Independent Inquiry into Unauthorised Disclosure of Confidential Information for New Zealand Transport Agency (NZTA)

Final Report

31 July 2020

Michael Heron QC

Contents

Executive Summary

1. NZTA's board (**Board**) commissioned this inquiry (**Inquiry**) to determine how confidential information ended up in the hands of the media. I was tasked with investigating the unauthorised disclosure of the confidential information, reviewing NZTA's internal procedures to see if appropriate protections were in place and making any relevant recommendations.

2. The full background, process, findings and recommendations of my Inquiry are set out in the body of this report, but the high-level points can be summarised succinctly.

3. The Inquiry has not revealed the source of the leaks. My investigation suggests that the leaks resulted not from a failing of information security or technology but rather, more likely, from one or more human actors who deliberately disclosed confidential information to the media.

4. Given the likelihood that the disclosure was caused by human actors, I suggest that the issues NZTA needs to consider are issues of people and culture, rather than technology (although technological and IT protections can also be improved). There are a number of measures that NZTA could take to address these issues. They include:

    a) Taking steps to improve internal culture, including addressing approaches to information management, the need to maintain confidentiality, and NZTA's role in upholding public confidence by treating information appropriately;
    b) Providing NZTA email addresses to Board members;
    c) Ensuring that Board information loaded to Diligent is watermarked with the name of the person using it and the date and time at which it was accessed;
    d) Ensuring that it is not possible to print or export documents from Diligent;
    e) Considering process for instructing Diligent to add and remove access rights;
    f) Ensuring that staff and Board members are trained in how to use and distribute confidential and sensitive information; and
    g) Undertaking further investigation into technological and IT tools that may make it easier for NZTA to track how its information is used and to prevent disclosure outside of NZTA.

Background and TOR

5. On around 18 October 2019 NZTA became aware that a document written by a former Board member had been leaked to the media. In the weeks that followed, media reports referred to the content of other documents that were confidential to NZTA. The information related particularly to NZTA's work on the Auckland Light Rail (**ALR**) project.

6. On 20 October 2019, Stuff.co.nz published an article by Thomas Coughlan entitled "Light rail reality: The six power point slides that stopped a city" containing reference to a document written by a former Board member that was circulated to the Board (as it was then constituted) in August 2019 (the **August 2019 Document**). That document was distributed by email to Board members and forwarded by the then Chair to the interim CEO. It carried with it an expectation of confidence (as with other Board material). It is not clear how it reached Mr Coughlan.

7. As more articles were published, it became apparent that other confidential information had been or was being leaked. The precise documents or information leaked was not clear.

8. It appears that the leaked information included Board materials from November 2018, including one official Board paper and one report on ALR. These materials would have been seen by and available to Board members, certain executive leadership team (**ELT**) members, relevant support persons, and ALR personnel. Again, it is not clear how the materials reached the media.

9. It has not been possible to further particularise the precise form of the material disclosed to the media. I asked Stuff to assist the Inquiry and it declined to do so (see further below).

10. This report will therefore refer broadly to "Documents" thought to have been leaked and to their "Unauthorised Disclosure". My enquiries have considered the type of information, the type of documents, and the access that people in and outside of NZTA would have had to them in the usual course of business.

11. NZTA takes the Unauthorised Disclosure seriously. The Documents were confidential and had not been released to the public. No party was authorised to do so by NZTA. Accordingly, its Board took action to initiate this Inquiry. On 31 October 2019 the Terms of Reference (**TOR**) for this Inquiry were finalised. The TOR are included in Appendix A to this report.

12. In conducting the Inquiry, I was required to:

    a) Meet with the Board Chair;
    b) Interview former and current Board members, senior NZTA personnel, and other relevant personnel;
    c) Review email and document management systems; and
    d) Review internal procedures alongside good practice standards and guidelines published by the State Services Commission.

13. The TOR mandated that I produce a report that commented on the Unauthorised Disclosure, the adequacy of internal processes and whether there were any other matters which ought to be considered by the Board.

14. This report will address the matters stipulated by the TOR. It will also, by necessity, make recommendations in respect of NZTA's internal processes and procedures, and raise certain matters that the Board of NZTA ought to consider further.

15. The focus of the Inquiry was on NZTA's internal systems and processes for data management and security, its internal culture, and the best practice model for protecting information. These are issues that face not just this agency, but public and private sector agencies generally.

Process

16. The process for the Inquiry was dictated by the TOR, the rules of natural justice, and the requirements of NZTA.

17. The first step involved discussing the relevant issues and concerns with NZTA staff and the Board Chair. This enabled me to understand the context of the Inquiry and led into the interview and document review stage.

18. I reviewed an array of material made available to me by NZTA, including internal NZTA policies, work completed by NZTA personnel and advisors, Board materials, and internal reports. I also reviewed the Documents. In several instances, I requested and was provided with copies of emails sent and/or received by agency members. I did not have access to private email accounts of any person, nor could I reasonably have reviewed all such accounts.

19. I also had the opportunity to interview more than 20 NZTA personnel (both current and former). Each interviewee was invited to an interview and provided with the TOR and the media release explaining that the Inquiry was underway. Where requested, sample interview questions were provided prior to the interview.

20. No one was required to accept the invitation to interview. I am grateful to those who spoke to me and helped me gain insight into NZTA's internal workings, the minds and concerns of its people, and the many facets of the agency.

21. Interviews were not recorded; they took place both in person and by phone. Notes were taken and then provided to interviewees for their review and clarification. Where necessary, the notes were updated in consultation with interviewees.

22. In addition, through NZTA I requested that certain internal forensic IT analysis be carried out in an attempt to determine whether (and, if so, how) certain NZTA information might have been disclosed by electronic means. No external IT review has been conducted to date. There was insufficient evidence to suggest that an external analysis would have assisted in these circumstances.

23. The rules of natural justice require that I do not make adverse findings against any individual or body without first giving them an opportunity to be heard.

24. For that reason, I provided a preliminary report dated 24 January 2020 to NZTA's legal team for review and assistance with minor details. A draft report dated 18 February 2020 was then made available for comment to certain NZTA executives and former Board members. Portions of the report were, likewise, provided to Stuff and Mr Coughlan. Another version was provided for the NZTA Board to review on 21 April 2020; NZTA requested that that version be finalised on 31 July 2020. Where necessary and/or appropriate, this report reflects the feedback I received.[1] External circumstances have caused some delay in producing this final report.

