Prohibiting the use of TikTok

Talking Points

- Our Government prioritises the protection of our information, people and assets from compromise and harm.
- Currently, a risk-based approach towards use of social media platforms is applied across Tasmanian Government agencies.
- Leading Australian Government intelligence and security agencies have identified one of the specific concerns with the use of TikTok is the extensive collection of user data and potential exposure to directions from a foreign government.
- Based on the Australian Government's decision to prohibit TikTok on government-issued devices, we determined that the security risk posed by the platform is such that our Government should make the same decision in the interests of protecting our resources.
- We are continuing to monitor the national policy settings and will be guided by national intelligence and security agencies as we work to implement the ban, including any exemptions that may be relevant.
- Exemptions may apply in certain official circumstances, where the known and considered risks are outweighed by the benefit of the use of TikTok.
- Our Government is currently leading and delivering various security uplift activities, led by the Department of Premier and Cabinet.
- Ensuring a nationally consistent approach towards security is a primary focus of this work and continues to be the preferred methodology in securing our Tasmanian Government resources.

Additional Talking Points

- The use of social media platforms can expose the Government to broad security risks, including:
    - Phishing: An attempt to gain access to information or systems by tricking people to click on links or share information, through purportedly legitimate companies.
    - Misinformation: The sharing of false or inaccurate information.
    - Disinformation: Information intended to mislead, particularly through propaganda.
    - Identification: Identifying one of our employees, their workplace or their colleagues.
    - Social engineering: An attempt to gain information, or access to it, through manipulation.
- The Australian Signals Directorate provides the following advice regarding the use of TikTok:
    - Do not use it on a phone that can access any official information, for example any Tasmanian Government workplace communication (such as email, MS Teams etc).
    - If a phone does have TikTok installed, keep the phone away from any sensitive conversations.
    - Remove metadata (such as location information) from photos and videos before uploading them to TikTok.

Tasmania's Protective Security Policy Framework

- To support our priority of protecting our information, people and assets from compromise and harm, Cabinet endorsed the Tasmania's Protective Security Policy Framework (TAS-PSPF) – a nation leading framework applying nationally consistent protective security principles.
- Work is ongoing to look at technical controls that will support the ban of TikTok and provide capacity to manage future security risks, which includes the implementation of the TAS-PSPF.

Background

- Recent national and international conversation regarding the use of social media platforms (specifically TikTok) on government-issued devices has been topical due to security concerns.

- Progressively, all Five Eyes intelligence alliance countries have moved to ban TikTok on government-issued devices due to these concerns.

- The Australian Government made the decision to prohibit TikTok on 4 April 2023.

- The Tasmanian Government announced the banning of TikTok on government issued devices on 6 April 2023.

- Intergovernmental consultation has been conducted, ensuring a collective understanding on the work being undertaken in the prohibition of TikTok across all jurisdictions.

- Some of the social media platforms currently used by Tasmanian Government employees include Facebook, Instagram, WhatsApp, Messenger (collectively known as Meta), TikTok, Twitter, WeChat and LinkedIn.

Ministerial Portfolio: Minister for Science and Technology

Output: 3.1 - Information Technology and Digital Services Strategy and Policy Development

Overview, Budget and Staffing - Information Technology and Digital Services Strategy and Policy Development

Talking Points

Overview

- Digital Strategy and Services (DSS) is a part of the Government Services division within the Department of Premier and Cabinet (DPAC). The Government Services division also includes Service Tasmania.
- DSS advises and supports the Minister for Science and Technology; and the Tasmanian Government and its agencies to achieve priority objectives, core business outcomes, programs and services through the provision of fit-for-purpose digital policy and digital services.
- DSS works with client agencies to identify common needs and synergies, aggregate demand, consolidate capability, and recommends and provides digital and technology solutions.
- The DSS mission is 'working together to lead the digital transformation of the Tasmanian Government through the delivery of trusted advice, strategies and services.'
- DSS current priorities include:
    - Progressing and supporting key actions associated with the Tasmanian Government's digital transformation strategy - Our Digital Future.
    - Delivering the Tasmanian Government Cyber Security Program.
    - Supporting the Government's roadmap for digital reform of the Tasmanian State Service, including opportunities for service improvement through digital transformation recommended in the Independent Review of the State Service.

- Responding to the national digital transformation agenda and coordinating the associated intergovernmental relationships driven by the Data and Digital Ministers.
- Continuing to deliver critical whole of government digital infrastructure services to Tasmanian Government agencies and organisations, supporting the service-lifecycle and progressing major contract renewals and service improvements.

Additional Talking Points

Supporting key actions associated with ***Our Digital Future***

- DSS is involved in supporting the delivery of the following major actions outlined in Our Digital Future: Tasmanian Government strategy for digital transformation:
    - Supporting transformative digital projects that improve the delivery of frontline services to Tasmanians.
    - Facilitating the development of a whole-of-government technology roadmap.
    - Facilitating the development of new frameworks for information management and data governance.
    - Continuing to develop policy and champion the adoption of distributed cloud services across government agencies.
    - Implementing cyber security programs that prioritise critical asset protection across government.
    - In conjunction with the Department of State Growth, working with industry, business and education partners to develop and promote digital education, career pathways and workforce capability.
    - Supporting and promoting initiatives across government that provide inclusive strategies for digital literacy and inclusion. Including the coordination of priorities for digital inclusion across government in conjunction with community and industry stakeholders.

Supporting the Government's roadmap for digital reform

- The Tasmanian Government supports, or supports in-principle, all 77 recommendations of the Independent Review of the State Service (the Review), focused on ensuring that the State Service is fit for purpose for Tasmania today and into the future.
- The Review noted that 'digitisation' and 'digitalisation' represented a core strategy that could help secure efficiencies in the delivery of government services and improve the experience of working in and with government.
- The Review recommended a three-tiered strategy for digital reform:
    - The central allocation of funding to incentivise the digitisation of manual process to bring existing services up to a standard that meets current community expectations (Recommendation 26).
    - The implementation of a functional leadership model across the key digital platforms that provide the foundation for digitalisation across the State Service (Recommendation 22).
    - To support whole-of-government coordination and governance of digitalisation, with a renewed mandate to drive whole of government consistency and improvements in the foundations of digitalisation (Recommendation 24).
- In 2021 the Government committed to invest $4.3 million to begin the development of a digital Service Tasmania portal to provide Tasmanians with a secure and easy-to-use access point for Government services, which will be accessed through a single login.
- Service Tasmania is working with DPAC's DSS to progress the initial phase of the digital services portal.
- Discussions are also progressing across government focusing on digital identity policy, capability, security, and interoperability.
- This early work will allow Service Tasmania to begin its digital services journey and also aligns to the State Service Review (Recommendation 65).

- This supports customers to have more choice in how they access government services, and progresses alignment of digital, in-person and over-the-phone service channels.

Responding to the national digital transformation agenda

- There is a comprehensive national digital transformation agenda being progressed through the Commonwealth Data and Digital Ministers' Meeting.
- DPAC and DSS coordinate, attend and participate in various meetings, governance and working groups in support of the national agenda.
- Key initiatives include intergovernmental data sharing, digital inclusion and participation, digital services design and delivery, and digital identity.

Delivering the Tasmanian Government's Cyber Security Program

- The 2023-24 Budget provides funding to commence the development a sustainable whole-of-government functional leadership model for cyber security services, linked to the establishment of up to four sector based cyber hubs to operate across government.
- This initiative of $3.3 million will be funded from the Digital Transformation Priority Expenditure Program within Finance-General and will leverage capabilities developed as part of the existing Government cyber security programs
- In 2020-21, an additional $4.9 million over four years was committed to improve the Government's ability to protect Tasmanians' data and minimise the potential for disruption of government services from cyber security threats. Key initiatives established under the Program include:
    - Building cyber security incident response capacity and capability.
    - Supporting Tasmanians who have been affected by identity theft.

- Increasing cyber security awareness across government to ensure staff understand their role in reducing cyber security risks.
- Implementing role specific cyber security training for staff that will enable them to recognise cyber security threats and to respond appropriately.
- Upskilling cyber security professionals across government with the latest techniques.

- DSS is also involved with the national cyber security agenda, actively participating in the National Cyber Security Council and its associated working groups, cyber security exercises and collaboration with the Victorian Joint Cyber Security Centre (JCSC).

Whole of government digital infrastructure services

- DSS delivers a range of government-to-government services that underpin service delivery and operations across the Tasmanian Government. This includes the management of infrastructure and services contracts in excess of $40 million per year, providing savings to government through scale of economy and management efficiencies.

- The DSS portfolio of services includes:
  - The provision of services and contracts for over 17,000 telephony services across all agencies supporting key citizen services such as Service Tasmania and the COVID Hotline.
  - Management of supplier arrangements for critical network and internet communications services supporting government business across 960 locations in 128 towns including schools, Service Tasmania shops, hospitals, and fire stations.
  - Processing of over 1.1 million individual payslips, with a total value of more than $2 billion dispersed annually.

Coordinating d**igital inclusion priorities**

- Improving digital inclusion and participation within Tasmania is a cross sector, multi-discipline, and broad geographical issue that affects a great number of Tasmanians.
- The Digital Community objectives and priorities in Our Digital Future outline the Tasmanian Government's action plan for digital inclusion.
- The Premier's Economic and Social Recovery Advisory Council final report and the recent Tasmanian Audit Office report COVID-19 – Response to social impacts: mental health and digital inclusion highlights further work is required, including establishing a clear governance framework for cross-agency oversight and improvements to digital inclusion, developing Key Performance Indicators, engaging with local communities to address digital inclusion at a local level and expanding access to existing government facilities which provide digital capability.
- The 2023-24 Budget provides $150,000 to fund the development of a Tasmanian Government Digital Inclusion Strategy.
- In conjunction with Government, community and industry stakeholders DPAC Digital Strategy and Services will coordinate the development of an agreed set of priorities for digital inclusion across government.
- This will establish a mechanism to work with the community and industry to create a sustainable and viable inclusion strategy, and to validate performance indicators that will allow the government to measure the value of specific initiatives.

Budget

- Digital Strategy and Service (DSS) consolidates Output 3.1 Information, Technology and Digital Services Strategy and Policy Development and Output 3.3 – Delivery of IT Services, both of which are represented in Table 1 below.

Table 1 – 2022-23 and 2023-24 Comparison

Title	2022-23 $'000	2023-24 $'000
3.1 Information, Technology and Digital Services Strategy and Policy Development	2 536	3 429
3.3 Delivery of IT Services	23 994	23 987
Digital Strategy and Service	**26 530**	**27 416**

Budget Background

- The DSS expense budget decreased by $3.3 million from $30.8 million in 2013-14 to $27.4 million in 2023-24. Several factors impacted the budget during this period:
    - a reduction in budgeted FTEs;
    - reduced information technology expenditure due to the transition of software, infrastructure and services to the cloud; and
    - changes to whole-of-government information technology service offerings.
- DSS has been transitioning to a revised operating model focused on supporting government agencies through their transition to contemporary IT delivery models in line with the Government's cloud computing policy.
- In recent years the Agencies have been transitioning away from owning and maintaining IT infrastructure, towards consumption based (or cloud-based) IT delivery models.
- The timing of this transition sees less expenditure occurring within DSS to operate and maintain legacy infrastructure centric services, and that the divestment in these services is currently running behind new investments in new value creating whole of government digital services – which are expected to increase over time.

