INQUIRY INTO THE USE OF EXTERNAL SECURITY CONSULTANTS BY GOVERNMENT AGENCIES

Publication date: 18 December 2018

Doug Martin

Simon Mount QC

Contents

Appendices

Preface

This report responds to the Terms of Reference set for us by the State Services Commissioner, Peter Hughes, to address public concern about the use of external security consultants by government agencies to undertake intrusive activities.

The issues traversed in this Inquiry go to the heart of public trust and confidence in the state sector. Our objective has been to undertake a comprehensive and thorough inquiry to provide sunlight on the concerns raised. These were not only raised by organised interests such as Greenpeace and more established groups. They were also conveyed to us by representatives of community groups and individuals – ordinary New Zealanders who have grown concerned about the relationship between government agencies and external security consultants.

The Inquiry was provided with wide-ranging powers, including the ability to summons witnesses and to compel information. We would like to acknowledge the efforts of those employees in government agencies who worked hard to satisfy our many information requests. We would also like to acknowledge the response from the external security consultants themselves who have cooperated with the Inquiry.

We acknowledge the assistance and advice provided by the Office of the Ombudsman, the Office of the Privacy Commissioner, the Office of the Inspector General of Intelligence and Security, the Independent Police Conduct Authority, the Office of the Chief Archivist and the Private Security Personnel Licensing Authority.

We particularly acknowledge the assistance and support provided by Sarah Baddeley and Ben Craven from MartinJenkins and Associates, and Danielle Kelly from Bankside Chambers. We also appreciated the support of staff from the State Services Commission. They all worked hard to assist us to carry out the Inquiry, ensuring that it was completed in the required timeframe.

Doug Martin

Simon Mount QC

1 Executive summary

Background

1.1 In early 2018 public questions arose about whether Southern Response Earthquake Services Ltd, a government-owned company, had used Thompson and Clark Investigations Ltd to conduct surveillance of individual insurance claimants.[1] In response, the State Services Commissioner appointed Doug Martin to undertake this Inquiry, focusing on whether surveillance had taken place and whether there had been any breaches of the Code of Conduct for the State Services.[2]

1.2 In the following weeks Greenpeace questioned the apparently close relationship between the Ministry of Business, Innovation and Employment (MBIE) and Thompson and Clark. Media requests under the Official Information Act 1982 also led to questions about Thompson and Clark's relationship with employees at the New Zealand Security Intelligence Service (NZSIS) and the Ministry for Primary Industries (MPI). In early July 2018 MPI referred evidence of potential serious staff misconduct to the Serious Fraud Office.[3]

1.3 These developments led to the broadening of the Inquiry – first to include MBIE, then to include a wider group of 131 government agencies and subsidiaries subject to the Code of Conduct, together with the Crown Research Institutes. The Police were not within the scope of this Inquiry, but undertook their own internal review from October to December 2018.

1.4 On 26 July 2018, given the expanded scope, the State Services Commissioner appointed Simon Mount QC to join Doug Martin in conducting the Inquiry. Both Mr Martin and Mr Mount were delegated the Commissioner's powers under the State Sector Act 1988 for the purposes of the Inquiry.

1.5 The Inquiry's Terms of Reference are set out in Appendix 1. In summary, the Inquiry focused on two key questions:

- a How and why have government agencies used external security consultants, and in particular have external consultants been used to carry out surveillance?
- b What relationship have government employees and agencies had with Thompson and Clark?

1.6 In the absence of any universal definition, the Inquiry adopted a broad meaning of the terms 'surveillance activities' and 'surveillance', including any close observation of people, places, things or information, with or without the use of devices. The Inquiry's definition includes closely following or tracking people in public or private places. It may also extend to activities that interfere with a reasonable expectation of privacy. This definition may, for example, include joining a closed social media group under false pretences or an assumed identity if

1 See Patrick Gower, '$180k of taxpayer money used to spy on Kiwis after Christchurch earthquakes' (www.newshub.co.nz/home/new-zealand/2018/03/180k-of-taxpayer-money-used-to-spy-on-kiwis-after-christchurch-earthquakes.html).

2 The Standards of Integrity and Conduct for the State Services (www.ssc.govt.nz/code), in this report referred to as the 'Code of Conduct'.

3 MPI Statement regarding Thompson and Clark Investigations Ltd, 5 July 2018 (www.mpi.govt.nz/news-and-resources/media-releases/mpi-statement-regarding-thompson-and-clark-investigations-ltd/).

that enables the covert collection of information about an individual in breach of a reasonable expectation of privacy. The Inquiry recognises that this definition is broader than that adopted by many private investigators in the industry when focused on their specific regulatory regime. It is important to emphasise that the Inquiry does not suggest surveillance can never occur, but rather that it requires proper justification, management and oversight when carried out by a government agency. The definition is adopted for the purposes of this Inquiry, which focuses on the ways in which government agencies have used private investigators for surveillance activities. The Inquiry does not express any view about the way in which 'surveillance' should be defined in other contexts – for example in the regulatory regimes that apply to law enforcement bodies or private investigators.

1.7 The Inquiry undertook more than 100 interviews, including of several key witnesses under oath. Most participants provided information voluntarily, including Thompson and Clark Investigations Ltd, but the Inquiry also issued compulsion notices to Thompson and Clark to ensure completeness, and interviewed two witness under summons. The Inquiry also sought and reviewed documents from government agencies, and reviewed the results of internal investigations carried out by agencies at the Inquiry's instigation. In some cases, these involved comprehensive forensic searches of email and invoicing systems.

Thompson and Clark Investigations Ltd

1.8 Thompson and Clark is a private investigation and corporate intelligence company that specialises in security risk management. It was established in 2003 and its founding directors are former police officers now acting as licensed private investigators. The company bolsters its workforce with private investigators and analysts working on contract, many of whom have backgrounds in the New Zealand Police and related fields. Thompson and Clark's clients include private companies and government agencies.

1.9 Thompson and Clark describes its business as using an intelligence-led approach to 'clarify ambiguity in support of decision making under conditions of uncertainty'. The company has adopted the concept of a 'fusion centre' from the law enforcement and intelligence field. This approach brings multiple sources of information together in a single entity. The company positions itself as being expert in 'issue motivated groups', a label it has applied to various environmental, animal rights, peace and other 'activist' groups.

1.10 Thompson and Clark's activities were last considered by the State Services Commissioner in 2008. The company had used paid informants to infiltrate one or more groups on behalf of Solid Energy, drawing criticism from the government and the opposition. Following this, the State Services Commissioner warned departmental Chief Executives in February 2008 that purchasing covertly obtained information beyond what is required for statutory functions risks bringing the State Services into disrepute.

The use of external security consultants by government agencies

Surveillance

1.11 There was no evidence of widespread surveillance by external security consultants on behalf of government agencies.

1.12 However, the Inquiry did find evidence that nine agencies have engaged external security consultants to carry out surveillance to varying degrees since 2004. These were all forms of surveillance that required proper management and oversight to avoid the legal and ethical risks inherent in surveillance by external consultants. The Inquiry found that Southern Response, the Ministry of Agriculture and Forestry, Crown Law and the Ministry of Social Development breached the Code of Conduct.

Southern Response Earthquake Services Ltd

1.13 There was no evidence that Southern Response used Thompson and Clark to carry out targeted surveillance of individual claimants, or discriminated against disaffected claimants in settlements. However, the Inquiry found that over more than two years from 2014 to 2016, Southern Response engaged Thompson and Clark to attend five meetings of disaffected claimants. The initial motivation for this was to monitor and assess risks and threats to staff in the context of the highly charged post-earthquake environment in Christchurch. Southern Response mitigated those risks over time, for example through physical security measures and staff training in de-escalation strategies. Despite the reduced risk, the company continued using Thompson and Clark to monitor and in some cases record meetings. In this latter period, the primary benefit to Southern Response lay in monitoring its corporate reputation, rather than managing security risks.

1.14 Of particular significance, the Thompson and Clark contractor engaged on behalf of Southern Response attended and recorded several meetings described as ‘claimants only’ or ‘strictly claimants only’ and in particular two meetings led by lawyers, which involved discussion of legal options and strategy. Thompson and Clark provided Southern Response with a transcript of comments made at one of those meetings, and told Southern Response not to disclose where they had got it from, to avoid prejudicing the ability to obtain closed-source information. The comments were recorded by an unlicensed investigator, potentially unlawfully.[4] It was not possible to make findings on the legality of the recordings themselves,[5] because they were destroyed by the contractor and not retained by either Thompson and Clark or Southern Response.

1.15 Southern Response’s actions were inconsistent with Code of Conduct standards from the second meeting, when the company learned the contractor had recorded a closed meeting to

4 It is an offence for a person to act as a private investigator without a licence: Private Security Personnel and Private Investigators Act 2010, s 23. The individual who attended the meeting disputes that he was acting as a private investigator, as discussed further below. It is not the Inquiry’s role to determine whether the contractor was in breach of the Act.

5 If the recordings had intentionally captured private conversations between third parties, this could have breached the Crimes Act, s 216B.

discuss legal options, and allowed this to continue without proper controls in place.[6] The electronic recording of meetings in these circumstances was inconsistent with the Code's restriction on activity likely to harm the reputation of the organisation, as well as the Code's requirements to act fairly, impartially and responsibly. The use of a recording device involved an element of surveillance, and the contractor's implied representation that he was a claimant perhaps even bordered on infiltration. However, the Inquiry's findings do not turn on these conclusions – Southern Response was in breach of the Code whether or not the contractor's actions were a form of surveillance. The failure to keep records of the activities was also inconsistent with the Code's requirement to treat information with care.[7] The actions of the unlicensed private investigator were potentially unlawful. Southern Response relied on an assurance from Thompson and Clark in its proposal that all investigations would be conducted in accordance with the law, but the unusual nature of the engagement should have put Southern Response on notice of the need for further care. Finally, the recordings themselves may have been unlawfully obtained, although it was not possible for the Inquiry to make a finding on this given that the recordings were not retained.

1.16 While Southern Response was genuinely concerned about health and safety risks, the Inquiry does not consider that health and safety obligations require or justify surveillance of individuals or groups by external security consultants in circumstances such as these. The company's other actions to mitigate the risks were appropriate, including physical security measures, and staff training in de-escalation strategies. For more serious concerns, the proper response was to seek assistance from the Police.[8]

Ministry of Agriculture and Forestry

1.17 In 2005 and 2006 the Ministry of Agriculture and Forestry (MAF) engaged Thompson and Clark to attend two conferences of interest to the animal rights movement. The engagement flowed from concern about the potential escalation of protest action by the animal rights movement. The Inquiry accepts the concern was genuinely-held, if perhaps over-stated, based on isolated incidents of direct action and awareness of overseas trends.

1.18 At the first conference, MAF paid for Thompson and Clark to 'monitor' activists, likely involving surveillance, and to liaise with a paid informant. At the second, MAF contributed to the fees for a paid informant within the animal rights group.

1.19 Both engagements breached the Public Service Code of Conduct requirement to respect the rights of the public, in particular to respect the privacy of individuals.

1.20 The Ministry terminated the arrangement in 2008 after the State Services Commissioner's guidance referred to in paragraph [1.10] above. We did not see any evidence of further surveillance carried out by external consultants for the Ministry or its successor organisation

[6] The Inquiry was satisfied that the Board did not know the meetings were recorded electronically.

[7] Technically the breach of the Code of Conduct occurred only from 1 January 2015, when the State Services Commissioner applied the Code to Southern Response. This covered the public meetings recorded on 16 June 2015 and 12 May 2016. Before 1 January 2015, Southern Response's actions would have breached the Code had the Code applied directly to the company.

[8] Southern Response did contact the Police on a number of occasions during the relevant period, and in the Inquiry's view this was a sufficient response, together with the other steps taken.

MPI.[9] The amalgamation of MAF and other agencies to form MPI gave the larger organisation greater in-house investigative capability.

Crown Law Office / Child, Youth and Family / Ministry of Social Development

1.21 From approximately 2000, Crown Law acted on behalf of Child, Youth and Family to defend a civil claim brought by two brothers alleging they were abused in state care. From July 2006, Child, Youth and Family became part of the Ministry of Social Development. Prior to that it was a separate department.

1.22 In 2007, Crown Law, on behalf of MSD, instructed private investigators to assist with the case in the lead-up to trial. Crown Law's instructions were broad, including seeking any information that could be used to cross-examine a group of similar fact witnesses to be called by the claimants. Crown Law did not rule out low-level surveillance in the lead up to the trial. There were indications in the file that the investigators did use techniques involving low-level surveillance, or something close to it, together with a covert approach for at least one person of interest. The Inquiry found the broad nature of the instructions to the private investigators, without explicit controls to protect privacy interests, breached the Code of Conduct requirement to respect the rights of the public, individual privacy and avoid activities that might harm the reputation of the State Services.

1.23 It was not possible to make a definitive finding in relation to a specific allegation of surveillance of one of the claimants' witnesses, although the Inquiry could not rule out some form of close observation having occurred.

