Manatū Taonga Ministry for Culture & Heritage

MANATŪ TAONGA SITUATION REPORT	
EVENT NAME: Tuia 250 Voyage Trainee Privacy Breach	**Report Number:** #3 **(updated information in red)**
From: Bernadette Cavanagh, Chief Executive, MCH	**Date issued:** 25/08/2019 **Time issued: 2.45 pm**

Event details

There has been a digital privacy breach involving personal information collected by Manatū Taonga Ministry for Culture and Heritage (MCH). The breach affects 302 applicants to MCH's Tuia 250 Voyage Trainee programme. On Thursday 22 August, MCH became aware that images of applicants' identification documents such as passports, birth certificates and driver licences were available online. Applicants had submitted these documents to the Tuia 250 website as part of the online application process. The website is specific to the Tuia 250 commemoration and was procured from a web developer.

Response structure

- A Cross-Government Response Team has been assembled
- MCH is the lead agency and is being supported by incident response specialists from MSD
- The team is operating according to National Security System procedures
- MCH has received advice from a range of government agencies including Government Chief Privacy Officer, Office of the Privacy Commissioner, State Services Commission, Department of Internal Affairs, MBIE, MFAT, NZTA, GCSB and NZ Police.

Response objectives

- Build a comprehensive understanding of the situation and the information that has been compromised
- Minimise harm to affected individuals
- Communicate openly and transparently with affected individuals and the public
- Ensure the Ministry can deliver Tuia 250 securely and confidently.

Information security

- All copies of personal information were removed from the Tuia 250 website on Thursday 22 August
- Some images are still appearing in online searches
- We have been working with Google and other search engine companies to remove images from their caches
- MCH contracted Aura Information Security on Friday 23 August to analyse the server logs from the Tuia 250 website to assess what level of breach occurred
- Aura Information Security advised that content uploaded by users was widely accessible due to insufficient access controls on the Tuia 250 site
- Forensic testing indicates that 302 applicants' information had been accessed over the past four days, in some instances multiple times
- Given that the information has been available on the website since 2 June, the information could have been accessed many times prior to this

- The Chief Executive of MCH sent an email to all public service Chief Executives on Sunday morning advising them of this incident. Paul James, Chief Executive of DIA, also emailed Chief Executives reminding them of Government Chief Digital Officer guidance on security and privacy policy good practice, and asking them to provide assurance that they have adequate security and privacy controls in place for any public facing websites
- MCH has initiated testing of its other websites to be assured that there are no further vulnerabilities in our digital presence.

Communications

With affected individuals

- MCH (with the assistance of MSD, DIA and MBIE) has been calling all affected individuals to explain the situation, apologise and offer remediation, such as replacing compromised identification documents
- All 302 people have now been contacted. Most have been spoken to and the balance have received an email. We will continue trying to reach those people that we have not yet spoken to.
- MCH has established an 0800 number that affected individuals can call to discuss any concerns. DIA is staffing this 0800 number today, and MCH will manage the number from 6.30 am tomorrow
- DIA is establishing a special operations team to oversee all passport enquiries and renewals for affected New Zealanders. We will discuss with NZTA processes for renewing driver licences where this is requested by the individual.
- MCH has a dedicated page on its corporate website to keep people informed
- MCH will agree protocols with partner agencies to ensure all sensitive information shared during the response is appropriately managed
- Affected individuals have indicated a general understanding of the situation, and they are cooperating with the Government's process for replacement of identity documentation. The Ministry will be meeting the costs of replacement documents.

With media

- MCH issued a media advisory at 7.00am Sunday 25 August inviting media to a press conference at 11.00am
- The Chief Executive of MCH, Bernadette Cavanagh, fronted the media conference, supported by Paul James, Chief Executive of DIA and Government Chief Digital Officer, who answered questions related to government digital systems
- The media reporting has been largely factual to date, but media focus is turning to tracking down affected people and endeavouring to find out who the website provider is
- There have been a few requests for interviews this afternoon. The communications team is managing these requests
- MCH is monitoring and responding to social media posts
- We will continue to monitor media coverage and we will advise you of developments.

With stakeholders

- MCH will brief the Tuia 250 National Coordinating Committee on the response at a scheduled teleconference meeting tomorrow morning
- There is a range of other stakeholders that we will be contacting over the coming days, for example the crew of the Tahitian vaka.

Independent review

• Terms of Reference are being developed for a comprehensive independent review, to be commissioned by the Chief Executive of MCH, of the Ministry's decisions and processes relating to:
  • procurement and management of the website used to receive applications for the Tuia 250 trainee crew programme, and
  • the circumstances that led to the breach of applicants' personal information
• The scope of the review is likely to cover:
  • the governance and management of the Tuia 250 Voyage Trainee programme
  • the website procurement process and contract management
  • the security of the website itself
  • how decisions and processes differed from Government Chief Digital Officer guidance on security and privacy policy good practice.

Next steps
• A further situation report will be provided by 8.00pm Sunday 25 August.