Table 2– 2013-14 to 2023-24 Comparison

Title	2013-14 $'000	2020-21 $'000	2021-22 $'000	2022-23 $'000	2023-24 $'000
3.1 Information, Technology and Digital Services Strategy and Policy Development	1 300	1 928	2 425	2 536	3 429
3.3 Delivery of IT Services	29 468	25 993	23 306	23 994	23 987
Digital Strategy and Service	**30 768**	**27 921**	**25 731**	**26 530**	**27 416**

Table 3– Cyber-Hubs Initiative

Title	2023-24 $'000	2024-25 $'000	2025-26 $'000	2026-27 $'000
Cyber-Hubs	500	900	928	955

1. This initiative is funded from the Digital Transformation Priority Expenditure Program in Finance-General.

Staffing

- Paid FTEs have increased by 2.9 from 57.7 at 31 March 2022 to 60.6 at 31 March 2023.

Table 4 – FTE comparison – March 2021 – March 2023

Title	31 March 2021	31 March 2022	31 March 2023
Paid FTE	52.5	57.7	60.6

Performance information

- Table 5 summarises Digital Strategy and Services performance against key metrics for service delivery. KPIs reported are average of scores across all agencies.

- The Digital Services Strategy 'Customer Satisfaction' performance measure has been replaced in 2022-23, from a percentage measure to a rating 0 – 5 system (5 highest). Due to the timing of this change a 2021-22 Actual is unavailable.

Table 5 – Performance comparison 2020-2021 to 2023-2024

Performance Measure	Unit of Measure	2020-21 Actual	2021-22 Actual	2022-23 Target	2023-24 Target
Information, Technology and Digital Services Strategy and Policy Development					
Percentage of Tasmanian Government Departments that are adopting key digital policies.	%	100	100	100	100
Delivery of IT Services					
Service level agreement performance and compliance	%	89	91	>90	>90
Proportion of whole-of-government contracts managed by Digital Strategy and Services that are validated and current.	%	100	100	100	100
Customer satisfaction	Rating	na	3	4	4

Data Sharing and Information Management

- The imperative to share data and improve the way information is managed has increased in recent years as all Australian governments rallied to respond to and plan their management and recovery from the COVID-19 pandemic.
- The Tasmanian Government continues to participate in a range of local and national data sharing and management reforms and is a signature of the data sharing agreement between the Commonwealth and State and Territory governments
- At the national level the Tasmanian Government has been involved with:
    - the development of the Australian Government's *Data Availability and Transparency Act 2022*; and
    - the implementation of an Inter-Governmental Agreement (IGA) for data sharing, including participation in various data sharing and systems reform initiatives linked to this agreement.
- The Tasmanian Government also supports the recommendations of the Tasmanian State Service Review, which outlines opportunities for data sharing and recommends the development of a whole-of-government capability for sharing, linking and analysing data (Recommendation 19).
- While recommendations from the Commission of Inquiry into the Tasmanian Government's responses to child sexual abuse in institutional settings are due later this year, we are not waiting to take action where it is clear it is needed now. We are looking at legislative solutions to make it easier to share information about risk to children.
- Moving forward the Tasmanian Government is committed to continued involvement with the National Data Sharing IGA and its related projects and initiatives.
- The Tasmanian Government is also progressing work aligned with *Our Digital Future* and the recommendations of the Tasmanian State

Service Review to establish a data strategy and improve whole-of-government data governance, security and sharing capabilities (Recommendations 22,24,25 and 26).

- The Tasmanian Government is currently developing a Data and Information Management strategy which will contain key initiatives and future strategic direction as custodian of critical data and information resources.

FAQs

What national data sharing initiatives has the Government been involved with?

- Data Sharing Projects include – Road Safety, Waste Management, Natural Hazards and Emergency Management, Family, Domestic, and Sexual Violence, Closing the Gap and Veterans' Health.

- Systems reform projects include – Establishing an Australian Data Network, developing standard operating procedures for data sharing activities, improving discoverability of priority data, and developing a share-once use-often model for administrative data.

How will the Government protect the privacy and confidentiality of Tasmanians' data?

- Continued implementation of the Tasmanian Government Cyber Security Program to help improve the level of trust and resilience in its systems and to safeguard government-held information and services.

- Implementation of the new Protective Security Policy Framework (PSPF) that includes protocols to align information security and information classification with similar protocols used by other Australian governments.

- Participation in the development of the National Data Security Action Plan that will focus on data security policy settings for state and territory governments, industry and the broader economy.

- Participation and accreditation with the *Data Availability and Transparency Act 2022* which establishes a best practice scheme for sharing government data.

Background

Inter-Governmental Agreement (IGA) on Data Sharing

- National Cabinet requested (through Data and Digital Ministers) the development of a new intergovernmental agreement on data sharing, and this was signed off at National Cabinet on 9 July 2021.
- A second work program has commenced under the IGA.
- Work Program Projects under the IGA
    - Closing the Gap community infrastructure – Data sharing on infrastructure in discrete first nations communities.
    - Multilateral Data Sharing Agreement – To support the NDDA (details below) a further sharing agreement is being considered.
    - National Data Catalogue – Formation of an agreed national data catalogue to support national efforts on data sharing.
- Relevant Tasmanian Government portfolio agencies have participated in the data sharing projects (eg. Department of State Growth on Road Safety).

National Disability Data Asset

- The National Disability Data Asset (NDDA) seeks to establish a national database co-ordinating commonwealth, state and territory data to provide insights on disability in Australia.
- The National Disability Data Asset Memorandum of Understanding was signed in 2023 by Minister Palmer.
- The creation of the national approach follows a two-year pilot between the commonwealth and two other states. The pilot engaged broadly with the disability community on data use, ethics and privacy.
- Representative governance and administration bodies will be established to guide the NDDA.
- To provide the services and technical capacity to support the NDDA the Australian National Data Integration Infrastructure (ANDII) will be created. ANDII will initially support the NDDA, but it is anticipated that future national assets would reuse the infrastructure and associated services and governance.

The *Data Availability and Transparency Act 2022*

- The *Data Availability and Transparency Act 2022* (DAT Act) came into effect in April 2022.
- The legislation establishes a new, best practice, scheme (the DATA Scheme) for sharing Australian Government data, underpinned by strong safeguards and simplified, efficient processes.

- The DATA Scheme is focused on: increasing the availability and use of Australian Government data; helping to deliver government services that are simple, helpful, respectful and transparent; informing better Government policy and programs; and supporting world-leading research and development.

- Under the DATA Scheme, the Tasmanian and other state and territory governments would take on the role of users and data service providers. Government users and service providers are required to be accredited under the Scheme.

- The DAT Act contains general privacy protections that minimise the sharing of personal information, prohibit the re-identification of data that has been de-identified, and prohibit the storage or access of personal information outside Australia.

- The experience and capabilities developed through participation in the DATA Scheme are expected to provide spill over benefits for data sharing and management practices in the Tasmanian Government.

The Tasmanian State Service Review (TSSR)

- The TSSR recommendations related to data and digital include:

    - Recommendation 19 – develop a stronger whole-of government capability for sharing, linking and analysing data and assign a functional leader to deliver service to, or build capability across all agencies.
    - Recommendation 22 – That the Government, through the heads of agency, develop a platform-based functional leadership mode; for the ongoing development and integration of consistent core business systems across all agencies.
    - Recommendation 24 - That the TSS incorporate platform-based functional leadership into the digital services governance framework and replace the Digital Services Board with heads of agency meetings. This has now progressed with the formation of the Secretaries Board.
    - Recommendation 25 - Amend the terms of reference of the Deputy Secretaries Digital Services Committee to include the Chief Information Officer as a member. This has been progressed through the formation of the Data and Digital Committee, a subcommittee of the new Secretaries Board.
    - Recommendation 26 - That the TSS progressively eliminate 'manual only' business processes, and that the government fund a small, centrally funded resource to drive the digitalisation of existing business processes.
    - Recommendation 34 - That the Department of Health continue to develop the Human Resource Information System (HRIS) to provide the foundation for a whole-of-government system, with clear whole-of-government business requirements for accurate and timely reporting to heads of agency, the Head of the State Service, the Employer and Parliament.

Our Digital Future

- Under the Digital Government section, *Our Digital Future* identifies a specific action (3.1) to *develop new frameworks for information management and data analytics.*

Ministerial Portfolio: Minister for Science and Technology

Output: 3.1 Information Technology and Digital Services Strategy and Policy Development

DSS Use of Consultants

Talking Points

- The Department of Premier and Cabinet (DPAC)'s Digital Strategy and Services (DSS) division entered into seven consultancy contracts, valued at $50,000 or greater, during the period 31 March 2022 to 31 March 2023.
- The total value of these contracts is $757,998, with six contracts awarded to Tasmanian businesses.
- For all seven contracts awarded, the Department undertook procurement processes in accordance with the applicable Treasurer's Instructions, including Treasurer's Instruction PF-2 – *Buy Local Policy*.
- All contracts valued at $50,000 and over are reported on the Tasmanian Government Tenders website.

Background

- DSS ensures that its procurement activities are undertaken in accordance with the mandatory requirements of the Treasurer's Instructions relating to procurement, including Tasmanian businesses are provided with every opportunity to compete for DSS's business. It is DPAC's policy to support Tasmanian businesses whenever they offer best value for money for the Government.

- A 'consultant' is a particular type of contractor, usually engaged to provide recommendations, specialist or professional advice; as distinct from a 'contractor' who is engaged to provide specified goods or services and usually works under the supervision of an Agency officer.

- 'Contract value' is the total maximum value of the services over the term of the contract. This includes the value of any options for extension, as well as disbursements and other out-of-pocket expenses.

- 'Tasmanian Business' is as a business operating in Tasmania that has a permanent office or presence in Tasmania and which employs Tasmanian workers as per Treasurer's Instruction PF-6.

- All awarded contracts having a value of $50,000 or greater are reportable by the Department (as per Treasurer's Instruction PF-5 – Accountability and Reporting).

- The engagement of external consultancy services and specialist perspectives has been required to:

    - Prepare a telephony data document to enable a proof of concept for a Tasmanian Government telephony database to be developed.

    - Provide technical support services for the Networking Tasmania Evolution Program.

    - Develop and advise on a whole-of-government Network Security Framework.

    - Review DSS's existing Identity Management Services environment and prepare a recommendations report.

    - Develop a cyber security strategy for the Tasmanian Government.