1.24 The Ministry of Social Development was aware of the potential use of low-level surveillance and a covert approach. The Inquiry did not see any evidence that MSD queried this or sought any assurance that individual privacy would be properly weighed and protected. Accordingly, the Inquiry found that MSD was in breach of the Code of Conduct, although at the lower end of the scale, given that Crown Law had primary responsibility to manage the litigation and direct the private investigators.

1.25 The Ministry of Social Development also informed the Inquiry that it used private security consultants for surveillance in four investigations into specific cases of fraud or suspected fraud. The Chief Executive assured the Inquiry that these engagements were appropriate and well-managed, and the Inquiry did not consider that there were grounds to indicate a breach of the Code of Conduct.

1.26 Finally, the Ministry used private investigators to conduct 'mystery shopping' exercises in 2010–2011 in relation to alleged predatory practices by traders targeting beneficiaries. The Inquiry did not consider these engagements breached the Code of Conduct.

Ministry of Business Innovation and Employment (MBIE)

1.27 In 2015, MBIE used external security consultants to undertake two surveillance operations while enforcing compliance in the residential building and construction sector in Auckland. The purpose of both operations was to obtain evidence of alleged non-compliance with statutory requirements. The operations were carried out by licensed private investigators.

[9] MAF also appears to have used an external security consultant for surveillance in the wildlife enforcement area in 2004 as part of the multi-agency Wildlife Enforcement Group.

The Inquiry considered that these operations did not give rise to concerns under the State Services Code of Conduct.

Accident Compensation Corporation

1.28 ACC has for many years engaged external security consultants to help detect and prosecute fraud. In some cases the external consultants carry out visual surveillance, including taking photographs and video of claimants to support prosecutions.

1.29 The ACC investigation unit has developed a standard operating procedure to govern the use of visual surveillance in these investigations. This 16-page document has been prepared with legal advice, and provides a detailed framework designed to ensure that surveillance is carried out lawfully and ethically. The Inquiry was not made aware of any recent concerns about ACC's use of surveillance in this context. The current processes governing surveillance appear to be well-developed and appropriate.

Maritime New Zealand

1.30 In 2008, Maritime New Zealand engaged external security consultants to conduct surveillance of a ferry to enforce the Maritime Transport Act 1994 following concerns raised about safety standards. The Inquiry considered that this operation did not give rise to concerns under the Code of Conduct. However, there should have been a written contract with appropriate safeguards.

Department of Internal Affairs

1.31 The Department of Internal Affairs uses external security consultants to locate and confirm the identity of people who are to be deprived of citizenship. Private investigators are used where the individual concerned is thought to be difficult to locate or might be seeking to avoid authorities. Surveillance techniques have been used in at least two of these cases. The Inquiry did not find a breach of the Code of Conduct. However, there should have been a written contract with appropriate safeguards.

Ministry of Health

1.32 The Ministry of Health engaged external security consultants to undertake public health enforcement functions, including 'mystery shopping'. The element of subterfuge arguably makes this a form of surveillance, but in this context it was relatively low-risk and well-controlled. In our view the contracts were managed appropriately. However, the arrangements have been in place for a significant period, are outdated, and should now be reviewed.

Cyclops Monitoring Ltd

1.33 Four government agencies – Land Information New Zealand, the Canterbury Earthquake Recovery Agency, Housing New Zealand and the Ministry of Education – engaged Cyclops Monitoring, a company associated with Thompson and Clark,[10] to monitor security cameras. Two of these engagements were for a brief trial period only.[11] Cyclops Monitoring takes live

[10] Until 6 July 2018 Cyclops Monitoring Ltd and Thompson and Clark Investigations Ltd had the same two directors. The two companies have at all times had the same two shareholders.

[11] The Ministry of Education and Housing New Zealand.

pictures from the client's cameras, and records and monitors those images in a central location using both automated systems and human oversight.

1.34 The service provided by Cyclops appears unobjectionable as far as any individual camera or site is concerned. However, privacy concerns could arise from a large network of cameras fed to a single source operated by a private company. In our view, considered privacy controls are required by government agencies to ensure their involvement in any such network is appropriate. The Inquiry did not find any breaches of the Code of Conduct, but further attention to this area would be justified in any future engagements.

Receiving information obtained through surveillance

1.35 As well as the direct forms of surveillance listed above, several agencies received information from Thompson and Clark, and in some cases that information may have been obtained or informed by surveillance. In particular, there was evidence that Thompson and Clark obtained information from surveillance in at least two categories:

a **Traditional surveillance:** Thompson and Clark conducted large-scale surveillance of Greenpeace through close observation, supported by extensive searches of the Motor Vehicle Register, and some access to other databases including the Driver Licence Register. Thompson and Clark's justification for searching the motor vehicle database was that they were acting on behalf of MBIE and the Police (although those agencies categorically denied that this was the case).

b **Social media monitoring under assumed identities:** Thompson and Clark monitored social media using false profiles, and told the Department of Conservation that it monitored 'closed sources of information for analysis'.[12] This suggested that Thompson and Clark had access to closed sources, and likely conducted social media monitoring under false pretences in a way that may in some cases have constituted surveillance under the definition used in this report.[13]

1.36 The Inquiry was concerned about the risk that some government agencies may have received information, for example about the capabilities or plans of Greenpeace, that was informed by surveillance. In the case of Greenpeace that surveillance was carried out for private clients in the oil and gas industry. This included information provided by Thompson and Clark as registered police informants as part of MBIE's 'Operation Exploration'.

1.37 Thompson and Clark's threat assessments, newsletters and situation reports about 'issue motivated groups' were also potential vehicles for information based on surveillance. While the information in the newsletters was typically described as 'open source', derived from open web pages, there was a risk that some information may have been informed by the types of surveillance described above. The agencies at greatest risk of receiving this

12 Email from Director of Thompson and Clark to officials at DOC and other agencies, 21 September 2016.

13 In the Inquiry's view, it may be a breach of a reasonable expectation of privacy for a person to join a closed social media group under a covert or false identity. This type of conduct may therefore be a form of 'surveillance', requiring appropriate controls and management, depending on the context and circumstances. Social media monitoring of this sort is not necessarily a breach of the Code of Conduct, as this depends on the purpose, context and management of the activity.

information were MBIE and NIWA, and the Inquiry saw some limited evidence that may have fallen into this category.[14]

1.38 While the Inquiry did not see widespread examples of government agencies receiving surveillance information, agencies need to be careful that their use of these types of services does not create a perception of tacit governmental approval of this form of surveillance.

Engagements not involving surveillance

1.39 Government agencies engage external security consultants for many purposes that do not involve surveillance. These include comparatively low-risk activities such as serving documents, acting as security guards, and assessing building security. The full range of engagements is summarised in Appendix 4.

1.40 The Inquiry was satisfied that engagements of external consultants in this broad category were appropriate, including:

a advice to Southern Response, the Department of Conservation, NIWA, Plant and Food and AgResearch on physical security threats

b services to Southern Response, NIWA and the Department of Conservation to train employees in de-escalation strategies

c advice to Southern Response, MBIE, the Department of Conservation, Te Papa, and MFAT (indirectly) on event security.

The relationship between government agencies and external security consultants

Professional distance

1.41 Government agencies and their employees must uphold appropriate standards of impartiality and objectivity in their dealings with private security consultants, in accordance with the Code of Conduct. The Inquiry found a number of areas in which this did not occur.

MBIE (New Zealand Petroleum and Minerals)

1.42 While senior executives at MBIE were attuned to concerns about the perception of bias towards the interests of the petroleum and minerals sector, interactions between MBIE (specifically New Zealand Petroleum and Minerals – NZP&M) and Thompson and Clark lacked the necessary objectivity and professional distance in two main respects.

1.43 First, MBIE's leadership of 'Operation Exploration', a key interagency governance mechanism, did not sufficiently ensure that Thompson and Clark, who were acting on behalf of the oil and gas industry, were kept at an appropriate arm's length from the operational and planning processes of the government's enforcement of the Crown Minerals Act 1991. MBIE

[14] See the discussion of the Threat Assessment provided to NIWA from paragraph [3.153] below. The full list of government clients receiving such reports was Southern Response, the Department of Conservation, the Ministry of Agriculture and Forestry, MBIE, AgResearch, Scion, GNS and NIWA. Thompson and Clark disputes providing information derived from surveillance to government clients, other than to Operation Exploration as registered informants.

uncritically adopted the construct of 'issue motivated groups' to guide the design of its enforcement function, and this was problematic: see paragraph [1.51] below. This mechanism enabled Thompson and Clark to embed itself as a crucial participant within the regulatory and enforcement function, despite the fact they represented private economic interests. This risked creating at least a perception of conflict of interest and was poor regulatory practice.[15]

1.44 Second, some interactions between MBIE staff and Thompson and Clark further indicated a lack of appropriate professional distance.

1.45 It was necessary for the Inquiry to look at the cumulative effect of the relationship, the actions that were taken, and the role MBIE as an organisation had to play in that dynamic. Overall the Inquiry found that MBIE's conduct, considered as a whole, breached the Code of Conduct by failing to maintain the level of objectivity and impartiality that the Code requires.

New Zealand Security Intelligence Service

1.46 The Inquiry reviewed a number of emails between an employee of the New Zealand Security Intelligence Service (NZSIS) and Thompson and Clark. These occurred in the context of the NZSIS's role in supporting the implementation of the Cabinet-approved Protective Security Requirements across government. The emails displayed a degree of informality and closeness that was inconsistent with the professionalism expected of state servants. The emails involved an NZSIS employee assisting Thompson and Clark's business development in a way that was related to his role but without an appropriate degree of detachment. These emails risked harming the reputation of the NZSIS and were therefore inconsistent with the Code.[16] We agree with the conclusion of an internal NZSIS review that any breach was at the lower end of the scale.

1.47 While the Inquiry received no evidence that the NZSIS directly engaged Thompson and Clark or any other external security consultants, the NZSIS identified a small number of other interactions and provided information about them to the Inspector General of Intelligence and Security for her review. The Inspector-General is considering these records separately.

Department of Conservation (DOC)

1.48 In 2015, the Department of Conservation engaged Thompson and Clark to carry out a security risk assessment of DOC's involvement in the Mystery Creek Fieldays.

1.49 Following that, the DOC employee responsible for the Fieldays stand exchanged a number of emails with a director of Thompson and Clark about business development opportunities for Thompson and Clark, including the names and contact details of people within DOC.

1.50 While aspects of the emails were, in hindsight, overly familiar, the Inquiry did not find a breach of the Code of Conduct.

[15] Through its participation in this group, MBIE received at least some information arguably obtained by surveillance. This was video surveillance footage taken by Thompson and Clark from a vessel at sea and later used in a successful prosecution of Greenpeace. Because the privacy interests at stake appear to have been minor, there is no issue of a possible breach of the Code of Conduct.

[16] The SIS did not become part of the Public Service until 28 September 2017: State Sector Act 1988, Schedule 1.

Issue motivated groups

1.51 As noted above, Thompson and Clark regularly employed the concept of 'issue motivated groups' in newsletters and threat assessments. Various groups were described in this way, including Save Animals from Exploitation (SAFE), Oil Free Otago, Climate Justice Taranaki, Farmwatch, the Green Party, the Mana Movement, Greenpeace and some iwi groups.[17]

1.52 While the label can have some potentially valid application, it can give rise to human rights concerns if it is applied indiscriminately – for example to those protesting legitimately and peacefully – and can take the focus away from risk-based analysis. The label can also de-legitimise groups and inhibit constructive relationships between the government and stakeholders or interest groups.

1.53 The Inquiry cautions government agencies, outside the Police and specialist intelligence agencies, against relying uncritically on the concept of issue motivated groups.

Secondary employment

1.54 The Inquiry found a number of instances where Thompson and Clark approached state servants to work for Thompson and Clark, and vice versa. In some cases, state servants agreed to work for Thompson and Clark while retaining their government jobs.

1.55 Secondary work for private security consultants is very likely to lead to a conflict of interest for any state servant working in a compliance, intelligence or enforcement function. These employees typically have privileged access to private information that must be treated with care and used only for its intended purpose. There is a high risk of actual or apparent conflict, and employment of this type is presumptively improper.

1.56 Two employees of the Ministry of Agriculture and Forestry undertook secondary employment for Thompson and Clark in breach of the Code of Conduct, one from 2011 to 2012 and the other from 2013 to 2014. Both have since left the state sector. The Serious Fraud Office is currently investigating this matter, and it is not the purpose of this Inquiry to make findings of civil or criminal liability.

1.57 More broadly, the Inquiry found that MAF did not have adequate measures in place to ensure all employees respected individual privacy, complied with the Code of Conduct, and avoided any secondary employment that presented a risk of a conflict of interest. MAF's organisational culture in the relevant division provided weak protection against abuse. The successor entity, MPI, has recently taken steps to identify its key fraud and corruption risks, including its open information environment. This remains a work in progress. The Ministry has also taken a number of other steps to protect the management of information, including establishing a Security and Privacy Directorate led by a Chief Security Officer.