Participation of Stuff

25. I requested the opportunity to speak with Mr Coughlan of Stuff about the information that was disclosed to him, making it clear that I understood his (and Stuff's) wish to keep sources confidential and to protect the integrity of the journalistic process.

26. Media outlets such as Stuff have long been regarded in law and in the community as "surrogates of the public",[2] playing an integral role in protecting the public's interest in the broadest range of matters. They routinely hold themselves out as such. I suggested to Stuff that a failure to assist the Inquiry might be considered a failure to uphold its responsibility as such a surrogate, given that NZTA is a public entity and the protection of its information and the integrity of its systems is a public interest issue.

27. Nonetheless, I was informed (through Mr Coughlan's editor) that Mr Coughlan and Stuff would not assist. Stuff replied to repeated requests for assistance that it was comfortable in its refusal to assist in these circumstances.

Findings and Recommendations

28. Perhaps unsurprisingly, no one was able or willing to offer any direct evidence as to the source of the Unauthorised Disclosure of the Documents. The IT forensics were similarly inconclusive. Although some of the people I interviewed shared their suspicions, I have not uncovered any probative evidence that suggests a particular person or group is responsible. Accordingly, I cannot fairly reach any conclusion on that issue.[3]

29. I conclude that the most likely scenario is a deliberate "leaking" of information by one or more human actors. I reach that conclusion on the basis of several factors. The articles published by Stuff refer to a large "leak" of material from NZTA. No specific technological, process or systems failure has been shown to have caused the leaks. Each interviewee with

[1] This report was produced with assistance from Charlotte Agnew-Harington, junior barrister, and Lucy Heron, summer clerk.
[2] See, for instance, *R v Liddell* [1995] 1 NZLR 538 (CA) at 547.
[3] A reviewer in my position must base his or her conclusions on probative material – see Philip A Joseph, *Constitutional and Administrative Law in New Zealand* (4th ed, Brookers, Wellington, 2014) at [25.4.8] and *Re Erebus Royal Commission* [1983] NZLR 662 at 671.

access to the relevant material denied any action which could have contributed to the disclosure and no one advanced a theory other than deliberate leaking. The refusal of Stuff to provide any assistance or comment suggests its motivation is to protect a source or sources.

30. Although there is no probative evidence as to who leaked the Documents, a very small circle of people received the August 2019 Document. That Document was sent first to the then Board members, then forwarded by the Chair to the interim CEO. The August 2019 Document, like the others, was clearly not for disclosure or dissemination. Disclosure to the CEO was not expressly authorised but, in my mind, was understandable and reasonable in the circumstances.

31. Each of these recipients assured me that they did not have any hand in, nor any knowledge of, the Unauthorised Disclosure of the August 2019 Document. I have no reason to doubt each individual assurance I was given. The IT analysis did not provide any evidence to contradict that. Yet someone did disclose the material.

32. The Unauthorised Disclosure need not be the result of the actions of a single person. It is possible that multiple people were involved in passing confidential information to the media, either working together or as individuals. It was suggested to me that perhaps the leak of the August 2019 Document prompted the leak of other materials. That suggestion cannot be ruled out.

33. There are a range of possible motives that might have driven someone (or several people) to share information with the media. It was suggested that the leak might be politically motivated, intended to discredit the agency's Minister or the agency itself.

34. Similarly, it might be that the motivation came from a desire to reveal publicly the issues and considerations facing NZTA in regards to ALR. Other motives are possible, but speculation as to those is unhelpful.

35. Motivation aside, the factors listed below are, to my mind, likely to have contributed to the Documents being leaked:

    a) It was expressed to me many times, and often with regret, that NZTA has a culture of leaking information. That is not to say that the whole organisation leaks. Rather, it was suggested that NZTA confidential information often finds its way to the public domain, seemingly from sources within the organisation.
    b) NZTA documents are not always saved to NZTA's secure document management system (InfoHub), meaning that individuals may have locally saved copies that are not necessarily able to be tracked by NZTA.
    c) Board materials may be able to be printed and emailed and are not generally watermarked or otherwise labelled, such that they could be distributed without being able to be traced.
    d) Sensitive material is not always shared securely. For instance, sensitive documents may be distributed by unsecured emails (including to non-NZTA email addresses).
    e) Board members do not use NZTA email addresses and on occasion receive confidential material on their personal email systems (as with the August 2019

Document). In addition, it is apparent that multiple individuals may have access to a single email address, without there being a mechanism to determine who has accessed or dealt with a particular email.

36. In light of my findings and guidance from the public and private sectors (summarised in Appendix B), I consider there are a number of steps that NZTA could take to ensure it is better equipped to protect confidential information.

Improving internal culture around information

37. A key theme of the interviews I conducted with NZTA personnel was that NZTA has a "culture of leaking". It was expressed to me many times that although NZTA generally has sound information management practices and policies, no amount of policy or IT security can prevent motivated individuals from deliberately leaking information. This must be true of any organisation, whether public or private. There is no easy fix.

38. Many interviewees offered theories as to why they think the organisation leaks. Chief amongst these was the premise that individuals may leak information to sway public debate, to "expose" things that they do not agree with or are unhappy with, or to cause organisational or political harm.

39. This is primarily a cultural issue, and the Board and senior management of NZTA are best placed to determine how it ought to be addressed. From my interviews, it appears that part of addressing this issue will mean ensuring people feel they can express their views and have them heard in a process which is transparent and in good faith. This is quintessentially a matter for the current Board and management.

Providing NZTA email addresses to Board members

40. Unlike staff, NZTA Board members are not provided with NZTA email addresses. Anecdotally, this appears to be the position for many boards.

41. The provision of NZTA email addresses to Board members seems sensible and would provide NZTA with the ability to oversee emails sent to and from the Board. Although it would not prevent emails being sent to private email addresses, given that Board members are an integral aspect of the organisation and in receipt of extensive confidential information, it would seem to be a logical step to consider.

Using additional features within Diligent

42. I understand that it is possible to turn on settings in Diligent that apply watermarks showing the name of the person who accessed the document and when they accessed it. I suggest NZTA take advantage of this function and ensure it applies whenever a document is opened (not just when it is printed or saved).