    - Deliver Threat and Risk Assessments for whole-of-government services.

    - Analyse, develop, and deliver project management artefacts for the Project Practice and Service Stream Alignment project.

Attachments

A. List of consultants engaged by DSS (31 March 2022 – 31 March 2023)

Attachment A – List of Consultants Engaged by DSS

Digital Strategy and Services division – List of consultants engaged with a value greater than $50,000 for period from 31 March 2022 to 31 March 2023

Consultant name	Contract Title	Contract Description	Contract Term	Tasmanian Business?*	Contract Value? (exc GST)#	Spend Against Contract
3 Tier Technology Pty Ltd	Telephony Data Requirements	The Supplier will provide a telephony data document to enable a proof of concept for a Tasmanian Government telephony database to be developed.	*18 April 2022 - 30 June 2022 (period of option to extend: 1 July 2022 - 30 September 2022)	Yes	$50,000	$42,787.50
CGI Technologies and Solutions Australia Pty Limited	Networking Tasmania Evolution Program - Procurement Technical Support Services	The Supplier will provide technical support services for the Networking Tasmania Evolution Program.	*11 May 2022 – 21 October 2022 (extended until 23 December 2022)	Yes	$99,999	$61,892.97
CGI Technologies and Solutions Australia Pty Limited	Whole-of-Government Network Security Framework – Consultancy Services	The Supplier will provide consultancy services for the development of a Whole-of-Government Network Security Framework for the Tasmanian Government.	12 December 2022 – 17 May 2023	Yes	$241,001	$24,000.
Telstra Corporation Limited	Forefront Identity Management Discovery Services	The Supplier will perform a review of the Customer's existing Identity Management Services environment and prepare a recommendations report.	26 September 2022 - 28 November 2022 (period of option to extend: 29 November 2022 to 28 February 2023)	Yes	$67,200	$66,240.
Deloitte Risk Advisory Pty Ltd	Tasmanian Government Cyber Security Strategy	The Supplier will develop a cyber security strategy for the Tasmanian Government.	26 September 2022 – 16 December 2022 (extended until 31 March 2023)	Yes	$99,800	$79,840.

CyberCX Pty Ltd	Whole-of-government Services – Threat and Risk Assessments	The Supplier will perform Threat and Risk Assessments for whole-of-government services, as required by Digital Strategy and Services. The use of this company was supported by the Australian Government given the Cyber incident occurring.	1 December 2022 - 1 December 2023 (period of option to extend: 2 December 2023 - 1 June 2024)	No	$99,999	$26,875.
GMC Enterprises Pty Ltd	Project Practice and Service Stream Alignment	The Supplier will deliver project management artefacts to Digital Strategy and Services, and conduct analysis, development, delivery and change management services for the Project Practice and Service Stream Alignment project.	1 December 2022 – 1 December 2023	Yes	$99,999	$31,737.75

* Issued prior to 1 July 2022

GoAnywhere Compromise

Talking Points

- The Tasmanian Government has been impacted as part of a global campaign of malicious activity by cyber criminals that has affected numerous customers of Fortra's GoAnywhere Managed File Transfer (MFT) system.

- I need to stress that this compromise was not a compromise of Tasmanian Government systems, but that of a third-party provider.

- Investigations identified that the Department *for* Education, Children, and Young People's (DECYP) GoAnywhere MFT service, hosted by Fortra, was compromised as part of this campaign.

- To date, approximately 16,000 documents have been publicly disclosed by the criminal organisation involved in the compromise.

- The data disclosed related to current and historical DECYP financial information.

- The Government has communicated with those Tasmanians whose data has been disclosed by cyber criminals on the dark web; and has also communicated with individuals and businesses not directly impacted by the April 7 disclosure, but who may potentially be affected by the compromise should more data be disclosed.

- At all times, the Government's proactive approach has been focussed on communicating factual information to keep the community informed, but not alarmed.

- It is important to understand that until data was released by the criminals on 7 April 2023, the Government had no confirmation of the loss of information. Until that time, the Government was only aware that there had been a compromise of GoAnywhere's system.

- The Tasmanian Government has not received any demands from the cyber criminals; however, it continues to monitor the situation and is ready to respond should more data be publicly disclosed.

- The Government has also confirmed that it will not pay a ransom to criminals as a result of this sort of cyber-attack, in line with Australian Government advice.

- On 7 April, a dedicated Tasmanian Emergency Information Service (TEIS) call centre was stood up and available to assist all Tasmanians with advice and support. As at 28 April there had been 401 enquiries made to this service.

- The Tasmanian Government remains committed to communicating with affected individuals, minimising any harm to those impacted by the compromise and supporting them if required.

- On 1 May, the Government launched a public campaign focussing on how Tasmanians can better protect their data online, how to recognise a scam, and what to do if they become a victim of a scam.

Additional Talking Points by Subject

When did the government first become aware that it had a data breach?

- On 25 March 2023 the Australian Cyber Security Centre contacted the Tasmanian Government regarding claims from a cyber-criminal organisation that it had stolen data from the Tasmanian Government.

- When the initial claims were made they were difficult to verify without the disclosure of any data.

- The Tasmanian Government Cyber Security team immediately initiated a response focused on containing any active compromise and assessing any potential sources of compromise and data exfiltration.

- All agencies were involved in supporting the initial response as part of the Tasmanian Cyber Incident Management Arrangements.

- The criminal organisation in question had been linked to the exploitation of a vulnerability associated with the GoAnywhere MFT system. This fact guided the initial and subsequent investigations.

- On 27 March 2023 DECYP provided the Tasmanian Government Cyber Security team with information relating to their GoAnywhere MFT service and the investigation focussed its inquiry in this area.

- On 7 April 2023 a data breach was confirmed when approximately 16,000 DECYP invoices generated by a third-party provider were disclosed by cyber-criminals. Until this date the Government had no confirmation of the loss of data.

- Prior to being notified on 25 March 2023 of the claims by the criminals, DECYP was aware of a vulnerability with the GoAnywhere system but did not have knowledge that information had actually been stolen. The earlier details are as follows:

    - On 1 February DECYP were advised via email to check a GoAnywhere service portal for advice re a service update.

    - The advice from GoAnywhere indicated they were investigating potentially suspicious activity on the GoAnywhere MFT cloud instance, and while the investigation was underway, they would out of caution implement a temporary service outage for the GoAnywhere MFT cloud instance.

    - On 6 February DECYP was informed of a software vulnerability within the GoAnywhere MFT system and took the appropriate remediation actions, with all action being completed by 7 February.

    - On 11 March DECYP received advice from the GoAnywhere MFT vendor Fortra that its managed GoAnywhere MFT cloud instance had been subject to unauthorised activity between 28 January and 31 January 2023, prior to any knowledge of the vulnerability (also referred to as exploitation of a zero-day vulnerability).

    - The advice from Fortra to DECYP was that they had little visibility at that time of any data being extracted as a result of the unauthorised activity.

Why did the Government advise the public when it did, or why did it take you so long to inform the public?

- The Tasmanian Government response plan was managed in four phases – containment, assessment, notification, and review. This approach aligns with the Australian Information Commissioner's Guidelines for notifiable data breaches.

- I want to make it abundantly clear that the Government followed established approaches to managing this type of event and did so based on factual and technical advice.

- As is common in cyber breaches, information relating to the nature of the incident and the extent of any data beach was complex and imperfect during the early response phases. Our understanding only increased as a complex investigation progressed.

- This incident effectively began as an allegation that criminals had stolen information from the Tasmanian Government. The response team's initial priority was to examine the credibility of that allegation, ascertain if an active cyber security breach needed to be contained, and to understand what, if any data may have been stolen.

- Data breaches can involve different types of information and give rise to a range of actual or potential harm to individuals and organisations. They need to be dealt with on a case-by-case basis, with an understanding of the emerging facts and risks posed by the breach and the actions that would be most effective in reducing harm.

- Given the potential nature of the data sets managed within DECYP and not knowing fully what data may have been compromised, the Government's notifications strategy followed a principle of 'responsible release', looking to minimise the possibility for harm, generally in line with our duty of care and focused on individuals considered to be at greater risk if their data was exposed.

- The Tasmanian Government notification and harm assessment outcomes were well within the expectations outlined in the Australian Information Commissioner's guidelines for notifiable data breaches.

- On Saturday 25 March the Tasmanian Government was notified of an alleged compromise or theft of data. This notification initiated a preliminary investigation and analysis process.

- On Friday 31 March, as the Minister for Science and Technology I issued a media release to say that the Tasmanian Government was investigating a data breach of a third-party file transfer service.

- On Wednesday 5 April DECYP emailed 10,559 creditors. This was a proactive email outlining that data may potentially be at risk. Schools received the same information, to share with parents and carers.

- On Friday 7 April DECYP data was released to the dark web. Analysis of the data indicated that it related to 16,000 financial documents including school invoices and debtor statements.

- On Friday 7 April DECYP sent 8,893 emails to the parents, carers and businesses identified in the data that was disclosed.

- In exercising an abundance of caution and taking the duty of care seriously, on Monday 10 April DECYP emailed all potentially impacted stakeholders from the last five years. 145,683 emails were sent to debtors, creditors and approximately 1,600 previous DECYP employees, notifying them that their data may be at risk.

What has the Government done to support the community, and minimise harm associated with this incident?

- Following notification of the incident the Tasmanian Government activated the Tasmanian Cyber Incident Management Arrangements and stood up an Incident Management Team (IMT) to contain any ongoing activity and to investigate sources of potential data exfiltration.

- The State Emergency Management Committee (SEMC) was convened on 5 April and briefed on the incident.

- The Tasmanian Government has been proactive in communications with potentially impacted individuals.

- DECYP proactively emailed 10,559 creditors on 5 April outlining that data may potentially be at risk. Schools received the same information to share with parents and carers.

- On 10 April DECYP emailed all potentially impacted stakeholders from the last five years. This included 145,683 emails sent to debtors, creditors and approximately 1,600 previous DECYP employees, notifying them that their data may be at risk.

- Letters (surface mail) were also sent to parents, carers, and businesses where email addresses were not available (approximately 2,500 letters).

- An additional 40,195 letters were also sent where emails failed to deliver and to those for whom DECYP did not have an email address registered from the 145,683 contacts.

- All DECYP staff - including The Office of the Education Registrar; Teachers Registration Board; The Office of Tasmanian Assessment, Standards and Certification; TasTAFE; and the Commissioner for Children and Young People - were also contacted.

- The Tasmanian Emergency Information Service (TEIS) was activated to handle public calls for further information.

- TEIS operators took 356 calls between 7 April and 21 April. The TEIS hotline was extended until 6pm on 28 April to manage the anticipated increase in enquiries when approximately 8,000 staff and school communities returned from holidays, and more than 40,000 letters reached households and businesses.

- Harm minimisation measures were put in place for at-risk individuals. The Department of Justice and the Tasmania Police Safe at Home Coordination Unit (SFCU) reviewed data holdings to determine vulnerable or at-risk individuals. Some individuals were identified and triaged, with referrals made to the Family Violence Unit for further contact.