1.58 In 2014, an employee from a justice sector agency approached Thompson and Clark about potential employment opportunities. Some months later Thompson and Clark offered the employee work on an 'open source research project'. By this time the employee was an intelligence analyst at Maritime New Zealand. The employee sought approval to do this work and the Chief Executive approved it. However, for unrelated reasons the employee did not take up the position.

[17] Iwi groups included those in areas of exploration activity and protest, including Northland, the East Coast and Taranaki.

1.59 Secondary employment of this nature would have constituted a conflict of interest and should not have been approved. In the circumstances, the granting of approval fell just short of breaching the Code of Conduct.

Access to NZTA databases

1.60 As the custodian of key databases including the motor vehicle register, the New Zealand Transport Agency (NZTA) engages with private security consultants to facilitate access to the motor vehicle register through a statutory approval process. The Inquiry examined, first, whether NZTA adequately managed Thompson and Clark's access to the motor vehicle register, and second, how Thompson and Clark apparently obtained private information from NZTA databases through an intermediary.

1.61 As to the first question, the Inquiry found that Thompson and Clark searched the motor vehicle register thousands of times over the years 2012–2017. NZTA's systems were not sufficiently robust to ensure this access was for proper purposes, and the available evidence suggests there were instances of improper access. NZTA has been working to improve its historically weak oversight systems, including commissioning an external review in 2017. It recently declined to renew Thompson and Clark's access to the motor vehicle register.

1.62 The second question involved an NZTA employee in 2011 supplying personal information to a MAF employee who, unknown to NZTA, passed it on to Thompson and Clark. The request appears to have originated with Thompson and Clark, who in this way improperly obtained access to personal information. The MAF employee obtained the information from NZTA in his capacity as a member of the 'Combined Law Agency Group' in Auckland (CLAG). This was and continues to be a multi-agency body designed to facilitate information sharing among agencies. At the time NZTA had no effective procedures in place to ensure that information shared through the CLAG was managed appropriately. That has since improved, with NZTA implementing a protocol in April this year to govern this information sharing. However, the failure to manage access to information in 2011 was a breach of the Code of Conduct by NZTA.[18] Circumstantial evidence suggests that there were further similar breaches in the following two years.

[18] NZTA did not treat information with care, as required by the Code. This was a breach by NZTA as an organisation; the Inquiry does not find that the individual employee breached the Code.

Consolidated list of agency-specific findings

Engagements involving surveillance

Breaches of the Code of Conduct

Southern Response acted inconsistently with the Code of Conduct from 13 March 2014 to 31 December 2014, and was in breach of the code from 1 January 2015 to 12 May 2016 when the Code formally applied to the company. On behalf of Southern Response, Thompson and Clark attended and recorded several closed meetings of insurance claimants that discussed options for legal action against Southern Response. The recordings were made by a contractor who was not a licensed private investigator, and the recordings may themselves have been unlawful, but it was not possible to make findings because the recordings were not retained – itself a breach of the Code.

The **Ministry of Agriculture and Forestry** breached the Code of Conduct by engaging Thompson and Clark to attend two conferences of interest to the animal rights movement in 2005 and 2006. At the first conference, MAF paid for Thompson and Clark to 'monitor' activists, likely involving surveillance, and to liaise with a paid informant. At the second conference, MAF contributed to the fees for the paid informant within the animal rights group. This breached the Public Service Code of Conduct requirements to respect the rights of the public and the privacy of individuals.

In 2007, **Crown Law**, on behalf of MSD, instructed private investigators to assist with a civil case alleging abuse in state care (the White case). Crown Law's instructions were broad, including seeking any information that could be used to cross-examine a group of similar fact witnesses to be called by the claimants. Crown Law did not rule out low-level surveillance in the lead up to the trial. There were indications in the file that the investigators did use techniques involving low-level surveillance, or something close to it, together with a covert approach for at least one person of interest. The Inquiry found the broad nature of the instructions to the private investigators, without explicit controls to protect privacy interests, breached the Code of Conduct requirement to respect individual privacy and avoid activities that might harm the reputation of the State Services.

The **Ministry of Social Development** was aware of the potential use of low-level surveillance and a covert approach in the White case. The Inquiry did not see any evidence that MSD queried this or sought any assurance that individual privacy would be properly weighed and protected. Accordingly, the Inquiry found that MSD was in breach of the Code of Conduct, although at the lower end of the scale given that Crown Law had primary responsibility to manage the litigation and direct the private investigators.

No breach found

MBIE's use of licensed private investigators to conduct surveillance in Operations Woodland and Lee in accordance with MBIE's regulatory responsibilities did not breach the Code of Conduct. However, there should have been a written contract for the work undertaken in Operation Lee.

The Inquiry was not made aware of any concerns about **ACC's** use of surveillance in the context of specific investigations into ACC fraud. The current processes governing surveillance appear to be well-developed and appropriate, and no Code breach was found.

The **Department of Internal Affairs** did not breach the Code of Conduct in using private investigators to conduct surveillance of people subject to cancellation of citizenship. However, there should have been written contracts with appropriate safeguards.

MSD's Chief Executive assured the Inquiry that the department's use of external security consultants for surveillance in four investigations into specific cases of fraud or suspected fraud were appropriate and well-managed. There do not appear to be any grounds for finding a breach of the Code of Conduct. The Inquiry also found the use of external security consultants to conduct mystery shopping exercises in 2010–2011 in relation to alleged predatory practices by traders targeting beneficiaries did not breach the Code of Conduct.

Maritime New Zealand did not breach the Code of Conduct when engaging a private investigator to conduct surveillance of a ferry when enforcing safety legislation. However, there should have been a written contract with appropriate safeguards

The **Ministry of Health** did not breach the Code when contracting mystery shopper services. The day-to-day management of the contracts was appropriate, but the Ministry should consider reviewing its contracting arrangements, as they are now outdated.

Various agencies' use of remote camera monitoring services by Thompson and Clark's associated company Cyclops Monitoring did not breach the Code of Conduct. However, further attention to this area would be justified in any future engagements.

Engagements not involving surveillance

DOC's engagement of Thompson and Clark to carry out security risk assessments and related services did not breach the Code of Conduct.

AgResearch's engagement of Thompson and Clark was adequately governed, responded to a specific set of threats, did not involve surveillance, and was not inconsistent with the Code of Conduct.

Southern Response acted reasonably in engaging Thomson and Clark to provide services other than surveillance, including threat assessments and security reviews. There was no breach of the Code.

NIWA's direct engagement of Thompson and Clark did not give rise to concerns under the Code.

The **Ministry of Health's** engagement of external security consultants to support regulatory and enforcement activities did not give rise to concerns under the Code of Conduct. However, the arrangements have been in place for a number of years and should now be reviewed as they are outdated.

Ōtākaro's engagement of Thompson and Clark for physical security reviews and related services did not give rise to any concerns under the Code of Conduct.

MBIE's engagement of Thompson and Clark to provide security services at a petroleum conference did not give rise to any concerns under the Code of Conduct.

MFAT's involvement in a third-party engagement of Thompson and Clark in relation to a TPP protest did not give rise to any concerns under the Code of Conduct.

Te Papa's engagements of Thompson and Clark for security reviews were low-risk and short-term, and did not give rise to concerns under the Code of Conduct.

Plant and Food's engagements of Thompson and Clark were low-risk and short-term, and did not give rise to concerns under the Code of Conduct.

The relationship between government employees and agencies and Thompson and Clark

Breaches of the Code of Conduct

MBIE's management of its regulatory responsibilities in the petroleum and minerals area, compounded in some instances by employees not maintaining an appropriate professional distance, contributed to a perception of bias by some stakeholders and was evidence of poor regulatory practice. Considering its conduct as a whole, the organisation breached the Code of Conduct, by failing to maintain the level of objectivity and impartiality that the Code requires.

The email contact between an **NZSIS** employee and a Thompson and Clark Director risked harming the reputation of the NZSIS and was therefore inconsistent with the Code. The Inquiry agrees with the conclusion of an internal NZSIS review that any breach was at the lower end of the scale.

Two former **employees of MAF** carried out secondary employment with Thompson and Clark in breach of the Code of Conduct. The same employees accessed NZTA information on behalf of Thompson and Clark, directly or indirectly, breaching individual privacy and in breach of the Code of Conduct requirement to treat information with the level of care expected by the public.

NZTA's prior lack of oversight of authorised access to the motor vehicle register, and the lack of formality and care in information sharing through the Combined Law Agency Group (CLAG), left both those forms of access open to exploitation, and breached the Code's requirement to treat information with the level of care expected by the public.

No breach found

Aspects of emails between a **DOC** employee and Thompson and Clark were overly familiar, but the Inquiry does not consider that they involved a breach of the Code of Conduct.

The Chief Executive of **Maritime NZ** gave approval for an employee to undertake secondary employment with Thompson and Clark. Given the nature of the employee's work as an intelligence analyst and the risk of a conflict of interest, the application should not have been approved. In the circumstances this fell just short of breaching the Code of Conduct.

2 The legal and ethical framework

Overview

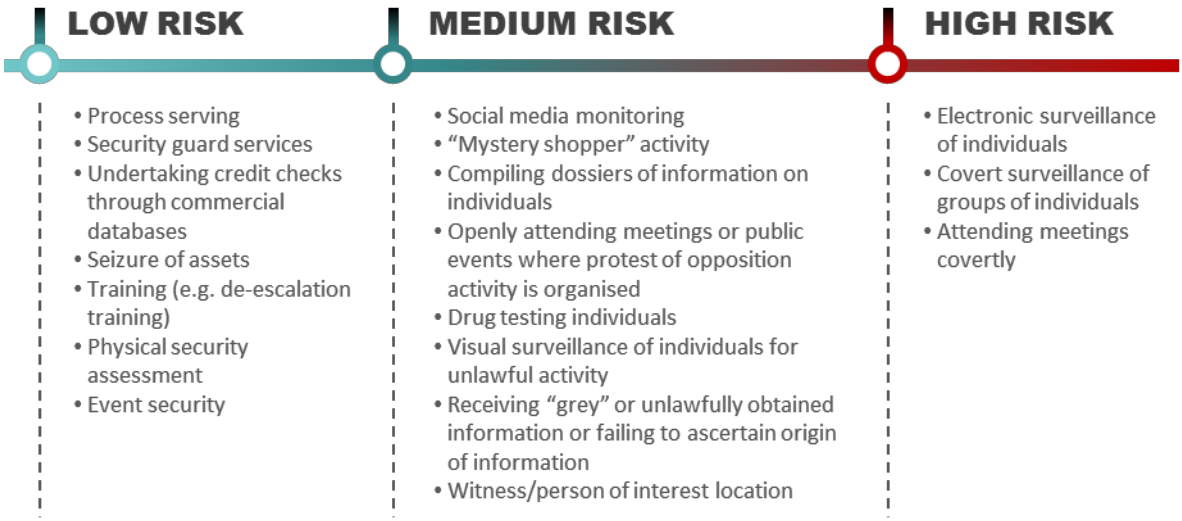
2.1 The Inquiry's starting point is that any engagement of or interaction with external security consultants must be:

- lawful
- consistent with the Code of Conduct
- governed, managed and administered in accordance with good practice.

2.2 Many routine engagements of external security consultants are low-risk, in the sense that they are unlikely to be unlawful or to lead to breaches of the Code of Conduct. Other activities carry higher legal and ethical risks. These higher-risk activities may be justified and proper, but they require more careful management and controls.

2.3 In broad terms, the types of engagement can be represented on a continuum from low to high risk:

Figure 1: Risk-based model of engagement



2.4 Again in broad terms, the key factors that increase the level of risk include:

- The use of surveillance devices
- Covert activity
- The use of false pretences
- Where the purpose is broad, or not related to law enforcement or a specific threat to staff

- An activity that is highly intrusive, given the time, place and circumstances
- Politically motivated activity, or activity that engages human rights
- Activity that is commissioned by an in-house group without sufficient oversight or controls.

2.5 As the legal and ethical risks increase, it is important to implement appropriate controls, such as:

- Ensuring the activity is well-documented, with clear instructions and parameters
- Ensuring that records are preserved
- Undertaking a legal review of purpose and controls
- Requiring senior approval or sign-off
- Explicitly requiring compliance with the State Services Code of Conduct
- Complying with guidelines for sensitive expenditure

The legal framework governing surveillance

2.6 The Inquiry is required to report on 'surveillance activities' carried out on behalf of government agencies. In general, surveillance involves close monitoring or observation of people, places, objects or information. However, the precise meaning of the term 'surveillance' can vary with context. In this Inquiry, the focus extends to surveillance activities that have the potential to interfere with reasonable expectations of privacy. This may include:

- Surveillance using electronic devices, such as video cameras or audio recorders
- The use of tracking devices on people or property
- Close or sustained in-person observation, with or without the use of devices
- Covert activity of any sort.

2.7 The Inquiry's approach includes following and close observation of people in public places, whether or not a reasonable expectation of privacy would be found to exist. The Inquiry's approach is adopted for the purposes of this Inquiry, which focuses on the ways in which government agencies have used private investigators for surveillance activities. The Inquiry does not express any view about the way in which 'surveillance' should be defined in other contexts – for example in the regulatory regimes that apply to law enforcement bodies or private investigators.