43. This is an additional security feature that would mean that anything on Diligent that was printed or photographed would be imprinted with the name of the person who accessed it. This may dissuade anyone from seeking to disseminate Board information by using either of these methods.

44. Further (and as set out below), I understand that until recently it was possible for users to print and export (i.e. save locally) materials from Diligent. This function was, sensibly, removed following the Unauthorised Disclosure. I consider that removing such a function is sensible and would caution against its reinstatement. In the interests of maintaining the security of the agency's information and the integrity of its operations, I consider that security concerns necessarily need to bow to convenience of access.

45. It also came to my attention in the course of the review that Diligent receives and responds to requests and instructions from various people within NZTA. In most instances, I expect that this is unlikely to create problems. In certain circumstances, however, this could lead to people being given inappropriate access to information, such as where a blanket instruction to provide access is given without knowledge of all the possible (inappropriate) ramifications. I suggest NZTA reflects on whether more limited authorisation (or oversight over the same) regarding instructions to Diligent is appropriate. Consideration could be given to a single authorising person or position. I understand Diligent has processes for authorising appropriate representatives that will assist.

Providing further training

46. Relevant staff, contractors and Board members should as a matter of course be trained in how to identify, deal with, and protect confidential or sensitive information. They ought also be trained in the proper mechanisms for dealing with suspected information security breaches. I got the impression from interviewees that the level of understanding of NZTA procedures was variable and, in some cases, limited.

Considering further IT solutions

47. NZTA has its own IT expertise and will have its own ideas about the adequacy and next steps for developing its IT security framework. As outlined above it appears to me that the Unauthorised Disclosure had more to do with people than technology.

48. NZTA will no doubt continually review its IT systems from an information management and security perspective, with a view to ensuring these meet best practice standards and are adequate to ensure information security.

49. I understand that NZTA is already considering how it might create mechanisms for preventing disclosure of confidential material outside of NZTA (e.g., preventing the accidental or deliberate emailing of confidential information to a non-NZTA email address). These innovations require the development of IT solutions alongside internal policies and training that ensure NZTA personnel know and understand what is expected of them.

50. Putting these solutions in place requires time, new technology, and buy-in from staff, contractors, and Board members. NZTA is expected to continue to monitor and upgrade its IT systems regularly. External auditing may assist.

A note on dealing with disclosure

51. The recommendations above go to systems and processes for *preventing* disclosure. I comment, briefly, on the options available to organisations like NZTA when faced with a breach of confidentiality by human actors.

52. NZTA was warned that Stuff had received a copy of the August 2019 Document and that a story was being written about it. Questions have been asked about what NZTA's options were at that stage.

53. There are various actions that NZTA might have taken. One was to make no comment and provide no information. Another might have been to discuss the article with Stuff and seek to prevent or limit publication. Another might have been to immediately adopt a reactionary public relations campaign to negate or critique what was published by Stuff. There may have been a chance to seek an injunction preventing publication.[4]

54. Each of these options has its own pros and cons. In this case, the current Board Chair chose to accept that publication would go ahead and, rather than seeking to prevent publication, commissioned this Inquiry to focus on how the Unauthorised Disclosure happened in the first place. In the future, a different approach may be necessary to deal with a different situation.

55. Ultimately, when faced with a known disclosure, it will be for the Board and senior management to determine the appropriate response. Relevant considerations may include the extent of harm that will result from publication, the extent to which the proverbial cat is out of the bag, and the ultimate efficacy of each option. In this case, the response from NZTA was reasonable in the circumstances (although some argue a stronger response was warranted).

About NZTA

56. NZTA is an independent statutory body established by s 93 of the Land Transport Management Act 2003 (**LTMA**). It is a Crown Entity for the purposes of the Crown Entities Act 2004.

57. According to s 94 of the LTMA, NZTA's objective is to "undertake its functions in a way that contributes to an effective, efficient, and safe land transport system in the public interest." Its functions include managing, regulating, and funding New Zealand's land transport system, co-operating with approved organisations, and advising the Minister as requested.

58. The LTMA also sets out NZTA's "operating principles".[5] These stipulate that NZTA must meet various objectives, including exhibiting "a sense of social and environmental

[4] By way of example, the Commerce Commission recently obtained an injunction preventing publication of confidential and sensitive information that might have been accessed via stolen goods. See https://comcom.govt.nz/news-and-media/media-releases/2019/court-order-made-to-protect-confidentiality-of-information-contained-on-stolen-computer-equipment, accessed 20 January 2020.
[5] See section 96.

responsibility" and ensuring that it acts in a transparent manner when making decisions under the LTMA. NZTA also has a role to play under various other Acts, regulations, and rules.[6]

59. NZTA's functions include contributing "to an effective, efficient, and safe land transport system in the public interest".[7] In practical terms, this means that the agency builds and maintains New Zealand's roads and highways, regulates New Zealand's transport safety, and caters broadly for the nation's land transport needs.

60. NZTA employs around 1,500 people. It also engages a very significant number of contractors throughout the country.

61. Since 2017, one of NZTA's key projects has been developing the plan for ALR. NZTA received the mandate from Minster of Transport to do so in 2017; before then, the project had primarily been overseen by Auckland Transport and Auckland Council (with funding from NZTA).

62. ALR is seen as a key project for NZTA, as well as a key priority for Government and for Auckland's future development. The ALR project is led by a small, dedicated team within NZTA with close oversight from the Board. That team includes a number of NZTA staff, as well as contractors and secondees from other organisations.

63. NZTA's governance is directed by its Board, which itself is a creature of statute.[8] Board members are neither employees nor contractors. They are Ministerial appointees. The NZTA board is required to have between six and eight members, each of whom are to be appointed in accordance with the Crown Entities Act.[9]

64. Board members of Crown Entities owe duties to the Minister and to the relevant entity as both a board and as individuals.[10] They are required to act with honesty, integrity, good faith, and appropriate skill and care.[11] Further, section 57 of the Crown Entities Act provides:

> (1) A member of a statutory entity who has information in his or her capacity as a member that would not otherwise be available to him or her must not disclose that information to any person, or make use of, or act on, that information, except—
>
> (a) in the performance of the entity's functions; or
>
> (b) as required or permitted by law; or
>
> (c) in accordance with subsection (2); or
>
> (d) in complying with the requirements for members to disclose interests.
>
> (2) A member may disclose, make use of, or act on the information if—

[6] Details can be found on NZTA's website: https://nzta.govt.nz/about-us/about-the-nz-transport-agency/our-legal-framework/, accessed 12 November 2019.
[7] See further s 95 LTMA.
[8] Section 98 LTMA.
[9] Section 98 LTMA.
[10] Sections 58 -59 Crown Entities Act.
[11] Sections 54 – 56 Crown Entities Act.