- DECYP stood up temporary call centres in Hobart, Launceston and Devonport to contact vulnerable people. DECYP worked closely with Tasmania Police's Safe at Home Coordination Unit to ensure all vulnerable people were notified.

- The Tasmanian Government also engaged the following organisations to support or provide advice.

    - IDCare – to provide harm minimisation support and advice in addition to victim support services for affected individuals.

    - ID Support NSW - to work with the Tasmanian Government to get email communications out in a timely manner.

    - CyberCX – to investigate the extent of the compromise and review the security and configuration of the GoAnywhere MFT DECYP environment.

    - ACSC - for incident assistance, guidance and advice; and to provide cyber security threat intelligence and information sharing with other jurisdictions.

    - The AFP also agreed to extend Operation Guardian's remit to include harm minimisation support for Tasmanians impacted by the data disclosed in this incident.

What is the Government doing now? Is it going to happen again?

- Whilst there have been no further data disclosures by the cyber criminals since 7 April 2023, the Government still considers the incident to be active and continues to manage the consequences and security response under Tasmanian Emergency Management Arrangements and the Tasmanian Cyber Incident Management Arrangements respectively.

- The Government has a well-formed Consequence Action Management Plan and DECYP have finalised an internal Data Drop Response Plan, Vulnerable Cohort Management Plan and Assessment Process underpinned by a risk assessment.

- The Tasmanian Cyber Security Team continues to investigate and review the incident in conjunction with other third-party experts.

- The Tasmanian Cyber Security Team is also continuing to monitor threat intelligence for any additional data disclosure and for associated malicious activity.

- Any new data disclosure may require additional communications with affected individuals and where people are identified as vulnerable to potential harm, the Government will implement additional supports to minimise the risk.

- The Government also acknowledges that information released onto the internet by the cyber-criminals is permanently disclosed.

What risk assessment process does the Government go through before it starts using products - including the GoAnywhere product?

- The Government takes a risk-based approach to assessing and adopting ICT enabled solutions within government.

- For systems that pose a high risk to the Government, such as Finance systems, a detailed technical risk assessment (TRA) is performed.

- An independent cyber security risk assessment was performed as part of the Government's move of its financial systems to the cloud.

- The *Tasmanian Government Cloud Policy* requires agencies to adopt a cloud-first, value-for-money and risk-based approach to the implementation of ICT services and solutions.

- The risk assessment considered GoAnywhere as one of the integration components for the broader financial system solution and made recommendations about control configurations to be implemented by agencies in order to secure its use. For obvious security reasons it would be inappropriate to release to details publicly of the controls in place to manage cyber risks.

Is the Government still using GoAnywhere? What has been done to reassure the public it should be continued to be used?

- Six Tasmanian Government agencies use the GoAnywhere software.

- The Government routinely shares information with third-party service providers to efficiently and effectively carry out its business. The involvement in third parties is commonly accepted practice world-wide for many digital applications.

- In the case of GoAnywhere MFT, its purpose has been to facilitate financial transactions with creditors and business partners.

- The GoAnywhere MFT service hosted by Fortra is a reputable security accredited service.

- Unfortunately, the GoAnywhere MFT software system was the victim of a zero-day software vulnerability – a security vulnerability caused by a software defect that was not known at the time it was exploited by cyber criminals, and before the vendor or the Government was able to react.

- In this case Fortra quickly introduced a patch to close the vulnerability.

- All software solutions include some risk of previously undetected security vulnerabilities being exploited by cyber criminals. Changing products is unlikely to reduce the risk in this instance.

- As well as strengthening its own software development processes, the vendor has also provided updated best practice security guidance containing controls which, in the highly unlikely event of a similar software bug being found, would better protect government data from being accessed illegally.

Further Issues - Only If Asked

If asked – What information (or categories of information) was disclosed?

- Data may include some, or all, of the following data:
    - names
    - addresses
    - school name
    - DECYP reference number (for identification of types of service – it is only for internal use)
    - child name
    - home room
    - year group
    - Business names
    - Learners Date of Birth (TasTAFE only)
    - Centrelink Reference Numbers (TasTAFE only)

If asked – Has the Government breached the Privacy Act?

- The Commonwealth Privacy Act does not place any obligations on the Tasmanian Government.

- The Tasmanian Government is subject to the Personal Information Protection Act.

- Unlike the Privacy Act (Part IIIC), the Personal Information Protection Act does not provide for notification of data breaches.

- The Government is continuing to monitor its compliance with obligations under the Personal Information Protection Principles, particularly regarding data security.

If asked – What was the purpose of the letter from Jenny Gale and the State Controller?

- I understand the purpose of the correspondence was to encourage more informed coverage of the incident, specifically information about the threat facing the Tasmanian community.

- The responsibility and decision-making for communications in this cyber security emergency sat with the Secretary of DPAC, as the head of the Response Management Authority, and the State Controller, due to the

activation of the Tasmanian Emergency Management Arrangements in response to the incident.

- The letter made an offer of briefings, and subsequently the Secretary of DPAC and other government officials undertook a series of face to face briefings to explain the possible consequences. These briefings were well received.

If asked – Will the Government consider compensation for individuals adversely affected by the data breach?

- The Government would look at any liability, harm or detriment arising from the data breach, on a case-by-case basis.

- Once aware, the Government moved quickly to remove the risk exposure for individuals perceived to be most vulnerable. These individuals were contacted directly, and additional resources were put in place to provide support.

If asked – what emergency management plans are in place for coordinating a cyber security incidents?

- The Tasmanian Government Cybersecurity Incident Management Arrangements (TCIMA) specify the arrangements for handling cyber security incidents across Government.

- The TCIMA is closely aligned with similar national Cybersecurity Incident Management Arrangements (CIMA) coordinated by the National Cyber Security Committee.

- The TCIMA describes various cyber security conditions and the associated incident management roles and responsibilities, set out incident management relationships and handovers and focus on the responsibilities for detecting, assessing, and responding to incidents.

- Tasmanian Government Cybersecurity Incident Management Operating Handbook provides details of the operational aspects of the Tasmanian Government Cybersecurity Incident Management Arrangements.

- The Tasmanian Cyber Security Policy also requires agencies to have prepared incident management and business continuity plans to facilitate response, recovery and restoring to business-as-usual conditions.

- Tasmanian Emergency Management Arrangements (TEMA) describes the governance and coordination arrangements, roles and responsibilities for emergency management in Tasmania and for cyber security incidents that escalate to emergency level consequence management conditions.

- DPAC Digital Strategy and Services is the assigned Response Management Authority (RMA) for managing and coordinating incidents that trigger thresholds for a cyber emergency response under the TEMA.

- A key learning from the GoAnywhere Compromise is that there needs to be a State Special Emergency Management Plan (SSEMP) for cyber security. This plan will outline the specific state arrangements to manage the risks posed by cyber security incidents. Digital Strategy and Services, as the RMA, have commenced the development of the SSEMP for cyber security.

Background

- On 25 March 2023 the Australian Cyber Security Centre contacted the Tasmanian Government Chief Information Officer regarding a third-party report that 'Cl0p' (Clop) had announced they had compromised 'tas.gov.au'.
- Cl0p is a well-known cyber-criminal organisation that has been active for several years and are known to publish the data of its victims.
- Cl0p reported to the media that it had successfully stolen data from more than 130 organisations globally since January 2023 by exploiting a vulnerability in a product called GoAnywhere Managed File Transfer (MFT). Subsequent media reports supported these claims as organisations that use the product disclosed that they had become victims of data breaches.
- In response to the announcement, the Tasmanian Government activated its cyber incident management arrangements, stood up an Incident Management Team (IMT) and investigated the suspected breach.
- The cyber incident investigation focussed on GoAnywhere MFT due to the claims made by Cl0p in the media. The Tasmanian Government has deployments of GoAnywhere MFT and was informed of the software vulnerability on 6 February 2023 and took the appropriate remediation actions, with all action being completed by 7 February.
- There are six agencies using GoAnywhere MFT to support information transfers for their finance systems. In response to a remediation request, agencies reported the following:
    - Department of Health (DoH) confirmed they had an on-premise instance of GoAnywhere which was patched on 7 February.
    - Treasury confirmed they had an on-premise instance of GoAnywhere which was patched on 7 February.
    - DPFEM confirmed they had an on-premise instance of GoAnywhere which was patched on 7 February.
    - DPAC confirmed they had an on-premise instance of GoAnywhere which was patched on 7 February.
    - Justice confirmed they had an on-premise instance of GoAnywhere which was patched on 7 February.
    - DECYP advised that they had a cloud-based instance of GoAnywhere which had been patched by the vendor by 7 February.
- All agencies using GoAnywhere MFT have been provided with the vendor "hardening" guide and are applying the recommendations within it.
- The Tasmanian Government, through DECYP, received advice on 11 March 2023 from the vendor (Fortra) that the DECYP GoAnywhere MFT cloud instance had unauthorised activity in it between 28 January and 31 January 2023 by an unauthorised party who had exploited a zero-day vulnerability. The Tasmanian Government Cyber Security team became aware of this on 27 March 2023 and focussed the investigation in this area.
- Fortra advised that they had addressed the vulnerability and provided indicators of observed malicious activity, however they advised that they had no evidence of data being stolen. This advice and indicators were provided to the Australian Cyber Security Centre (ACSC) for further analysis.
- On 5 April the State Emergency Management Committee (SEMC) was convened and briefed on the incident. DECYP proactively emailed 10,559 creditors advising them that

data may potentially be at risk. Schools were notified and provided the information to share with parents and carers.

- On 7 April approximately 16,000 DECYP invoices which were generated by a third-party provider were disclosed by the cyber-criminals. In response:
    - SEMC met and agreed to activate the Tasmanian Emergency Management Arrangements (TEMA) to level 2 whilst responding to the incident and managing consequences.
    - The Ministerial Emergency Management Committee met and were briefed on the incident.
    - A Public Information Unit (PIU) was stood up to manage communications.
    - The Tasmanian Emergency Information Service (TEIS) was activated to handle public calls for further information.
    - DECYP informed all people with a valid email address whose data was disclosed.
    - Harm minimisation measures were put in place for at-risk individuals. Justice and the TasPol Safe Families Coordination Unit (SFCU) reviewed data holdings to determine vulnerable or at-risk individuals. Some individuals were identified and triaged, with referrals made to the Family Violence Unit for further contact.
- The Tasmanian Government has been proactive in communications with potentially impacted individuals:
    - On 7 April DECYP sent 8,893 emails to parents, carers and businesses regarding data that had been leaked.
    - DECYP emailed all potential stakeholders from the last five years: 145,683 emails were sent to debtors, creditors and approximately 1,600 previous DECYP employees, outlining that their data may potentially be at risk.
    - Letters (surface mail) were sent to parents, carers, and businesses where email addresses were not available (approximately 2,500 letters) regarding data that was leaked.
    - An additional 40,195 letters were also sent where email failed to deliver and to those for whom DECYP did not have an email address registered from the 145,683 contacts.
    - All DECYP staff including The Office of the Education Registrar, Teachers Registration Board, The Office of Tasmanian Assessment, Standards and Certification, TasTAFE and the Commissioner for Children and Young People were also contacted.
    - A cohort of firearms licence holders who undertook training with TasTAFE were identified, however further investigations revealed that they are unlikely to be impacted and so no further action has been taken with this cohort.
- When the proactive consequence management activity was completed, the SEMC agreed to de-activate. The Tasmanian Government has engaged the following organisations in response to the compromise:
    - IDCare – to provide harm minimisation support and advice in addition to victim support services for affected individuals. The Tasmanian Government has set up an IDCare referral page and allocated a code (TAGV23) for individuals to use if required.
    - ID Support NSW - to work with Tasmanian Government to get email communications out in a timely manner. A capability has been set up to send on behalf of tasinfoservice@notifications.tas.gov.au for any future bulk mail-outs.
    - CyberCX – to investigate the extent of the compromise, review the security and configuration of the GoAnywhere MFT DECYP environment, and provide advice on media and consequences.