2.8 The Inquiry's interpretation of the concept of surveillance may extend to include social media monitoring where this is done covertly or using false identities – for example where a closed group is joined under false pretences or an assumed identity if this allows the covert collection of information about one or more individuals, in breach of a reasonable

expectation of privacy. Such activity therefore warrants appropriate management and oversight.[19]

2.9 The New Zealand Law Commission's recent review of the Search and Surveillance Act 2012 concluded that social media monitoring should be governed by a 'policy statement' regime,[20] because it may breach reasonable expectations of privacy. The approach adopted in this report focuses on the narrower class of social media monitoring of closed groups using false identities. This is a breach of the terms of service for major social media platforms including Facebook[21] and LinkedIn.[22] The Inquiry does not suggest that all social media monitoring automatically constitutes surveillance, but focuses instead on the narrower class of monitoring closed groups with assumed identities, which the Inquiry considers requires particular management and oversight.

2.10 The primary justification for surveillance by government agencies is to uphold the law by detecting or preventing breaches of the criminal law.

Surveillance activities by government agencies

2.11 Any use of surveillance by the government must be lawful. While not all surveillance by government agencies requires a warrant or specific statutory authority,[23] government surveillance must comply with the general law. The law in this area is complex and developing; however, it is clear that surveillance by government agencies without a warrant may be unlawful if it involves:

a **A criminal offence** – A surveillance activity will be a criminal offence if it involves a person using a device to record a private communication between other people,[24] or making an intimate visual recording of a person.[25]

b **Trespass to land or property** – A surveillance activity will be unlawful if it involves entering land without the express or implied permission of the owner or occupier.

c **An unlawful invasion of privacy** – A surveillance activity will amount to the tort of invasion of privacy if it is a highly offensive and unauthorised intrusion into seclusion in breach of a reasonable expectation of privacy.[26]

19 The Inquiry considers this broader approach is appropriate in the context of the present inquiry but expresses no view whether this type of surveillance should be regulated under the Search and Surveillance Act. In particular, it is acknowledged that there is scope for disagreement about the boundaries of privacy in the social media context.

20 New Zealand Law Commission, Review of the Search and Surveillance Act 2012, NZLC R141: https://www.lawcom.govt.nz.

21 < https://www.facebook.com/terms.php>.

22 < https://www.linkedin.com/legal/user-agreement#dos>.

23 On this point there is some dissent, but it is the position of the leading cases: see *Hamed v R* [2011] NZSC 101, especially per Blanchard J; and *Lorigan v R* [2012] NZCA 264, from [28].

24 Crimes Act 1961, s 216B.

25 Crimes Act 1961, s 216H. Other activities incidental to surveillance that may amount to criminal offending include being on property without lawful excuse (Summary Offences Act 1981, s 29); and peeping or peering into a dwelling house, or loitering near a dwelling house at night (Summary Offences Act 1981, s 30).

26 See *C v Holland* [2012] NZHC 2155; [2012] 3 NZLR 672; and *Faesenkloet v Jenkin* [2014] NZHC 1637. For example, in *C v Holland* a video taken of a woman in a shower, without her knowledge, was held to be an invasion of privacy under this tort.

d **Unlawful warrantless surveillance** – Surveillance of a type that specifically requires a surveillance device warrant under the Search and Surveillance Act will likely be unlawful if carried out by the government without a warrant. This includes the use of a surveillance device to observe a private activity in private premises, or a private activity in the curtilage (outside area) of private premises for more than a specified period.[27]

e **An unreasonable search in breach of s 21 of the New Zealand Bill of Rights Act 1990** – A surveillance activity by a government agency will be a search where it intrudes into a reasonable expectation of privacy, and the search will be unreasonable where it is unlawful,[28] or where the intrusion is disproportionate to the agency's law enforcement or other interest in the intrusion.[29]

f **An unjustified intrusion by the state into other rights** – Broad surveillance activities by a government agency may intrude into or limit other rights under the New Zealand Bill of Rights Act, such as the rights to freedom of expression (including the right to protest and advocate), freedom of association or assembly, and freedom from discrimination (particularly discrimination on the grounds of political opinion).[30] Where the activity does limit one of those rights, the intrusion must be reasonably justifiable in light of the agency's law enforcement or other interest in the surveillance.

g **Collection of personal information in breach of the Privacy Act 1993** – A surveillance activity may breach the privacy principles set out in the Privacy Act, particularly if the information collected through surveillance is not necessary for a lawful purpose connected with the function of the government agency, or if the surveillance activity is unlawful or unfair, or intrudes unreasonably on the personal affairs of the individual concerned.[31]

2.12 Government agencies carrying out surveillance activities must also comply with laws and guidelines applying to general government activities, including the requirements to:

- Keep accurate records of their affairs[32]

27 Search and Surveillance Act 2012, s 46. Also any use of a tracking device; the use of a surveillance device that involves trespass to land or goods; or the use of an interception device to intercept a private communication.

28 Unlawful searches will usually breach s 21: see *Hamed v R* [2011] NZSC 101.

29 Although the test is 'reasonableness', not 'proportionality', it is clear that an assessment of whether a search is 'reasonable' involves balancing the degree of intrusion against the purpose of the intrusion: see *Hamed v R* [2011] NZSC 101 at [172] per Blanchard J; and *R v Jefferies* [1994] 1 NZLR 290 (CA), at 319 per Thomas J: 'What is required…is an assessment as to whether, in the particular situation, the public interest in being left alone by government must give way to the government's interest in intruding on the individual's privacy in order to advance its goals, notably those of law enforcement.'

30 These rights are recognised in the New Zealand Bill of Rights Act 1990 (ss 14, 16, 17 and 19); and can only be subjected to limits that are prescribed by law and demonstrably justified in a free and democratic society: s 5. State surveillance activity may limit these rights if, for example, members of the public feel unable to express controversial political views, or unable to participate in protest activity, because of a fear of being monitored by the state. (Note also the Human Rights Act 1993 and the Intelligence and Security Act 2017.)

31 Privacy Act 1993, s 6; especially principles 1 and 4, but see also the other principles dealing with collection and use of personal information. Personal information is defined as 'information about an identifiable individual', which may capture a range of information that may be gathered through surveillance. While s 11(2) of the Privacy Act provides that the information privacy principles do not confer legal rights enforceable in a court, a breach of the principles is still contrary to law. Enforcement mechanisms are contained in the Privacy Act, including to the Human Rights Review Tribunal, and breaches of the principles may also be relevant in Courts: see *R v Alsford* [2017] NZSC 42, at [38].

32 Public Records Act 2005.

- Release information to an applicant unless a specified exception applies[33]
- Give an applicant information about any personal information the agency holds about them, if the applicant asks for it[34]
- Comply with guidelines dealing with procurement.

2.13 These requirements support independent oversight of government activity, including surveillance, through various mechanisms, including the Ombudsman, the Privacy Commissioner, the State Services Commissioner, the Auditor General, the Independent Police Conduct Authority, and the Inspector General of Security and Intelligence.

Engaging external security consultants to carry out surveillance

2.14 Engaging an external security consultant to carry out a surveillance activity should not operate to defeat the legal requirements that would otherwise apply to government surveillance activities, or the protection of oversight mechanisms. In our view any legal requirements applying to Crown agencies apply equally to activities carried out by contractors working for government agencies, and government agencies must have appropriate controls in place to ensure that all contractors meet these requirements.

2.15 Where the Government engages an external security consultant or contractor to undertake surveillance activities, additional requirements must also apply in order to ensure the activity is lawful:

a The contractor must be licensed under the Private Security Personnel and Private Investigators Act 2010.

b The contractor must comply with the private investigators' code of conduct,[35] which (among other things) limits the type of surveillance that can be carried out of people who are on private property.[36]

2.16 The Inquiry understands some private investigators take the view that surveillance activities are unobjectionable if they are not prohibited or regulated by the private investigators' code of conduct. However, private investigators must also comply with the general law, and the code of conduct explicitly preserves the applicability of "any rule of law or any other enactment relating to unlawful conduct", including without limitation the Privacy Act 1993 and Crimes Act 1961.[37] In addition, when acting for a government client, an investigator must comply with the State Services Code of Conduct. For this reason, a government agency should draw to the attention of any external security consultants or contractors that they must comply with the State Services Code of Conduct when acting on an agency's behalf.

33 Official Information Act 1982.

34 Privacy Act 1993.

35 Private Security Personnel and Private Investigators (Code of Conduct – Surveillance of Individuals) Regulations 2011.

36 The code prohibits the use of surveillance equipment to conduct surveillance of any person in a private dwelling without the occupier's consent. Surveillance of any person on private property can also only be done if the surveillance is from a public place and it is of activity that is otherwise observable without any equipment. The code also prohibits the installation of surveillance equipment in private property, except with the consent of all the lawful occupiers of the property. Surveillance of a person in a public place is not restricted. See Regulation 6.

37 Private Security Personnel and Private Investigators (Code of Conduct – Surveillance of Individuals) Regulations 2011, r 5.

The State Sector Standards of Integrity and Conduct (the Code of Conduct)

2.17 The State Services Code of Conduct requires that a higher test be applied to activities of government agencies than might be expected to apply to commercial entities or other sector participants that are not state servants. The Code itself states general principles that should be applied with judgement, and includes a requirement that state servants must be:[38]

- Fair – This includes treating people fairly and with respect
- Impartial – This includes maintaining political neutrality
- Responsible – This includes acting lawfully and objectively and using organisational resources carefully and only for intended purposes
- Trustworthy – This includes being honest and avoiding activities that may harm the reputation of the organisation or the State Services.

2.18 Compliance with the Code requires state servants to have regard for:

- The spirit of service to the community
- The obligation that organisations have as part of executive government
- The role of the State Services in supporting parliamentary democracy
- The value of state servants having a lively interest in political matters.

2.19 In this report we use the phrase 'inconsistent with the Code' in situations where the Code did not technically apply to the agency at the relevant time.[39] The Inquiry also took the view that an agency can be in breach of the Code as well as individuals.

2.20 In carrying out its Terms of Reference, the Inquiry met with agencies relevant to the application of the Code, including the Office of the Ombudsman, the Office of the Privacy Commissioner, the Office of the Chief Archivist, the Inspector-General of Intelligence and Security, the Independent Police Conduct Authority, and the Private Security Personnel Licensing Authority.

[38] See http://www.ssc.govt.nz/code. Before July 2007 the applicable document was the Public Service Code of Conduct. The obligations were not materially different, and included the obligations to act honestly, faithfully and efficiently, respecting the rights of the public including the privacy of individuals, and avoiding conduct that could bring the employer into disrepute, whether connected to the employee's official duties or otherwise. This last obligation was expressed at a high level as an obligation not to engage in conduct that might bring the department into disrepute through "private activities", although the commentary made it clear that the requirement applied equally to activities connected with official duties. The Inquiry has proceeded on the basis that the obligation was not materially different prior to July 2007.

[39] In some cases, for example Southern Response and the SIS, this was because the Code was applied part way through the relevant period. In other cases, for example the Crown Research Institutes, the Code does not technically apply, although its principles are applicable.

Good practice in governance, management and administration

2.21 All engagements of external security consultants should be governed in accordance with their risk. In particular, high-risk engagements should be well-documented and be governed under a contract, and both the initial engagement and any particularly risky activities should have sign-off at an appropriate level of management. Mechanisms should be in place to ensure that decisions are made according to clearly articulated principles, that legal risk is checked and managed, and that there is appropriate oversight throughout the engagement.

2.22 When engaging external security consultants, agencies should also check that private investigators are licensed, and should carry out due diligence on the contractors, including being mindful of and managing potential conflicts of interest.

An example– ACC's Standard Operating Procedure

2.23 As noted earlier in this report, the ACC investigation unit at times engages external security consultants to carry out investigations where a person's entitlement to ACC payments is in serious question. The investigation unit has a Standard Operating Procedure (SOP) governing the use of visual surveillance in these investigations.

2.24 The SOP:

a Provides controls for when visual surveillance may be undertaken, including the procedure for commissioning visual surveillance, factors that should be considered before undertaking visual surveillance, and a requirement that visual surveillance may only be undertaken by a trained ACC investigator and must be approved by the investigator's manager

b Sets out surveillance activities that would or may be unlawful and should not be carried out

c Includes rules around record keeping and storage, including a requirement to log activities, a requirement to transfer raw footage to ACC, and rules to manage the data after that point.

2.25 All investigators, including those contracted, must comply with the SOP.

2.26 In short, the SOP provides an appropriate framework for carrying out surveillance activities in a manner that is lawful, that complies with the Code of Conduct, and that is managed and administered in accordance with good practice.

3 The use of external security consultants by government agencies

Introduction

3.1 The Inquiry's Terms of Reference focus on the use of external security consultants for surveillance, but more broadly require us to report on 'any engagement' of external security consultants by government agencies. As set out in Appendix 2, the Inquiry's methodology largely excluded forms of engagement with low legal and ethical risk, such as security guard services, alarm monitoring, and IT security services.

