Te Kāwanatanga o Aotearoa
New Zealand Government

Internal Affairs
Te Tari Taiwhenua

Lessons learnt

Transfer of the National Emergency Management Agency
November 2025

Purpose of this document

1. This document was created at the conclusion of the substantive work to transfer the National Emergency Management Agency (NEMA) into the Department of Internal Affairs (DIA) as a departmental agency. It provides an overview of the project, a summary of successes, the challenges, and actionable recommendations for future transfers.
2. The NEMA transfer project was significant, complex, and large in scope and scale, that was delivered on time, within budget, in a very short timeframe. Equally, it was a project marked by high pressure, with avoidable challenges.
3. The intention of this report is to help improve efficiency with future transfers, prevent repetition of mistakes, and ensure positive lessons are integrated into standard practices.

Process for capturing the lessons learnt

4. The lessons learnt consolidates feedback from several sources. The feedback reflects the views of:
    a. Project governors and leadership
    b. Project participants
    c. DIA internal workstream leads and business groups
    d. Information technology and information management external vendors, and
    e. NEMA staff.
5. The insights were captured from workshops with project governors and participants facilitated by David Miller of Fore Consulting, through workshops with resources who played a critical role in the transfer, individual conversations with project participants, and a survey distributed to NEMA staff following the transfer.
6. The information gathered showed common themes, and forms the observations, themes, and recommendations in the lessons learnt.

Project Overview

This section provides the background to the decisions that brought the transfer into effect, the project objectives, timeline, budget, and governance structure.

Formal decisions to bring the transfer into effect

7. NEMA resided within DPMC as a business unit from 2014 until 2019 when it formally became operationally independent as a departmental agency, with DPMC responsible for providing its corporate functions. In turn, DPMC's corporate support is provided by Central Agencies' Shared Services (CASS), a unit within The Treasury. This means four agencies (DIA, NEMA. DPMC, and CASS) needed to be involved in any discussions relating to the transfer of NEMA to DIA.

8. In April 2025, Cabinet agreed in principle to the transfer, citing alignment of DPMC's work to support the Prime Minister, and relevance to DIA's work that intersect strategically and operationally with the emergency management sector, namely local government, community development, and Fire and Emergency legislation. Additionally, it was noted DIA has experience hosting agencies and inquiries. [CAB-25-MIN-0108]
9. On 28 June 2025, a cohort of Ministers[1] agreed to the transfer of resources and appropriation from DPMC to DIA to bring the transfer into effect. The Order in Council was published in the *Gazette* on 31 July 2025, marking the point at which the transfer was officially publicly known [DPMC-2024/25-988]. The transfer took effect as intended on 25 September 2025.

Objectives of the project

10. The direction from Cabinet provided clarity on the objective: to transfer NEMA as a departmental agency from DPMC to DIA. Additionally, the project was clear that the operational transfer requires the cooperation of four agencies:
    - DIA, as the host agency, requires its internal systems and processes to be set up to accept NEMA, and requires the information and data to be readily available and shared from the current host agency DPMC, and CASS.
    - NEMA, as the departmental agency, requires all host agency critical services to be operational on or before 25 September, so that it can receive DIA's services from 25 September, and the transfer to DIA is not disruptive to staff or operations.
    - DPMC and CASS are required to share all information with DIA that is relevant to the transfer to ensure they can fully remove NEMA as a departmental agency on 25 September 2025, or arrangements are in place between DIA and DPMC or CASS if full removal on that date is not possible.

Leadership of the transfer project was in two stages

Stage 1: led by DPMC

11. As the outgoing host agency, DPMC led the first stage of the transfer project covering the period requiring ministerial and Cabinet decisions to confirm the transfer. The initial intention was the leadership of this stage of the project would shift to DIA upon Ministers agreeing to the transfer of resourcing and appropriation on 28 June 2025.
12. The governance of the project reflected the focus at the time. Stage 1 under DPMC's leadership ensured the necessary decisions and information were provided to Ministers to make timely key decisions. Likely transfer workstreams and broad deliverables were identified.

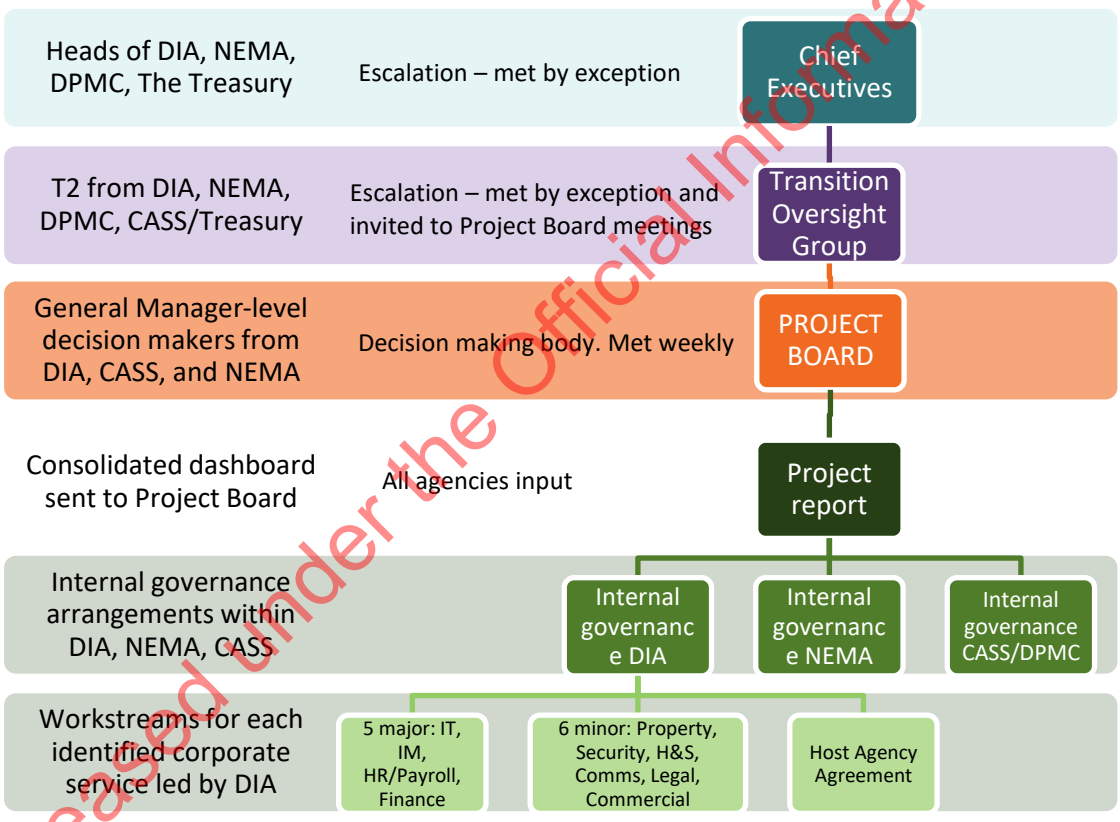
Stage 2: led by DIA

13. DPMC continued to lead the project after 28 June, to mitigate concerns that the transfer might be publicly discussed with staff and vendors ahead of the Order in Council being

[1] The Ministerial portfolios tasked with reaching agreement were: the Prime Minister, Minister of Finance, Minister for Public Service, Minister of Emergency Management and Recovery, Minister of Internal Affairs

published. Therefore, DIA effectively only took over leadership of the transfer on 31 July 2025.

14. In anticipation of assuming project leadership, DIA established cross-agency governance, confirmed project workstreams to implement the necessary transfer elements, and engaged with key vendors in information technology and information management to confirm availability to assist with the transfer.
15. Project Managers were assigned to the larger workstreams (such as Finance, Information Technology and Information Management). Workstream leads and decision makers were confirmed, and a project reporting structure put in place.
16. Governance arrangements recognised the short timeframe to implementation, and the multiple, cross-agency workstreams feeding into the process. Terms of reference defined the governance arrangements, described the roles and accountabilities of governance members, and ensured the Project Board members and attendees understood and accepted their assigned roles and accountabilities.
17. A visualisation of the project governance and arrangements is provided below.



Budget

18. Agencies determined their own internal transfer budgets through the best-known information at the time. For DIA, this was guided by previous experience of actual costs required to establish independent functions such as departmental agencies or inquiries, and a clear corporate cost structure. It was not informed by detailed discovery of the specific costs and resources to transfer NEMA out of DPMC/CASS into DIA.
19. The Cabinet and Ministerial decisions noted the expectation the transfer would be fiscally neutral. Agencies funded the transfer through underspend and carry over.

What went well

The transfer took place on the prescribed date

20. Agencies successfully completed a significant level of work to transfer people, data, and information from DPMC/CASS to DIA in a short space of time (discovery to implementation was around 10 weeks). Participants prioritised their time and resources to achieve the deadline and developed pragmatic approaches where different delivery timeframes were needed (such as aligning to accounting cycles or implementing more complex aspects of the transfer).
21. In this short space of time, contracts were novated or put in place, people were paid on time and correctly, recruitment for additional roles was completed or well underway, and relationship contacts were confirmed. Devices were set up and tested, the schedule of induction and training activities was put in place and well socialised, and NEMA staff were able to operate within a new and very different environment relatively easily and quickly. In the space of around two weeks, it was possible to transition most queries and issues away from dedicated support to BAU activities.

Objectives were clear

22. All participants were clear that the objective was to transfer NEMA to DIA as a departmental agency, and what that entailed for each agency. The transfer objectives, rationale, and key dates were communicated well and often. People were aware of the transfer and understood that the transfer date was fixed.

Project governance, reporting and resourcing were responsive and informative

DPMC and DIA established a clear governance framework and project reporting template that could be readily shared within organisations and easily communicated to Chief Executives. Governance members were accessible and available at short notice.

In stage 2, the governance structure empowered decision makers to progress issues at a Project Board level, rather than depending on the time and energy of deputy secretaries to approve the decisions being taken. Participation at project meetings was prioritised by agencies.

23. Agencies assigned very senior staff to positions of project leadership and engagement, with high levels of experience guiding the decisions. The senior primary points of contacts were well known, visible, and readily contactable.

The transfer was a positive experience for NEMA staff

24. Feedback on the transfer experience for NEMA was gathered through a formal survey to all NEMA staff and anecdotal comments captured by project managers and business partners.
25. The overwhelming feedback from NEMA staff is the transfer was well communicated, the products and services are of a high standard, and the project was delivered by DIA in a very tight timeframe with minimal disruption to NEMA's core business (including the

agility to pause tasks to enable NEMA to respond to the severe weather events in late October).

26. DIA was able to clearly articulate how it approaches its role as the host agency, its corporate service offering, and develop pragmatic approaches to assist NEMA with the change. The feedback noted commitment and goodwill between DIA and NEMA, with high levels of collaboration in person and through shared online tools. The experience was enhanced by DIA resources co-locating with NEMA at key points of the transition, to resolve technical issues and establish ongoing relationships. Change management messages were developed together, ensuring the communications were accurate, well-paced, and framed in a way that would resonate for NEMA staff.

What were the challenges

Project leadership shifted too late to the incoming host agency

27. The focus for DPMC in leading stage 1 of the transfer project, and for DIA leading stage 2, was markedly different, reflecting the different perspectives of the work the agencies were required to do to complete the transfer. Consequently, when DIA took over the project leadership, very little of the detailed discovery had been undertaken, requirements were not gathered and a clear scope had not been documented or agreed.

28. This left insufficient time to determine the best transfer approach. It also took substantial time to be granted access to the DPMC/CASS technical environment so scoping was not as detailed as would be desirable. This created assumptions and misunderstandings, with grey areas determined by the transferring agency or outgoing host agency as being 'in scope' but deemed 'out of scope' by DIA and vendors. It meant there was insufficient time to validate assumptions made about the scope, such as actions that should have been included but were not identified or were missed until after go-live. Until the detailed discovery was undertaken, DIA only had a high-level and inadequate understanding of what the transfer might entail.

29. Exacerbating the late shift of project leadership were strained relationships at times between agencies. The agency with the project leadership was able to direct and lead how the project progressed, with any delays directed at the incoming host agency for moving away from "lift and shift".

30. DIA had the ultimate responsibility for the project outcomes and receiving the transferring agency. It is not reasonable to expect the incoming host agency (and in this case, noting the size and scale of DIA) to change its corporate service structure and offering to match the outgoing host agency. DIA needed to be in a stronger position from the outset to direct, dictate, and lead the project culture, project messaging, discovery of the systems and processes in DPMC/CASS, and set expectations of agencies and vendors.

31. The known key Cabinet milestones are all milestones within a single project that could be managed within one project leadership from the outset, recognising ownership of the Cabinet and Ministerial papers sits with the outgoing agency. If it is not possible to have one agency with single project leadership, the latest the incoming agency should take over the project leadership is as soon as Cabinet has provided its agreement (in this case, the 7 April Cabinet decision).

Governance membership was inadequate in parts

32. The membership of governance groups reflected the input from agencies at the time, notably in the absence of detailed discovery. A breakdown of the membership positions is provided below.

Transition Oversight Group: tier 2 from DIA, NEMA, DPMC, CASS/Treasury

- DIA (Chair): Deputy Secretary Enterprise Services
- NEMA: Deputy Chief Executive Strategic Enablement
- CASS/Treasury: Chief Financial Officer
- DPMC: Deputy Chief Executive Corporate and Chief People Officer

Project Board: tier 3 general manager level decision makers from DIA, NEMA, DPMC, CASS/Treasury

- DIA
  - (Chair) Machinery of Government Lead
  - Chief Financial Officer
  - Chief Information Officer (delegated)
  - Director Branch Performance Enterprise Services
- NEMA: Manager Business Performance
- CASS/Treasury: Chief Financial Officer

The phrase "lift and shift" created assumptions and barriers

34. From the beginning, the transfer was framed as a "lift and shift of NEMA". This gave rise to assumptions that the transferring departmental agency would see no difference in its devices, systems and processes. DPMC and CASS assumed their role in transfer activities would be light touch and require little effort to move information to the DIA environment.

35. The term "lift and shift" created an assumption that all agencies have the same systems and processes regardless of size and breadth, or that the incoming host agency would adapt to replicate the outgoing host agency's offering. It meant that any conversation suggesting different systems and processes were deemed out of scope.

36. The reality was substantially different to "lift and shift". DIA's corporate offerings and technical environment are not the same as DPMC/CASS's. Significant work was required by all agencies to accurately and securely transfer material between different technology platforms, and agencies had different tools and technical environments, ways of using these, and different corporate expectations.

37. DIA subsequently needed to invest considerable time finding ways to move or replicate information that did not mirror DIA's approach but did not negatively impact on DIA's internal operations. Outgoing host agencies were unprepared for the level of work required to transfer NEMA's data out of their agencies and were slow to provide data necessary for a transfer, had not checked data for accuracy, prevented access to trusted vendors to assist with the work, and were critical of DIA for creating more work on limited resources.

38. Terminology such as "lift and shift" downplays the complexity of a transfer and the work required to bring a transfer into effect. It is also incorrect from the experience of the transferring departmental agency as it creates an assumption that the departmental agency will experience no change in their systems and processes with the new host agency.

39. As the project progressed, major issues arose relating to information technology and information management transfer matters. The membership of the governance groups meant decisions on escalated issues were being made by non-technical members who did not fully understand the outgoing agency's technical environment. Thus, the lens applied was risk avoidance and to push back matters as being outside a "lift and shift".