    - ACSC - for incident assistance, guidance and advice; and to provide cyber security threat intelligence and information sharing with other jurisdictions.

- In addition to the TEIS activation, DECYP stood up temporary call centres in Hobart, Launceston and Devonport to contact vulnerable people. The call centres worked closely with Tasmania Police's Safe at Home Coordination team to ensure all vulnerable people were notified. By 12 April, all vulnerable people had been notified and the dedicated DECYP contact centre was stood down.
- On 9 April, joint correspondence from the Secretary of DPAC and the State Controller was sent to all political parties and media editors, requesting a more united approach to media coverage in relation to the data breach.
- On 12 April 2023, briefings for the media and opposition parties were provided to address transparency concerns.
- The AFP have agreed to extend Operation Guardian's remit to include harm minimisation support for Tasmanians impacted by the data disclosed in this incident.
- The TEIS operators took 356 calls between 7 April and 21 April. TEIS was extended until 6pm on 28 April to manage any potential increase in enquiries with approximately 8,000 staff and school communities returning from holidays, and more than 40,000 letters reaching households and businesses.
- Since 25 March, the Tasmanian Government has experienced seven (7) Distributed Denial of Service (DDOS) attacks which have been effectively mitigated by the Government's cyber security defences. Given the distributed nature of the attack, it is not certain whether this activity is attributable to cl0p, however other victims of clop malicious activity have reported being subjected to DDOS attacks during the activity.

Correspondence to politicians and the media

- There was a very real risk that media attention would encourage other offenders or motivate the criminal actor to increase their efforts and put more data, and more Tasmanians, at risk. It is the role of the public sector to provide advice as it deems appropriate. It is then up to the judgement of those receiving the advice to decide whether to heed it or not.
- Verbal advice was received from Commonwealth security agencies and the Australian Federal Police (AFP) about how cyber criminals react to media coverage. Verbal advice through the telepresence room or through secure telephone call is regularly done with Commonwealth agencies. There are even matters that we are sometimes unable to talk to the Government about given the security classifications.
- Following the public notification of the data breach, there was a notable increase in distributed denial of service (DDOS) attacks against Tasmanian Government networks. Similarly, there was also an uplift in potentially malicious scanning and probing activity detected on some DECYP websites.

Tasmanian Government Cloud Policy

- The Tasmanian Government Cloud Policy requires agencies to consider a 'cloud-first' (hosted services) strategy for ICT solutions where it can establish value-for-money and appropriate risk management.

- The policy applies to all Tasmanian Government agencies, and it was developed to provide a consistent, risk-based approach to the Tasmanian Government's adoption of cloud services.
- The Tasmanian Government Cloud Policy endorses the Australian Government's principles-based approach for the adoption of cloud services –
    - Make risk-based decisions when applying cloud services
    - Design services for the cloud
    - Use as much cloud as possible
    - Avoid customisation and use services 'as they come'
    - Monitor the health and usage of services in real time
    - Take full advantage of cloud automation practices

Selection and use of the GoAnywhere MFT solution

- The Tasmanian Government takes a risk-based approach when adopting ICT enabled solutions and services.
- For systems that pose a high risk to the government, such as finance systems, a detailed technical risk assessment (TRA) is performed.
- An independent cyber security risk assessment was performed as part of the Tasmanian Government transition of its financial systems to the cloud.
- The risk assessment considered GoAnywhere MFT as one of the integration components to support operations post transition and made recommendations about control configurations to be implemented by agencies in order to secure its use.
- In a contemporary digital world, government needs to have some way of moving data between different systems and service providers.
- Managed file transfer (MFT) is a technology that provides for the secure transfer of data. One of the core functionalities of MFT is the ability to secure files in transit and at rest, and to provide reporting and auditing of file activity. MFT is differentiated from other approaches to file and data sharing by its focus on managing the secure transfer of large file sizes and volumes of data between third parties.
- Six agencies use the GoAnywhere MFT software, however only DECYP had transitioned its GoAnywhere MFT solution to the hosted cloud service provided by Fortra.
- All software solutions include the risk of experiencing a software bug or security vulnerability.
- Following the recent third-party compromise, the Department for Education Children and Young People (DECYP) are developing a new standard for third-party services, including the development of improved contract terms and conditions that can be used in conjunction with the Tasmanian Technology Contract Conditions (TTCC) used for ICT procurement.
- This standard will then be incorporated into a broader whole-of-government policies and standards for software, services and information security.
- DECYP is also obtaining advice as to whether they should continue to utilise the services of the existing (impacted) supplier.

- Again this advice will also inform the broader whole of government position relating to managed file transfer services.

Retention of personal information

- The Archives Act 1983 stipulates that Tasmanian government organisations must not dispose of records unless approved by the State Archivist.
- In addition to the Archives Act, the collection, maintenance, use and disclosure of personal information relating to individuals is regulated by the Personal Information Protection Act 2004.
- The Archives Act 1983 (Tasmania) designates responsibility to the State Archivist to determine the minimum period of time that State records and information are to be retained and via this process also identify the portion that will become State archives.
- This responsibility is actioned via the development and use of:
    - General retention and disposal schedules for records and information created via common administrative functions conducted by government organisations
    - Agency specific retention and disposal schedules for records and information created by government organisations in the process of conducting their core business functions
- Agencies use these tools to designate retention periods for their records and information. For education organisations some individual student records are classified as 'permanent', retained by the organisation and ultimately transferred to the Tasmanian Archives when business need ceases.
- Agencies classify types of information based on their core functions, but for education organisations student records would be classified as 'permanent', retained by the organisation and ultimately transferred to the Office of the State Archivist. In response to the Royal Commission into Institutional Responses to Child Sexual Abuse and the Commission of Inquiry the State Archivist has imposed a disposal freeze on student related records that may be of relevance.
- To support understanding of the requirements of the Archives Act, the State Archivist provides policies, standards and advice.
- In accordance with information and records management policies and standards set by the State Archivist, government organisations are encouraged to develop their own policies and procedures managing their records and information and to apply retention and disposal schedules that are relevant to them.
- In November 2022 Cabinet authorised the introduction of a Protective Security Policy Framework for the Tasmanian Government.
- The new Tasmanian Protective Security Policy Framework (TAS-PSPF) includes protocols to align information security and information classification with similar protocols used by other Australian governments.
- Under the TAS-PSPF Each agency is responsible for maintaining the confidentiality, integrity and availability of all official information and agencies are required to –

- adhere to whole-of-government protective security policies and procedures relating to the management of information security. This includes the policies, standards and advice provided by the State Archivist in relation to the retention (or otherwise) of state records and information.
- adopt the Australian Government Protective Security Policy Framework and related documentation for the classification, protective marking, transfer, handling and storage requirements of information (in any format) relative to its value, importance and sensitivity.
- ensure the security of technology and information assets to safeguard data, information and privacy, and to ensure continuous delivery of government business during all stages of the asset lifecycle.

- The Department of Premier and Cabinet (DPAC) is responsible for whole-of-government implementation of the TAS-PSPF.
- Implementation of the TAS-PSPF is funded in the 2023/2024 budget.
- DPAC is also responsible for ongoing monitoring and assurance of whole-of-government security maturity and reporting to Cabinet.
- The monitoring function will be facilitated via agencies' annual reporting, where collected data will inform review and evaluation.
- Following any review, deficiencies, trends and improvements will be identified and addressed where necessary, as often many security risks are shared/common across Tasmanian Government agencies. Annual reporting data will also be used to understand the rigour applied to each agency's risk assessment processes.

Potential future consequences:

- There have been no further data disclosures by the cyber criminals since 7 April 2023, however they are likely to disclose the remainder of the data that was stolen. It is unknown whether they will disclose the data in small tranches, nor whether they will disclose everything that was stolen in a single release - nor when this might happen.
- Any new data disclosure will require additional communications with affected individuals and where people are identified as vulnerable to potential harm, the Tasmanian Government will implement additional supports to minimise the risk.
- The investigations have provided the IMT with evidence that only financial data has been stolen, however it is possible that cyber-criminals may have accessed other information which has not been detected during the investigation.
- The Tasmanian Government developed consequence management plans (CMAP) as part of the incident management process, in line the processes set out in the Tasmanian Cybersecurity Incident Management Operating Handbook and the Tasmanian Emergency Management Arrangements (TEMA).
- The current CMAP outlines the key response actions for the reasonable worst-case scenario and the least worst-case scenario should additional data be disclosed. As part of the CMAP DECYP have finalised a detailed internal Data Drop Response Plan, Vulnerable Cohort Management Plan and Assessment Process underpinned by a risk assessment.

- Tasmanian Government information that is released onto the internet by the cyber-criminals is permanently disclosed. The Tasmanian government will be implementing long term strategies to support harm minimisation for people that are, and will be, impacted by the incident.

Attachments below

A. Schedule of key dates and activities
B. Tasmanian Emergency Management Arrangements – Public Information providers/Response Management Authority Responsibilities

Attachment A - Summary of key dates and activities

Key Dates	Summary of Key Activities and Actions
30 - 31 January 2023	• DECYP GoAnywhere MFT cloud instance compromised by cyber-criminal
1 February 2023	• DECYP were advised via email to check a GoAnywhere service portal for advice re a service update. • The advice from GoAnywhere indicated they were investigating potentially suspicious activity on the GoAnywhere MFT cloud instance, and while the investigation was underway, they would out of caution implement a temporary service outage for the GoAnywhere MFT cloud instance.
3 - 4 February 2023	• Malicious activity including data exfiltration occurs on a file transfer service for a third-party service provider which connects to DECYP GoAnywhere instance.
6 February 2023	• The Tasmanian Government was informed of a software vulnerability within the GoAnywhere MFT system and took the appropriate remediation actions, with all action being completed by 7 February.
11 March 2023	• DECYP received advice from the GoAnywhere MFT vendor Fortra that DECYP's managed GoAnywhere MFT cloud instance had been subject to unauthorised activity between 28 January and 31 January 2023, prior to any knowledge of the vulnerability (also referred to as exploitation of a zero-day vulnerability). • The advice from Fortra to DECYP was that they had little visibility at that time of any data being extracted as a result of the unauthorised activity.