(a) the member is first authorised to do so by the board or, in the case of a corporation sole, by the responsible Minister; and
(b) the disclosure, use, or act in question will not, or will be unlikely to, prejudice the entity.

Interviews

65. A key part of the Inquiry involved interviewing more than 20 past and present NZTA personnel, including Board and ELT members, and senior staff. All of these people were identified to me as people that may have had knowledge of the Documents and/or the Unauthorised Disclosure.

66. Interviewees were asked about their role within the agency, their access to and use of ALR information, the Documents, NZTA's information management processes, its culture, and whether they had any information about the Unauthorised Disclosure.

67. Every person I interviewed had a unique perspective and story. They were, without exception, helpful and cooperative participants in this process.

68. The interview process did not lead to the discovery of any evidence as to who or what was responsible for the Unauthorised Disclosure. That said, certain themes emerged:

    a) NZTA people generally have faith in each other and in the organisation. Each person I spoke to professed their incredulity that the Documents could have been leaked by anyone they knew, though at the same time had theories (in general terms) as to how or why the Documents might have been leaked. This suggests to me that on a person level, individuals within NZTA have confidence in each other, but that there may be room for improvement in terms of broader systems and culture.
    b) Nonetheless, it was often acknowledged that NZTA has been "leaking" for some time. Interviewees generally put this down to a cultural dynamic whereby highly skilled and passionate people would, on occasion, take it upon themselves to disclose sensitive information in circumstances where they considered that NZTA was not performing adequately or serving the public interest appropriately.
    c) NZTA's specific policies on information management are not well known. To the extent that people know they exist, they are generally unsure of details and of where to find the policies.
    d) Issues around access and navigability of InfoHub are deterrents against its use. As a result, it appears reasonably common for NZTA personnel to bypass the platform by saving documents locally, even though InfoHub is the official repository of NZTA information. This creates information integrity issues for the organisation and individuals.
    e) Diligent is a useful tool for Board members, though it could perhaps be better utilised to enable better tracking of documents.
    f) The fact that Board members do not have NZTA email addresses creates a level of vulnerability. The people I spoke to had varying views on the merits of Board members being given NZTA email addresses, but there was a general consensus view that the use of "personal" email addresses created some vulnerability and

diminished visibility (in contrast to the oversight NZTA enjoys over staff with agency email addresses).

g) Using hard copies of Board materials and other sensitive information makes it easy for information to be disclosed without being able to be traced. It would be unrealistic to suggest that an organisation like NZTA go entirely paperless, but some held the view that the time for hard-copies of Board materials has passed.

IT Analysis

69. The interview process was coupled with some forensic IT analysis. I requested that such analysis be undertaken to work out where the Documents thought to have been leaked were held within NZTA, and how they had been dealt with.

InfoHub document trails

70. I asked that NZTA report on how the Documents had been used and dealt with on the NZTA system. Some, but not all, of these questions were able to be answered. In particular, I requested that NZTA advise where the Documents were stored and how they were dealt with. NZTA's inquiries were able to detect relevant documents and emails.

71. Copies of some of the Documents were located within InfoHub. Where a Document had been saved to InfoHub, NZTA provided audit trails that showed when and by whom that Document was created, copied, printed, moved, opened or downloaded. Although this was useful, it did not reveal how any of the Documents reached the media.

72. The InfoHub searches were completed using the precise file names of the Documents thought to have been leaked to the media. It is possible that a Document also existed within InfoHub under another file name, and/or that materials *not* saved to InfoHub might have been leaked. Such documents would not (and could not) have been included in the searches. There are, therefore, obvious limits on this line of investigation.

73. NZTA was able to pull the InfoHub information from its system quickly and efficiently, which is a testament to the utility of the system and the staff who operate and use it. Although I note that InfoHub is not universally liked within NZTA, it did give me and NZTA visibility on how the Documents had been used.

74. As mentioned above, however, InfoHub has its limits. I understand that Board members do not have access to InfoHub. InfoHub is NZTA's official document repository, meaning that NZTA staff and personnel are generally expected to save all NZTA material on the platform. However, I was told many times that InfoHub is "clunky" and difficult to navigate, and that for this reason people store documents in other places, including local hard drives or cloud storage.

75. Although it is possible for NZTA to search for materials saved in such ways, it is harder to search across such accounts.

76. It is clear that the InfoHub tracking system is not a conclusive record of how, when, and by whom NZTA documents are dealt with. It is perhaps not unsurprising, therefore, that the InfoHub analysis could not provide definitive answers to the questions posed by the Inquiry.

Email Trails

77. NZTA's searches provided information as to emails and documents that sit within the NZTA system that might have been relevant to the Unauthorised Disclosure. Ultimately, however, email investigation did not provide an answer as to how or why the Documents reached the media.

78. Given that Board members do not have NZTA email addresses the email forensics were limited accordingly. Although I understand that the other Documents were made available via Diligent, the August 2019 Document was sent from one former Board member's private email address to the private email addresses of the other members. It was then sent to the Interim CEO's NZTA email address. The IT analysis has not shown that it was otherwise sent or distributed within NZTA's email system.

79. That is not to say that is has not been distributed outside of NZTA's online eco-system. Given the lack of NZTA email addresses, there is a significant limitation in transparency that exists between Board members and NZTA. There are no such limitations in respect of NZTA employees (including senior management). This raises the question as to whether NZTA Board members ought to be required to use NZTA email addresses.

80. Personal email accounts were not reviewed as part of this Inquiry. I did not have power to require those be made available, nor did it seem to me to be a useful exercise given the low likelihood of evidence being uncovered.

Obligations of trust and confidence

81. Other than as discussed, there was no material put to me to suggest a significant weakness in NZTA's procedures or systems. For reasons discussed above, it appears most likely that the Unauthorised Disclosure of the Documents was a result of human behaviour, rather than a technological failing or system attack.