40. With the benefit of hindsight, the governance structure needed to include information technology decision makers from CASS for the outgoing host agency. Potentially, the membership of the outgoing and incoming host agencies needed to be mirrored.

Although agencies noted the strategic priority of the transfer, internal prioritisation was inconsistent

41. At a strategic level, all participating agencies recognised the priority of the transfer and had captured it as such in internal and external business plans.

42. However, the scale of the transfer was not consistently communicated within agencies, tended to sit with a single business group, and was expected to be achieved as part of substantive role activities. Consequently, agencies' internal business groups either were exceedingly busy and actively involved or conversely did not recognise the transfer as a high priority and were not involved or came in quite late.

43. This put pressure on agencies as people needed to be released from other work, or the necessary transfer work could not be achieved faster. As an example, for the incoming host agency, internal business groups with expertise in professional project management were aware of the transfer, but were not able to see how the transfer was of greater priority than other priorities. Professional project resources were therefore not allocated early enough in preparation of the lead agency shift.

The transfer date was not informed by an implementation plan

44. The transfer date of 25 September 2025 was determined early in the process as optimal for alignment with payroll cycles, with an underlying assumption that the transfer would be relatively straight forward as a "lift and shift".

45. However, the date was determined in the absence of the necessary discovery into the work required to transfer information and data between quite different systems and processes and develop the necessary degree of change management support.

46. Without the discovery phase, the work required for all agencies to do the substantive transfer was unknown and proved to be much more involved than anticipated. For CASS as the outgoing host agency, it has necessitated short term and costly contract extensions and ongoing allocation of resources to support NEMA beyond the anticipated end-date. For DIA, resources to support the ongoing work has resulted in additional internal costs, created substantial unanticipated work, and put existing resources under additional pressure.

47. As a result, while it was possible to transfer most of the corporate functions on 25 September 2025, the project needed to create additional stages to align with different business cycles (such as financial month-end) and to transfer more complex components (such as information management and the National Crisis Management Centre).

The post-transfer technology support and project structure was underestimated

48. The formal project structure formally closed shortly after the substantial project elements had successfully transferred after 25 September 2025. In the lead up to the transfer, and a few weeks following, dedicated information technology support was available for NEMA staff. However, from DIA's perspective, once the initial issues diminished to routine matters (such as password resets) retaining a dedicated team was no longer an optimal allocation of resources. A decision was made to move to BAU, where NEMA raise issues through standard internal processes, and could escalate matters through their Business Partners and the Relationship Manager.

49. It became apparent in the lead up to an emergency activation that some aspects of the transfer had not been adequately completed by the vendor, meaning NEMA staff were unable to access the emergency environment in the bunker through their DIA devices.

50. Additionally, recognising some aspects of the transfer occurred after 25 September, it may have offered assurance to NEMA to continue a project reporting cycle and governance structure (even if by exception only) until all stages of the transfer were agreed as completed.

51. It has already been described that the discovery phase made it known that the scale of the information technology and information management changes for NEMA were beyond a "lift and shift", and that the restricted timeframe made a fulsome discovery impossible. The constrained timeframe also meant it was not possible to run scenario testing, particularly in an emergency environment. With these known factors, dedicated information technology support and residual transfer reporting needed to remain in place for longer.

The transfer budget was not informed by true costs

52. Agencies set their own transfer budgets based on best known information when the original estimations were undertaken in February 2024. Agencies funded the transfer budget through baseline savings and carry over. Therefore, while sound consideration was given to likely costs, it was not informed by detailed discovery and the impact of a constrained timeframe on resourcing.

53. While most agencies were able to fund and absorb additional costs through baseline, the budgets did not fully capture the scale of the work that was clearer after discovery work was undertaken. This is partly reflected in the need at one stage for agencies to provide a joint contribution towards an outgoing agency's unanticipated transfer costs.

54. The constrained timeframe also meant the true costs did not reflect the additional internal resources that contributed additional hours for many weeks to the project.

55. A transfer budget informed by detailed discovery, including the resources that reflect delivery timeframes, would provide a more accurate picture of true costs, and potentially avert the need for agencies to seek support to cover unanticipated shortfalls. While the respective agencies' transfer budgets appear to have operated within budget, it is likely the actual costs are under-represented.

Lessons to apply for future transfers

56. These insights should be considered at the outset for future transfers of this nature, within the context and risks of a future transfer. The lessons learnt provided below are not in order of importance or priority.

Lessons learnt for Machinery of Government transfers
Lesson learnt 1: single project leadership Project leadership must sit with the incoming host agency from the outset.
Lesson learnt 2: agile governance membership Regularly review governance structures and membership to reflect and mirror the key organisational decision makers relevant to the project at that time from outgoing and incoming host agencies, with members of sufficient seniority to facilitate early resolution as issues arise.
Lesson learnt 3: language reflects the change in systems and processes The language that describes the transfer should be clear that the transferring departmental agency will experience a change in systems and processes (and desist from using the term "lift and shift").
Lesson learnt 4: agencies signal the priority internally and resource accordingly Agencies must ensure consistent internal understanding of the priority and allocate suitable resources well in advance to prepare for the transfer.
Lessons learnt 5: detailed discovery informs transfer date Complete detailed discovery of the transfer requirements, ideally before determining the transfer date.
Lesson learnt 6: agencies operate with clear objectives Ensure the objectives of the transfer are clear and well communicated, including the detailed scope of what is required to be transferred and details of the end-services to be provided by the incoming host agency.
Lessons learnt 7: budget is informed by detailed discovery Develop or revise transfer budgets for the incoming and outgoing host agencies after detailed discovery has completed and build in the timeframe for delivery.

Document 2

Priority Routine

Internal Affairs
Te Tari Taiwhenua

Internal Affairs briefing

Hon Brooke van Velden
Minister of Internal Affairs

Title: **Digital identity system and privacy protections**

Date: 16 December 2025

Key issues
Your portfolio responsibilities include legislation that governs the primary identity records of New Zealanders and enables the provision of key digital identity services including the RealMe Identity Verification Service and the Confirmation Service. Your work sits alongside the Minister for Digitising Government's responsibilities for the broader digital identity system. These responsibilities include work on an all of government app and wallet, which could be used to securely store digital credentials issued by government agencies (including DIA) or the private sector. The Digital Identity Services Trust Framework Act 2023 (DISTF Act) sits within the Digitising Government portfolio. The DISTF Act is the foundational legislative framework to digital identity and regulates the opt-in accreditation and provision of secure and trusted digital identity services for transactions between individuals and organisations in the public and private sector. Modern digital identity credentials, that could be used under the DISTF system, are designed to be privacy protecting. 9(2)(h) [redacted] 9(2)(f)(iv) [redacted]

Action sought	Timeframe
Consider the contents of this briefing, and if you wish to **discuss** with officials in early 2026 **Forward** this briefing to the Minister for Digitising Government	At your convenience

Contact for telephone discussions (if required)

Name	Position	Contact Number	Suggested 1st contact
9(2)(a) [redacted]	General Manager, Policy	9(2)(a) [redacted]	✓
Kelsea Whyte	Policy Manager	9(2)(a) [redacted]	

Return electronic document to:	Josh Ward, Joshua.Ward@dia.govt.nz
Hukatai reference	6KWWFJMNQWZ4-1227312906-6015
Ministerial database reference	IA202510608

Purpose

1. This briefing provides you with information on your role in the digital identity system and how modern digital identity credentials issued by the Department of Internal Affairs could fit within the broader digital identity system that the Minister for Digitising Government administers.

Executive summary

2. You have portfolio responsibilities for legislation that governs the primary identity records of New Zealanders and enables the provision of key identity services including RealMe Identity Verification Service and the Confirmation Service. The Minister for Digitising Government is responsible for the broader digital identity system which is regulated by the Digital Identity Services Trust Framework Act 2023 (DISTF Act).

3. At the agency level, the Government Chief Digital Officer (GCDO) also sits within the Department and is responsible for all-of-government provision of digital identity infrastructure. This role is part of the Digitising Government portfolio.

4. The Digital Identity Services Trust Framework (Trust Framework) provides a regulatory system where public and private organisations can apply to be accredited as a trusted digital identity service provider. An accredited provider must have strong privacy practices in place.

5. The Department holds core identity information which could be valuable as modern digital identity credentials, created and used within the Trust Framework system. These types of credentials are designed to be privacy-protecting. 9(2)(h) [redacted]

6. 9(2)(f)(iv) [redacted]

You are responsible for the legislation governing primary identity records

7. As Minister of Internal Affairs, you are responsible for a suite of legislation that governs New Zealanders' primary identity records. The key pieces of legislation are:

Title	Primary function of legislation
Births, Deaths, Marriages, and Relationships Registration Act 2021 (BDMRR Act)	Provides for the notification, registration, and verification of life events. There is a separate Marriage Act 1955 under the Justice portfolio that covers process and restrictions on marriage.
Citizenship Act 1977 (Citizenship Act)	Sets out eligibility and types of New Zealand citizenship.
Citizenship (Western Samoa) Act 1982	Sets out eligibility and New Zealand citizenship status for citizens of Samoa.
Passports Act 1992 (Passports Act)	Sets out provisions around issuing passports and other travel documents.
Electronic Identity Verification Act 2012 (EIV Act)	Enables an electronic, verified identity (RealMe verified identity) to be used with specified participating organisations. This is a secure way for people to prove who they are online when dealing with government and approved private sector services, reducing the need to turn up in person and the time it takes to process a person's application.

Identity Information Confirmation Act 2012 (IIC Act)	Allows approved organisations to electronically check certain identity information against the Department's records. This helps to reduce fraud and the time it takes to process a person's application.

8. The registers maintained by the Department contain valuable identity information and are the authoritative source of many New Zealanders' name, date of birth and citizenship status. The legislation in your portfolio sets out how and what information is collected and recorded, and how identity information is shared and/or accessed.

9. Information on the Department's registers can already be accessed by other government agencies and non-government organisations in specific circumstances under an Approved Information Sharing Agreement (AISA).[1] Information can also be shared using physical certificates, like birth certificates, although these often contain more information than is necessary to access most services. The registers are administered by the Registrar-General of Births, Deaths and Marriages, who is appointed under the BDMRR Act.

10. Based on the legislation in your portfolio, and the information that the Department holds, the Department provides the following key identity services:

    10.1 **RealMe Identity Verification Service** – a secure way for people to prove who they are online when dealing with government and approved private sector services, reducing the need to turn up in person and the time it takes to process a person's application;

    10.2 **RealMe login service** – a single username and password that lets people log into multiple government services, reducing the need to remember multiple credentials;

    10.3 **Confirmation service** – a secure way for organisations to check whether a person's details are accurate, reducing fraud and the time it takes to process a person's application; and

    10.4 **Identity Check** – a secure way for people to use traditional identity documents (passports and driver licences) to prove who they are online without having to get a digital identity through RealMe.

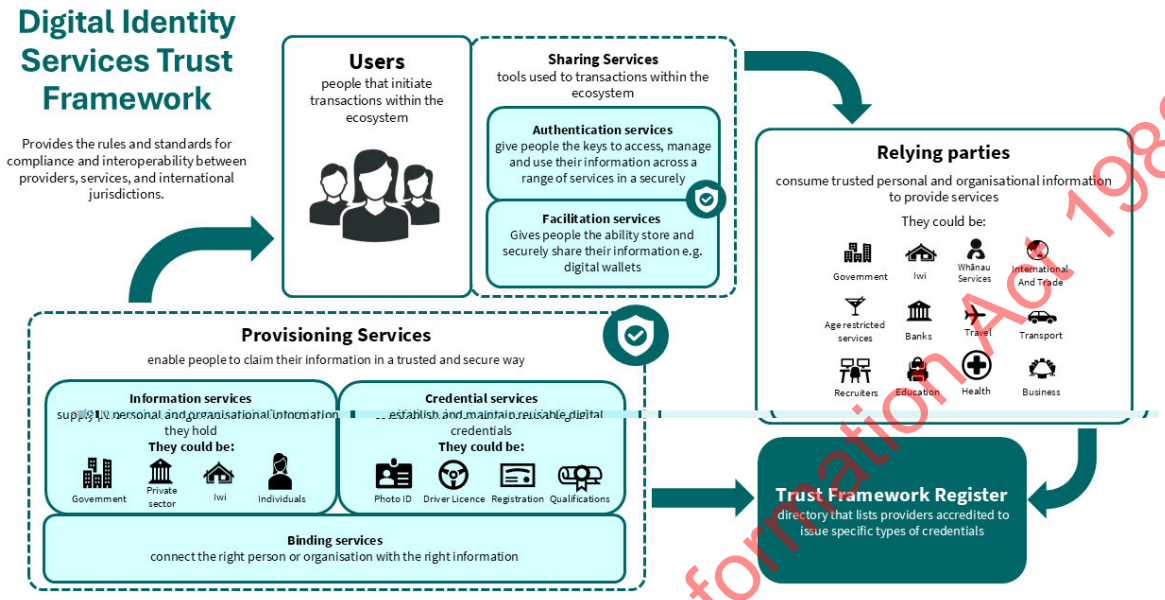
The Minister for Digitising Government is responsible for the broader digital identity system

11. The Minister for Digitising Government is responsible for the broader digital identity system which is regulated by the Digital Identity Services Trust Framework Act 2023 (DISTF Act). The DISTF Act regulates the opt-in accreditation and provision of secure and trusted digital identity services for transactions between individuals and organisations in the public or private sector. The use of the Trust Framework will not be compulsory for individuals or organisations. Government agencies issuing credentials will be required to seek accreditation if they are using the Trust Framework infrastructure.

[1] For example, there is an AISA which allows death information to be shared to a range of Government agencies, organisations and other groups such as registered charities to make it easier for organisations to get access to correct, reliable death information so they can improve the services they provide.

12. These digital credentials have the potential to be used in online, in-person and offline contexts. This legislation sits within the Digitising Government portfolio and is administered by the Department. Diagram A shows the DISTF system.

Diagram A – the DISTF system



13. To become accredited as a provider (services depicted in light blue in Diagram A), an organisation must meet a set of rules to demonstrate that they should be trusted. The rules set the requirements for providers and services becoming accredited. They cover requirements for:

    13.1 Identification management - determining the accuracy of information, binding that information to the correct individual or organisation, and enabling the secure reuse of the information;

    13.2 Privacy and confidentiality - ensuring the privacy and confidentiality of the information of individuals or organisations is maintained;

    13.3 Security and risk - ensuring information is secure and protected from unauthorised modification, use, or loss;

    13.4 Information and data management - for record keeping and format of personal and organisational information, to ensure a common understanding of what is shared; and

    13.5 Sharing and facilitation - facilitating the sharing of information with relying parties including authorisation processes.

14. The DISTF Act makes these rules legally binding for organisations that are accredited. This means that users and relying parties can trust that an accredited organisation issuing a digital credential has confirmed the correct information is contained on the credential and that the credential is being issued to the person to whom the information belongs. They can also trust that an accredited provider of a wallet has sufficient security and data management policies in place to keep the credential secure.

The Government Chief Digital Officer is responsible for digital leadership across agencies

15. At the agency level, the Government Chief Digital Officer (GCDO) also sits within the Department and is responsible for all-of-government provision of digital identity infrastructure. One of the functions of the GCDO is to ensure government agencies can make and issue digital credentials in a safe and secure manner that also avoids agencies duplicating ICT systems. This work sits within the Digitising Government portfolio.