3.2 This chapter of the report primarily addresses surveillance, but also reports on some other uses of external consultants by government agencies. A summary of all uses reported by government agencies is set out in Appendix 4.

Background

3.3 The use of external security consultants by government agencies came to public attention in 2007–2008 when an investigative journalist published details of Solid Energy's use of a paid informant through Thompson and Clark. The informant was paid to infiltrate the group 'Save Happy Valley', which was opposed to the planned open-cast coal mine in the upper Waimangaroa Valley on the West Coast.[40] In addition, it appears a second informant was paid to infiltrate two other groups: the Wellington Animal Rights Network and Peace Action Wellington.[41] Solid Energy described its actions as legal, ethical and moral, but the Prime Minister, Minister of State Owned Enterprises, and Opposition were all critical of the conduct.[42] In particular, the Minister of State Owned Enterprises said the use of paid informants was 'not acceptable', and 'a step too far for a State Owned Enterprise'.

3.4 Following this, in February 2008 the State Services Commissioner warned departmental Chief Executives that purchasing covertly obtained information beyond what is required for statutory functions risks bringing the State Services into disrepute. He specifically noted that purchasing information about the 'political views or lawful actions of groups and individuals' was problematic, and added:

> *Sometimes departments and agencies may be concerned about possible threats to the safety of their staff. In that case the best approach is to seek advice from the Police.*

40 See: <http://www.stuff.co.nz/national/377237/Private-investigators-still-digging-on-West-Coast>

41 See: < http://www.nickyhager.info/i-was-paid-to-betray-protesters/>.

42 See: < https://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=10442369?>

3.5 Despite these events, it appears Thompson and Clark attempted to recruit a further paid informant from within the Save Happy Valley group in Christchurch in 2009.[43] Thompson and Clark says it has not conducted any similar infiltration since this time. In the section below, the Inquiry considers whether the payment of an agent to attend and record a 'strictly claimants only' meeting discussing legal strategy was conduct bordering on infiltration.

The use of external consultants for surveillance

3.6 As described above, the Inquiry adopted a broad definition of 'surveillance', including any close monitoring or observation of people, places, things or information, with or without the use of devices, that interferes with a reasonable expectation of privacy. Where an activity could potentially interfere with a reasonable expectation of privacy the Inquiry considered it, even if it was not obvious that there had in fact been such an interference. The Inquiry focused on surveillance of members of the public, and did not look at surveillance that was carried out to investigate suspected employee fraud.

3.7 The Inquiry found no evidence of widespread or routine surveillance of individuals by external security consultants on behalf of government agencies. The table of responses by agency in Appendix 4 contains a summary of the information received.

3.8 However, nine agencies did engage external security consultants who carried out surveillance, or activities close to surveillance:

a **Southern Response Earthquake Services Ltd** engaged Thompson and Clark between 2014 and 2016 to attend meetings of claimants, including closed meetings discussing legal options. The contractor who attended made electronic recordings of several meetings, which were available to Southern Response.

b **The Ministry of Agriculture and Forestry** engaged Thompson and Clark to attend two conferences of interest to the animal rights movement in 2005 and 2006. This likely involved surveillance of activists, and in one case the payment of money to a person who had covertly infiltrated an activist group.

c **The Crown Law Office** engaged external security consultants on behalf of MSD to make enquiries in relation to individuals involved in civil claims alleging abuse in state care in 2007. The investigators took some steps that were at least close to surveillance, and the broad instructions did not rule out low-level surveillance.

d The **Ministry of Social Development** was the defendant in the state care case handled by Crown Law, and knew of the steps being taken without apparent objection. MSD also used private security consultants to carry out surveillance in three cases of fraud or suspected fraud.

e **MBIE** engaged external security consultants to conduct surveillance in 2015 in relation to two specific investigations into breaches of building and construction regulations.

f **ACC** engaged and continues to engage external security consultants to conduct surveillance in relation to investigations of entitlements under the ACC scheme.

[43] See: < http://www.stuff.co.nz/national/377237/Private-investigators-still-digging-on-West-Coast >

g **The Department of Internal Affairs** uses external security consultants (private investigators) to locate and confirm the identity of people to be deprived of citizenship. In two cases this has involved surveillance.

h **Maritime New Zealand** engaged an external security consultant to conduct surveillance in 2009 in relation to an investigation into a potential maritime safety issue.

i **The Ministry of Health** engaged and continues to engage external security consultants, including Thompson and Clark, in relation to public health enforcement functions.

3.9 The circumstances, nature and extent of surveillance by external security consultants on behalf of each of these agencies is described in detail below.

Southern Response Earthquake Services Ltd

Southern Response acted inconsistently with the Code of Conduct from 13 March 2014 to 31 December 2014, and was in breach of the code from 1 January 2015 to 12 May 2016 when the Code formally applied to the company. On behalf of Southern Response, Thompson and Clark attended and recorded several closed meetings of insurance claimants that discussed options for legal action against Southern Response. The recordings were made by a contractor who was not a licensed private investigator, and may themselves have been unlawful, but it was not possible to make findings because the recordings were not retained - itself a breach of the Code.

Context

3.10 Southern Response Earthquake Services Ltd is a Crown-owned Company that was formed in 2012 from AMI's earthquake claims division in order to respond to the claims arising from the earthquakes in Canterbury between September 2010 and April 2012.

3.11 Southern Response engaged Thompson and Clark and another external security consultant to carry out a range of services between 2014 and 2017.[44] At the time, Southern Response was operating in a highly charged environment resulting from the significant trauma experienced during and following the earthquakes, as well as from grievances created by Southern Response's approach to settling claims. The earthquakes had a profound impact on those directly and indirectly affected, and there was frustration and anger from claimants dealing with the emotional stress arising from the earthquakes themselves and from Southern Response's approach.[45]

[44] The second security consultant was not engaged in relation to any surveillance activities.

[45] Studies undertaken following the earthquakes found an impact on the mental health of individuals. 'All Right?', an initiative led by the Canterbury District Health Board and the Mental Health Foundation, has undertaken research among Cantabrians on their mental health and wellbeing. In April 2017, All Right? released a survey on Cantabrians' mental health as the region recovers from the earthquakes. The research showed that while there has been some improvement in how people are feeling since the survey was first carried out in 2012, 64% of those surveyed reported that they are still grieving for what they have lost. Of particular relevance to the inquiry, the research also showed that unsettled insurance claims were having a negative impact on how people feel. More than a third of those with an unsettled claim said their living situation was getting them down – nearly three times as many as for those with settled claims (11%); and almost half of those with an unsettled claim said they were struggling to deal with things that have happened as a result of the earthquakes, compared to a quarter of people with settled claims (24%).

3.12 Through late 2013 and early 2014, claimants were increasingly dissatisfied with the pace at which Southern Response was resolving claims. This period saw the emergence of a number of organised public groups, more frequent complaints from claimants about the company, and a number of public protests.

3.13 Significantly, from early 2014 until the Inquiry began in early 2018, there were also specific threats of harm and harassing behaviour towards individual employees and board members, including at least five direct death threats (which were reported to the Police), seven further serious threats of harm, and 22 cases of harassment or abuse, including the targeting of staff in the community outside working hours.[46] Southern Response took these matters seriously, and had extensive health and safety policies and procedures.

Southern Response's engagement of Thompson and Clark

3.14 Against this background Southern Response engaged Thompson and Clark to undertake various activities from 2014 to 2017 as set out in the timeline on the following page. The majority of the activities did not involve surveillance and are addressed below, from paragraph [3.140]. There was no evidence that Southern Response used Thompson and Clark to carry out targeted surveillance of individual claimants, or discriminated against disaffected claimants in settlements.

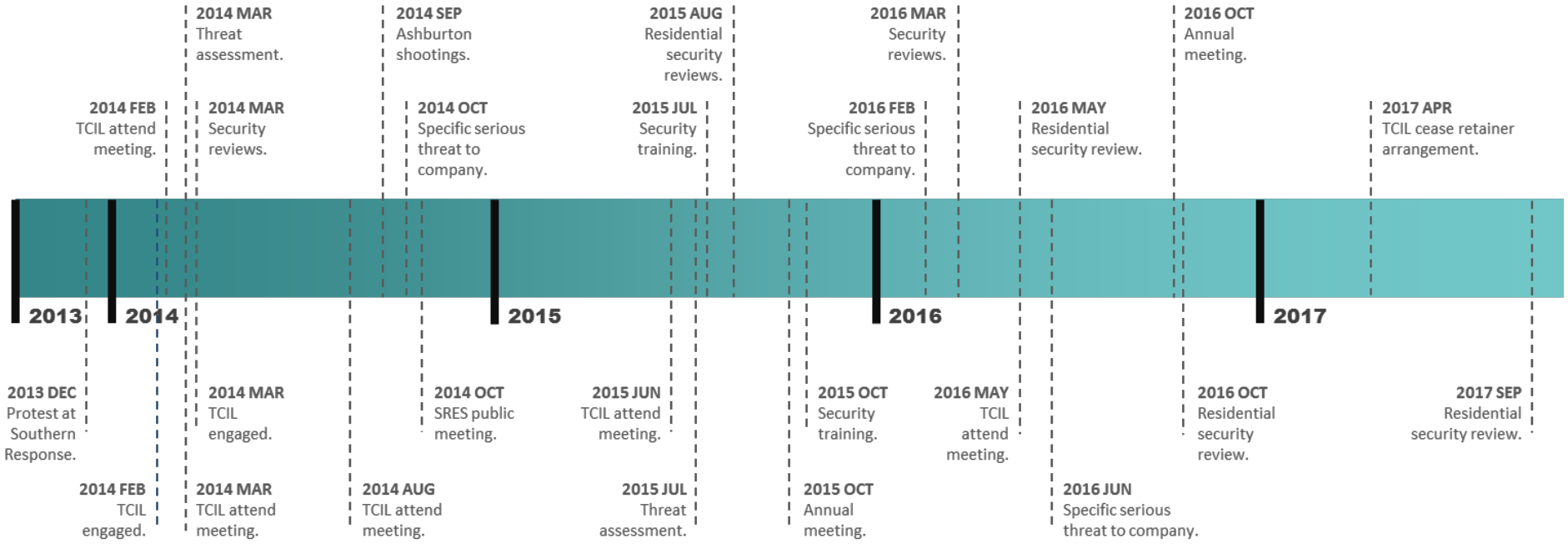
3.15 Thompson and Clark were identified by Southern Response as a preferred supplier of security, threat and risk-management services on the recommendation of an employee who had been aware of Thompson and Clark's work at the Crown Research Institute AgResearch. There was no formal contract. Rather, commissioning relied on a process of seeking a proposal for services, which was accepted or amended during the engagement.

3.16 The initial engagement of Thompson and Clark to conduct the first threat assessment was focused on the safety and security of employees and contractors and was endorsed by both the former Chief Executive and the Board Chair. However, day-to-day management of the relationship with Thompson and Clark was primarily (although not exclusively) managed from within the communications team.

[46] These were recorded on Southern Response's health and safety register from early 2014 to early 2018. The Inquiry's view is that these figures are likely to underestimate the actual numbers of incidents, as Southern Response identified that its reporting and recording of threats, abuse and harassment improved over time as it gained maturity in identifying health and safety risks.

Timeline of Southern Response-related events relevant to the Inquiry

The following is a summary of key events relevant to the Inquiry as it applies to Southern Response. It is not an exhaustive timeline but rather is indicative of major events that shaped the relationship between Southern Response and its overall security environment. [47]



47 Note "Ashburton shootings" is a reference to the murder of two WINZ employees by a disgruntled client in September 2014 . It is included as it sparked a step change approach to security across a number government agencies including Southern Response.

Surveillance activities

3.17 Between 2014 and 2016, a Thompson and Clark contractor acting on behalf of Southern Response attended and in several cases recorded public meetings held by groups of claimants. It is not clear whether the decision to attend the meetings was a recommendation from Thompson and Clark or a request from Southern Response, but Southern Response certainly knew of the attendance and recordings from an early stage. The meetings are summarised below in Table 1.

3.18 For each of the five meetings, a Thompson and Clark contractor registered, attended the meeting, and made notes of the proceedings. In several cases he made audio recordings. The contractor has given different accounts of what happened to the recordings, but it appears he uploaded at least some of them to a Thompson and Clark server, and the commissioning employee at Southern Response told the Inquiry she was aware of the recordings when the contractor reported back. The recordings were therefore available to Southern Response.

3.19 The contractor was not a licensed private investigator under the Private Security Personnel and Private Investigators Act 2010 at the time of the meetings. Under the Act, a licence is generally required for any person seeking information about the "character, actions or behaviour of any person" on a commercial basis.[48]

3.20 The contractor and Thompson and Clark argued there was no need for a licence in this case because the contractor's intention was not to seek or gather information about particular people, but rather to 'make an informed assessment of mood, motivation, intent, and capability of the general public mood of disaffection for SRES and its personnel'. In particular, Thompson and Clark drew a distinction between obtaining information about a person's 'actions and behaviour', and obtaining information about an individual's 'words'. They acknowledged that the contractor did obtain information about an individual's words, which they interpreted as a direct threat, but argued this did not fall within the definition in the Act because this was not information about the individual's 'actions or behaviour'. The Inquiry does not accept that distinction, particularly in relation to the focus on the individual at the 13 March 2014 meeting described below.[49]

3.21 The contractor did not identify himself as representing Southern Response. When interviewed by the Inquiry, he took the surprising position that he was not representing Southern Response because 'you can't say that dollar that Southern Response paid Thompson and Clark then went to me'. Again, the Inquiry does not accept that distinction. The contractor was undoubtedly present on behalf of Southern Response, albeit paid by Thompson and Clark, who on-charged Southern Response.