82. It is trite to point out that individuals working within an organisation should not disclose that organisation's information without authorisation. Even more so, perhaps, to state that they ought not deliberately leak information to the media.

83. Both the law and commercial practice impose obligations on employees, contractors and Board members to ensure that confidential information is treated appropriately and is not disclosed without authorisation.

84. These obligations can be found in NZTA's Code of Conduct, as well as the contracts between NZTA and its employees and contractors. The Code of Conduct similarly governs the Board, but in the absence of a contract (given Board members are appointed, not contracted), a Board member's duty of confidentiality comes from the Crown Entities Act. People in

receipt of confidential information from NZTA may also be bound by common law and/or equitable duties of confidence.

Code of Conduct

85. NZTA's Code of Conduct sets out "the way we work here" for NZTA personnel. It makes it clear that NZTA is accountable to Government and works to "help create a better New Zealand". The Code of Conduct is stated to apply to everyone within NZTA, including employees, contractors and Board members. While it ought to be read as a whole, I quote those aspects of the Code that I consider are particularly salient to this Inquiry:

    a) We act professionally when commenting publicly on matters relating to the Transport Agency, and in a manner that reinforces our commitment to customers and the community.
    b) We follow the Transport Agency's policies and carry out our work unaffected by our personal beliefs.
    c) We act in a way that upholds the Transport Agency's reputation. We don't criticise current or proposed government policy, Transport Agency programmes or projects, or the activities of other government agencies.
    d) We ensure all information and statements provided to the media are authorised.
    e) We recognise that the standard of integrity expected from the state sector is sometimes higher than what's expected of other people.
    f) We understand that conduct outside of work may damage the trust and confidence the Transport Agency, our communities and stakeholders have in us. We make sure our non-work interests and activities don't harm the Transport Agency's reputation.
    g) We respect the authority of the government and do our jobs in a way that maintains their confidence and trust.
    h) We demonstrate honesty. We are truthful, open, accurate and authentic in our dealings with others.
    i) We disclose any situation that has the potential to impact on the Transport Agency's reputation, including any actual and potential conflicts of interest, criminal charges, bankruptcy or other matters.
    j) We look after our information as it is a Transport Agency asset that belongs to us all.
    k) We store our information in our information management system securely so it can be easily found and used by others, now and in the future.
    l) We take all steps to ensure that our systems and information remain secure and are not compromised in any way. We make sure we have a good working knowledge of the security and privacy practices that are relevant to our work and we follow them.
    m) We create and manage accurate, complete and accessible records of our decisions and actions and store them in our information management system.
    n) We ensure we treat information with care and only use it for proper purposes.
    o) We handle official information appropriately and respect people's rights to privacy.

86. The Code of Conduct contains a declaration, where it asks employees to acknowledge that they have been given a copy of the Code and the relevant guide before confirming that "as an employee of the Transport Agency, I shall comply with these documents and any modifications or updates communicated to me". There is space for the employee to then write their name, sign, and date the declaration.

Information and Data Management Policy

87. NZTA's internal Information and Data Management Policy (**Information Policy**) was drafted to "ensure staff understand their responsibilities in respect to creating, managing and using of information (including data and records) at the NZ Transport Agency". It applies to all staff, including contractors and people employed by third-party service providers. It also applies to information created or received by or on behalf of NZTA, and all systems and applications involved in the creation, management, and disposal of information.

88. Given the public nature of NZTA, the Information Policy operates in a broader public context. The Information Policy states that that context includes the Public Records Act 2005, the Privacy Act 1993, and the Official Information Act 1982.

89. The Information Policy states that "[a]ll staff have a responsibility to ensure the information created as part of their business activities is appropriately retained and available for use, and that compliance with information management legislation and standards is supported."

90. The obligation to "ensure information is appropriately protected and secure" is express: "[a]ll staff have a responsibility to protect information on behalf of customers and the Government and all staff are responsible for ensuring their management and use of information supports this."

91. According to the Information Policy, NZTA people are required to:

    a) Assess and appropriately classify information they create or manage. Unclassified information is open information. This is the default position.
    b) Restrict access to information "where necessary" (such as where information could lead to the identification of an individual, is commercially sensitive, or relates to national security).
    c) Follow the guidelines for managing restricted information.
    d) Ensure that access, use, and distribution of information is appropriate.
    e) Take steps to prevent unauthorised access, distribution, or use of information.
    f) Report information breaches (or suspected breaches).

92. The Information Policy is informed by and refers to other governmental guidance on information management, including Archives New Zealand's Information and Records Management Standard, the New Zealand Data and Information Management Principles approved by Cabinet, and the Government's Protective Security Requirements (**PSR**).

93. The Information and Records Management Standard was issued under s 27 of the Public Records Act. It is built around three key principles:

    a) Principle 1: organisations are responsible for managing information and records.
    b) Principle 2: information and records management supports business.
    c) Principle 3: information and records are well managed.

94. Minimum compliance requirements attach to each principle and are further articulated by way of examples that demonstrate the practical steps that might be required to achieve compliance. Of particular note:

    a) Staff and contractors must understand the information and records management responsibilities that attach to their roles, including relevant policies and procedures;
    b) Information and records management must be design components of all systems and service environments where risky or high value business is undertaken;
    c) Information and records management must be designed to safeguard information and records with long-term value;
    d) Information and records must be protected from unauthorised or unlawful access, alteration, loss, deletion and/or destruction; and
    e) Access to, use and sharing of information and records must be managed appropriately in line with legal and business requirements.

95. The principles approved by Cabinet are similarly broad and provide high-level guidance on how information should be managed. They include that personal, confidential, and classified information should be protected. Further, agencies are "stewards of government-held data and information and must provide and require good practices which manage the data and information".

Media Policy

96. NZTA's Representing Us in the Media Policy (**Media Policy**) sets out the "rules and responsibilities for Transport Agency staff when engaging or interacting with news media." It applies to all staff and contractors.

97. It stresses that NZTA is a "transparent, honest and responsive source of information" for the media. Under the Media Policy, the overall responsibility for managing national media issues sits with the Senior Manager, Media, while regional media managers have responsibility for regional issues.