16. Work of the GCDO includes the procurement of infrastructure to support the public and private sector digital identity ecosystem and includes:

    16.1 **Govt.nz app and built-in digital wallet:** On 9 December 2025, the Government released its Govt.nz app. Functionality planned for early next year will include a built-in digital wallet that will allow New Zealanders to hold and use accredited digital credentials on their own smartphone.

    An encrypted digital wallet is a secure way of storing digital credentials: The Govt.nz wallet is similar to digital wallets already in the market, for example, those produced by Apple and Android, but ensures that credentials produced by the New Zealand Government will always be able to be accommodated. The wallet uses encryption technology to securely store and display digital credentials. 9(2)(f)(iv) [redacted]

    16.2 **NZ Verify app**: the NZ Verify app allows anyone to verify a digital credential. For instance, a bartender needing to verify a patron's digital Kiwi Access Card or a police officer needing to verify a driver's digital driver licence.

    16.3 **Digital Credential Issuance Platform**: the digital credential issuance platform allows any government agency to issue credentials while reducing costs across the public sector and ensuring all agencies meet the same high standards for privacy and security.

17. Government agencies are at varying stages of digital transformation for the services they provide to customers but generally want to get more services provided online. The GCDO is working with several public and private sector organisations to deliver services using the all-of-government infrastructure in early 2026.

Modern digital identity credentials are designed with privacy at the forefront

Digital credentials provide greater security than physical identity products

18. Digital credentials are a way for people to prove their identity and share information about themselves. They are an electronic version of one or more pieces of information about a person. Digital identity credentials can be more privacy enhancing than physical identity products for the following reasons:

    18.1 they are securely stored and encrypted on a user's device compared to a plastic or paper physical credential that can be held and viewed by anyone in its possession;

18.2 they are only accessible using a strong authenticator like Face or Touch ID, it is not enough to just be in possession of the credential;

18.3 unlike a physical credential, if the digital credential is lost, it is inaccessible and unusable because of the two protections above. In addition, an issuer can revoke a credential, or a user can remotely disable or wipe their device, in near real time;

18.4 users only need to share the relevant information on a credential rather than all the information. For instance, rather than sharing your entire physical driver licence (with name, address, date of birth, driver licence number) a user can simply share their photo and that they are over 18 to purchase an age restricted product;

18.5 physical credentials can be more easily tampered with, altered or forged. A digital credential (with a well secured private key) is practically impossible to forge; and

18.6 a photocopy or scan of a physical document can be reused without the holder ever knowing. Digital credentials prevent this because the credential itself is never transferred. Instead, the wallet generates a one-time presentation that cannot be reused in another context.

Digital identity credentials are created with built-in privacy features

19. When a credential is issued, it is signed with the issuer's **private key**.[2] This creates a **cryptographic signature**[3] that cannot be forged. Anyone can then use the matching **public key**[4] to check that the credential is genuine and has not been changed.

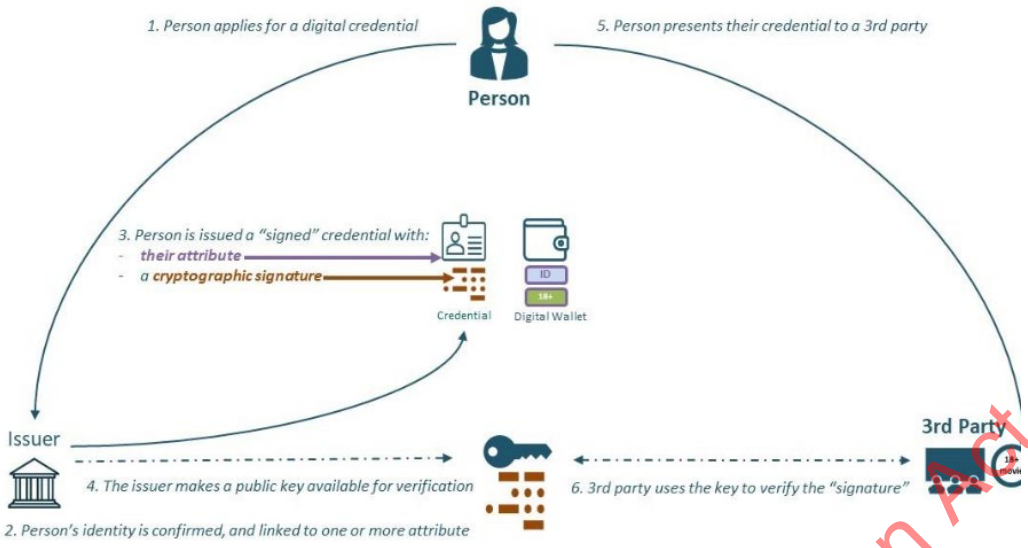
20. These public and private keys come as a pair generated by an algorithm and work together to protect data. This is the same way the chip in a New Zealand passport works. A high-level depiction of how a verifiable digital credential works is shown in **Diagram B**.

[2] *Private key* – A code uniquely associated with the owner and not made public. The private key is used to compute a digital signature that may be verified using the corresponding public key.

[3] *Cryptographic signature* - A de-identified piece of code, generated through the use of mathematical techniques, that is used by a third party to test the integrity and authenticity of a verifiable credential and the data contained within it.

[4] *Public key* - A cryptographic key that is used to confirm a verifiable digital credential really came from the issuer, and that it has not been changed since it was issued.

Diagram B – how a verifiable digital credential works



Digital credentials are stored securely on a user's device

21. Digital credentials are held in the secure chip on a user's device and therefore is in their sole control. Digital credentials stored securely on a person's own device will require authentication like face or touch ID by the credential holder to use. Authentication happens via the device, not an app account.

22. Only the rightful user can view and present credentials within a digital wallet. If the device is lost or stolen, no one else can access the digital wallet without the credential holder's biometrics.

Using digital credentials ensures greater privacy controls

23. Credentials can be used in person or online and can be used device-to-device without internet connectivity. The user must authorise every transaction or presentation of a credential, including what information is presented (for instance, only showing that someone is over 18 rather than all the information on their driver licence). There is no ability for a third party to access a user's data without their explicit consent at the time of presentation.

24. The presentation of a credential, once approved by the user, is only between the user's digital wallet and the third party. This presentation is end-to-end encrypted meaning only the intended recipient can see the presented information.

25. The issuer and wallet provider have no ability to view a user's credentials. Only the user can view or present the credential. This means no new central database is created, nothing is stored in the cloud, and therefore security is greatly improved. For example, if a rental car company was verifying a digital driver licence, or a police officer needed to see a person's licence, they would use their device to verify the credential on the user's phone.

26. This ensures individuals remain in control of what information they choose to share, and when. If a device is lost, the credentials would need to be reissued by the issuing agency, just as with a lost physical document.

27. The issuer of the credential (for instance, a government agency) is not aware of when a user presents their credential, again enabling the privacy-preserving elements.

However, that issuer can suspend or revoke credentials at any time. An example of how a digital credential could be used is provided at **Appendix A**.

9(2)(h)

9(2)(f)(iv)

[5]See IA20256958 - New digital identity legislation objectives and policy approach

9(2)(f)(iv)

Next steps

34. Officials are available to discuss this briefing with you and answer any further questions you might have. We are also able to demonstrate the digital identity technology, including the wallet and use of demonstration credentials should you find this useful.

Recommendations

35. We recommend that you:

a)	**consider** the contents of this briefing; and **agree** to discuss this briefing with officials at your convenience	**Agree / Disagree**
b)	**forward** this briefing to the Minister for Digitising Government	**Agree / Disagree**

9(2)(a)

Hon Brooke van Velden
Minister of Internal Affairs
_____/_____/_____

Appendix A: Opening a bank account with a digital credential

9(2)(f)(iv)

Document 2a

Proving your identity to open a bank account

Scenario: Helen owns a small architecture studio in Lake Hāwea, near Wanaka. She likes technology and appreciates being able to work online. Helen wants to open a new Kiwiana Bank account, to get a better interest rate for a fixed term deposit. **Helen must prove her identity to Kiwiana Bank to open her new account[1].**

Potential future state - Using a digital credential		Current state - Using physical documents	
	Helen downloads an accredited digital wallet on her smartphone. This is because she knows it will meet standards for privacy, security and operability. Helen protects her digital wallet using the existing Touch or Face ID authenticator she already uses on her phone. Her digital wallet provider cannot access her wallet nor see the wallet's contents. This step takes her approximately **5 minutes**.		Helen visits the website of Kiwiana Bank. She prints out an application form to open a bank account. Her printer is out of cyan coloured ink, even though she's only printing in black and white! She has to change the cartridge. She then prints and completes the form. She fills in her **name, date of birth, street address** and **phone number.** Helen provides them an **email address**. She **signs** the form**.** This step takes her approximately **15 minutes**.
	Through the digital wallet app, Helen applies to DIA for a digital identity credential. This is because she knows it is trusted and seen as authoritative. She can use it can prove her identity to Kiwiana Bank and to government and other organisations in the future. She only needs to do this once. Helen shares her **name**, **date of birth**, **place of birth** and a selfie **photograph** with DIA, along with an **email address** and **phone number** for contact purposes. She also provides her **passport number**. This is so DIA can match Helen and her information against her passport records. With a match confirmed, DIA creates her **digital identity credential** and issues it into her wallet. This step takes her approximately **15 minutes**.		The bank account application form lists the documents Helen needs to prove her identity. It will not accept her passport as it has expired. She chooses her **full New Zealand birth certificate** and **driver licence** instead. Helen has to hunt out her birth certificate, she cannot remember where it is. It takes some time. This step takes her approximately **30 minutes**.
	Helen visits the website of Kiwiana Bank. On its application page, she completes her bank account application form online. The application form asks for her **name, date of birth, street address** and **phone number**, along with an **email address,** and presents a QR code asking for these via a digital wallet. This step takes her approximately **5 minutes**.		Helen spends an hour on hold, to book an appointment at Kiwiana Bank to prove her identity and open her account. The bank does not provide an option for her to book her appointment online. This step takes her approximately **60 minutes**.
	Helen uses her wallet to scan the QR code, and it informs her that Kiwiana Bank is requesting some specific attributes from her DIA credential. The request includes a link to the bank's privacy policy. She quickly reads about how they will manage her information. This step takes her approximately **5 minutes**.		Helen drives to the bank for her appointment. The closest Kiwiana Bank branch is in Wanaka. It is about 15 km away. It takes her about 20 minute to drive each way, and it is only open three days a week. She has to find parking when she arrives. This step takes approximately **60 minutes**.
	In her digital wallet, Helen's consents to sharing the requested details, and her wallet asks her to authenticate with her Touch or Face ID before sending her credentials to Kiwiana Bank. Only a representation of the requested attributes from her **digital identity credentia**l is sent to the bank. Kiwiana Bank receives a representation of the information from Helen's **digital identity credential** and uses it to create her new account. It keeps **a record that a digital identity check was undertaken** but does not need to scan and store any hard copy documents from Helen. This step takes her just **a few seconds**.		Helen gives her **application form** to the Customer Service Officer (CSO) opening her new bank account. She also provides her **birth certificate** and **driver licence** which are scanned and uploaded on to the bank's database. The appointment takes about 45 minutes as the CSO has to type all Helen's details into the database. Helen's **birth certificate** has the following information: • **Her name** • **Her name at birth** • **Her sex** • **Her date of birth** • **Her place of birth** • **An indication of if she was a citizen at birth** • **Any name changes she has had** • **Her mum's name** • **Her mum's name at birth** • **Her mum's occupation** • **Her mum's age** • **Her mum's place of birth** • **Her dad's name** • **Her dad's name at birth** • **Her dad's occupation** • **Her dad's age** • **Her dad's place of birth** Helen's **driver licence** has the following information: • **Her name** • **Her date of birth** • **Her driver licence number** • **Her drive licence restrictions** • **Her organ donor status** • **Her address** • **Her signature** This step takes her approximately **45 minutes**.
	To download a new wallet, create a new digital identity, and open a bank account and **prove her identity online** has taken Helen less than **30 minutes** in a single session. Now that she has the wallet and credential on her phone, it will be even faster next time she needs to prove her identity. The bank has only collected, used and stored the identity information about Helen that it needs to, to open and operate her account. **The online process has saved Helen about 3 hours.**		To open a bank account and **prove her identity in person** has taken Helen approximately **210 minutes** spread across several days. The bank has collected, used and stored a wide range of identity information about Helen, along with identity information about her **parents**.

[1] Please note, this example is illustrative only. It is designed to compare the process and identity information involved in an online process verses and process using hard copy identity documents. Kiwiana Bank is not a real bank.

Document 3

Priority **Routine**

Internal Affairs
Te Tari Taiwhenua

Internal Affairs briefing

Hon Brooke van Velden
Minister of Internal Affairs

Title: **Supplementary advice to the Governance and Administration Committee on the Regulatory Systems Amendment Bill**

Date: 16 January 2026

Key issues
We seek your approval to provide the attached supplementary advice to the Governance and Administration Committee (the Committee) on the Regulatory Systems (Internal Affairs) Amendment Bill (the Bill). The supplementary advice responds to the Committee's request for further information about timeframe issues for passing the amendments to the Fire and Emergency New Zealand Act 2017, including issues associated with passing the Bill after 1 April 2026. This request followed submissions from the Insurance Council of New Zealand and IAG New Zealand to the Committee that advised it was critical that the Bill be passed before 1 April 2026. We advise that passing the Bill by 1 July 2026 is important to avoid requiring late implementation changes for the insurance sector. We also advise that passing the Bill by 1 April 2026 would provide legal certainty for issuing insurance renewals and might reduce administrative costs. The Government has not prioritised the Bill for Q1, so it will not be passed by 1 April. We recognise this advice surfaces the issues that may occur. For context, the advice notes that if the Bill is passed shortly after 1 April, the scale of risk would be relatively small. We seek your approval to provide this advice by 23 January 2026, so that it can be considered at the Committee's next meeting on 28 January 2026.

Action sought	Decision
We recommend that you **approve** the attached supplementary advice to be sent to the Governance and Administration Committee.	**Yes** / **No**

Name	Position	Contact Number	Suggested 1st contact
Louise Cooney	Policy Manager	9(2)(a)	✓
9(2)(a)	General Manager	9(2)(a)	

Return electronic document to:	9(2)(a)
Hukatai reference	PKR5P44QH4K4-787772508-1682
Ministerial database reference	IA202610762

9(2)(a)

Hon Brooke van Velden
Minister of Internal Affairs

_____/_____/_____

Internal Affairs
Te Tari Taiwhenua

Regulatory Systems (Internal Affairs) Amendment Bill

Supplementary information to the Governance and Administration Committee

23 January 2026

Request for further information

1. On 10 December 2025, the Governance and Administration Committee (the Committee) requested further advice on the issues related to timeframes for the new Fire and Emergency insurance levy raised by the Insurance Council of New Zealand (ICNZ) and IAG New Zealand (IAG) in their submissions to the Committee.
2. The Department of Internal Affairs' (the Department) response, set out below, can be read in conjunction with previous advice provided to the Committee on the amendments being made to the Fire and Emergency New Zealand Act 2017 (the FENZ Act). See paragraphs 328 – 337 of the departmental report for that advice.