48 Private Security Personnel and Private Investigators Act 2010, s 5.

49 The requirement to hold a licence is not dependent on whether the activities constituted 'surveillance', or whether the meetings took place in public.

3.22 In addition to the recordings, the Thompson and Clark contractor provided reports of things said at the meetings to Southern Response, either orally or through Wordpress. After the 13 March 2014 meeting, the contractor provided Southern Response with a one-page transcript of comments made by an attendee.[50]

3.23 Three of the meetings were closed forums, advertised as being for claimants only:[51]

a The meeting on 11 February 2014 was described in publicity by organisers as a 'closed forum'. Media were allowed for the first five minutes, then asked to leave. At least one attendee recalls that the MC asked anyone from Southern Response who was present to leave. Thompson and Clark's contractor accepted that such a comment was made, but said it only applied to 'Southern Response employees', and he did not consider himself to be an employee. It appears that video footage from approximately 12 minutes of this two-hour meeting, featuring a lawyer, was posted by a claimant online.

b The meeting on 13 March 2014 was advertised as 'strictly for Southern Response claimants only'. Again, at least one attendee recalls that both the media and 'anyone from Southern Response' were asked to leave. This meeting discussed a possible class action lawsuit and canvassed strategies to increase claimants' influence and leverage over the actions taken by Southern Response. While legal privilege would not have applied to the communications, at a broader level the nature of the discussion would potentially have conveyed tactically useful information to Southern Response – even if it merely confirmed the state of readiness of the claimant group.

c The meeting on 16 June 2015 was a further closed forum to discuss the class action lawsuit. Again the Inquiry was told that anyone from Southern Response had been asked to leave.

3.24 In contrast, the two meetings on 2 August 2014 and 12 May 2016 were open to the public, including media, and widely attended. Parts of the meetings were recorded and published on other public platforms.

3.25 One attendee who gave evidence on oath told us that his expectation at the closed meetings was that the discussions would be private as between claimants. He believed this was the general expectation of those attending. He said there was an expectation that nobody from Southern Response would be present, and certainly that Southern Response would not be recording the discussions. As noted above, both the Thompson and Clark contractor and the claimant recalled that the media and 'anyone from Southern Response' (or words to that effect) were asked to leave after the first few minutes of the closed meetings.

[50] The transcript focused on comments of a potentially inflammatory nature, rather than legal strategy. Thompson and Clark argued that the comments were a 'direct threat' and 'direct incitement', although the Police did not consider the matter needed to be dealt with as a formal complaint – see further discussion below.

[51] Facebook posts supplied by Thompson and Clark indicated that potential claimants were also welcome to attend.

3.26 Thompson and Clark argued the meetings were properly described as public. They relied in part on Facebook posts that suggested the organisers allowed a person to attend who was not yet a claimant (she was at an earlier stage of the process), and the fact that a link to the March event was shared to a Residents Association account. These points are well made but do not materially change the position. There is no dispute that 'anyone from Southern Response', or words to that effect, was asked to leave one or more of the closed meetings. In that context, there was an explicit limitation on attendance at the meetings that must be taken into account when assessing compliance with the Code of Conduct requirements.

3.27 Thompson and Clark also argued the actions were justified because the meetings fell within the definition of 'public place' in the Summary Offences Act 1981, and because the tickets to the events did not contain an express exclusion. They further relied on the private investigators' code of conduct,[52] which allows licensed private investigators to engage in surveillance of people in public places. However, the Summary Offences Act 1981 defines 'public place' for the purpose of particular criminal offences such as offensive behaviour, not in a general way for all purposes. As noted above, the private investigators' code of conduct does not affect the general law, and applies only to licensed private investigators.[53]

3.28 Moreover, the Inquiry's focus is on potential breaches of the State Services Code of Conduct, and classifying the meetings as 'public' for some purposes does not relieve Southern Response of the need to comply with the Code. From the Inquiry's perspective, the key point is that there was a reasonable expectation at the closed meetings that any comments made after Southern Response was asked to leave the room would not be provided to Southern Response, particularly with the assistance of electronic recordings made without permission. That expectation existed regardless of whether the venue could be classified a public place.

3.29 Following the closed meeting on 13 March 2014, Thompson and Clark informed Southern Response that during the meeting an adviser to the claimants had encouraged people to 'go around and have a chat [to Southern Response board members] at 2 am Sunday morning'. Thompson and Clark supplied Southern Response with a transcript of the comments, created from the audio recording, and advised Southern Response to raise this statement with the Police. At that time, a Thompson and Clark contractor told Southern Response not to tell the Police how it knew about the alleged statement because this could compromise 'closed source' information:

> *"At the moment I would not like to see the recording published as it will be open to OIA in the future. It could also affect our future ability to obtain close source information."*

3.30 A few days later, the same Thompson and Clark representative reiterated to the then Chief Executive of Southern Response that he should put pressure on the Police to talk to the individual concerned, but that there should be no mention of the recording. He went as far as to suggest the Chief Executive could misrepresent the source of the information to Police.

3.31 These emails lend support to the conclusion that recording the 'claimants only' meetings involved an element of surveillance, perhaps even bordering on infiltration. The inference is that Thompson and Clark knew claimants would not have spoken as freely if they knew someone on behalf of Southern Response was present and recording the proceedings. That

[52] Private Security Personnel and Private Investigators (Code of Conduct-Surveillance of Individuals) Regulations 2011.

[53] Private Security Personnel and Private Investigators (Code of Conduct-Surveillance of Individuals) Regulations 2011, r 5.

is why revealing the existence of the recording would compromise Thompson and Clark's ability to obtain similar, 'close source', information in the future.

3.32 Southern Response's then Chief Executive followed Thompson and Clark's advice and raised the concern with the Police. The Police Officer involved recalled a general discussion about the individual and the statements made. The Officer told the Chief Executive that the statements did not warrant further action, which might be inflammatory for the company's relationship with the individual; and that an alternative course of engaging with the individual might be a better approach. As the concerns did not result in an official complaint, there was no requirement for the Chief Executive to provide the NZ Police with relevant evidence to support Southern Response's concern, including the recording. Had the concern resulted in a complaint and the Chief Executive withheld the recording, or misrepresented the source of the information, this would have been inconsistent with the State Services Code of Conduct.

3.33 Neither the recordings nor the Wordpress blog were retained by either Thompson and Clark or Southern Response.[54] An email sent by Thompson and Clark in March 2014 suggested the company was generally concerned 'to get around disclosure, privacy and OIA issues'. Thompson and Clark told the Inquiry it 'does not retain information unless there is a reason to do so.' This contrasts with Thompson and Clark's standard terms and conditions, which in 2016 stated that both parties to a contract must keep full records relating to the delivery of the services for seven years after the end of the contract. Because of the lack of records in this case it has not been possible for the Inquiry to establish specifically what was recorded and what information was provided.

3.34 In particular, given the absence of records, the Inquiry cannot discount the possibility that recordings may have captured private conversations. The Inquiry has not been able to corroborate the suggestion that other attendees made recordings, and one of the organisers told the Inquiry he did not believe others were recording. Moreover, the key point was that the recordings were passed on to Southern Response – effectively placing the company 'in the room', contrary to the express wishes of the meeting organisers.

3.35 The original purpose in attending these meetings was to use any intelligence gathered to update the threat assessment relating to the physical safety of staff. However, the tasking of Thompson and Clark to attend these public meetings did change over time. As Southern Response mitigated the risks to staff (actual and perceived), the primary benefit to Southern Response lay in monitoring its corporate reputation, rather than managing security risks.[55]

3.36 While Southern Response was genuinely concerned about health and safety risks, the Inquiry does not consider that health and safety obligations require or justify surveillance of individuals or groups by external security consultants in circumstances such as these. The company's other actions to mitigate the risks were appropriate, including physical security, staff training and de-escalation strategies. These steps are described in more detail below in the 'Engagements not involving surveillance' section. For more serious concerns, the proper

[54] Thompson and Clark informed the Inquiry that this was their standard procedure and that they have previously taken the same approach with other clients. The exception to this was an excerpt from a transcript of the public meeting on 13 March 2014, which was available in hard copy in files provided by Thompson and Clark.

[55] Email from Thompson and Clark to Southern Response dated 8 June 2015.

response was to seek the assistance of the Police, who have the expertise to assess and deal with threats to individuals.[56]

Table 1: Surveillance activity undertaken at meetings

Date	Meeting type	Description	Speakers	Comment on nature of meeting
11 February 2014	**Closed** Forum – Panel Discussion – Donation Charge	Southern No Response claimants meeting • General meeting with a variety of speakers • Jack Mann Auditorium • Media present (before and after - but not during meeting) • Components of this meeting remain hosted on the video sharing website Vimeo.	Insurance Adviser Chartered Accountant/Claimant Registered Professional Surveyor Registered Quantity Surveyor Chartered Professional Engineer MC Claimant and City Councillor	320 estimated claimants attended. Only claimants invited via loopsuite. Media interviewed some speakers outside after forum. Claimants did not want their photos taken by media. Class Action raised.
13 March 2014	**Closed** Forum - Claimants only meeting - Free	Honour Your Promise Action Meeting • Potential class action discussion • Westpac Hub, Christchurch • Tickets generally available through Eventbrite platform • Media present (before and after - but not during meeting).	Claimant Lawyer Chartered Accountant/Claimant MC Claimant/Media personality	150 estimated claimants attended. 'Strictly for SR claimants only'. Specifically talked about Class Action and answered questions about mechanics, possible strategies and chances of success of such action. Media interviews outside before and after.
2 August 2014	**Open** "Insurance Forum" for claimants across a range of insurers - $10.00 per person entry fee	Claimants for Claimants Meeting • Focus on all insurers including EQC • Tickets generally available through Eventbrite platform • Media present (before, during and after).	Insurance Adviser Registered Quantity Surveyor Lawyer bringing a class action Foundation subject matter expert Chartered accountant/claimant Registered professional surveyor Chartered professional engineer MC and claimant	300 estimated claimants. Eventbrite tickets numbered 256 tickets however there were also a number of door sales.

[56] Southern Response did contact the Police on a number of occasions during the relevant period, and in the Inquiry's view this was a sufficient response, together with the other steps taken. The Inquiry did not directly assess the actions of the Police, but was satisfied that the Police took all relevant matters into account and appropriately assessed the risk.

16 June 2015	**Closed** Meeting, registration required	Southern Response Class Action Meeting • Focused class action discussion • Tickets generally available through Eventbrite platform • Christchurch Transitional Cathedral.	Lawyer bringing class action Barrister (QC) bringing class action Litigation Lending Services	Second meeting arranged by legal firm bringing class action.
12 May 2016	**Open** Meeting to explain EQC Action Group Settlement	EQC Fix 'Public' Meeting • General meeting with a variety of speakers • Christchurch Transitional Cathedral.	EQC Action Group chair Lawyer representing EQC Action Group Insurance Lawyer Senior Lecturer, Massey University Chartered Accountant/claimant MC and claimant	Meeting media release. Open meeting – EQC were invited but declined to come.

Application of the Code of Conduct

3.37 In the Inquiry's view it was a breach of the Code of Conduct for Southern Response to have a representative attend and record closed forum meetings for 'claimants only', particularly where legal strategy was discussed. This breached the Code's restriction on activity likely to harm the reputation of the organisation, as well as the Code's requirements to act fairly, impartially and responsibly. The failure to keep records of the activities further breached the Code's requirement to treat information with care.

3.38 Thompson and Clark did not consider their activities to be surveillance. However, in our view the electronic recording of closed meetings on behalf of a government agency was a form of 'surveillance' under the definition adopted for the purpose of this Inquiry. Whether or not these actions constituted 'surveillance', Southern Response's conduct was inconsistent with and breached the requirements of the Code of Conduct noted above. In substance, the conduct could even be described as bordering on infiltration, given that the contractor at least tacitly assumed the role of a member of the claimant group while being paid by Thompson and Clark.[57]

3.39 As noted above, Thompson and Clark placed particular weight on the Summary Offences Act 1981 and the private investigators' code of conduct. However, that position was both misplaced,[58] and too narrow.[59] Southern Response had obligations under the Code of Conduct, and there should have had a broader focus on the legal and ethical risks involved in these particular circumstances.

[57] The Inquiry interprets 'infiltration' to involve a person participating in the activities of a group under false pretences, representing that he or she is a member of the group while in fact secretly reporting on the group's activities to others.