98. The thrust of the policy is to direct all media queries and requests to certain staff members who are designated media spokespeople. Anyone who is a not a designated spokesperson is required to refer media queries to either a regional manager or the Senior Manager.

ALR probity regime

99. Since August 2019 the ALR team has had a "probity" regime. Under that regime, members of the team are subject to separate and distinct obligations over and above those found in the Code of Conduct. Those obligations include obligations of confidentiality. Consultancy services providers and other contractors assume further confidentiality and privacy obligations. Contractors may also be required to enter into non-disclosure agreements.

100. The probity requirements make it clear that the team operates on a "need to know basis", meaning that information is generally only available to those to whom it is directly relevant. Disclosure or dissemination of information about the ALR team's work is only to be

undertaken by the head of the team, or otherwise by another person at his or her instruction.

101. Individuals (being NZTA staff and individuals from supplier organisations) are required to confirm their agreement with the ALR probity requirements, at which point their name is added to a list that records those who are bound by the regime. The regime is overseen by the team's General Counsel and has been approved by independent auditors.

How NZTA personnel view their roles in relation to confidential information

102. The NZTA personnel I interviewed generally had a clear understanding of their obligations to protect NZTA information. Without reference to formal policy, contract, or other written rules, they know that confidential, sensitive, and Board information is information that they must protect. Particularly in respect to Board and ALR documents, the people I spoke to had not only a clear understanding of the confidentiality of the information they were dealing with, but also an instinctual or habitual awareness of the need to keep it confidential.

103. At a Board level, although formal policies may not be uniformly understood, there was no uncertainty as to the obligations of Board members to maintain the confidentiality of Board information. The Board members (former and current) were clear that they considered that the material made available to them in their capacity as Board members was to be treated as confidential and held in confidence. It was "for Board eyes only". The Documents were understood to be confidential and not for disclosure beyond NZTA.

Information and Systems Management

104. NZTA uses two main document management platforms: InfoHub and Diligent.

InfoHub

105. The InfoHub platform is used by NZTA to store and share data within the agency. It is the "official" repository of NZTA information. Board members do not have InfoHub access.

106. A person logging into InfoHub while connected to the NZTA system does so using single-factor authentication. When a user logs in remotely (i.e. when they are not on the NZTA network), there is a two-factor identification process that must be completed (once that process is completed the system reverts to single-factor security).

107. Files that are stored in InfoHub become trackable. This means that once a file has been uploaded onto the platform, it is possible to see who created, accessed, copied, moved, printed, opened or downloaded it.

108. NZTA staff are expected to use InfoHub for storing all agency-related material. It is common for staff to simply store information and data locally using other platforms.

109. The reluctance to use InfoHub stems from a lack of speed and user-friendliness. In particular, InfoHub's many layers and compartments mean it can be difficult to navigate and somewhat inefficient.

110. That being said, it was also expressed to me that InfoHub is a sensible and useful tool. It has clear utility value: it allows multiple users to access and edit files and enables NZTA to track how a file has been used and by whom. This focus on sharing and transparency is, obviously, appropriate within an organisation that is as large and multi-faceted as NZTA.

Diligent

111. The Diligent Boards App (Diligent) is, according to the diligent.com website, the "most widely used board portal in the world". It allows Board documents to be stored and accessed on a web platform that is remotely accessible. It allows for offline access.

112. When a user accesses material via Diligent they do so via either a web interface or an app (the app being the preferred option for most users). When a user logs in, the Board books will automatically download to the app, where they can be accessed and annotated while offline. No local file is created on the user's system.

113. NZTA Board members access Diligent using single-factor identification.

114. NZTA policy dictates that all Board material is to be loaded to Diligent in advance of Board meetings, although in practice Board materials on occasion are sent by email (due to time constraints). Such documents will not necessarily be password protected (as with the August 2019 Document).

115. Board papers and other materials make their way onto Diligent via the Board Secretary, who receives them (generally by email) from the person or team in charge. After attaching a Board paper number (to Board papers only) the Board Secretary will then upload the document to Diligent, where it can be accessed by Board members prior to, during, and after the relevant Board meeting.

116. Access to Diligent is carefully managed and is restricted to Board members, some ELT members, and certain staff with an administrative or Board-support function. That being said, issues can arise due to the fact that Diligent receives and responds to instructions from multiple people at NZTA. In future, I suggest that NZTA considers whether a single individual be authorised to instruct Diligent as to access rights, and confirms with Diligent that it will only action requests that have been made or confirmed by that individual.

117. Once uploaded, files sit in Diligent and remain accessible to Board members, meaning that unless expressly restricted prior to their first login, a new Board member will have access to documents that were uploaded prior to their appointment. Older materials may also be archived, meaning that the documents will not be available offline and (generally) that any notes a user has made on their copy of a document will be lost. Archiving does not, however, mean that access rights change. A user who is new to Diligent may still have access to archived documents, unless their access to a particular document or documents has been specifically restricted.

118. Board members who have resigned or retired lose their access to Diligent at that point.

119. Diligent prides itself on its ease of use and access, but also on its security. Diligent answered many questions about how its app works. Around the date of certain of the Documents:

    a) People with access to Diligent included Board members, the Board secretary, and certain other NZTA staff with an administrative function. Since then, certain users have changed.
    b) It was possible to print and export materials from Diligent.
    c) There was capacity within Diligent to download and save documents locally.
    d) Board members and senior staff had greater access and a broader range of functions available to them within Diligent.

120. Although the Diligent system makes it possible to track which users had what access rights, Diligent does not allow tracking of how someone has used a specific document. Diligent therefore cannot provide complete information as to the movements of a particular document.

121. Board members found that Diligent was useful and effective. Board members considered access and use rights differed within Diligent. However, the team at Diligent suggests, rather, that Board members would generally have the same or similar access rights. This is likely to be an issue of how different users understand and use the Diligent software. For instance, one Board member told me that it was possible to print documents from Diligent, while others said that they had no such capability.

122. Other than as discussed above, the information and systems management of NZTA does not appear to have directly contributed to the Unauthorised Disclosure.

123. To conclude, I have not seen evidence to suggest that a failure of technology caused the leaks. There are strengths and weaknesses within the various technological platforms utilised by NZTA and there are steps which can be taken to improve overall digital security. The biggest risks for NZTA appear to be of the human and/or cultural variety. NZTA's management is best placed to determine how those risks should be addressed.