Key Dates	Summary of Key Activities and Actions
25 March 2023	• Australian Cyber Security Centre contacted the Tasmanian Government (through DPAC) regarding claims from a cyber-criminal organisation that it had stolen data from the Tasmanian Government – the Cl0p group had posted on their website allegations that they had stolen data from 'tas.gov.au' • Tasmanian Government investigation into the allegation commenced covering state and local government organisations (tas.gov.au). • The criminal organisation in question had been linked to the exploitation of a vulnerability associated with the GoAnywhere MFT system. This fact guided the initial and subsequent investigations
27 March 2023	• DECYP advise Tasmanian Government Cyber Security team of an incident in their GoAnywhere instance. • Tasmanian Government CIO activates the Tasmanian Government Cyber Incident Management Arrangements (TCIMA) in response to the threat and advice. • Incident Management Team (IMT) was formed to coordinate and respond to the incident. • IDCare engaged to support Tasmanian Government with victim support
29 March 2023	• SEMC met (Deputy State Controller chaired the meeting) o Update provided by DSS to SEMC members to provide situational awareness and to refer members to the Cyber Security Policy. • Watching brief at this stage
31 March 2023	• The Minister for Science and Technology issued a media release to say that the Tasmanian Government was investigating a data breach of a third-party file transfer service
4 April 2023	• Extraordinary meeting of the Ministerial Emergency Management Committee held for a preliminary briefing on the incident. Deputy State Controller in attendance. • Public Information Unit (PIU) activated to manage communications for the incident

Key Dates	Summary of Key Activities and Actions
5 April 2023	• State Emergency Management Committee was briefed and a response plan approved. Emergency Management arrangement established at level 1. • TCIMA operating level escalated to level 3 • DECYP emailed 10,559 creditors. This was a proactive email outlining that data may potentially be at risk. • DECYP also emailed parents of students advising them of a potential data breach. • Communication was sent to all TSS staff by Head of State Service regarding the incident. Separately DECYP and TasTAFE staff received communication with agency specific content.
7 April 2023	• Cyber-criminal releases first tranche of stolen data. Approximately 16,000 PDF documents - principally invoices and letters including five (5) screenshots. • Tasmanian Government Cyber Incident Management arrangements and Emergency Management Arrangements escalated from level 1 to level 2. • SEMC met and agreed to activate the Tasmanian Emergency Management Arrangements (TEMA) to level 2. • The Ministerial Emergency Management Committee briefed on the incident. • Victims of data disclosure were directly notified - DECYP sent 8,893 emails regarding data that was leaked. These were to the parents, carers and businesses identified in the data that was disclosed. • Harm minimisation measures were put in place for at-risk individuals. Justice and the Tasmania Police Safe Families Coordination Unit (SFCU) reviewed data holdings to determine vulnerable or at-risk individuals. Some individuals were identified and triaged, with referrals made to the Family Violence Unit for further contact. • Public information hotline (TEIS) activated with 1800 567 567 to handle public calls for further information.

Key Dates	Summary of Key Activities and Actions

8 April 2023	• Web and social media content updated with information about the breach.
	• SEMC meeting
	  o State Controller advised that a Situation Report would be sent to Ministers at 1600 that afternoon.
	  o State Controller directed the IMT to prepare a one-page brief on the guidance provided on the Australian Cyber Security Centre (ACSC) site.
	• Secretary DPAC proposed to brief the Opposition about the situation.

9 April 2023	• Joint correspondence from the Secretary of DPAC and the State Controller was sent to all political parties and media editors, explaining the public information arrangements in relation to the data breach. • DECYP stand up contact centres and proactively attempt to contact at-risk families. • TCIMA operating level escalated to level 2.

10 April 2023	• DECYP emails potentially impacted stakeholders using IDSupport NSW services – 145,683 emails were sent to debtors, creditors and approximately 1,600 previous DECYP employees, notifying them that their data may be at risk.
	• DECYP contact centres stood down.
	• SEMC meeting
	  o Secretary DPAC advised that she had written to external stakeholders (media and opposition) requesting they adjust their public statements in accordance with the guidance provided by the ACSC.
	  o State Controller advised she would be briefing the political parties on 11 April.

11 April 2023	• Brief Greens • Brief Labor
12 April 2023	• SEMC meeting • Letters sent to the people without a known or valid email address. • Media briefing. • PLP briefing

Key Dates	Summary of Key Activities and Actions
14 April 2023	• SEMC meeting to de-escalate from level 2 to level 1 as per the Emergency Management Arrangements • Brief to Legislative Council members • State Controller wrote to Secretary DPAC (RMA) to advise of de-escalation and to request the development of a State Special Plan for Cyber and a review of the guidelines for Public Information
18 April 2023	• PIU is stood down. Responsibility for communications is managed by DPAC
19 April 2023	• Letters are sent to the remainder of potentially impacted people with incorrect, failed email attempts or unknown email addresses.
1 May 2023	• "Defend your Data" public cyber awareness campaign launched. • Public information hotline is transferred to DECYP for answering

2.4.3 Public information providers

Public information providers are organisations and individuals that are authorised to provide public information before, during and after emergencies, such as:

- Municipal Council mayor or another authorised local spokesperson
- Hazard Advisory Agency spokesperson
- Response Management Authority spokesperson
- State Operations or Control Centre
- State Controller
- Department of Premier and Cabinet whole-of-government Public Information Unit (PIU).

2.4.4 Response Management Authority responsibilities

Public information activities are managed by the Response Management Authority's communications section, operating in accordance with the Response Management Authority's incident management system. A Response Management Authority may request assistance from other agencies, including:

- additional staffing resources, deployed under the *Interoperability Arrangements for the Sharing of Skilled Resources in Tasmania* to work within the response management authority's incident management structure
- use of whole-of-government communications channels, such as the TasALERT website and social media channels or the Tasmanian Emergency Information Service (TEIS)
- activation of a whole-of-government Public Information Unit.

Ministerial Portfolio: Minister for Science and Technology

Output: 3.1

Our Digital Future and Government Digitalisation

Talking Points

- *Our Digital Future*, the Tasmanian Government's digital transformation strategy, articulates the Government's commitment to helping and inspiring our communities, businesses, industries, and government agencies to develop digital maturity.

- It establishes the Tasmanian Government's vision, priorities, principles, and objectives for digital transformation across three critical priority areas - community, economy and government.

- The Tasmanian State Service Review (the Review) also aligns closely with the priorities for digital government outlined in *Our Digital Future*.

- The Review noted that 'digitisation' and 'digitalisation' represents a core strategy that could help secure efficiencies in the delivery of government services and improve the experience of working in and with government.

- The Review recommended a three-tiered strategy for digital reform:

    - The central allocation of funding to incentivise the digitisation of manual process to bring existing services up to a standard that meets current community expectations (Recommendation 26).

    - The implementation of a functional leadership model across the key digital platforms that provide the foundation for digitalisation across the State Service (Recommendation 22).

    - To support whole-of-government coordination and governance of digitalisation, with a renewed mandate to drive whole of government consistency and improvements in the foundations of digitalisation (Recommendation 24).

- The Tasmanian Government will increase its commitment to digital transformation in 2023-24, with $78.6 million allocated for investments in ICT to support service delivery, up from $68.7 million in 2022-23.

- Through 2023-24, the Government will continue to progress strategic investments through the Digital Transformation Priority Expenditure Program,

the Digital Health Transformation Program and Project Unify with Department of Police, Fire and Emergency Management.

- Over the forward estimates the government has allocated $311 million for investment in ICT. This is in addition to ongoing operational expenditures for Agency ICT service delivery.

- New investments include –

    - $3.3 million to bolster Government cyber defences through the establishment of a new Cyber-Hubs initiative which will see the development of a new whole-of-government shared operating model for cyber security services. This will build on capabilities being developed as part of the current four-year $4.9 million program announced in 2020-21.

    - $150,000 to fund the development of a Tasmanian Government Digital Inclusion Strategy.

- The Government's approach to date has been to encourage the progressive integration of multiple government systems, while ensuring that government-held information and services continue to be secure.

- In line with *Our Digital Future* and the State Service Review, the Tasmanian Government is actively progressing the foundations to support the introduction of digital services that are easy to access, understand and use.

- Following the four-year $4.3 million commitment in the 2021-22 Budget, Service Tasmania is progressing with work to establish a digital services portal called 'myServiceTas' to provide Tasmanians with a secure and easy-to-use access point for government services, accessed through a single login (as per Review Recommendation 65).

- Digital transformation in Service Tasmania will support customers to have more choice in how they access government services, and progresses alignment of digital, in-person and over-the-phone service channels.

- As well as enabling community and economic benefits, digital transformation can also realise greater cost efficiencies and productivity benefits for government.

Further Talking Points – Only If Asked

If asked – What is the government doing to address digital inclusion and digital literacy issues?

- The Digital Community objectives and priorities in *Our Digital Future* outline the Tasmanian Government's action plan for digital inclusion.
- Improving digital inclusion and participation within Tasmania is a cross sector, multi-discipline, and broad geographical issue that affects a great number of Tasmanians.
- A number of government agencies, NGOs and private sector bodies are also providing focussed services and programs to further digital literacy and inclusion throughout Tasmania.
- The Premier's Economic and Social Recovery Advisory Council final report and the recent Tasmanian Audit Office report COVID-19 – Response to social impacts: mental health and digital inclusion highlights further work is required, including establishing a clear governance framework for cross-agency oversight and improvements to digital inclusion, developing Key Performance Indicators, engaging with local communities to address digital inclusion at a local level and expanding access to existing government facilities which provide digital capability.
- There is also potential benefit in identifying further data to best target investment, assistance in co-ordinating existing efforts, development of a whole-of-government future road map and a cohesive interface with NGOs and private sector providers.
- The 2023-24 Budget provides $150,000 to fund the development of a Tasmanian Government Digital Inclusion Strategy.
- In conjunction with government, community and industry stakeholders DPAC Digital Strategy and Services will coordinate the development of an agreed set of priorities for digital inclusion across government.
- This will establish a mechanism to work with the community and industry to create a sustainable and viable inclusion strategy, and to validate performance indicators that will allow the government to measure the value of specific initiatives.
- In 2023 the *Digital Ready for Daily Life* program will focus on helping vulnerable Tasmanians who seek digital assistance to take advantage of the every-day opportunities that technology provides. Following a successful pilot delivering digital assistance at three neighbourhood houses in the Northern Suburbs of Launceston, discussions with the Department *for* Education, Children and Young People to partner via their 26Ten Local literacy for work and life program, are

well progressed. This will provide the opportunity to include digital assistance and capacity building as part of the embedded community programs in four communities (Glenorchy, Clarence Plains, Launceston Northern Suburbs and the Huon Valley).