[58] The private investigators' code of conduct did not apply in this case because Contractor A was not licensed, and the definition of 'public place' in the Summary Offences Act 1981 is not a definition of general application, but rather applies for specific purposes. In addition, many surveillance activities take place in public places, for example tracking and following an individual in a public street. It is therefore incorrect to suggest that classifying a location as a public place precludes an activity being described as a form of surveillance.

[59] As set out in Chapter 2 above, the engagement of external security consultants by government agencies must be lawful, consistent with the Code of Conduct, and well governed/managed.

3.40 In any case, the engagement of Thompson and Clark was poorly managed and lacked the oversight and safeguards required, particularly once it must have become clear to Southern Response that Thompson and Clark's contractor had made an audio recording of a 'closed forum' meeting. The deficiencies with the engagement included the following:

a There was no written contract clearly communicating Southern Response's expectations.

b Oversight was minimal and predominantly carried out by Southern Response's communications team. There was no explicit mechanism for ensuring an appropriate level of sign-off for surveillance activities. The Board – and most importantly the Board Chair, were not made aware of what was occurring. The Chair had previously expressed concern about the potential use of surveillance in an email to the former Chief Executive, the communications team and Thompson and Clark at the initial engagement.[60]

c When surveillance was carried out, there were no checks in place to ensure it was lawful and appropriate and being carried out by a licensed operator.

d There were no processes in place to ensure that appropriate records of the investigator's attendance at the meetings were kept, either by Southern Response or Thompson and Clark. This was contrary to Thompson and Clark's standard terms and conditions, and defeated the oversight mechanisms normally available through the Official Information Act and Privacy Act.[61]

3.41 The Inquiry does not consider it would ever be appropriate for a government agency to attend a closed meeting and record proceedings in a non-transparent way, particularly a meeting discussing litigation against the Crown.[62] This finding does not turn on the existence of legal privilege, but rather on the appropriateness of Southern Response's actions and an application of the Code of Conduct.

3.42 In this case two meetings were held in part to discuss legal action against Southern Response. In the absence of the recordings and blog posts, the Inquiry has not been able to determine the extent to which any legal advice or strategy was made available to Southern Response. However, in our view it was inappropriate for any information from such a meeting – not only legal analysis or strategy – to be disclosed to Southern Response. For example, it may have been strategically helpful for Southern Response to know how well funded and organised the proposed action was, what the level of preparation was, and the general mood of the claimant group. All information of that type had the potential to be useful to Southern Response and damaging to the claimant group.

3.43 In that context, the fact that Southern Response engaged external security consultants to attend the meetings, particularly once the company was aware of the electronic recordings,

60 Email from Southern Response Chair dated 14 January 2014.

61 Southern Response received advice in May 2014 that the Chief Archivist considered that Southern Response did not fall under the definition of 'public office', and therefore was not required to keep records under the Public Records Act 2005. However, failing to maintain these records was poor practice.

62 Technically the breach of the Code of Conduct occurred only from 1 January 2015, when the State Services Commissioner applied the Code to Southern Response. This covered the public meetings attended on 16 June 2015 and 12 May 2016. Before 1 January 2015, Southern Response's actions would have breached the Code had it applied directly to the company. In this report the phrase 'acted inconsistently with the code' is used to cover situations where the Code did not directly apply at the relevant time.

at the very least risked damaging public confidence - even if the initial motivation was benign. The actions may also have been unlawful: the recordings were made by an unlicensed private investigator, and may also have breached the Crimes Act 1961 or constituted the tort of invasion of privacy, or both.[63] It is clear that Southern Response did not consider these legal and reputational risks. In addition, the failure to ensure records were kept of the attendance at meetings was inconsistent with and breached the Code's requirement to treat information with care.

3.44 While there was perhaps a case for openly attending meetings to inform the preliminary assessment of threat of harm to Southern Response and its employees in the face of threats, the more likely benefit in the long run was in informing an assessment of the extent of negative public sentiment towards the company, and the associated risks to corporate reputation and brand, rather than risks of physical harm and injury. The Inquiry acknowledges that managing corporate reputation is a legitimate goal, however this does not justify Southern Response's actions in this case.

3.45 For the above reasons, Southern Response acted inconsistently with the Code of Conduct from 13 March 2014, and was in breach of the code from 1 January 2015 until 12 May 2016 when the Code was formally applied to it.

Ministry of Agriculture and Forestry

The Ministry of Agriculture and Forestry breached the Code of Conduct by engaging Thompson and Clark to attend two conferences of interest to the animal rights movement in 2005 and 2006. At the first conference, MAF paid for Thompson and Clark to 'monitor' activists, likely involving surveillance, and to liaise with a paid informant. At the second conference, MAF contributed to the fees for the paid informant within the animal rights group. This breached the Public Service Code of Conduct requirements to respect the rights of the public and the privacy of individuals.

3.46 The Ministry of Agriculture and Forestry engaged Thompson and Clark to attend two animal rights-related conferences in 2005 and 2006.[64] The engagements were authorised and paid for by MAF's special investigations group. The Inquiry heard that the engagement was prompted by a concern that animal rights protests were escalating, and had the potential to replicate some of the more extreme forms of protest that had occurred in the United Kingdom. The senior manager responsible for the unit through this period described it to the Inquiry as a 'volatile period for animal rights activism'.

3.47 In 2005 MAF paid Thompson and Clark to attend a conference of scientists involved in the use of animals in research and teaching.[65] The conference attracted protesters from the animal rights movement. Thompson and Clark told MAF in advance they had "tasked their people in the field" in preparation for the event. The company's invoice included reference to liaising with a covert human intelligence source ("CHIS"). Thompson and Clark told the

63 Crimes Act liability could arise, for example, if the contractor deliberately recorded private conversations between claimants close to him to which he was not a party. There is no evidence to suggest that occurred, but in the absence of the recordings it is not possible to rule it out.

64 The Ministry also received regular monthly reports. This is discussed in the section 'Receiving Information Obtained Through Surveillance' below.

65 The Australian and New Zealand Council for the Care of Animals in Research and Teaching (ANZCCART). See www.anzccart.org.nz. It is not clear whether Thompson and Clark attended the conference as delegates, or as observers of the protest action, although the latter is more likely.

Inquiry they 'more than likely' carried out surveillance, including following activists involved in protesting at the conference. The hourly rate charged to MAF was the rate charged for surveillance.

3.48 The following year, Thompson and Clark put a proposal to MAF to attend a "major animal rights conference" in Wellington. The company saw this as "a great opportunity to obtain relevant intelligence on New Zealand's Animal Rights Activists". They outlined their proposal "to have physical attendance of two operatives, an internal source (CHIS) and matters to be collated by our analyst." As above, the acronym CHIS stands for 'covert human intelligence source', i.e. a covert informant within the animal rights group. The proposal included $2000 for "CHIS funding". MAF contributed roughly a third of the total funding sought.

3.49 Media reporting in 2007 identified an informant who allegedly infiltrated animal rights and peace groups in Wellington on behalf of Thompson and Clark. The individual was reported to have attended the 2005 protests at the conference described above, and as having continued to be active for Thompson and Clark in 2006.[66]

3.50 The Ministry terminated its relationship with Thompson and Clark in 2008 after receiving the State Services Commissioner's guidance following the 'Happy Valley' incident. We did not see evidence of further instances of surveillance carried out by external consultants for the Ministry or its successor organisation MPI.

3.51 For completeness, the Inquiry was given records of a joint operation by the Wildlife Enforcement Group that likely involved surveillance in August 2004 relating to smuggling wildlife to or from New Zealand. This surveillance was not undertaken by Thompson and Clark.

Application of the Code of Conduct

3.52 MAF breached the Public Service Code of Conduct in force at the time by engaging Thompson and Clark to attend two conferences of interest to the animal rights movement in 2005 and 2006. At the first conference, MAF paid for Thompson and Clark to 'monitor' activists, likely involving surveillance, and to liaise with a paid informant. At the second conference, MAF contributed to the fees for the paid informant within the animal rights group. This breached the Public Service Code of Conduct requirements to respect the rights of the public and the privacy of individuals.

3.53 In the period following 2008, the Ministry took steps to improve its oversight. This included developing a policy on the use of external parties for enforcement-related intelligence information in July 2008.

Crown Law Office / Child, Youth and Family / Ministry of Social Development

In 2007, Crown Law, on behalf of MSD, instructed private investigators to assist with a civil case alleging abuse in state care (the White case). Crown Law's instructions were broad, including seeking any information that could be used to cross-examine a group of similar fact witnesses to be called by the claimants. Crown Law did not rule out low-level surveillance in the lead up to the trial. There were indications in the file that the investigators did use techniques involving low-level surveillance, or

[66] See https://www.gmwatch.org/en/news/archive/2007/6687-qi-was-paid-to-betray-protestorsq-2752007

something close to it, together with a covert approach for at least one person of interest. The Inquiry found the broad nature of the instructions to the private investigators, without explicit controls to protect privacy interests, breached the Code of Conduct requirement to respect individual privacy and avoid activities that might harm the reputation of the State Services.

The Ministry of Social Development was aware of the potential use of low-level surveillance and a covert approach in the White case. The Inquiry did not see any evidence that MSD queried this or sought any assurance that individual privacy would be properly weighed and protected. Accordingly, the Inquiry found that MSD was in breach of the Code of Conduct, although at a lower level than Crown Law. The breach was at the lower end of the scale given that Crown Law had primary responsibility to manage the litigation and direct the private investigators.

Context

3.54 From approximately 2000 Crown Law acted on behalf of the Department of Child, Youth and Family[67] to defend a civil claim brought by two brothers who alleged they were abused in state care (the 'White' case).[68] The litigation was treated as a test case, in part to address questions of limitation, financial loss and damages, which would be of broader application in future claims. Child, Youth and Family, through Crown Law, devoted considerable resources to defending the claim. From July 2006, the Department of Child, Youth and Family became part of the Ministry of Social Development. The Crown's legal team included a number of lawyers from Crown Law, plus an external senior counsel and support from MSD lawyers and social workers. The case went to trial over several weeks between June and November 2007.

3.55 As part of its preparation for trial, Crown Law instructed a private investigation company, Insurance and Commercial Investigations Ltd (ICIL), to assist the legal team. The tasks included low-risk steps such as searching public databases to find contact details for witnesses, compiling and analysing documents, and assisting counsel to brief witnesses in person. However, there were also higher-risk instructions as described below, which had the potential to involve in-person observation and covert activity.

3.56 The primary investigator was a former Police detective from ICIL. At least two other investigators also worked on the case, either as employees or contractors of ICIL. The Inquiry saw invoices totalling more than $90,000 paid to ICIL over 6 months from January to July 2007. While the invoices did not include reference to the number of hours worked, this amount of money indicates a near full time equivalent workload. This would not have been purely field investigation work; considerable time was spent briefing witnesses and assisting with other trial preparation tasks.

3.57 There was no record of a written contract, and the investigators were largely tasked by members of the legal team, sometimes by email and sometimes orally as the case developed. File notes indicate Crown Law wanted a very broad inquiry into the circumstances of all witnesses, including life experiences and medical history.

3.58 In January 2007, there was a meeting of the Crown Law and MSD legal team with the lead private investigator. The question of surveillance was raised, and the legal team did not rule

[67] At the time, Child, Youth and Family was a separate Department.

[68] See *White v Attorney-General* CIV-1999-485-85, High Court Wellington, 28 November 2007, Miller J.

out some low-level surveillance closer to trial. In March 2007 an investigator referred to a proposed covert approach, without objection from the legal team.

3.59 In February 2007, MSD raised a concern about the reputational risk for the organisation if MSD staff knew that a private investigator was interviewing them. It was suggested that the investigator be presented as part of the litigation team, rather than as a private investigator.

3.60 There are indications in the file that the investigators used methods that may have either involved low-level surveillance or something close to it. In April 2007 an investigator conducted enquiries into a potential Crown witness including extensive checks of databases, but also 'pretext visits' to the man's home and neighbours. The investigators noted down car registration numbers, the man's appearance as he came home, and the view, from the outside, of the interior of the man's home. The lead investigator took the view that this activity was not surveillance as he understood the term, because it did not involve following the individual from place to place or over an extended time.

3.61 In early April 2007, the legal team tasked the investigators to make enquiries about the plaintiffs' similar fact witnesses. There were approximately 13 or 14 such witnesses, who provided statements that they experienced abuse similar to the plaintiffs in the relevant institutions. The first on the list was the witness described below, who alleged he encountered men watching him and his home.

3.62 In June 2007, the investigators were asked to make very broad inquiries about the similar fact witnesses including anything in their adult lives that might be used in cross-examination.

3.63 Around the same time, the sister of one of the plaintiffs complained that one of the investigators behaved in a demanding and aggressive way. This was denied by Crown Law, and the Attorney-General was briefed. Internal documents at the time stated that the private investigators had not undertaken surveillance work.

Specific allegation of surveillance

3.64 Earlier this year one of the similar fact witness for the plaintiffs in the White case gave a public interview, among other things describing having encountered two men watching him and his home during the lead up to the trial in 2007.