Appendix A – Terms of Reference

TERMS OF REFERENCE FOR INDEPENDENT INQUIRY

Date: 31 October 2019

Background: There have been recent unauthorised public disclosures of information relating to the New Zealand Transport Agency (***Transport Agency***) and an unsolicited proposal made to the Government by NZ Super/CDPQ for the delivery of light rail in Auckland. This includes certain information referred to in media stories published on Stuff by Thomas Coughlan on and following 22 October 2019.

The information included confidential and/or commercially sensitive material and free and frank advice and opinions intended to support decision-making (***confidential information***).

The Board of the Transport Agency (***Board***) wishes to appoint an independent person to undertake an inquiry, which will involve:

(i) investigating the unauthorised disclosure of the confidential information (together ***Unauthorised Disclosures***),

(ii) reviewing the Transport Agency's internal policies, procedures, processes, practices and conduct expectations relating to information access and use (***internal procedures***) to provide assurance that appropriate protections are in place to prevent such disclosures being made, and

(iii) making any relevant recommendations to improve the internal procedures.

Inquiry: The inquiry will include:

- Meeting with the current Board Chair to discuss the scope, purpose and phasing of the inquiry.

- Interviewing Board members (including former Board members) and senior Transport Agency management personnel with known access to, or knowledge of, the information that is the subject of the Unauthorised Disclosures.

- Interviewing any other relevant persons.

- Review of access to, and other use of, email and document management systems, including Diligent and Infohub (used by the Transport Agency to manage and distribute information, including at Board level).

- Reviewing relevant internal procedures, and any general good practice standards or guidance provided by the State Services Commission, and compliance with them.

General: The inquiry may be carried out in phases, as may be agreed between the Board Chair and the reviewer. These terms of reference may be amended or supplemented by agreement between the Board Chair and the reviewer.

The Transport Agency will provide reasonable assistance to the reviewer in conducting the inquiry, including providing documentation and materials and specialist forensic support for the investigation phase, and encouraging its employees, contractors and former Board members to be available for interviews.

Any interviews conducted as part of the investigation phase will be carried out in a manner that complies with the principles of natural justice and any applicable laws. All interviews should be conducted consistent with the Transport Agency's commitment to the principles and objectives contained in the Transport Agency's behavioural codes of conduct and related policies. Otherwise, the reviewer shall be free to determine the procedure for the inquiry.

Report: Based on the above, the reviewer will then report regarding:

- The nature, manner and timing (if ascertainable) of any Unauthorised Disclosures and any other unexpected or unusual activity identified with respect to confidential or other information.

- Whether the actions or activities identified during the investigation phase complied with relevant internal procedures.

- The adequacy of the internal procedures for protecting and preventing unauthorised access to and use (including disclosure) of, confidential information, and including roles and responsibilities within the Transport Agency relating to such matters.

- Whether current internal procedures for such matters (in particular, Board-only information) is consistent with good practice for an organisation such as the Transport Agency and if not, what steps should be taken to rectify or improve the position.

- Whether any other related matter arising from the course of the inquiry (or any part of it) ought to be considered or investigated to enable a complete report to be provided to the Board.

If requested by the Board Chair, the reviewer will also make recommendations on the extent to which the report or extracts of it should be made public or made available (including in draft) for review any affected persons.

Timing: The reviewer is requested to commence, prioritise and report back findings on the investigation phase as soon as reasonably practicable after appointment.

The reviewer is to report draft inquiry findings to the Board (through the Board Chair) in writing by 13 December 2019 (or such other date as may be mutually agreed), for review by the Board and (as determined by the Board) any affected persons, and no later than 24 December 2019 (for final report).

Appendix B – Guidance on Information Management Best Practice

124. This Inquiry raises issues about how information – in particular, confidential information held by public bodies – ought to be managed. These issues are not unique to NZTA, nor to the public sector. Information management and security is a key priority for public and private organisations. As technology advances, the issues perhaps become more pressing, but so too do the tools for keeping information safe.

125. As part of this review, I have searched for guidance on how an organisation should best manage the information it holds. The guidance I have seen focuses more on the relevant principles than the specific processes. The most obvious theme is the need to keep information that is confidential (for personal, commercial, or security reasons) safe, given the interests and expectations of the parties who have provided it. The focus here is on information where there is a clear understanding or expectation of confidence. I summarise some of the guidance below.

State Services Commission

126. The State Services Commission (**SSC**) publishes guidance for state sector agencies and servants on how to manage sensitive information.

127. In *Maintaining Confidentiality of Government Information*,[12] the SSC emphasises that government information (including information held by an agency that is not within the public domain) ought to be treated with care in accordance with law and agency policy. It ought not be released without the authorisation of the agency's Chief Executive, and staff are required to "meet high standards to maintain the trust and confidence of the public and Ministers".

128. The SSC also advises that "Chief executives must ensure their agency's policies and procedures about handling information are followed", and that "all staff understand their obligations in dealing with information".

129. The *Standards of Integrity and Conduct* (**State Servants' Code**) came into effect on 30 November 2007. It offers high-level guidance as to how state servants are required to operate, given their unique role carrying out "the work of New Zealand's democratically elected governments".

130. The State Servants' Code is built on four key principles of fairness, impartiality, responsibility, and trustworthiness. The responsibility facet requires that state servants act lawfully, "treat information with care and use it only for proper purposes", and work to improve their agency's performance and efficiency. The trustworthiness element stipulates that they should be honest and avoid activities (privately or professionally) that may harm the reputation of their organisation or the state services generally.

[12] See https://ssc.govt.nz/resources/maintaining-confidentiality-government-information/. Published 30 January 2017 and accessed 20 November 2019.

131. Further guidance on the State Servants' Code includes *Understanding the code of conduct – Guidance for State Servants*.[13]

Office of the Privacy Commissioner

132. While the remit of Privacy Act 1993 and the Privacy Commissioner are primarily about personal information (meaning information about an identifiable individual), the Privacy Act provides information privacy principles that articulate how information ought to be handled by organisations.

133. The Privacy Act provides 12 information privacy principles which set out how an agency should handle personal information.

134. The Act advises that organisations must take reasonable steps to use and store information securely. For example, a locked cabinet may be required for physical documents, with password protection necessary for electronic files. It is important that information can only be accessed by the appropriate people, and information must be secure during transit.