- The following key initiatives provide additional examples of programs that have been established in Tasmania to address digital inclusion and digital literacy:
    - Initiatives such as the Launceston City Deal are exploring how to engage the community on digital inclusion in alignment with a place-based approach.
    - Leveraging trusted community programs such as the 26Ten Build Your Business and Build Your Community programs have shown that combining digital literacy into existing outreach programs can be highly successful in overcoming trust and access barriers.
    - Libraries Tasmania continue to offer access to computers and computing basics courses and tutorials. The Digital Connections Grants program provides funding to many community-managed Online Access Centres around the state.
    - To reduce the digital divide for our learners, the Department *for* Education, Children and Young People is investing an additional $5 million to bolster the pool of devices in our public schools, ensuring families who are unable to provide this technology can continue to support their child learning at home.
    - The Government has also been working with telecommunications partners to provide improved access to digital infrastructure and mobile services in rural and regional Tasmania as part of the Commonwealth Regional Connectivity Program, successfully partnering with Telstra in rounds 1 and 2 to secure funding.
- The Tasmanian Government was also an active participant in the national cross-jurisdictional Digital Inclusion Working Group (DIWG), with the Department of State Growth leading one of three priority digital inclusion initiatives.
- The Tasmanian-led project gathered information on the range of government digital inclusion programs being delivered across the country. The initiative highlighted the breadth and scale of activities across jurisdictions and allowed jurisdictions to share relevant learnings in the scoping, implementation and evaluation of digital capacity building programs.
- NGOs and the broader private sector have an ongoing interest and participation in addressing the digital divide. Regional or State based co-ordination across NGO, private and the public sectors is on a best effort basis.

Background

Our Digital Future

- In June 2020, following extensive public consultation with industry, community groups and government stakeholders, the Tasmanian Government released its first strategy for digital transformation – *Our Digital Future*.

- *Our Digital Future* established the Tasmanian Government's vision, priorities, principles, and objectives for digital transformation across three critical priority areas - community, economy and government.

- Priorities:
    - Priority 1 - Our Digital Community – All Tasmanians should have an equal opportunity to interact with digital services and information in ways that are easy to use, convenient and readily available.
    - Priority 2 - Our Digital Economy – Tasmania's economy will be bolstered by the competitive advantage, productivity growth and prosperity enabled by knowledge-driven digital transformation.
    - Priority 3 - Our Digital Government – The Tasmanian community is best served by a progressive government that puts the contemporary needs and expectations of citizens first, transforming the way it works and the way services are delivered.

Investment for ICT to Support Service Delivery

Table 1. Movements in investment for ICT to support service delivery

	2019-20	2020-21	2021-22	2022-23	2023-24
Investment in ICT to Support Service Delivery	$21.9m	$15.3m	$36.7m	$68.7m	$78.6m
% of total infrastructure investment	3.0%	2.1%	4.4%	5.0%	6.0%

Note: investment excludes operational expenditures in ICT to support ongoing service delivery across government.

Table 2. Specific investments in ICT to support service delivery ($ millions)

Investment	Estimated Total	2023-24	2024-25	2025-26	2026-27	Over the Forward Estimates
Digital Transformation Priority Expenditure Program	N/A	25.0	25.0	25.0	25.0	100.0
Digital Health Transformation	475.0	40.0	40.0	40.0	60.0	180.0
Project Unify	46.1	12.9	9.1	9.1		31.1
Cyber Security *	2.7	0.6				0.6
Total	198.8	78.6	74.1	74.1	85.0	311.7

* The broader cyber security program is $4.9m over four years, only a portion of this initiative is capital for investment in ICT to support service delivery.

Data and Digital Governance

- Responding to recommendations in the Tasmanian State Service Review, the Tasmanian Government reviewed and restructured the digital services governance framework to streamline support for digitalisation across the Tasmanian State Service (Recommendations 24 and 25).

- In April 2022 a Data and Digital Subcommittee to the Secretaries Board was established with members from the Digital Services Advisory Group, made up of CIOs and IT Directors. Moving forward the committee will be expanded to include senior officers with data management accountabilities.

- The endorsed role for the Data and Digital Subcommittee is to:
    - oversee whole-of-government digital initiatives (including relevant State Service Review recommendations);
    - monitor progress and the delivery of significant government digital priorities (including *Our Digital Future*);
    - lead engagement and collaboration across government agencies to promote a user-focused, and 'one government' approach to the design and delivery of digital services; and
    - to facilitate the establishment of effective data governance and data sharing capabilities across government.

Whole-of-Government Data and Digital Work Program

- The Data and Digital Subcommittee is progressing an indicative work program comprising existing whole-of-government digital projects along with new opportunities that incorporate recommendations from the State Service Review and priority actions from *Our Digital Future*.

- The work program comprises five active work streams:
    - Digital Services – initiatives to progress digital services delivery across government.
    - Common Systems and Platforms – the consolidation of common digital systems and platforms used by government.
    - Data and Information Management – establishing a data and information management framework to provide governance and support for data sharing and essential information management practices.
    - Cyber Resilience and Risk – building capabilities to increase cyber security and resilience across government.
    - Digital Workforce – establishing pathways for attracting and retaining talent, and to develop the appropriate digital skills and competencies for government employees.

Service Tasmania digital transformation progress

- Service Tasmania is progressing work to establish a digital services portal called 'myServiceTas' to provide Tasmanians with a secure and easy-to-use access point for Government services.

- Tasmanian company Intuit Technologies was awarded the contract for initial development and build activity for stage 1 of myServiceTas, which has now commenced.

- On completion of stage 1 Tasmanians will be able to access key transport services and transactions such as management of driver licences, vehicle registrations, and updating an address.

- Current timelines anticipate a launch of myServiceTas in early 2024.

- In July 2022 Service Tasmania also launched its new website with a focus on making services easier to find.

- Between 31 March 2022 and 31 March 2023, the Service Tasmania website received 1.7 million unique page views, which is an increase from the 2021-22 figure of 1.2 million visits over the same period.

- Customer satisfaction has also significantly risen since the launch of the new website.

Digital inclusion issues and challenges

- Improving digital inclusion and participation within Tasmania is a cross-sector, multi-discipline, broad geographical issue that affects a great number of Tasmanians.

- The shift of digital services as a primary channel for critical services and information is accelerating due to increased efficiencies and a growing demand by digital natives to access services when and where they need it.

- This is leading to real world impacts as access to emergency information, basic services, education, connections to support networks and the broader economy is creating a two-speed community.

- There is a need for longitudinal data on the scale of the problem to best target investment, greater co-ordination of existing efforts and partnership arrangements to leverage existing successful community programs to include digital literacy and target areas with critical access barriers.

- A lack of situational awareness and a roadmap is a barrier to improved coordination of efforts across the public sector.

- The Australian Digital Inclusion Index (ADII) 2021 highlights the ongoing trend of services such as health and education shifting to part or whole online delivery, and how this is leading to higher risks of citizens being excluded. This results in lost opportunities and restricted options for work, education, citizenship and social connection.

- The 2021 Australian Digital Inclusion Index identified that COVID-19 caused a rapid digital transformation with many services and workplaces moving online. However, early data suggests the pandemic has not necessarily been a strong driver of digital inclusion and in some respects, appears to have reinforced the uneven distribution of digital participation by increasing online activity among people who were already more likely to be online, with the most pronounced effect being on those with children and in metropolitan areas.

- Areas of low digital inclusion are at risk of being left behind in the post-COVID economy. As services from health to education shift in whole or part to modes of automated, online delivery, the consequences of exclusion for these Australians are likely to translate into lost opportunities and restricted options for work, education, citizenship, and social connection.

- Tasmania scores the lowest on the 2021 Australian Digital Inclusion Index, though there have been some improvements from the previous year. With the exception of Hobart, all local government areas within the state score below the national average.

- From an OECD Survey undertaken in 2011-2012, the proportion of the Tasmanian population with sufficient problem-solving skills in technology-rich environments was the second lowest in Australia.

- The Tasmanian Government actively engages in national discussions and efforts to improve the access, affordability and capability of Tasmanians to engage with the digital economy and community.

Ministerial Portfolio: Minister for Science and Technology

Output: <output Number>

Whole of Government Cyber Security

Talking Points

- Cyber-attacks are increasing in frequency, scale, sophistication, and severity. Last year, the Tasmanian Government cyber security team responded to 210 incidents which is an increase of over 180% from the previous year.

- For security reasons, it is not appropriate to publicly discuss or disclose the details of any security incidents, however events ranged from responding to phishing incidents, the mitigation of denial-of-service attacks on government infrastructure and services, through to managing the local consequences of large-scale third-party data breaches.

- Notable incidents requiring a co-ordinated Tasmanian Government response included – the Optus, Medibank and Latitude Financial data breaches, and the recent GoAnywhere MFT compromise.

- The Tasmanian Government is committed to protecting critical systems and information from malicious cyber activity and supporting Tasmanians who have been impacted by cyber-attacks.

- The Tasmanian Government is increasing its investment in cyber security – building on the current four-year $4.9 million program announced in 2020-21 and recognising the elevated threat environment that we live in.

- The Tasmanian Government will commit a further $3.3 million to bolster our cyber defences through the establishment of a new Cyber-Hubs initiative which will see the development a new whole-of-government shared operating model for cyber security services.

- This initiative will be funded from the Digital Transformation Priority Expenditure Program within Finance-General (Treasury) and will leverage capabilities developed as part of the existing Government cyber security programs.

- This funding sits on top of the ongoing commitment of $988,000 per annum established with the whole-of-government cyber security to sustain services.

- On 2 May 2023 I launched the "Defend Your Data" campaign to help keep Tasmanians safe online. The campaign aims to raise awareness and give the public some simple steps to help protect themselves and keep safe online. Advertisements have run in major media outlets and will run in regional papers over coming weeks. Details can be found at www.defendyourdata.tas.gov.au

- Cyber security is a global issue of increasing concern, and that is why we have provided ongoing investment in capabilities and resources for cyber security.

- Additional government investment in cyber security will also create opportunities for local businesses to provide services that will assist agencies to tackle the increasing range of cyber threats.

Additional Talking Points by Subject

Cyber-Hubs Initiative

- The *Cyber Hubs* program aims to establish a sustainable operating model to manage cyber security risk across government.

- The program will implement a whole-of-government shared operating model for cyber security services, linked to the establishment of up to four cyber security hubs operated by lead agencies across government, with a central hub located in DPAC Digital Strategy and Services (DSS) division to coordinate whole-of-government services and to facilitate governance.

- This is a critical initiative and government priority which is identified in the Tasmanian Government digital transformation strategy (*Our Digital Future*) as part of the digital government priority and the objective for "securely-managed government information and technology systems, able to support efficient, joined-up public services".