Passing the Bill by 1 July 2026 is important for supporting the implementation of the Fire and Emergency levy

3. The redesigned Fire and Emergency insurance levy will come into effect on 1 July 2026. The insurance sector has been working since December 2024 to make changes to their systems necessary to implement the redesigned levy. This includes incorporating the levy regulations made in December 2024, along with the amendments to the FENZ Act proposed in the Regulatory Systems (Internal Affairs) Amendment Bill (the Bill).
4. Passing the FENZ Act amendments before July 2026 will support the effective and efficient implementation of the levy. If the FENZ Act amendments are not passed before 1 July, then it would require insurers and insurance intermediaries to reverse or change some of the work undertaken on implementation since late 2024. This would create unnecessary costs, and late system changes may not be completed before the new levy comes into effect.
5. Paragraphs 334-337 of the departmental report describe the intended issues that the Bill is intending to resolve (broadening the definition of residential property, ensuring commercial personal property is leviable, and addressing transitional arrangements for insurance contracts that undergo a variation). The benefits of these amendments – to reduce administrative costs, to better align the legislation with insurance sector systems and to ensure Fire and Emergency's funding needs are met – would also not be achieved until the legislation is passed.

Passing the Bill by 1 April 2026, or close to this date, will support more consistent practice and reduce the risk of administrative costs

6. In their submissions to the Committee, ICNZ and IAG advised that the Bill needed to pass by 1 April 2026, to provide a legal basis for levy payments that are stated on insurance renewals issued approximately three months before the contract period begins.
7. The Department acknowledges that some challenges arise if the Bill is not passed by 1 April 2026, particularly for some insurance intermediaries. They will need to decide whether to:
    a. issue renewals based on the current provisions of the FENZ Act and risk these provisions being changed before the contract begins, leading to a need to correct payments later and potential penalties; or

b. issue renewals based on the anticipated changes to the FENZ Act, taking on the risk of those changes not coming into place before July 2026 and operating under an unclear legal basis.

8. On balance, the Department considers it likely that most insurance intermediaries will opt to incorporate the anticipated changes to the FENZ Act in their insurance renewals. Their systems will have been updated with those changes incorporated. ICNZ notes in paragraph 28 of its submission:

> "…there would also be no ability for insurers to change their approach at this time (i.e. April 2026) as system changes will have long been locked in by that point."

9. However, there are over 100 insurance intermediaries in the New Zealand market, and we are not certain that all of them will be subject to the same system constraints. Some intermediaries might opt to issue renewals on the basis of the current provisions of the FENZ Act. In particular, some intermediaries may choose to not apply the levy to commercial personal property in their renewals to reduce premiums for customers. There would be transaction costs from correcting these payments later and a risk of penalties being applied under the FENZ Act to the insurance intermediaries for underpayments of levy.
10. The closer the Bill is passed to 1 April, the smaller the risk of inconsistent insurance renewal practices. If passage occurs later, a growing number of renewals will be issued without the new provisions, and intermediaries may become increasingly uncertain about the legislation's timing as 1 July 2026 approaches.

The risks associated with passing the Bill after 1 April 2026 are mainly associated with insurance contracts that include commercial personal property

11. Levy payments for residential and mixed-use properties should generally be the same under the current legislation as under the proposed amendments in this Bill. The risk of penalties being applied to insurance intermediaries is therefore low in relation to levy payments for residential or mixed-use property. The Department also notes that the earliest insurance renewals, issued three months before the contract period, are typically issued for commercial insurance contracts, rather than for residential insurance.
12. The Department considers that the greatest risk of inconsistent practice would be in issuing renewals that include commercial personal property. This risk may be partially mitigated as some insurance intermediaries may still interpret the existing provisions as requiring the collection of levy on commercial personal property, despite the ambiguity in the drafting of the FENZ Act.

Summary

13. Passing the FENZ Act amendments before the new levy comes into effect would support the smooth implementation of the levy, as the work undertaken by the insurance sector to change its systems has incorporated the changes proposed in the Bill. Passing the FENZ Act amendments before 1 July 2026 would also secure the revenue from levying commercial personal property.
14. Passing the FENZ Act amendments before 1 April 2026, or as close to that date as possible, would provide certainty for the insurance sector that they have a robust legal basis for issuing early insurance renewals and would reduce the risk of inconsistent practice in issuing insurance renewals. This would reduce potential administrative costs that could arise from having to correct levy payments at a later date. The further out from 1 April that the FENZ Act amendments pass, the greater the risk that inconsistent practice will occur.

Document 4
Priority **Routine**

Internal Affairs
Te Tari Taiwhenua

Internal Affairs briefing

Hon Brooke van Velden
Minister of Internal Affairs

Title: **Deployment of AI at DIA**
Date: 22 January 2026

Key issues
The Department has established a framework for the safe and responsible adoption and use of AI. The Department's AI policy is consistent with all-of-government guidance. The policy includes the requirement for human oversight of AI use and how staff should manage information when using enterprise AI tools. Any AI initiatives developed by the Department will undergo the same risk, privacy and security processes as any other technology implementation. The Department has established an AI programme team, with the purpose of building AI capability across DIA and accelerating the safe, effective adoption of AI. The Department sees potential benefits in AI. Most initiatives so far are producing productivity gains rather than direct savings. This appears to be consistent with the feedback we are receiving from other organisations and countries.

Action sought	Timeframe
Agree to discuss this briefing with officials	29 January 2026

Contact for telephone discussions (if required)

Name	Position	Contact Number	Suggested 1st contact
Murray Davey	Chief Digital Officer	9(2)(a)	✓
Myles Ward	Deputy Secretary Digital Services	9(2)(a)	

Return electronic document to:	Murray Davey, murray.davey@dia.govt.nz
Hukatai reference	2DX73NE7NTN2-2141378227-2431
Ministerial database reference	IA202610832

Purpose

1. This briefing outlines the approach that the Department of Internal Affairs (the Department) has taken to safely adopting and using Artificial Intelligence (AI), and the early AI opportunities the Department is exploring.

Background

2. On 1 December 2025, we briefly discussed with you the Department's deployment of AI. You requested a further discussion on this topic. This briefing provides background information for that discussion on 29 January 2026.

3. Cabinet is encouraging the uptake of AI in the Public Service, recognising that it provides significant opportunities for Government service delivery as well as improving productivity, driving efficiency, and delivering better value for money.[1]

4. The Government Chief Digital Officer's (GCDO) AI Work Programme aims to accelerate the uptake of AI through the Public Service by modelling best practice in safe and responsible AI use. This includes releasing the Public Service AI Framework and Responsible AI Guidance for the Public Service.

5. The GCDO AI Work programme has recently been refreshed to 2027, with the forward work programme focused on leading work on Common Use Tools, Safe and Responsible AI, Customer and Partnerships, and AI Workforce. The Minister for Digitising Government sent you and other Ministers a letter about the refreshed work programme on 18 December 2025.

6. Most government departments are adopting AI. The Department is leveraging AI resources and forums established by the GCDO and sharing information with other Departments to enable learning and reuse across the Public Sector.

The Department has established a framework to safely adopt and use AI

7. The Department's approach to the adoption of AI started with establishing a framework for the safe and responsible use of AI and a programme to coordinate this work across the Department.

This framework aligns with all-of-government guidance…

8. The Department has published an AI policy which is aligned to the GCDO AI Guidance and the Public Service AI Framework. The policy is principle based and sets out how AI should be adopted and used within the Department. This includes the requirement for human oversight of AI use and how staff should manage information when using enterprise AI tools.

…establishes clear roles and responsibilities…

9. Clear roles and responsibilities for AI have been established. The Department's Chief Digital Officer has been designated as the senior responsible official for AI and will oversee the Department's overall adoption of AI. Responsibility for implementation and use of specific AI solutions sits with Deputy Secretaries and business owners using existing business and governance processes.

10. An AI Enablement Group has been established. It brings together business leaders with privacy, security and digital expertise to provide advice, guidance and recommendations on AI initiatives to business groups. It will help build the Department's maturity in the use of AI and enable the Department to adapt our advice to business groups quickly as the AI landscape evolves.

[1] As noted in ECO-24-MIN-0119 and CAB-25-MIN-0216.

11. An AI Community of Practice (CoP) has been formed. This group is open to all staff, fostering knowledge sharing and continuous learning. The CoP follows a Share – Connect – Learn model and has good participation across the department, with over 100 attendees at its monthly meetings and a range of internal and external speakers presenting.

…and embeds existing risk and security processes.

12. The Department's existing policies, risk, privacy, security and governance processes all still apply to the use of AI. This means that any AI initiatives will undergo the same risk, privacy and security processes as any other technology implementation.

13. In addition to this, the Department is currently developing an AI Risk Management Framework. This integrates specific AI considerations into the existing processes, to provide a structured and repeatable approach to identifying and managing AI related risks across the organisation.

The Department is taking a deliberate approach to our adoption of AI

14. The Department has established an AI programme team, with the purpose of building AI capability across the organisation and accelerating the safe, effective adoption of AI. The AI programme team's deliverables include:

    14.1 Identifying and prioritising potential AI initiatives across the department.

    14.2 Delivering selected initiatives with a focus on value and reuse.

    14.3 Delivering an education programme for staff on how to learn, use and get business value from AI tools.

    14.4 Developing guidance to support the Department and business groups in the adoption and use of AI.

15. The AI Programme has a maturing pipeline of over 50 initiatives. These range in size and stage of development from exploratory ideas to early pilots already operating in small groups.

16. The Department is taking an iterative, learning approach. Most AI initiatives that are already operating are only being used by small groups of people and are internal to the Department. This reflects that we are still early in the adoption cycle and enables us to learn from these. We expect that as we develop some of the initiatives in the pipeline that these will be made available to larger groups across Te Tari.

17. Currently the only enterprise-wide AI tool is Microsoft Copilot Chat, which exists within our existing secure Microsoft Cloud environment. Staff have been instructed not to use this with sensitive documents or personal information while we learn and get familiar with using AI tools.

18. To date the Programme has focused on providing education on the use of Microsoft Copilot Chat to staff as they all have access to this tool and it enables them to get familiar with using AI. The next area of focus will be to deliver education sessions for leaders to enable them to start thinking about where they could use AI to deliver their services.

Potential benefits include productivity gains and improved services

19. There is general enthusiasm for the adoption of AI across the organisation. As awareness and comfort with the tools are growing, staff are identifying new opportunities to explore.

20. Most initiatives so far are producing productivity gains rather than direct savings. This appears to be consistent with the feedback we are receiving from other organisations and countries. This suggests direct savings from AI may not be achieved in the short term and may only materialise when our use of AI and the capabilities in the market mature over the next few years. This would be consistent with the adoption of previous technologies (such as the Internet and Smart Phones).

21. Our trials and business group engagement to date highlight several areas where AI can improve services and internal operations:

    21.1 Productivity and workflow support: summarisation, drafting assistance, knowledge search, and guided processes that reduce manual workload

    21.2 Service improvement: better navigation of complex information, smoother customer interactions, more consistent responses, and reduced processing times

    21.3 Regulatory and compliance functions: pattern analysis, risk identification, thematic review of high-volume information

    21.4 Training and workforce capability: onboarding support, reducing training pressure on experienced staff.

22. Early pilots, such as call summarisation in the Contact Centre, are showing productivity gains and helping staff build familiarity and trust in new tools. The Department is also leveraging experience from other agencies, in this case we were able to learn from ACC, MBIE and Inland Revenue who were already adopting AI for the same purpose.

23. The Department sees potential benefits in AI and is taking a deliberate approach to the safe and responsible use of AI.

Recommendation

24. We recommend that you **agree** to discuss this briefing with officials. **Yes/No**

Murray Davey
Chief Digital Officer & GM Enterprise Digital Services

Hon Brooke van Velden
Minister of Internal Affairs

_____/_____/_____

Document 5

Priority **Routine**

Internal Affairs
Te Tari Taiwhenua

Internal Affairs briefing

Hon Brooke van Velden
Minister of Internal Affairs

Title: **Advice on the use of Artificial Intelligence generated endorsements in online casino gambling advertising**

Date: 4 February 2026

Key issues
This briefing provides you with further advice on Artificial Intelligence (AI) generated endorsements as part of the suite of advertising regulations to establish the Online Casino Gambling regime. In November 2025, Cabinet agreed to prohibit the use of paid endorsements and agreed in-principle to prohibit the use of AI to endorse operators or online casino gambling products, subject to you receiving further policy advice. AI generated endorsements are used by operators internationally, and there is evidence that they are also being used to target New Zealanders. AI generated endorsements are similar to human ones. Both are a highly impactful form of advertising that can exacerbate gambling harm and mislead consumers. This briefing provides options for your consideration and identifies a recommended approach to the use of AI generated endorsements, which aligns with Cabinet's in-principle decision and would prohibit advertising content where operators use a person's likeness or AI generated content to suggest or mimic a human endorsement. We expect that the most common example of such content would be the use of AI generated or computer-generated avatars that mimic human influencers to promote online gambling. Subject to your agreement, draft regulations will be included in the final package of regulations on advertising, harm prevention and minimisation, consumer protection and cost recovery matters intended to go to Cabinet for approval in late May 2026.

Action sought	Timeframe
Discuss advice with officials at the regulations deep dive on 10 February.	By 10 February 2026
Indicate your preferred approach to the regulation of AI generated endorsements.	By 13 February 2026

Contact for telephone discussions (if required)

Name	Position	Contact Number	Suggested 1st contact
Kelly Miller	Policy Manager	9(2)(a)	✓
9(2)(a)	General Manager, Policy	9(2)(a)	

Return electronic document to:	Manasi Nair, Manasi.Nair2@dia.govt.nz
Hukatai reference	NNZF57N5FNJM-1924615558-264
Ministerial database reference	IA202610890

Purpose

1. This briefing seeks your consideration of options for the regulation of AI generated endorsements, and agreement to prohibit online casino gambling operators from using a person's likeness or AI generated content to suggest or mimic a human endorsement.

2. This paper outlines the potential benefits and risks of such content in online casino gambling advertising. On balance, we recommend prohibiting operators from using this content in their advertising.

Executive summary

3. The briefing advises you on whether to prohibit online casino gambling operators from using a person's likeness or AI generated content to suggest or mimic human endorsements. Cabinet has already agreed to ban paid endorsements and agreed *in principle* to restrict use of a person's likeness or AI to endorse operators or online casino gambling products, pending further advice. These AI endorsements—including synthetic influencers, deepfakes, and other likeness-based representations—are increasingly used internationally and have already been observed in New Zealand, creating risks of consumer deception and contributing to gambling harm.

4. While existing frameworks such as the Fair Trading Act 1986, the Defamation Act 1992, and the New Zealand Advertising Standards Authority guidelines provide some protection, they are not designed to proactively minimise gambling harm. These endorsements can normalise gambling in ways similar to human endorsements and deepfakes carry additional harms, including misuse of individuals' identities. Other jurisdictions (e.g., the United States of America, the United Kingdom, and the European Union) have taken steps to restrict false or AI-generated endorsements, signalling a global trend toward tighter regulation.

5. This paper proposes three regulatory options: maintaining the status quo, requiring disclosures on AI generated content, or prohibition. We recommend the third option (prohibition). This option would be most effective at closing a potential loophole in the regulations, ensure clear expectations for operators, and strengthen harm-prevention measures as the regulated online casino market is established.

6. If you agree to prohibit this form of advertising, we will work with the Parliamentary Counsel Office to draft regulations for inclusion in the draft regulations package to be considered by Cabinet in May/June 2026.