135. Principle 5 explains that an agency that holds personal information shall ensure:

    a) That the information is protected, by such security safeguards as it is reasonable in the circumstances to take, against loss, access, use, modification or disclosure, except with the authority of the agency that holds the information;
    b) That if it is necessary for the information to be given to a person in connection with the provision of a service to the agency, everything reasonably within the power of the agency is done to prevent unauthorised use or unauthorised disclosure of the information.

136. Privacy Principle 11 also requires that organisations take care to ensure that personal information is not disclosed unless certain grounds exist.

Department of the Prime Minister and Cabinet

137. The Department of the Prime Minister and Cabinet (**DPMC**) states that "all information held by the government should be treated with care and protected from unauthorised or unlawful release."[14] Release can authorised by Cabinet, a Minister, officials with the relevant authority, or pursuant to an Official Information Act request.

138. Ministers and officials are required to take care when dealing with information they have about commercial entities that is not publicly available.

[13] See https://ssc.govt.nz/resources/code-guidance-stateservants?e198=action_viewall, accessed 20 November 2019.
[14] See https://dpmc.govt.nz/our-business-units/cabinet-office/supporting-work-cabinet/cabinet-manual/8-official-information-1, accessed 26 November 2019.

MBIE – business.govt.nz

139. Business.govt.nz is a platform hosted by the Ministry of Business, Innovation, and Employment (**MBIE**) and is designed to give small New Zealand businesses the tools they need to comply with the rules set by government.

140. It advises businesses to "plan to protect important data" and provides the following five-step strategy:[15]

    a) Identify everything that holds vital data. This is the information, records and systems that a business cannot do without, or would be most damaging if lost.
    b) Make protecting vital data a priority. Put extra security measures in place to protect sensitive data from different kinds of threats. This might be customer details, confidential agreements, financial records and any trade secrets or other intellectual property.
    c) Plan ahead for different scenarios. Map out a step-by-step approach of what to do if important data is lost, breached or hacked. You will be able to respond quickly — and have a better chance of minimising any negative impacts. Don't just think about it. Write it down.
    d) Make sure staff know what to do. This includes training or check-ins, and making sure passwords are protected and updated.
    e) Put your plan into practice. Test different scenarios regularly. Make any changes to your plan if it doesn't work as expected.

141. The website also discusses online behaviour, noting that "security breaches can often be caused by an employee doing something they shouldn't, usually inadvertently." It advises that if employees are using devices at or outside of work, the organisation should:

    a) Have an IT and social media policy so all employees know the relevant rules;
    b) Make sure employees are trained to keep data and systems safe; and
    c) Give staff "the right level of access" to systems and apps, and only give that access to staff who need it.

142. It says "staff awareness is key to preventing cybersecurity incidents and data breaches", and that everyone within a business needs to know how to keep data and systems secure.

Institute of Directors

143. The Institute of Directors (**IOD**) offers guidance as to obligations that directors (or board members) have in respect of confidential information. In 2017's *The Four Pillars of Governance Best Practice for New Zealand Directors* it sets out key considerations to help company directors navigate their roles.[16] The guidance primarily relates to the role and duties of directors, but helpfully sets out the steps that directors, and therefore

[15] See https://www.business.govt.nz/risks-and-operations/it-risk-and-avoiding-scams/protecting-business-data/, accessed 28 November 2019.
[16] See https://www.iod.org.nz/FourPillars, accessed 28 November 2019.

organisations more broadly, ought to take when it comes to ensuring the security of information.

144. The IOD suggests that boards should consider establishing committees specifically mandated to consider the risks associated with technology and information. Such committees would support the board's oversight of these areas. It goes on to state that "[i]ssues relating to company culture may also be important to this committee, such as appropriate policies and procedures and employee and board training and awareness".

145. The IOD expressly acknowledges that information security requires consideration of both technology and people. There is, inherently, a human element. The IOD quotes an anonymous technology CEO as saying "[b]usinesses lose sleep over the platform and the infrastructure but the reality is that your greatest security risks walk out your company door each night."

146. Further insights from the IOD's *Four Pillars* guidance include:

    a) Cybersecurity is a board-level concern;
    b) Company secretaries have a fundamental obligation not to misuse confidential information and should not divulge board information to, or discuss board matters with, management except where authorised to do so by the board;
    c) Issues around information leakage can be opportunities to consider "improved electronic storage of data and document control"; and
    d) Directors of private companies have certain obligations around their use of information, sourced from both the Companies Act 1993 and common law.

147. *Four Pillars* includes the IOD's Code of Practice for Directors, which states that "[t]his Code provides guidance to directors to assist them in carrying out their duties and responsibilities in accordance with the highest professional standards". In section 3.1 it states that "[d]irectors must observe the confidentiality of non-public information disclosed to them as directors and not disclose it to any other person without the authority of the board." Directors must also act in good faith and in the best interests of the company.

Policies of private companies

148. Some private companies publicise their approaches to information and security. For instance, both ANZ and Air New Zealand emphasise the importance of protecting their customers' privacy.

149. According to ANZ's Privacy Policy,[17] to protect information ANZ ensures its technology is up to date and that safeguards are in place to protect personal information from unauthorised disclosure. These safeguards include physical security (e.g. locks and security systems to protect paper and electronic data stores), and computer and network security methods (e.g. firewalls, identification codes and passwords). As well as this, ANZ says its security relations team keeps a close eye on online security systems around the clock, all year round.

[17] See https://www.anz.com.au/privacy/centre/policy/, accessed 28 November 2019.

150. Air New Zealand's Privacy Policy indicates it takes a similar approach.[18] Air New Zealand says it updates its privacy centre regularly to ensure it coincides with global laws and best practices. Like ANZ, Air New Zealand has devoted privacy and security teams tasked with keeping personal information safe. Air New Zealand claims it has physical and technological privacy measures in place (e.g. encryption) in order to combat the risk of unauthorised disclosure of information. Air New Zealand also says it trains employees in privacy, building a "culture of care" around managing personal information.

151. These companies show that a combination of physical and electronic privacy measures is essential, in conjunction with a culture that understands the importance of information management, to protecting an organisation's information.

[18] See https://www.airnewzealand.co.nz/privacy-policy-trust, accessed 28 Nov 2019.