- This initiative is also aligned with Tasmanian State Service Review recommendations, including the development and delivery of a platform-based functional leadership model for the integration of common business systems across Government (Recommendations 22 and 26).

- The following outcomes are expected to be realised from the proposed initiative:

    - Maximisation of existing and planned investments in cyber security, including outputs funded under the current Whole-of-Government Cyber

Security Program and for planned funding requested by agencies to address cyber security capability gaps.

- Increase flexibility with respect to resource deployment and the ability to prioritise baseline cyber security capability development in all agencies.
- Improvements in the options available for recruitment, development and retention of cyber security skills and resources.
- Better coordination and alignment of future budget requests for cyber security services and initiatives.
- Increased visibility of cyber security risk for agencies and across whole of government.

Existing Whole-of-Government Cyber Security Program

- In 2020-21, the Tasmanian Government increased funding for the Whole-of-Government Cyber Security Program to $4.9 million over four years.
- The Whole-of-Government Cyber Security Program has been designed to rapidly increase Tasmanian Government cyber security maturity in the context of the current threat landscape.
- The program has been focused on the following areas to reduce risk and provide value for money:
  - Building cyber security incident response capacity and capability by integrating it with national arrangements and rehearsing cyber security incident response plans to test that skills and resources can be deployed effectively.
  - Supporting Tasmanians who have been affected by identify theft by introducing a service, delivered through IDCARE, which provides advice on the steps that should be taken to minimise further risk of identify misuse.
  - Increasing cyber security awareness across government to ensure staff understand their role in reducing cyber security risks.
  - Implementing role-specific cyber security training that enables staff to recognise cyber security threats that are likely to occur in their day-to-day work and to respond appropriately.
  - Upskilling cyber security professionals across government with the latest techniques.

- Reducing the impact of malicious actors and aiding rapid remediation by detecting vulnerabilities in Tasmanian Government services at the earliest opportunity.
- Targeting investment to uplift whole-of-government cyber security maturity for the most effective cyber incident mitigation strategies to address the majority of cyber threats.

Incidents in 2022-2023

- Notable incidents that have required a response from the Tasmanian Government include – Optus, Medibank, Latitude Financial, and GoAnywhere.
- While some of these events are national events, work was required by our cyber team.

Further Issues - Only If Asked

If asked – Has there been significant under expenditure in the cyber security program?

- In 2020-21, the Tasmanian Government increased funding for the Whole-of-Government Cyber Security Program to $4.9 million over four years.
- This funding delivers programs and services that complement the work that agencies are doing. Each agency also has separate funding directed at cyber security uplift.
- An additional $688,000 has also been provided in on-going funding post June 2024, bringing the total on-going funding to $988,000, demonstrating a commitment to cyber security and ensuring the resilience of government services in the face of increasing cyber threats.
- To date, the program has spent $2.85million.
- Key achievements to date include –
  - Improved incident response capability through new support services for citizens and agencies, and new tools, processes and training for incident responders.
  - Improved knowledge and awareness of cyber security across the Tasmanian State Service through the delivery of targeted training.

- Improved access to cyber information through the centralised Tasmanian Government Cyber Website.
- Improved ability to protect publicly accessible websites and systems by identifying vulnerabilities.
- Development of an updated Tasmanian Government Cyber Strategy for 2024-2027 (currently in draft).

- In the early phases of the cyber program, there were delays in budget expenditure due to set-up timeframes for procurement, contract negotiations and staff recruitment challenges.
- The program has since accelerated, doubling expenditure and progress year on year, with a significantly smaller rollover expected to be carried forward into next year. This financial year has seen significant gains in progress due to contracts being in place with access specialist cyber skills.
- With respect to staff recruitment the current market for cyber talent has been very challenging, an issue acknowledged nationally and internationally with cyber skills in demand.

If asked – The Tasmanian government has the lowest cyber security expenditure of any state or territory, what is the Government doing to address that?

- The Tasmanian Government continues to provide ongoing investment in capabilities and resources for cyber security.
- In 2020-21, the Tasmanian Government increased funding for the Whole-of-Government Cyber Security Program to $4.9 million over four years.
- This funding included $688,000 to sustain central whole of government cyber security services on an on-going basis, bringing the total funding for central whole of government cyber security services to $988,000 per annum.
- In 2023-24 budget the Tasmanian Government is committing a further $3.3M to bolster our cyber defences with the Cyber Hubs Initiative.

If asked – What is the breakdown of incidents?

- The Tasmanian Government broadly categories its response into the following categories:
    - Addressing Tasmanian Government information leakage.
    - Investigating malicious activity;
    - Investigation of suspicious activity;
    - Rectifying security weaknesses; and
    - Minimising the harm from third-party cyber incidents and data breaches;
- All categories experienced an increase however the "Investigation of suspicious activity" and "addressing information leakage" almost doubled in volume.
- Two areas of response were added due to the increase in activity in those areas. These being "minimising the harm from 3rd party cyber incidents and data breaches" and "Rectifying security weaknesses.
- Whilst the volume of incident indicates an increase in activity, it does not reflect the amount or work effort required to respond to an incident. For example, the GoAnywhere compromise, whilst only representing only a single incident required an incident management team consisting of members from multiple agencies and has required many weeks to respond to.

Background

Cyber Security Incidents

- The Tasmanian Government Cyber Security team responded to 210 incidents in the past 12 months which is an increase of over 180% from the previous year. This includes the GoAnywhere compromise incident, state government agencies, statutory authorities and some local government organisations that have requested assistance.

- It is important to recognise that the GoAnywhere cyber compromise was the action of criminals and was not a compromise of Tasmanian Government systems.

Table 1 – Number of incidents requiring Tasmanian Government Cyber Security Team response.

	31 March 2021	31 March 2022	31 March 2023
Number of cyber security incidents	119	75	210

Table 2 – Breakdown of incident categories requiring Tasmanian Government Cyber Security Team response over the past year.

Category of Incident Response Activity	Percentage of the Total incidents
Addressing Tasmanian Government information leakage including stolen user credentials, passwords, accidental and malicious information disclosure (include the GoAnywhere Compromise)	59%
Investigating malicious activity such as phishing campaigns against government, installed malware instances, denial of service attacks against government, etc	10%
Investigation of suspicious and suspect activity including unusual network activity, threat hunting etc	19%
Rectifying security weaknesses such as remediating system vulnerabilities and system misconfigurations	5%
Minimising the harm to the Tasmanian Government and citizens from 3rd party cyber incidents and data breaches	7%

- For security reasons, it is not appropriate to publicly discuss or disclose the details of any security incidents. In the context of coordinating Tasmanian response to national incidents, the Tasmanian Government Cyber Security Incident Management Arrangements have been activated on several occasions in parallel with the national cyber security arrangements.

- The Tasmanian Government has cyber security incident management arrangements and all agencies are progressing the implementation of the incident response standard. These arrangements enable management of cyber incidents within a single agency and facilitate coordination across the Tasmanian Government if it impacts multiple agencies.

- Incident response management arrangements and operational procedures for whole of government incidents are regularly reviewed to capture the insights gained from each activation of arrangements. The expanded cyber security program in this budget includes "exercising" to further refine incident response arrangements and minimise the impact of cyber attacks.

- In the event of a cyber security incident, the Tasmanian Government has staff in agencies to respond which can be coordinated and augmented by the Tasmanian Government cyber security team. These resources can be further supplemented by the ACSC and/ or third party cyber security incident response experts if required.

Whole-of-Government Cyber Security Program

- Under the leadership of the Tasmanian Government Chief Information Officer (CIO), the Whole of Government Cyber Security Team currently has seven cyber security positions providing whole of government cyber security leadership, support, and advice to agencies.

- The Whole of Government Cyber Security Team also works with other Australian governments to support a nationally coherent and consistent approach to cyber security.

- The existing Whole-of-Government Cyber Security Program still has one more year of funding remaining on the capital investment component of the program.

- The 2020-21 Budget allocation of $4.9 million over four years for the Whole-of-Government Cyber Security Program significantly boosts the previous $300 000 per annum funding allocated to whole-of-government cyber security in 2018.

Table 2 - Program funding arrangements

	2020-21	2021-22	2022-23	2023-24	Total
	$'000	$'000	$'000	$'000	$'000
Whole-of-Government Cyber Security Program					
Capital Investment	179	1 038	888	605	2 710
Appropriation	200	628	688	688	2 204
Total	**379**	**1 666**	**1 576**	**1 293**	**4 919**

- An additional $688 000 per year was approved in the 2022-23 budget to supplement the previous $300 000 which was allocated in 2018. This brings the total annual funding to $988 000 per annum which supports the ongoing operation and support of services enabled during the four-year cyber security program.

- The additional funding enables a centralised uplift program to build cyber security capability across government that is composed of the following components:

- Vulnerability Management - aims to reduce the risk of public facing systems being compromised due to known vulnerabilities that can be exploited if not promptly rectified.

- Incident Response - integrate agency, whole-of-government and national arrangements to ensure incident response is effective and recovery costs minimised.

- Cyber maturity uplift for agencies - supporting agencies with targeted investment to improve overall cyber security baseline maturity across government.

- Cyber Security training and awareness - aims to provide cyber security training and awareness in three key areas – (i) creating baseline level awareness across the TSS so that all staff understand their security obligations, (ii) providing targeted training to build cyber security capability across the TSS, and (iii) providing targeted cyber security awareness for high-risk roles to reduce the impact of threats in the workplace.

- Allocation of the program budget expenditure over the program (four years) is summarised below:

Table 3 - Planned program expenditure by output across 4 years

Key Output	Budget $'000	Percentage of Total Budget
Vulnerability Management Initiative	900	18%
Incident Response Initiative	1 400	29%
Cyber Training and Awareness Initiative	1 100	22%
Agency Guidance Initiative	1 500	31%
Total Cyber Security	**4 900**	**100%**

Tasmanian Government Cyber Security Strategy

- In consultation with agencies, the Cyber Security Team has drafted a Cyber Security Strategy that details the vision and strategic priorities for Tasmanian Government cyber security over the next four years.

- The Strategy defines the guiding principles, and strategic priorities that are required to support the Tasmanian Government to safeguard citizen information and continue the digital transformation of service delivery.

- This Strategy is due to be tabled in Cabinet during August 2023.

Australia's Cyber Security Strategy 2023-2030

- Australia's Cyber Security Strategy 2020 (the Strategy) was released by the Australian Government Department of Home Affairs on 6 August 2020.

- The Australian Government are reviewing the Strategy and Home Affairs have released a discussion paper for stakeholder comment.

- An expert advisory board has also been established to assist and advise the Australian Government development of the new Cyber Security Strategy.

- Consultation is underway and feedback is being sought from States and Territories. The Tasmanian Government will be providing a submission in addition to feedback Tasmania has provided through the National Cyber Security Committee (NCSC) to Home Affairs.