Cabinet has already agreed to prohibit paid endorsements

7. Cabinet has previously agreed to prohibit the use of paid endorsements. A paid endorsement is an arrangement where an advertiser provides consideration to a person to act as a brand ambassador or provide a testimonial. Endorsements may be delivered by a well-known individual or by a layperson presented as a trustworthy or relatable voice. Operators will not be allowed to pay a person (such as an influencer, sports player, celebrity, or a tipster) to promote online casino gambling.

8. Paid endorsements are highly impactful, especially for children. They can normalise gambling behaviour, increase exposure, and contribute to problem gambling behaviours (IA20256569 refers).

Cabinet has also agreed in-principle to prohibit the use of AI for endorsements

9. In November 2025, Cabinet agreed in-principle to prohibit the use of a person's likeness or AI generated endorsements subject to you receiving further advice [ECO-25-MIN-0197 refers]. You advised Cabinet that you would confirm your position and seek Cabinet Legislation Committee agreement when you bring the regulations back for final approval. Due to time

constraints, we were unable to provide detailed advice on this issue ahead of your Cabinet paper being considered.

10. An AI generated endorsement is an advertisement that uses AI to create videos or images that appear to reflect a human endorsement. Because these do not involve a human receiving a payment or benefit for the endorsement, they are not clearly captured by the current prohibition on paid endorsements, yet they are associated with gambling harm and give rise to similar concerns as paid endorsements. AI generated endorsements also can cause specific harms associated with deepfakes, which we outline in detail below. This creates a loophole in the advertising regulations, which we consider should be addressed.

We have identified two forms of AI endorsements, and we are also proposing to limit 'use of a person's likeness' to ensure similar technologies are captured

11. The first form of AI generated endorsement we have identified is the use of synthetic influencers. These are AI generated personas created to look and behave like humans.[1] These "influencers" are used as brand ambassadors due to their ability to attract people's attention, highlighting a shift toward technology driven marketing. They are highly customisable as they range from hyper realistic personas to stylised cartoons or fantasy characters making them particularly appealing to Gen Z and people with high digital literacy. These features are desirable because they combine speed, cost, and full creative control, and brands are able to produce or hire these "influencers" to boost their engagement. Some synthetic influencers have their own fanbase, similar to real life influencers.

12. Deepfakes are the second form of AI generated endorsement we have identified. These are created by impersonating the identity or voice of a celebrity, influencer, or other individual without consent. Deepfakes can produce highly realistic content that appears to show an individual endorsing a product they have no association with, creating substantial risk of deception. They create harms for both the person whose identity is used, and those who view the content. We discuss this harm further at paragraph 17.

13. We also include the "use of a person's likeness" in this advice, alongside the two previously mentioned forms of AI endorsements. This ensures that our analysis also covers advertisements that use content created by a person (without the assistance of AI) that suggests or mimics endorsements, similar to a paid human endorsement. Examples of this would include digitally recreating a person's voice, and computer generated images (CGI). This would capture work that is done using computers to create digital characters that are not AI synthetic influencers and supports future proofing, as it would capture non-AI emerging technologies that depict or imitate humans.

Internationally, AI generated endorsements are an emerging trend

14. We have identified multiple instances of gambling operators using AI generated content to mimic endorsements made by real people.[2] These endorsements have either used a deepfake or synthetic influencers to make advertisements that appear more authentic or engaging.

15. AI generated endorsements are accessible and cost-effective. They can be created and deployed quickly and adapted for multilingual campaigns to reach a wider market. This reduces reliance on human influencers and streamlines production timelines by minimising talent coordination. They also allow real time tailoring, for example, automatically generating and rotating messages or testimonials by audiences and adjusting the content at pace to boost

[1] Kim, E., Kim, D., E, Z., & Shoenberger, H. (2023). The next hype in social media advertising: Examining virtual influencers' brand endorsement effectiveness. *Frontiers in Psychology, 14*, 1089051. https://doi.org/10.3389/fpsyg.2023.1089051

[2] See, for example a recent UK Advertising Standards Authority ruling. (2025, September 17). Dribble Media Ltd. ASA | CAP. https://www.asa.org.uk/rulings/dribble-media-ltd-g25-1300959-dribble-media-ltd.html

engagement on platforms. As a result, operators gain greater control over brand consistency and campaign efficiency. Together, these features make AI generated endorsements an efficient and scalable option for reaching diverse audiences at pace.

AI generated endorsements have very similar potential for harm as paid human endorsements, as well as some additional risks

16. Like human endorsements, AI generated endorsements can normalise and encourage gambling. Due to their human-like appearance, endorsements by synthetic influencers can be perceived as authentic and credible to consumers. [3] These personas can accumulate followers, foster trust, and exert significant marketing influence over time, creating effects comparable to human influencer endorsements even where audiences are aware that the persona is not a real person.

17. Deepfakes create a range of additional harms due to the negative impact on the person whose identity is used. We have already seen this form of advertising being used by a gambling operator to appeal to New Zealand audiences. In April 2025, a video used the likeness and synthetic voice of *Breakfast* host Jenny-May Clarkson to endorse a gambling app (Māori Game), which also featured a deepfake of Taika Waititi. [4]

18. The United Kingdom's Advertising Standards Authority (UK ASA) has reported that in 2024 celebrity deepfake advertisements were amongst the most reported scams. [5] Deepfakes can also target people with no public profile. Meta's Oversight Board [6] reviewed an AI generated gambling endorsement that used images of a schoolteacher, bus driver and grocery store worker to claim players could earn more from "Plinko" than these jobs. The post was viewed over 600,000 times before removal, highlighting the speed and reach of deceptive AI content and the limits of reactive moderation. [7]

International jurisdictions increasingly recognise the risks associated with AI generated endorsements

19. While there is limited information on how other jurisdictions regulate AI generated endorsements in gambling advertising, several jurisdictions have implemented broader restrictions on deepfake or fabricated endorsements. The U.S. Federal Trade Commission (FTC), for example, has ruled that "fake or false consumer reviews, consumer testimonials, and celebrity testimonials will be prohibited" [8], including AI generated fake endorsements. The FTC's 2023 Endorsement Guide also clarifies that synthetic influencers are "endorsers", and they must not mislead the public. The Guide also states that synthetic influencer endorsements must include disclosures that are clear and conspicuous.

20. Similarly, the UK ASA and Committee of Advertising Practice (CAP) codes include rules on misleading consumers, testimonials and endorsements, and guidance has emphasised the need for AI generated advertising to comply with existing requirements about false or misleading advertisements. They have also ruled against false celebrity endorsements that

[3] Heejae Lee, Mincheol Shin, Jeongwon Yang & T. Makana Chock (2025) Virtual Influencers vs. Human Influencers in the Context of Influencer Marketing: The Moderating Role of Machine Heuristic on Perceived Authenticity of Influencers, International Journal of Human–Computer Interaction, 41:10, 6029-6046, DOI: 10.1080/10447318.2024.2374100

[4] Breakfast host's warning as AI gambling ad captures likeness

[5] Advertising Standards Authority. (2025, February 13). *A year in scams: 2024 update on Scam Ad Alert system*. https://www.asa.org.uk/news/a-year-in-scams-2024-update-on-scam-ad-alert-system.html

[6] An independent board that reviews and can overturn Meta's content decisions.

[7] (2025, June 5). *AI-manipulated video promoting gambling* [Case decision]. https://www.oversightboard.com/decision/fb-o7ai7uax/

[8] Federal Trade Commission Announces Final Rule Banning Fake Reviews and Testimonials | Federal Trade Commission

suggest the endorsement or testimonial is genuine. The European Union's AI Act has introduced anti-manipulation prohibitions and transparency/labelling duties for deepfakes.

The risks from AI generated endorsements are not unique to gambling and there are already some legal protections in place in New Zealand

21. We recognise that the issues associated with synthetic influencers and deepfake endorsements extend well beyond online casino gambling. There are already legal protections in place to address some of the concerns. For example, section 9 of the Fair Trading Act 1986 (FTA) prohibits misleading or deceptive conduct in trade. Any concerns or breaches would be addressed through complaints to the New Zealand Commerce Commission. The FTA may apply to both the use of deepfakes and the use of synthetic influencers, if criteria for breach of section 9 are met. In addition to the FTA restrictions, the NZ ASA's Guidance on Generative AI warns against misrepresenting AI content, and the Commerce Commission requires truthfulness in endorsements.

22. The existing requirements in the online casino gambling regulations will also go some way to protecting consumers. For example, where a synthetic influencer is created and controlled by a third party, we expect that the existing prohibition on paid endorsements would apply, as the operator would still be entering a paid arrangement with a third party to endorse their products. Operators will also be required to ensure that advertisements are easily identifiable as advertisements.

23. The key limitation with these existing and pending controls is that not all AI generated endorsements are inherently misleading or deceptive, and the use of synthetic influencers and deepfakes does not necessarily require engaging with a third party.

24. There are other legal frameworks that individuals who have been personally harmed by deepfakes can access to seek a remedy (the Defamation Act 1992, the Harassment Act 1997 and the Harmful Digital Communications Act 2015 are potential examples).

25. While there are some existing legal protections, we consider a gambling-specific prohibition may have merit, as a direct response to this issue in the gambling context and the particular harms associated with highly influential gambling advertising. This could strengthen the regime's focus on minimising gambling harm.

We have identified three options for you to consider

26. Scenarios demonstrating how each option would work in practice have been attached at **Appendix A**. We have included examples of paid human endorsements and affiliate arrangements to show the wider regulatory approach.

Option 1: Do not introduce specific restrictions on AI generated endorsements

27. This option would continue to prohibit paid endorsements, as previously agreed. Use of AI endorsements would continue to be regulated within the existing legal framework provided for in the OCG regulations and relevant legislation like the FTA.

28. The key benefit of the status quo is that it enables a 'watch and wait' approach where we can see how other jurisdictions manage this risk and learn from their experience, rather than being a first mover. It also enables us to assess the extent of this issue in the newly regulated online casino gambling market, and to wait for potential development of wider legal controls on AI endorsements in New Zealand, given this is an increasingly common aspect of advertising across various sectors.

29. However, a 'watch and wait' approach also means that harm may occur in the interim, and use of unpaid AI generated endorsements is likely to continue. We know advertisements are run quickly with new advertisements being released every few days. This risk is heightened during

the market establishment phase, when operators are likely to significantly increase marketing spend to build market share. A reactive model in this context may allow harm to occur before any regulatory intervention takes place.

Option 2: Require disclosures on AI generated content

30. If this option was adopted, an operator would be required to disclose where advertising content is AI generated. We propose that disclosures should be prominent, unavoidable and accessible – for example, stating that the endorsement is generated by AI and is not a real opinion or person in both visual and audio formats at the beginning of the advertisement. This aligns with best practice guidance issued by the FTC for disclosures in advertisements.

31. When brands fail to disclose that the content is AI generated and instead suggest or mimic that it reflects a human endorsement, it could mislead consumers. Because these endorsements often mimic influencer content, it blurs the line between advertising and authentic opinion, undermining informed decision-making for consumers.

32. The key benefit of this option is that it would enable operators to access the commercial benefits of this form of advertising, while mitigating some of the risks. This approach would also be consistent with the FTC guidelines. It would also reduce the risk of consumers being misled by AI generated content, so it may be more effective at minimising harm and protecting consumers than Option 1.

33. The key risk is that this option may be less effective than a prohibition, for the following reasons:

    33.1 The disclosure could be missed by consumers, if included in an extensive list of other required disclosures. We note that Cabinet has also agreed that advertising must be easily identifiable and labels must be obvious, clear, prominent and upfront and must be separate from other disclosures. Multiple disclosures could also increase the compliance burden for operators, especially for short-form ads like those found on Instagram stories or TikTok videos where the length and content of the advertisement is already limited.

    33.2 Children are less likely to understand what disclosures mean, compared to adults.[9]

    33.3 Synthetic influencer endorsements can still be compelling and attractive to their audience, even when the audience knows the influencer is not a real person.[10] A disclosure would not be effective at reducing risk of harm for customers that already know the content of the advertisement is AI generated.

    33.4 This option would not capture other tools for suggesting or mimicking a human endorsement that do not use AI, such as CGI content.

34. If you agree to this option, we propose it be made clear that disclosures would not discharge or override an operator's obligations under other legislation, like the FTA.

Option 3: Prohibit operators from using a person's likeness or AI generated content to suggest or mimic a human endorsement (preferred option)

35. This option would prohibit operators from using a person's likeness or AI generated content to suggest or mimic a human endorsement. This would include endorsements that represent,

[9] Boerman SC and van Reijmersdal EA (2020) Disclosing Influencer Marketing on YouTube to Children: The Moderating Role of Para-Social Relationship. Front. Psychol. 10:3042. doi:10.3389/fpsyg.2019.03042

[10] Kim EA, Kim D, E Z and Shoenberger H (2023) The next hype in social media advertising: Examining virtual influencers' brand endorsement effectiveness. Front. Psychol. 14:1089051. doi: 10.3389/fpsyg.2023.1089051

simulate, or perform the function of an endorsement for online casino gambling, regardless of whether the content is presented as a real person or a synthetic persona.

36. We propose that 'suggest' would apply where the operator is implying or insinuating that the use of a person's likeness or AI generated content is a real human. 'Mimic' would apply where there is no implication or insinuation that the likeness or AI content is a real person, but the likeness or AI content closely resembles a real human. An example of content that 'mimics' human endorsement but does not 'suggest' it is a synthetic influencer that is open and clear to the audience that it is AI generated and not real.

37. Introducing this prohibition would close the loophole identified by officials and would prevent operators from using AI or CGI generated endorsements to advertise. This would protect consumers from potentially harmful or misleading marketing practices. It would also help ensure that consumers can make informed choices about their gambling behaviours.

38. This option will only apply to endorsements and would not apply to other forms of advertising or communications between an operator and customers for administrative purposes (administrative communications are not considered advertising). We are not seeking to restrict operators from using AI tools for legitimate service functions. This includes responding to comments on online platforms or generating content in multiple languages. We acknowledge that the use of AI for consumer interaction can enable operators to respond faster and improve their service quality.

39. Introducing a prohibition on AI generated endorsements would allow us to take a proactive regulatory approach. It would also provide operators with clear expectations on acceptable advertising practices in the online casino gambling market at the outset, before they develop and submit their advertising and marketing strategy to the Secretary.[11]

Next steps

40. Subject to discussion and your agreement, we will develop drafting instructions and work with the Parliamentary Counsel Office (PCO) to draft the regulations. If agreed, the draft regulations will be provided for your review ahead of seeking Cabinet Legislation Committee approval.

[11] Clause 18(1)(a) of the Bill requires prospective operators to include an advertising and marketing strategy as part of the pack of information that accompanies their licence application.

Recommendations

We recommend that you:

1.	**Discuss** this briefing with officials at your meeting with officials on 10 February 2025	**Agree/Disagree/Discuss**
2.	**EITHER**	
	(i) **Agree** to option 1: Do not introduce specific restrictions on AI generated endorsements	**Agree/Disagree/Discuss**
	OR	
	(ii) **Agree** to option 2: Require disclosures on AI generated content	**Agree/Disagree/Discuss**
	OR	
	(iii) **Agree** to option 3: Prohibit operators from using a person's likeness or AI generated content to suggest or mimic a human endorsement	**Agree/Disagree/Discuss**

9(2)(a)

Hon Brooke van Velden
Minister of Internal Affairs

_____/_____/_____

Appendix A: Scenarios demonstrating how requirements would apply under each option

Scenarios refer to an imaginary licensed online casino gambling (OCG) operator (CasinoX).

