations, as well as specialised cybersecurity firms, and have advised the ACSC.
- 20 October 2022, the Australian Federal Police (AFP) launched Operation PALLIDUS to investigate this cyber incident.
- 20 October 2022, Minister O’Neil held a press conference where the Medibank Private incident was discussed.
 - ‘What we learned yesterday is that communications have been made to Medibank from criminals who are claiming to have significant data of Australian citizens

and they have now demanded to enter into a negotiation with Medibank to hold that data effectively for ransom’.

- ‘What we know is that Medibank have confirmed today that the data being shown as a sample is their data’.
- 20 October 2022, Minister O’Neil discussed the Medibank incident with Sabra Lane on ABC radio.
 - ‘What has changed in the last 24 hours is that malicious actors have contacted the organisation claiming to have customer data’.
 - ‘It’s correct that someone claiming to have customer data has contacted Medibank to try to negotiate’.
- 21 October 2022, Home Affairs-led interdepartmental committee with government agencies on Medibank Private cyber incident update to discuss scope of data accessed and potential risks and responses.
- 21 October 2022, Minister O’Neil discussed the Medibank Private incident with Allison Langdon on the Channel 9, Today Show.
 - ‘In fact, we’ve actually agreed with Medibank to bring literally staff into their organisation to help them try to stop the really irreparable harm’.
- 21 October 2022, Minister O’Neil discussed the Medibank Private data breach with Natalie Barr on Channel 7, Sunrise.
- 22 October 2022, the National Coordination Mechanism (NCM) was activated to bring together agencies across the Government to discuss all response options, including health and wellbeing services, cybercrime .
- 23 October 2022, NCM meeting, led by Home Affairs.
- 24 October 2022, Home Affairs call with Medibank Private Senior Executive, Meaghan Telford.
- 24 October 2022, Home Affairs meeting with Minister’s Office to discuss Medibank Private and Cyber Security Strategy.
- 24 October 2022, Minister O’Neil meeting with ASD and AFP.
- 25 October 2022, NCM meeting, led by Home Affairs.
- 25 October 2022, Minister O’Neil held a teleconference with Medibank Private CEO David Koczkar.
- 25 October 2022, Medibank released a public announcement stating that they have received additional files from the criminal including a further 1,000 AHM policy records (which includes personal and health claims data).
- 25 October 2022, Minister O’Neil released a statement on the Medibank Private cyber incident.

- 25 October 2022, Minister O’Neil released a statement on the Medibank Private cyber incident.
 - Medibank advised the Australian Stock Exchange this morning that more customer data – and of broader scope – appears to have been accessed during the recent cyber incident.
 - Given the sensitive nature of the data, on Saturday I activated the National Coordination Mechanism to bring together agencies across the Federal Government, states and territories.
- 25 October 2022, Minister O’Neil released a statement on new cyber security measures in federal budget (cyber hubs and support for victims of scams through IDCare).
- 25 October 2022, Minister O’Neil addressed the Medibank Private incident in Parliament.
 - ‘The member might be aware that today Medibank provided an update on the consequences of the breach on their networks and confirmed that cybercriminals have taken more data than was previously reported’.
 - ‘Because of the way that the situation developed over the weekend through Friday and Saturday, on Saturday I asked my department to activate the National Coordination Mechanism to coordinate the work that's being done on Medibank’.
- 26 October 2022, Home Affairs meeting with ASD and AFP.
- 26 October 2022, Home Affairs call with Medibank Private Senior Executive, Meaghan Telford.
- 26 October 2022, Medibank Private provided an update on their investigation and advised that the criminal had access to all Medibank Private, AHM and international student customers’ personal data and significant amounts of health claims data.
- 27 October 2022, NCM meeting, led by Home Affairs, with attendees from Medibank Private, states and territories.

MEDIA ARTICLES

Date	Outlet	Reporting
13 October 2022	ABC News	Medibank Private says it has been hit by a cyberattack. The company said ‘unusual activity’ had been detected on its network, but there was no evidence that sensitive data had been accessed. Health insurer Medibank Private hit by cyber attack
13 October 2022	Medibank Private	We confirm we have successfully taken offline the AHM and international student policy systems and its data, and we are in the process of methodically and safely restarting the systems. Medibank cyber incident update
14 October 2022	Cairns Post	Medibank says no customer data was compromised. Medibank suffers ‘cyber incident’, crashes systems

14 October 2022	The West Australian	There may be a wait of weeks to determine what information was accessed in cyberattack. Medibank Private's 3.9 million customers face wait to learn if top secret information stolen in cyber attack
19 October 2022	The Sydney Morning Herald	Cybersecurity Minister Clare O'Neil's office released a statement on Wednesday night. "A significant cybersecurity incident has occurred within Medibank. The facts are continuing to be established", she said. The minister said she had spoken to the company's chief executive, the AFP and the ASD. Medibank Private hackers threaten to sell customer data in ransom demand
20 October 2022	ABC	Minister O'Neil says a ransomware attack on Medibank and the alleged removal of customer data has been referred to the AFP for investigation. Ms O'Neil confirmed the company was working with the Australian Cyber Security Agency and the ASD over the alleged ransom request. Medibank cyber attack and ransom demand referred to Australian Federal Police - ABC News
20 October 2022	The Guardian	Medibank says sample of stolen customer data includes details of medical procedures. "Combined with Optus, this is a huge wake-up call for the country. And [it] certainly gives the government a really clear mandate to do some things that, frankly, probably should have been done five years ago, "The threat that is being made here, to make the private personal health information of Australians made available to the public, is a dog act." Medibank says sample of stolen customer data includes details of medical procedures
21 October 2022	Yahoo News	Cyber Security Minister Clare O'Neil has described the country as being "behind the eight ball" on data theft, "at the end of the day, you can replace a credit card. This is health information, it is private and personal information of people that has no place being put into the public realm," she said. Medibank hack exposed cyber flaws: O'Neil
21 October 2022	9 News	Home Affairs Minister Clare O'Neil has warned the damage could be irreparable".

		Medibank cyber attack: Medibank CEO apologises for 'horrendous crime' as customers remain in the dark about extent of hack
22 October 2022	The Sydney Morning Herald	The government yesterday gave formal notice it was investigating which <i>Medibank</i> customers have had their Medicare card information exposed in the hack that has put up to 1 million people's details at risk. Online breach fines to hit \$50m
26 October 2022	The Sydney Morning Herald	Emergency action as scale of Medibank breach widens. "Home Affairs Minister Clare O'Neil told parliament yesterday that she had activated the NCM". "What we can see is <i>Medibank</i> is just as complex and urgent as some of what was dealt with [during the pandemic]". Emergency action as scale of Medibank breach widens
26 October 2022	The Australian	Medibank hack: all 3.9m customers hit by cyberattack. All 3.9m customers hit by cyber attack
26 October 2022	News.com.au	The federal government has undertaken emergency procedures to coordinate a response to the Medibank data breach. The national framework is empowered to organise all relevant agencies to respond to the hack. Medibank data breach prompts emergency action by govt