	Prohibited		Not in breach of the OCG advertising regulations, but may be in breach of related legislation (e.g. the FTA)		Allowed under the OCG regulations and related legislation (e.g. the FTA)

Scenario description	**Option 1 (No additional restriction)**	**Option 2 (mandatory disclosures)**	**Option 3 (no suggested/mimicked endorsements)**
CasinoX hires Lena Smith, a famous TV actor, to star in a series of commercials promoting their online slot games. CasinoX pays Lena $100,000 in exchange for her services.	Prohibited – As CasinoX has entered an arrangement to pay Lena in exchange for her acting as a brand ambassador, this would be a paid endorsement. Cabinet has agreed to prohibit this form of advertising.	Prohibited – paid endorsement	Prohibited – paid endorsement
CasinoX enters a partnership with Marty, an influencer who posts product reviews of OCG products to his followers. Marty includes an affiliate link to CasinoX's website in his videos, and CasinoX pays Marty a small fee for each person that creates an account through his link.	Prohibited – This is an example of a performance based affiliate arrangement as CasinoX pays a third party (Marty) for each successful sign-up. Cabinet has agreed to prohibit this form of advertising.	Prohibited – paid endorsement	Prohibited – paid endorsement
CasinoX provides a personalised link to its customers and promises customers they will get $10 in account credit for each person that signs up through their link.	Prohibited – This is another example of a performance based affiliate arrangement as the customer is a third party and CasinoX are providing a benefit to the customer to encourage them to seek new sign-ups.	Prohibited – paid endorsement	Prohibited – paid endorsement
CasinoX pays for a small group of influencers (Ava, Benny and Charlotte) to travel to Queenstown for three days, accommodation and activities included. In exchange for the trip, Ava, Benny and Charlotte agree to post 2x Instagram stories and 1x Facebook post promoting CasinoX's new online slot game.	Prohibited – While CasinoX are not paying money directly to Ava, Benny and Charlotte, they have entered an arrangement with A, B and C that they will pay for the trip (which has monetary value) in exchange for them promoting CasinoX. This would be a paid endorsement.	Prohibited – paid endorsement	Prohibited – paid endorsement
'Alicia Inez' is a famous synthetic influencer with 1.2 million followers across social media platforms. The account is created, owned and run by Trent. CasinoX enters an arrangement with Trent where they pay Trent $100,000 for Alicia Inez to promote their new online slot game across Alicia Inez' platforms.	Prohibited – While Alicia Inez is a synthetic influencer, the account is run by a third party (Trent). CasinoX has entered an arrangement with Trent to promote their new game, so this is a 'paid endorsement.' This is similar to how affiliate partnerships with betting websites are prohibited – even though the website isn't a 'person' there is a third party who controls the website that an operator contracts with.	Prohibited – paid endorsement	Prohibited – paid endorsement
John is a customer of CasinoX and really enjoys playing their online slot games. He tells his friends (Xavier, Yvonne and Zach) that he has won $1000 on CasinoX's platform and encourages them to sign-up as well.	Allowed – CasinoX has not entered an arrangement with John to promote them, and they are not providing John with any 'benefits' to encourage him to endorse the product to X, Y and Z.	Allowed – CasinoX has no control or involvement over John's personal opinion, and they are not publishing John's opinion as promotional material, so it isn't 'advertising content.'	Allowed – CasinoX has no control or involvement over John's personal opinion, and they are not publishing John's opinion as promotional material, so it isn't 'advertising content.'

CasinoX uses a CGI likeness of Lena (created by a human animator) in a series of advertisements promoting their slot games talking about how much she loves CasinoX.com. Lena has not consented to her likeness being used and has not been paid by CasinoX in exchange for them using her likeness.	Not in breach of OCG endorsement requirements because it is not a paid endorsement or an affiliate arrangement. However, the Fair Trading Act may apply, if it can be established that the ad is a false or misleading representation.	Not in breach of OCG requirements and a disclosure is not required because the content is not AI generated. However, the advertisement may breach the FTA.	Prohibited – CasinoX's advertisement is using Lena's likeness, so it is suggesting or mimicking a human (Lena's) endorsement.
CasinoX launches 'Nova' a fully AI generated virtual brand ambassador (who looks like a real person) that appears in social media posts saying 'I have won $1000 on CasinoX.com! My favourite game is [new online slot game]'	Not in breach of OCG requirements, as this is not a paid endorsement as Nova is owned/launched by CasinoX. This advertisement may breach the Fair Trading Act, if it is not actually possible for a person to win $1000 on CasinoX.com when playing that specific game.	Not in breach of OCG requirements, provided that the social media posts include a disclosure that Nova is an AI generated virtual brand ambassador, and not a real person, but the advertisement may breach the FTA.	Prohibited – CasinoX is suggesting that Nova is a human (that is a customer of CasinoX) so the ad is suggesting or mimicking a human endorsement.
CasinoX asks Lena if she is willing to star in an ad campaign for their new online slot game, but Lena says no. CasinoX creates a deepfake of Lena that appears in their ads, saying "CasinoX is my favourite online casino, I've personally won $1000 on their new slot game!"	Not in breach of OCG requirements, as CasinoX didn't enter a paid arrangement with Lena to use her likeness. However, this advertisement may breach the Fair Trading Act because it is falsely implying that Lena is a customer.	Not in breach of OCG requirements, provided that the advertisements include a disclosure that the deepfake is not Lena and that Lena is not endorsing CasinoX personally. However, the advertisement may breach the FTA.	Prohibited – CasinoX is suggesting that Lena is a brand ambassador and that the game she is endorsing is her favourite game, so it is suggesting a human endorsement.
CasinoX launches 'Awhi' a fully AI generated avatar who answers customer questions via live chat.	Allowed – administrative communications with customers are not 'advertising' for the purposes of the Online Casino Gambling Bill.	Allowed – administrative communications, not endorsement.	Allowed – administrative communications, not endorsement.
CasinoX creates a series of demonstration videos where Awhi provides a tutorial on how to play CasinoX's new game. The videos are intended to be advertisements – they are used in direct marketing to players and shown on CasinoX's social media pages. The video is factual, and Awhi doesn't provide any opinions.	Allowed – if the content isn't readily identifiable from context that it's an ad, it may require a disclosure that the content is an ad.	Allowed – provided that the advertisement includes a disclosure that Awhi is AI generated.	Allowed – the tutorial isn't suggesting or mimicking a human endorsement because Awhi is factually explaining how to play the game.
CasinoX features a CGI cartoon kiwi 'Beaky' in TV commercials and on their website as a character mascot for the brand.	Allowed under the Online Casino Gambling regulations, provided that the character's use does not reasonably appeal to people under 18 (Cabinet has agreed that advertisements must not reasonably appeal to audiences under the age of 18).	Allowed – no disclosure is required, as Beaky is not human-like or a person and is not AI generated content	Allowed –Beaky is not human-like and or a person, so the advertisement is not suggesting or mimicking a human endorsement.
CasinoX runs an ad campaign that features AI generated content (ads featuring El Dorado 'the city of gold' and towering piles of golden coins)	Allowed – no misleading conduct.	Allowed – however the operator would need to include a disclosure that the ad has AI generated content.	Allowed – no endorsement is being made.
CasinoX pays Lena $100,000 for a radio ad campaign. However, instead of recording her real voice, Lena agrees that CasinoX can digitally recreate her voice for the ad instead.	Prohibited – As CasinoX has entered an arrangement to pay Lena in order to use her digital likeness/voice in their ad campaign, this is a paid endorsement even though Lena is not physically appearing in the ad.	Prohibited – paid endorsement	Prohibited – paid endorsement

Document 6
Priority **Routine**

Internal Affairs
Te Tari Taiwhenua

Internal Affairs briefing

Hon Brooke van Velden
Minister of Internal Affairs

Title: **Discussion document on digital identity privacy and security issues – proposed structure and engagement approach**

Date: 5 March 2026

Key issues
You recently agreed to progress a discussion document on the privacy and security of digital identity for targeted consultation with sector experts [IA202611072 refers]. We now seek your feedback on the proposed framing and outline for the discussion document, and the engagement approach for consultation. This includes an updated stakeholder list refined to focus on privacy and security experts and those with an interest in this work. The discussion document will focus on how digital identity can ensure the privacy and security of identity information. We propose to approach the discussion on the privacy and security of information through each stage of the digital identity 'life cycle'. Following your feedback, we intend to provide you with a draft discussion document on 2 April 2026 and seek your approval to begin targeted consultation. This will allow targeted consultation to run from 20 April 2026 – 18 May 2026 and for a report back from consultation in June 2026.

Recommendations	Timeframe
Agree to the proposed framing of privacy as relating to the governance of information; **Agree** to the proposed framing of security as relating to the structures and processes to do with the management of information; **Agree** to frame the questions of the discussion document around each stage of the digital identity 'life cycle'; **EITHER agree** for the discussion document to focus on a comparison between the current centralised model of digital identity with a future decentralised model **OR agree** for the discussion document to focus on the current centralised model of digital identity; and **Provide** feedback on to the proposed stakeholder list.	By 10 March 2026

Contact for telephone discussions (if required)

Name	Position	Contact Number	Suggested 1st contact
9(2)(a)	General Manager Policy	9(2)(a)	✓
Kelsea Whyte	Policy Manager	9(2)(a)	

Return electronic document to:	9(2)(a)
Hukutai document reference	6KWWFJMNQWZ4-1227312906-6030
Ministerial database reference	IA202611309

Purpose

1. You recently agreed to progress a discussion document on the privacy and security of digital identity information for targeted consultation with sector experts[1]. We now seek your feedback on the proposed framing and outline for the discussion document, and the engagement approach for consultation.

2. This briefing contains:

   2.1 a proposed outline for the discussion document – **Appendix A**; and

   2.2 a proposed stakeholder list for targeted engagement – **Appendix B**.

Executive summary

3. The Department of Internal Affairs is progressing work on a discussion document focused on the privacy and security of digital identity information, following your agreement to undertake targeted consultation with sector experts. The document aims to support a broader conversation on how identity information held by the Department can be better protected, particularly in light of increasing public scrutiny following incidents such as the recent Manage My Health data breach.

4. The discussion document proposes to frame privacy and security as related but distinct concepts: privacy as the governance and control of identity information, and security as the integrity and protection of the systems and processes that manage that information. It will examine these issues across each stage of the digital identity life cycle—collection, storage, use, sharing, and disposal—and seek stakeholder views on the risks and opportunities associated with each.

5. A key decision for you is the preferred framing of the discussion document. While both the current centralised model and a potential future decentralised (verifiable credentials) model will be addressed, direction is sought on whether the document should primarily:

   5.1 focus on improving the privacy and security of the current centralised system; or

   5.2 focus on comparing the current model with a decentralised approach increasingly adopted internationally.

6. We propose a targeted four-week engagement with privacy and security experts, beginning 20 April 2026. Stakeholders include specialist consultants, businesses that handle identity information, major users of identity data, and relevant government agencies. Engagement would be undertaken through written submissions and optional workshops to support discussion of technical content.

7. Following your feedback on the proposed structure and engagement approach, a full draft discussion document will be provided to you on 2 April 2026 for feedback prior to consultation.

[1] IA202611072 – *Approach to a discussion document on the privacy and security of digital identity information,* 17 February 2026 – refers.

We have developed an outline for the digital identity discussion document and proposed engagement approach following your feedback on the direction

8. We recently sought your direction on a discussion document relating to the privacy and security of New Zealanders' information held and used by the Department of Internal Affairs (the Department) [IA202611072 refers].[2]

9. The recent Manage My Health data breach has resulted in greater interest and scrutiny in the privacy and security of digital identity products and services. It has also underscored the importance of strong stewardship of identity information held by government agencies.

10. You have indicated that your preference is to progress a discussion document to inform a broad conversation around the future of digital identity, with a specific focus on the privacy and security of identity information. This means considering whether there are ways to improve the privacy and security of the information held by the Department, such as through enabling (or requiring) data minimisation so that only necessary information is being shared, incorporating new technology, and requiring robust security measures. It also means understanding any concerns around privacy and security, and what aspects of our efforts to protect these things are considered effective.

11. You have also indicated your expectation that engagement with private sector privacy and security sector experts will be prioritised. This will allow us to gather expert opinion on how to best protect privacy and security of the information we hold on behalf of the public and identify where improvements may be made.

12. We have developed the framing and a structure with proposed content for the discussion document in line with your preference (with a breakdown at **Appendix A**). We have also developed a proposed engagement approach for your consideration, including an updated stakeholder list (**Appendix B**).

13. We seek your feedback on the direction of the discussion document and engagement approach ahead of providing you with a draft discussion document on 2 April 2026.

The discussion document should frame the privacy and security of digital identity information as connected, but distinct, issues relating to the governance of information and the structures that handle them, respectively

14. As part of the discussion document, we suggest framing what we mean by privacy and security in the context of digital identity.

15. **Privacy** in the context of digital identity could mean ensuring the privacy of personal and organisational information in digital identity systems, and focus on the governance of information. This includes:

    15.1 prioritising the control that people and organisations have over their identity information;

    15.2 ensuring that any new digital identity systems will promote and protect privacy or be privacy-enhancing by default; and

[2] IA202611072 – *Approach to a discussion document on the privacy and security of digital identity information,* 17 February 2026.

15.3 that digital identity systems should be transparent and provide users with the ability to know who has their data and what they do with it.

16. **Security** in the context of digital identity could mean ensuring the security of the structures and processes that allow for the handling and disposal of personal information. While it is clearly linked with privacy, it is distinct. This includes:

16.1 ensuring that information is protected from unauthorised access and is not corrupted, stolen, or misused;

16.2 ensuring that systems are secure using the most up-to-date and appropriate technology; and

16.3 considering the continuity of information – for example, in case of emergencies such as floods or earthquakes.

17. We also considered framing privacy and security by reference to relevant legislation and codes in New Zealand, such as the Privacy Act 2020 that governs privacy, the Bill of Rights Act 1990 that governs rights and freedoms, or the Protective Security Requirements, which outline the government's expectations on information security. However, framing the discussion document in this way would be less effective in seeking understanding of privacy and security as they relate to the way that digital identity information is used and managed in practice. The framing that we have proposed in paragraphs 14 to 16 also allows for consideration of relevant legislation and codes.

We propose the discussion on the privacy and security of information could separate each stage of the digital identity 'life cycle' – collection, storage, use, sharing, and disposal

18. For digital identity information to be used, it must be collected, stored, used, shared, and disposed of. The Privacy Act 2020 and the information privacy principles that it contains set out a legal framework to protect an individual's right to privacy of personal information during the different 'data life cycle' stages. In practice, the digital identity life cycle looks like:

18.1 before it can be used, information must be **collected**. This can be done in many ways – for example, when the birth of a child in New Zealand is entered into the birth register, or when someone registers a change in their name. Often, information is collected at the same time as it is being created.

18.2 information that is collected is immediately **stored**. This can be on an Excel spreadsheet, or as encrypted data on a server, or through a content management system. Information can be retained for different amounts of time, depending on what that information is used for.

18.3 information is then **used** for different purposes, such as where information is checked against an authoritative source for a RealMe verified identity, checking registry details when someone is applying to be a celebrant, or when someone is request a birth certificate for their child.

18.4 information can then be **shared** if appropriate, such as verifying age if someone is looking to access age-restricted products, or through information sharing agreements with other organisations and through RealMe.

18.5 at the end of the transaction, information that is no longer needed should be **disposed of** – such as selfies that are used to check against information in Identity Check.

19. We intend to ask stakeholders about their understanding of the privacy and security implications at each of the data life cycle stages. Examples of questions we could ask are provided under the proposed skeleton, attached as **Appendix A**.

The discussion document could focus on improving the privacy and security of our current centralised digital identity model, or it could focus on comparing the privacy and security of our current model with a future system based around verifiable credentials

How the discussion document is framed will affect how we discuss the data 'life cycle'

20. We will need to discuss both the current centralised model (discussed further below in paragraph 22) and a future decentralised model (discussed further below in paragraph 24) in the discussion document. We seek your direction as to which of those models you would prefer us to focus on, to help us frame how digital identity is discussed.

21. We could frame the discussion document in two possible ways: focusing how we discuss digital identity more on the privacy and security implications of our current, centralised, model of digital identity, or placing a greater focus on comparing the current model with a future, decentralised, model.

22. This is because the way that information is handled during the 'life cycle' – and as such the subsequent privacy and security concerns and questions we would ask – will be different between the centralised and decentralised systems. For example, a centralised system where information is shared by the government will have different risks to a decentralised system where information is shared by individuals.

We could focus the discussion document on the privacy and security of the current centralised model of digital identity…

23. The Department handles identity information currently in a centralised manner, through services like RealMe and Identity Check. This means that identity information is collected into, stored in, and used from databases that are managed by the government, and is shared in bulk, provided as a package of information, between RealMe participating agencies.

24. Other examples of centralised models are of MyID in Australia and Gov.UK in the United Kingdom, which relies on government servers to provide digital identity services.

… or we could focus the discussion document on a comparative review with a decentralised future model, which is the focus for some overseas jurisdictions and the Digital Identity Services Trust Framework

25. Many overseas jurisdictions, including Australia and the United Kingdom, are currently moving towards decentralised, credential-based models,[3] which would allow people to provide their identity and share information about themselves. New Zealand's Digital Identity Services Trust Framework is also now operational and sets out a legal framework to regulate the provision of decentralised digital identity products.

26. While the Department would still need to hold information in a centralised manner, there is an opportunity for us to focus the discussion document to seek expert views on whether a decentralised approach would work for the digital identity products and services that the Department may provide in the future. The discussion document could further consider future technologies stakeholders see as being particularly salient in the international landscape.

We have also developed a proposed engagement approach focusing on targeted consultation with privacy and security experts in the digital identity space

Targeted engagement will run for 4 weeks starting on 20 April 2026

27. We are proposing that engagement on the discussion document will begin on 20 April 2026 and run for 4 weeks, finishing on 18 May 2026. This is proposed to begin a week later than in the timeline of the previous briefing [IA202611072 refers][4] as we understand from your Office that this will give you sufficient time to provide feedback on the draft discussion document prior to starting targeted engagement. We intend to contact stakeholders with the discussion document and invite them to provide a written submission guided by questions throughout the document.

28. Similar to the information webinars run during targeted consultation undertaken on the video content consumer information (VCCI) system in June 2025, we could consider running workshops with groups of stakeholders to talk through the discussion document and invite questions and feedback. The information webinars were found to be useful in gathering focused feedback on the VCCI proposals. We believe workshops are likely to help stakeholders digest the technical information in the discussion document and encourage engagement. We would still make it known to stakeholders that we are available for one-to-one meetings should they wish to engage in that way.

The stakeholder list has been refined and additional stakeholders added following your previous feedback on the objectives of the discussion document

29. We have updated the list of stakeholders we are proposing to engage with based on the focus of the discussion document. This includes refining the previous list provided

[3] Australia have established a Trusted Digital Identity Framework and have begun to implement digital driver licences throughout states, and the United Kingdom have implemented a trust framework.

[4] IA202611072 – *Approach to a discussion document on the privacy and security of digital identity information,* 17 February 2026.

to you [IA202611072 refers],[5] and adding data privacy and security consultants as requested.

30. Stakeholders that could be involved in this targeted consultation have been organised into the following groups, in accordance with their interest and expertise regarding the content of the discussion document:

    30.1 **Group A: Experts with views on the privacy and security of identity information.** This includes data privacy and security consultants, privacy oversight bodies, cybercrime experts, digital and technology sector experts, and legal experts. We note that there is a chance the privacy consultants may wish to charge the Department for their time and expertise and we will keep you informed if this changes the nature of the consultation.

    30.2 **Group B: Businesses with experience handling identity information.** This includes banks, financial services, and telecommunications.

    30.3 **Group C: Users of identity information.** This includes e-commerce, retail and hospitality, transport providers, and mail and courier services. It also includes population groups.

    30.4 **Group D: Government agencies.** This includes agencies with an interest in the digital identity work, including the Public Service Commission, New Zealand Transport Agency, Treasury, Ministry of Business, Innovation and Employment, Ministry of Justice, Ministry of Social Development, the Department of the Prime Minister and Cabinet, Ministry of Education, and the Inland Revenue Department. These agencies have similar interests and experiences in holding personal information on behalf of the public.

31. A full list of all of the proposed stakeholders under these groupings can be found at **Appendix B**. This goes into further detail regarding why these stakeholders have been considered appropriate for targeted consultation. We seek your feedback on the proposed list of stakeholders, and whether you would like us to engage with all of these groups on this work, or some of them.

Next steps

32. Following implementation of your feedback on the proposed structure of the discussion document and engagement approach, we will provide you with a draft discussion document on 2 April 2026 and seek your approval to begin targeted consultation. The table below outlines the key milestones of this work:

Table One: Key milestones for the digital identity discussion document

Milestone	Timeframe
Feedback on the structure of the discussion document and engagement approach	10 March 2026
Drafting of the discussion document	Mid – Late March 2026
Briefing with the draft discussion document seeking feedback and approval to begin targeted consultation	2 April 2026

[5] IA202611072 – *Approach to a discussion document on the privacy and security of digital identity information,* 17 February 2026.

Feedback on the draft discussion document	15 April 2026
Targeted consultation	20 April 2026 – 18 May 2026
Submissions analysis	19 May – 8 June 2026
Briefing with report-back on findings from targeted consultation	Mid-June 2026

Recommendations

33. We recommend that you:

33.1	**agree** to the proposed framing of privacy as relating to the governance of information;	**Agree/Disagree/Discuss**
33.2	**agree** to the proposed framing of security as relating to the structures and processes to do with the management of information;	**Agree/Disagree/Discuss**
33.3	**agree** to frame the questions of the discussion document around each stage of the digital identity 'life cycle';	**Agree/Disagree/Discuss**
33.4	**EITHER**	
	33.4.1 **agree** for the discussion document to focus on a comparison between the current centralised model of digital identity with a future decentralised model	**Agree/Disagree/Discuss**
	OR	
	33.4.2 **agree** for the discussion document to focus on the current centralised model of digital identity; and	**Agree/Disagree/Discuss**
33.5	**provide** feedback on to the proposed stakeholder list.	**Agree/Disagree/Discuss**

9(2)(a)

Hon Brooke van Velden
Minister of Internal Affairs
/ /

Appendix A: Proposed outline for the discussion document on the security and privacy of the Department's digital identity systems

Appendix B: Proposed stakeholder list for targeted engagement

Appendix A: Proposed outline for the discussion document on the security and privacy of digital identity information handled by the Department in a decentralised model of digital identity

This document provides an updated proposed outline for a discussion document on digital identity. You have told us that you wish for the discussion document to focus on how the Department will be able to trust and have confidence in third parties that work with New Zealanders' digital identity information that is held by the Department – for instance, a potential future passport credential.

One of the key pieces of legislation regulating digital identity in New Zealand is the Digital Identity Services Trust Framework Act 2023 (the DISTF Act), administered by the Government Chief Digital Officer and the Digitising Government Portfolio. The DISTF Act establishes an accreditation scheme for digital identity service providers, the Digital Identity Services Trust Framework (the Trust Framework). The Trust Framework will enable the use of digital verifiable credentials in New Zealand which are held and controlled by individuals.

We propose focusing the discussion document on how best the Department can ensure the privacy and security of digital identity in a Trust Framework landscape. **We have set out a potential structure for this below, for your consideration.**

Background

This section would give an overview of how the Department currently handles digital identity information. It would then provide relevant context for this work, including recent data breaches, and current work being led by the Public Service Commission. It would then cover the 'life cycle' of digital identity information and how this looks in practice.

The Privacy Act 2020 and the information privacy principles that it contains set out a legal framework to protect an individual's right to privacy of personal information during the different 'data life cycle' stages.

The Department handles core identity information for New Zealand, including name and birth information. The Department maintains that information in registers that serve as an authoritative source for that information.

Through initiatives like the Digital Identity Services Trust Framework, there is an opportunity for increased efficiency through digitising processes. The recent Manage My Health data breach has resulted in greater interest and scrutiny in the privacy and security of digital identity products and services across the private and public sectors.

Digital identity information has a life cycle

- Discusses the scope of the document – i.e., we are talking about core digital identity information that we collect in our BDM register, passports information, and citizenship records. This could also include information that is *derived* from information that we hold at the moment (e.g., that someone may be "over the age of 18", rather than just their date of birth).
- For digital identity information to be "used" it must be collected, stored, used, shared, and disposed of.

- This is done by both the Department and, in a decentralised digital identity landscape, will also be done by third parties. It is likely that, if the Department creates a credential following a user's request, that third parties will take personal identity information entrusted to the Department through the life cycle.

Information about the move towards a new framework

- RealMe and Identity Check are the main ways that we provide digital identity services.
- There are an increasing number of threats to our current systems, and technology – as well as people's expectations on our infrastructure – has progressed since RealMe was established.
- Digital credentials are a way for people to prove their identity and share information about themselves. This new way of information sharing would be complementary to existing Approved Information Sharing Agreements (AISAs) which allow for information sharing between signatories and Application Programming Interfaces (APIs), which allow for different software applications to communicate and share data.
- Digital credentials will rely on different pieces of technology to share that information.

Explanation of a future model

- We could issue a consent based, standards-based digital credential that people can store securely and share privately from a digital wallet on their mobile device. These credentials will not be direct digital copies of today's documents, but newly designed credentials that better meet people's needs to prove who they are in a modern, digital world.
- The Digital Identity Services Trust Framework provides a legal framework for the provision of verifiable credentials through an accreditation scheme for digital identity service providers.
- Even if the credential is not retained, some information may be retained by third party relying parties if they are not part of the Trust Framework.
- There is a movement globally for digital credentials to be a legitimate form of identity product, and there is an opportunity for us to move in this direction for the Department's products.

Overview of objectives

Privacy in the context of digital identity deals with the governance of how information is handled:

- Prioritising user control and consent;
- Ensuring that our systems in a decentralised system are complying with privacy best practice and are privacy-enhancing; and
- Digital Identity systems are transparent and accessible.

Security in the context of digital identity focuses on structures and processes:

- Ensuring that information is not stolen or misused;

- Ensuring that systems are up to date; and
- Ensuring systems as a whole are secure, especially when information is being shared with third parties.

A **third party** includes a wide range of potential people and groups, such as:

- Suppliers of information – such as an organisation that provides digital identity services, like a digital wallet or an external credential provider, to individuals. They could be both Trust Framework accredited or not;
- Relying parties (e.g., a supermarket, a financial lending institution, or a bar) who may not hold onto information but will process that information – and could potentially retain some of it. In the discussion document, where we refer to relying parties specifically we will name them as such.

Questions on each part of the life cycle

The questions will follow the life cycle and ask stakeholders how they think the Department should safeguard the privacy and security of the digital identity information it handles.

Collection

Under a digital identity system that is focused on credentials, the Department will need to be able to continue to collect information that can be credentialised :

- Under a decentralised model such as the Trust Framework, should there be additional safeguards as to when information is able to be collected (especially given that it could be later used by third parties)?
    - What is the Department's responsibility in protecting identity information once it sits within a decentralised ecosystem?
- Should the Department prevent the collection of its information by third parties through the use of digital identity products and services?
- Should the Department be able to collect derived information?
- Are there other future models you can identify that could better preserve privacy and security for the identity information the Department handles?

Storage

Under a decentralised model of digital identity, the personal information that we collect (and are custodians of) will be used by third parties, with the user's consent. As part of this, some third parties may wish to store this information.

- Is this something you see as appropriate for third parties to be able to do?
    - If so, what are the minimum 'must have' controls/evidence that should be required before the Department allows a third party to handle/consume a Department created credential? Given that the Trust Framework does not deal with relying parties, are there additional safeguards and requirements needed?

- If so, are there additional protections that need to be put in place to ensure that storage is safe (e.g., should Department created credentials work exclusively with Trust Framework accredited providers?)
- What visibility should the Department require (e.g., storage locations, incident reporting) to maintain confidence in a decentralised ecosystem? Do these need to go above and beyond the controls in place under the Trust Framework?
    - Should the Department require that any subcontractors/downstream parties handling Department credential data meet the same conditions as the primary provider? What visibility should the Department require across the supply chain?
- If not, is there a way for the Department to be able to completely prevent third parties from being able to store any information that is important to the Department?
    - Would this be possible to achieve under the DISTF?
    - If not, what are other, effective ways to prevent our information from being stored by third parties, through technological or other means?
- Are there additional considerations around how we can (or should) restrict third parties from storing our information?
    - Should the default be 'access-based verification' rather than third party storage or bulk transfer?
    - How should AISAs or API's be treated under the new system?
- How can we consider data sovereignty in an appropriate manner in a decentralised system? Are there requirements or conditions we should impose on third parties if they are storing information the Department handles?
    - Would third parties need to, for example, store Department held information specifically in New Zealand based servers?
- Should there be additional safeguards as to when the Department can and cannot store information?
- Are there other future models you can identify that could better preserve privacy and security for the identity information the Department handles?

Use

Under a decentralised model of digital identity, people will present their identity information to third parties. Before this information is presented to third parties, the information would have been processed by the Department into a credential.

- What are the minimum 'must have' controls/evidence that should be required before the Department allows a third party – including a relying party – to handle/consume a Department issued credential presented by a user?
- What visibility should the Department require (e.g., usage logs, incident reporting) to maintain confidence in a decentralised ecosystem?

- Will the burden on our infrastructure be greater if more individuals or third parties wish to use our information? Does this expose us to further risk of threats from bad actors?
- Are there additional protections that need to be put in place to ensure that that use is legitimate (e.g., should the Department created credentials work exclusively with Trust Framework accredited providers?)
    - If we allow third parties to use our information, are there additional requirements or conditions that we should impose on them on top of what is set out under the DISTF Act so that we are satisfied they will handle information appropriately? If so, what could those be?
    - Should access to sensitive credential attributes require demonstrated capability (training/certification) for both agency and third-party personnel? If yes, what should be mandatory?
- If a third party fails to meet expectations (assurance, incident response, retention), what consequences should apply (e.g., suspension, revocation, limitation to low sensitivity attributes) and who triggers them?
- Are there risks that arise where the Department uses information from other government agencies or third parties? If so, what safeguards should there be as to when the Department can use that information? What considerations do you see being in play?
- Are there other future models you can identify that could better preserve privacy and security for the identity information held by the Department?

Sharing

Under a decentralised model, the information that we hold would be shared by individuals to third parties through verifiable digital credentials. The Trust Framework regulates this through an accreditation scheme for service providers.

- What are the minimum 'must have' controls/evidence that should be required before the Department allows a third party to handle/consume a Department credential?
    - Should access to sensitive credential attributes require demonstrated capability (training/certification) for third-party personnel? If yes, what should be mandatory?
- What visibility should the Department require (e.g., onward sharing, incident reporting) to maintain confidence in a decentralised ecosystem?
    - Should the Department require that any subcontractors/downstream parties handling Department credential data meet the same conditions as the primary provider? What visibility should the Department require across the supply chain?
- Would you support a proposal for the Department to produce an identity credential? Why/why not?
- If the Department were to produce a credential, what safeguards should there be when that information is shared? Is there any information that we currently hold that should not be credentialised?

    - Should the default be 'access-based verification' rather than third party storage or bulk transfer? If bulk transfer occurs, what explicit justification/controls should apply?

- If a third party fails to meet expectations (assurance, incident response, retention), what consequences should apply (e.g., suspension, revocation, limitation to low sensitivity attributes) and who triggers them?
- Should the Department restrict information sharing with third parties?
    - Should the Department block identity information we hold (or a credential we have produced) from being shared with a person or organisation that is not accredited under the Trust Framework?
    - What is the best way to be able to achieve this? Or are there ways to share less sensitive information with non-Trust Framework providers?
- Are there other future models you can identify that could better preserve privacy and security for the identity information that the Department handles?

Disposal

Under a decentralised model we will likely have less control over when information is disposed or destroyed.

- What are the minimum 'must have' controls/evidence that should be required before the Department allows a third party to handle/consume a Department credential? Do these need to go above and beyond the controls in place under the Trust Framework?
- Should third parties be required to dispose of Department held information as soon as possible after it has been used? Do you think this should be an additional requirement under the Trust Framework?
- If third parties hold or use our information, should they be subject to the same requirements as the Department when handling digital identity information?
- Are there additional disposal considerations that the Department will need to consider under a decentralised model (e.g., do we have a responsibility for when we are disposing of information that that information is similarly disposed of elsewhere?)? Is that possible using credentials? Is that wanted?
- Are there other future models you can identify that could better preserve privacy and security for the identity information the Department handles?

Appendix B: Proposed stakeholder list for targeted engagement

Group A – Experts with views on the privacy and security of identity information

Data privacy and security consultants	
Simply Privacy	*New Zealand's leading privacy and responsible AI consultancy. Have deep expertise with the Privacy Act, and skilled at identifying risks and solutions.* • *Experience advising Government agencies.* • *Approved supplier on the New Zealand Government marketplace.* • *Approved independent evaluator for the Digital Identity Trust Framework.*
Wrybill Privacy	*Privacy professionals that advise private businesses, government agencies and NGO's on how to use personal information safely and to its full potential. Subject matter experts on New Zealand privacy law and biometrics.* • *Experience advising Government agencies.* • *Approved independent evaluator for the Digital Identity Trust Framework.*
ThreeBlackCats	*Specialist privacy consultancy for organisations in New Zealand, Australia and internationally. Helps businesses create privacy programmes that ensure ongoing compliance, governance, and risk management, including privacy breach management.* • *Approved supplier on the New Zealand Government marketplace.*
Gen Privacy (Amelia Harris)	*Amelia Harris has a background in law and privacy. She has specialist expertise in privacy, data protection and AI governance, and helps businesses protect their client's data and build trust.* • *Member of the Privacy Foundation New Zealand.* • *Member of the Wellington Privacy Officer Roundtable.* • *Member of the International Association of Privacy Professionals.*
CyberTrust Consulting	*Boutique consultancy firm based in Wellington, servicing clients worldwide. Specialises in digital identity and cryptography,[1] including creating comprehensive policies and standards that provide a governance framework for access control, authentication and identity lifecycle. Helps organisations navigate risks, align to global standards, and future proof their systems against emerging threats.*
PrivSec Consulting	*Helps start-ups, established companies, service providers and Government agencies to keep stakeholder's data secure. Provides a pragmatic approach and range of services to assess risk and keep data secure and private.* • *Experience advising Government agencies.* • *Approved suppliers within the AoG Consultancy and Professionals Services Marketplace panel.*

[1] Cryptography means securing information by transforming it into an unreadable format (ciphertext) using mathematical algorithms and keys, ensuring confidentiality, integrity, authentication, and non-repudiation. Only authorised parties with the correct cryptographic key can revert ciphertext back to plaintext.

Privacy Solutions Ltd	*Over 20 years of global experience assisting and training businesses and Government agencies to comply with all laws and regulations that impact on the management and protection of personal information. Consultants have a background in law and implementation of privacy and information management. Knowledgeable about compliance with the Privacy Act.* • *Experience advising Government agencies.*

Privacy oversight bodies	
Office of the Privacy Commissioner (OPC)	*The OPC will be key to engage with as the primary regulator for privacy law in New Zealand. The OPC was notified by Manage My Health of the data leak and is working on the resulting Inquiry.*
Office of the Ombudsman	*Plays a critical role in how agencies manage, release and protect identity information under the Official Information Act. Offers an independent mechanism for addressing issues on how information is handled.*

Cybercrime experts	
National Cyber Security Centre	*New Zealand's lead operational cyber-security agency. Protects Government systems, high-sensitivity data, and the national digital infrastructure. Helps prevent cyber-attacks.*
Computer Emergency Response Team New Zealand	*Receives and responds to cyber-incident reports. Remains across and provides advice on emerging cyber threats.*

Digital and technology sector experts	
PwC	*PwC has a cybersecurity service that focuses on helping businesses understand their digital risk, and provides advice, solutions and data-based assurance to manage these risks. Digital identity is one of their four "pillars" of the service.*
EY	*EY has data protection and privacy services that help organisations stay current with leading services in data security and data privacy. Their consulting also advises on complying with regulation and addressing emerging cybersecurity threats.*
New Zealand Technology Association	*Described as "New Zealand's united voice for technology" with a mission to ensure technology is trusted and safe. Brings together companies, sector groups and associations across digital identity, cybersecurity, AI, and data-driven industries – useful to provide cross-sector perspectives on data privacy concerns.*
Trust Alliance New Zealand	*TANZ aims to enable verifiable, trusted data sharing through a secure, decentralised digital framework, allowing participants to share data while retaining control over who can access it, for how long, and for what purpose. Able to consult on the privacy aspect of data governance.*

Microsoft	*Microsoft is integrated into the Government's digital infrastructure. The company actively collaborates with agencies on compliance, security, and data sovereignty obligations to ensure it is aligned (including with the Privacy Commissioner).*
Digital Identity New Zealand	*Not-for-profit organisation focused on uniting New Zealand's digital identity, trust, and assurance community. Members are committed to security, privacy, accessibility and equity in the development of digital identity and trusted credentials.*
Global Benefits Group	*International insurance services company that is one of the world's major digital identity verification providers, and fraud and risk prevention specialists.*
NEC New Zealand Ltd	*Provides identity verification services, accredited under the Digital Identity Services Trust Framework. Emphasises privacy first in their design, using biometrics with strong protections against identity fraud.*
MyMahi	*Digital identity platform used widely in New Zealand schools, providing the Digital Learner ID. Key insights on ensuring the privacy and protection of identity data for young people.*
Amazon Web Services	*Provides infrastructure for managing identity data that is compliant with privacy regulations and meets Government requirements.*

Legal experts	
Law Society of New Zealand	*Provides legal insights on how the handling of identity information is consistent with privacy regulations and legislation, and where there may be risks (including cybersecurity) and opportunities to strengthen the system.*

Group B – Businesses with experience handling identity information

Business	Interest
Banks *ASB, ANZ, Westpac, Cooperative Bank Ltd, TSB Bank Ltd, Heartland Bank Ltd, Kiwibank* *New Zealand Banking Association*	*Banks, financial services, and telecommunication companies have an interest and expertise in handling public identity information and may be able to provide insight into risks they have experienced, and possible solutions.*
Financial services *Financial Markets Authority* *Financial Services Federation* *New Zealand Financial Innovation and Technology Association*	
Telecommunications *Spark, One New Zealand, 2degrees*	

Group C – Users of identity information

User Group	Interest
E-Commerce *Payments NZ, Eftpos New Zealand, Eftpos Now, Smartpay, TradeMe, Fishpond, Mighty Ape*	*Companies that process identity data constantly as part of their business will have valuable insight into risks that they see at the user-end, such as consistent or emerging fraud patterns, and if there are other inconsistencies occurring between the Department's data policies versus the actual application.* *In terms of the discussion document, this feedback will be most relevant for the information 'used' and 'shared' parts of the digital identity information life cycle.*
Retail and hospitality *Retail New Zealand* *Food and Grocery Council* *Hospitality New Zealand* *Restaurant Association*	
Transport providers *Board of Airlines Representatives* *New Zealand Cruise Association* *Hire Industry Association*	
Mail and courier *New Zealand Post, New Zealand Couriers, DHL, Pack and Send*	
Interest groups *Digital Equity Coalition Aotearoa, Mana Mokopuna, Data Iwi Leaders Group, Disabled People's Organisations Coalition*	*These groups may have feedback and views on whether the Department's handling of digital identity information is trusted and safe. There may be specific risks that they have knowledge of – for example, identity fraud trends targeting a specific population group.*

Group D – Government agencies

Agency	Interest
Treasury, Public Service Commission, MBIE, NZTA, MSD, Justice, DPMC, IRD, Education, Ministry for Pacific Peoples, Te Puni Kōkiri (TPK), Ministry for Ethnic Communities, Ministry for Women, Office for Seniors	*These agencies will have similar interests and experiences to share in holding and protecting personal information on behalf of the public, and an interest in a conversation on the future of digital identity information. We have included population agencies which may have insights into specific identity fraud trends or risks.*

Document 7
Priority **Routine**

Internal Affairs
Te Tari Taiwhenua

Internal Affairs briefing

Hon Brooke van Velden
Minister of Internal Affairs

Title: **Proposed discussion document: Privacy and security of digital identity information**

Date: 9 April 2026

Key issues
We have finalised a draft of the discussion document: ***Privacy and security of digital identity information,*** attached as **Appendix A**, and seek your views on it ahead of targeted engagement with security and privacy experts which we intend to hold between 28 April 2026 and 25 May 2026. We have identified some small risks and potential mitigations for your consideration ahead of targeted engagement. These include the risk of material provided for targeted consultation being shared more widely and a risk of excluding relevant perspectives on these issues. Overall, with the proposed mitigations suggested we assess the likelihood of these risks as low.

Recommendations	Timeframe
Agree to targeted engagement using the attached discussion document OR **Advise** officials of further changes requested to the attached discussion document	By 22 April 2026

Contact for telephone discussions (if required)

Name	Position	Contact Number	Suggested 1st contact
Fergus Broom	General Manager Policy	9(2)(a)	✓
Kelsea Whyte	Policy Manager	9(2)(a)	

Return electronic document to:	9(2)(a)
Hukutai document reference	6KWWFJMNQWZ4-1227312906-6041
Ministerial database reference	IA202611659

Purpose

1. This briefing attaches a draft of a discussion document *Privacy and security of digital identity information*, attached as **Appendix A**, ahead of targeted engagement with security and privacy experts between 28 April and 25 May 2026.

2. We seek your views on the attached document, and whether you would like any additional changes made before engagement.

In mid-March 2026, we provided your office a proposed skeleton for a discussion document

3. The document we supplied your office was consistent with our previous discussions held on 9 March 2026 with you around the focus and target audience for engagement on key privacy and security issues around digital identity information.

4. Further to your feedback, in the skeleton document, we focused more specifically on the privacy and security of providing information that the Department holds on behalf of New Zealanders to third parties under a decentralised system. We have followed this same approach in the draft of the discussion document attached to this briefing.

5. The discussion document has been prepared to support targeted consultation, focusing on the lifecycle of digital identity information – e.g. the collection, storage, use, sharing and disposal of information. We have addressed your most recent feedback on the skeleton document, and added a separate section on the proposal for the Department to produce an identity credential on page 18 of the discussion document. Throughout consultation, we will seek views from technical privacy and security experts, as well as informed users, on how digital identity information that is held by the Department can be kept private and secure when sharing information with third parties. The goal is to understand how best to maintain the privacy and security protections over the information that the Department holds on behalf of New Zealanders.

Further to any additional changes you would like made to the document, we can begin targeted engagement with stakeholders

6. You agreed to our proposed list of stakeholders, supplied in advice dated 5 March 2026 [IA202611309 refers]. We have also included this list as **Appendix B** to this briefing.

7. We plan for targeted consultation to run from **28 April 2026 – 25 May 2026.** Relevant stakeholders have been split into the following expertise/interest groups:

   7.1 **Group A:** Experts with views on the privacy and security of identity information

   7.2 **Group B:** Businesses with experience

   7.3 **Group C**: Users of identity information

   7.4 **Group D**: Government agencies

8. We intend to publish the discussion document on the Department's website so that it is visible to all interested parties but will only ask for feedback on it from targeted stakeholders. During the consultation period, we intend to use the following methods of consultation:

8.1 **Contact via email with the discussion document and invite written feedback:** we will contact all stakeholders on the approved list with the discussion document and request written responses;

8.2 **Offer or request to meet with stakeholders 1:1** during the consultation period: officials will be available during the four-week period for meetings with stakeholders should they wish to connect with us directly, and discuss and/or offer verbal feedback; and

8.3 **We may also hold workshops with groups of stakeholders:** officials will hold a number of workshops and invite different groups of stakeholders to engage on the content in the discussion document. This is intended to encourage engagement and help with digesting technical information.

We have identified some small risks relating to targeted engagement and proposed mitigations for your consideration

9. We have identified some small risks relating to targeted engagement on this issue. These risks range from somewhat likely to occur, to very likely to occur. However, with the identified mitigations, we consider that the residual or actual risk of each of the below situations is low.

Risk of confusion about the purpose of the discussion document

10. Some stakeholders have recently been involved in Digital Identity Services Trust Framework (DISTF) consultations and may think this work revisits settled issues. The scope of this work is distinct to the Trust Framework as it focuses on core identity information that the Department hold on behalf of New Zealanders, rather than personal information more generally. Clear messaging will be used to distinguish this work from the Trust Framework.

Risk of stakeholder responses being influenced by DISTF accreditation interests

11. Some agencies may tailor responses based on their current or future accreditation experiences. This is difficult to fully mitigate but will be managed by clear messaging about scope and noting this contextual factor in analysis where relevant.

Next steps

12. Once we have incorporated any further changes you may have on the discussion document, we intend to publish it on the Department's website on 28 April 2026 and begin contacting the identified targeted stakeholders.

13. We will work with your office to support any announcements you may wish to make about this work.

14. Following the conclusion of engagement, we will analyse and collate the responses received, and will provide you with a report summarising the results of the engagement in mid-June 2026. Officials will be available to discuss any follow up actions you may wish to take as a result of the information gained through engagement.

Recommendations

a) **EITHER**

i. **agree** to proceeding with engagement using the supplied discussion document — **Agree/Disagree/Discuss**

OR

ii. **advise** officials of further requested changes to the discussion document before engagement takes place — **Agree/Disagree/Discuss**

Fergus Broom
General Manager Policy

Hon Brooke van Velden
Minister of Internal Affairs
/ /

Appendix A: Draft discussion document

Appendix B: Stakeholder list