3.65 As a similar fact witness, the man had made a written statement describing his own experiences of abuse in state care. The plaintiffs' lawyers provided this statement to the Crown. The man did not ultimately give evidence in the trial for personal reasons, but he was also independently a claimant against the Crown represented by counsel.

3.66 The man gave evidence on oath to the Inquiry that he came home one day in winter 2007, around the time of the trial, to find two men sitting in a car outside his house watching him. He said the men had been there at other times over the previous three days, and he confronted them. The men acknowledged they were investigators and were watching him. They had the look of being Police detectives. The timing and circumstances led him to believe the men were investigators acting on behalf of the Crown / MSD. He could not think of any other plausible explanation for the men to be watching him at that time. Unfortunately, he did not take down the licence plate of the car.

3.67 As noted above, the file confirms that the private investigators instructed by Crown Law did make enquiries about the man around this time, as part of the broad instruction to find out

anything from the adult lives of the similar fact witnesses useful for cross-examination. In that context, Crown Law supplied the man's name and statement to the investigators.

3.68 When asked about this in February this year, a Crown Law spokesperson said: 'With respect to the claim that two men were parked outside a witness's address, we do not have any knowledge about that. From your description, it sounds like surveillance of a witness. The Crown would not instruct a private investigator to do that.'

3.69 The Inquiry found the man's account to be credible. It was described candidly, and the available material includes some corroborating information. As noted, the man was the first similar fact witness on the list supplied to the investigators, who had details of his home address. The investigators were ex-Police officers, and financial records indicate they spent many hours working on the case around the time the witness describes having been subject to close observation. Their tasking in relation to the similar fact witnesses was extremely broad, and did not rule out surveillance. The earlier note raising surveillance had not ruled it out, but suggested the possibility of some low-level surveillance closer to the trial, which started in June 2007. The focus on this man occurred in the period immediately leading up to the trial. There had also been reference to the use of a covert approach when seeking to locate a potential person of interest.

3.70 The lead private investigator strongly denied there had been surveillance of this witness. He said it was not logical for surveillance to have taken place, and it made no sense for the investigators to have acknowledged they were watching the witness when approached. He said it would have been standard practice for anyone conducting surveillance to deny it, and that if their cover had been blown in that way there would have been internal reporting. However, the investigators' notebooks were not found, and on the approach taken by the investigator, he would not have regarded close observation of the sort described by the witness as surveillance. The Inquiry was not able to speak to the other members of the investigation team.

3.71 Ultimately, the overall circumstances make it impossible to rule out the possibility that some form of close observation by members of the investigation team may have occurred, even if not carried out by the lead investigator. This would have been consistent with the type of low-level surveillance seemingly contemplated. The passage of time, the absence of the investigators' notebooks, and the lack of detail such as a car registration plate, make definitive findings impossible at this stage.

Application of the Code of Conduct – Crown Law

3.72 In the Inquiry's view, surveillance by the government of a participant in a civil case is generally improper, or at least highly unusual and something that would require careful oversight and controls to assess and balance privacy interests. The Solicitor-General confirmed to the Inquiry that this is also her view and expectation. This was reflected in Crown Law's response to a journalist's enquiry earlier this year, which stated the Crown would not instruct a private investigator to carry out surveillance of a witness.

3.73 On the evidence provided to the Inquiry, Crown Law was aware that private investigators, acting on its behalf, had signalled a covert approach and pretext visits. The steps taken in relation to one potential Crown witness at the very least bordered on surveillance. When surveillance was raised explicitly as an option, the legal team did not rule it out at a low-level closer to trial. Shortly before trial, Crown Law instructed the private investigators in broad

terms to investigate opposing witnesses to help the Crown in cross-examination. There were then credible allegations that one of those witnesses was subject to close observation, although it was not possible to reach a definitive finding whether the Crown's private investigators carried this out.

3.74 In the Inquiry's view, the broad instructions from Crown Law to the private investigators in this context, without controls to weigh individual privacy and avoid covert activity without specific oversight, did not provide sufficient protections to protect individual privacy, and risked harming the reputation of the Crown.[69] Accordingly, there was an institutional breach of the Code of Conduct by the Crown Law Office.

Application of the Code of Conduct – MSD

3.75 Crown Law had primary responsibility for managing the litigation and instructing the private investigators. For their part, MSD lawyers were involved in regular meetings with the legal team. In particular, MSD was aware of the instructions to the private investigators, and on occasion raised concerns about the scope and cost of the engagement.[70] MSD also approved the initial engagement of the investigators and paid the bills.

3.76 Members of MSD's legal team knew about the potential use of low-level surveillance and a covert approach. MSD was also conscious of the potential reputational effects of the investigators' actions in relation to its own staff, and made its views known in that regard. However, MSD staff do not appear to have queried the potential use of surveillance or a covert approach for non-MSD witnesses, nor sought any assurance that individual privacy would be properly weighed and protected. Accordingly, the Inquiry finds that MSD was in breach of the Code of Conduct, at a lower level than Crown Law. Given that Crown Law rather than MSD had primary responsibility to manage the litigation and direct the private investigators, and that the instructions to the investigators came from Crown Law, the Inquiry considers MSD's breach to be at the lower end of the scale. The Inquiry did not see anything to indicate that senior managers in the Ministry knew about or directed the potential use of surveillance or a covert approach.

Additional surveillance engagements by MSD

3.77 In addition, the Ministry of Social Development informed the Inquiry that it used private security consultants for surveillance in four investigations into specific cases of fraud or suspected fraud. The Inquiry was assured by the Chief Executive that these engagements were appropriate and well-managed. There do not appear to be any grounds for finding a breach of the Code of Conduct.

3.78 Finally, for completeness, the Ministry informed the Inquiry that it used private investigators to conduct mystery shopping exercises in 2010–2011 in relation to alleged predatory practices by traders targeting beneficiaries. The Inquiry does not consider these engagements breached the Code of Conduct.

69 The relevant conduct appears to have spanned both the current and previous codes of conduct, but as noted in section 2, the Inquiry does not consider there is a material difference between them as they apply here.

70 The concern about scope does not appear to have related to the potential use of low-level surveillance or covert measures, but rather to managing extent and cost of the engagement as the trial approached.

Ministry of Business Innovation and Employment

MBIE's use of licensed private investigators to conduct surveillance in Operations Woodland and Lee in accordance with MBIE's regulatory responsibilities did not breach the Code of Conduct. However, there should have been a written contract for the work undertaken in Operation Lee.

3.79 In the media coverage leading up to the Inquiry, Greenpeace raised particular concern that MBIE may have engaged Thompson and Clark in relation to the petroleum and minerals sector, which is administered by a particular division of MBIE – the New Zealand Petroleum and Minerals group (NZP&M). The Inquiry found that NZP&M did not engage or procure surveillance services from Thompson and Clark or other external security consultants.[71]

3.80 However, in other areas, MBIE has on occasion engaged external security consultants, including for surveillance.[72] In particular, MBIE engaged external security consultants to carry out covert surveillance in support of two investigations into regulatory non-compliance in the residential building and construction sector:

a Operation Woodland, in March to June 2015, was a significant investigation related to regulatory compliance in the residential building and construction sector in Auckland. This operation was conducted by Paragon Investigations Ltd in a subcontracted arrangement with two certified private investigators.

b Operation Lee, in September 2015, related to regulatory compliance in the construction sector. It was conducted by Strategic Security Services Ltd (no longer trading).

3.81 The surveillance focused on the residential construction sector in the Flat Bush area in Auckland. Regulatory and enforcement officials had been made aware of multiple potential offences, including using unlicensed building materials, removing building materials after inspection, and breaches of employment legislation and the Immigration Act 2009. The tasking concentrated on a limited number of residential construction job sites that were known to be under development by the target companies. Surveillance was undertaken at the site, and there was some physical tracking of individuals and taking of photographs as the operation tried to identify the supply of potentially faulty materials.

3.82 The purpose of both operations was to obtain evidence of alleged non-compliance across a range of regulatory jurisdictions, including: contravention of the Building Act 2004; breaches of minimum employment standards under the Minimum Wage Act 1983 and other statutes; breaches of the Immigration Act; breaches of the Companies Act 1993; assorted potential licensed building practitioner issues; and suspected tax fraud, which falls under the regulatory jurisdiction of the Inland Revenue Department.

3.83 The evidence obtained was insufficient to prosecute under the various MBIE enforcement arms, and the information gathered in the surveillance was instead passed on to the Serious Fraud Office and Inland Revenue.

3.84 Neither operation was carried out by Thompson and Clark. Both providers for these operations were licensed private investigators. Operation Woodland was conducted under a variation to an existing contract with the provider. Operation Lee resulted in MBIE incurring expenses of less than $10,000 and was not the subject of a contract. The operations were

[71] There was, however, a close relationship between MBIE and Thompson and Clark in this area, which is explored in Section 4.

[72] Other engagements include process serving and asset seizure.

overseen by a Governance group involving General Manager-level employees from different regulatory functions within MBIE. Funding for Operation Woodland was separately approved and the relevant Deputy Chief Executive was informed of the intention to progress a long-running, complex investigation through carrying out time-limited surveillance.

3.85 Operation Lee and some of MBIE's use of external security consultants for non-surveillance work (such as asset seizure) was undertaken without contract. However, a contract is necessary in our view for any engagement involving surveillance given its intrusive nature and the need to address the complex legal issues that arise from it.

Application of the Code of Conduct

3.86 Operations Woodland and Lee were undertaken by licensed private investigators consistently with MBIE's regulatory responsibilities, and the Inquiry considered that the investigators' activities did not give rise to material concerns under the State Services Code of Conduct. However, there should have been a written contract for the work undertaken in Operation Lee.

ACC

The Inquiry was not made aware of any concerns about ACC's use of surveillance in the context of specific investigations into ACC fraud. The current processes governing surveillance appear to be well-developed and appropriate, and no Code breach was found.

3.87 ACC has for many years engaged external security consultants to help detect and prosecute fraud. In some cases, the external consultants conduct visual surveillance, including taking photographs and video of claimants to support prosecutions.

3.88 The ACC investigation unit has developed a standard operating procedure to govern the use of visual surveillance in these investigations. This 16-page document has been prepared with legal advice, and provides a detailed framework designed to ensure surveillance is carried out lawfully and ethically, as described from paragraph 2.23 above.

3.89 Providers of these services form part of a small panel. Assurance reviews are undertaken periodically to assess compliance with the ACC Code of Conduct, which is consistent with the State Services Code of Conduct. The Inquiry received evidence of the range of investigative services provided to ACC, with a focus on the last four financial years. We received an assurance from the Chief Executive that he was confident appropriate controls and oversight were in place to manage the use of these providers.

3.90 The Inquiry was not made aware of any recent concerns about ACC's use of surveillance in this context. The current processes governing surveillance appear to be well-developed and appropriate.

Department of Internal Affairs

The Department of Internal Affairs did not breach of the Code of Conduct in using private investigators to conduct surveillance of people subject to cancellation of citizenship. However, there should have been written contracts with appropriate safeguards.

3.91 The Department of Internal Affairs uses external security consultants (private investigators) to serve notices of deprivation of citizenship, where initial inquiries have found that the intended recipient is likely to be difficult to locate. Private investigators may use surveillance techniques (close observation) where the individual concerned is thought to be difficult to locate or might be seeking to avoid authorities. The investigators engaged by the Department confirmed this to the Inquiry.

3.92 There have been 13 cases of deprivation of citizenship in the last six years, and at least two cases involving surveillance. In both cases the Department engaged Paragon New Zealand to carry out the surveillance, and the Department told the Inquiry the investigators are given specific instructions about how to operate and report. However, there were no written contracts.

Application of the Code of Conduct

3.93 The Department used external security consultants to carry out surveillance in very limited circumstances in order to enforce the Citizenship Act 1977. In these circumstances the Inquiry does not find a breach of the Code of Conduct although an appropriate written contract would have provided further safeguards.

Maritime New Zealand

Maritime New Zealand did not breach of the Code of Conduct when engaging a private investigator to conduct surveillance of a ferry when enforcing safety legislation. However, there should have been a written contract with appropriate safeguards.

3.94 In 2008 Maritime New Zealand engaged an external security consultant, Securitek NZ Ltd, to undertake surveillance after Maritime NZ received several complaints involving potentially significant safety issues relating to the operation of a particular vessel. Maritime NZ staff had failed to substantiate the complaints during visits to the vessel while it was operating, and they therefore engaged an external investigator to film the loading and unloading of the vessel and to travel on-board the vessel to observe the conduct of crew.

3.95 The operation, named ‘Operation Luna’, included two days of surveillance, with two private investigators conducting the operation around sailing times. The surveillance involved filming the loading and unloading of the vessel, in a place open to the public; and travel on the service to note and video or photograph items of interest during the journey.

3.96 The material collected provided Maritime NZ with sufficient information to require the operator to improve the loading and unloading of their vessel.

Application of the Code of Conduct

3.97 The procurement of services in this instance was directly relevant to Maritime New Zealand’s enforcement activities under the Maritime Transport Act 1994, and the surveillance was in response to a specific suspicion of offending under that Act. The decision to procure services in this way was made only after investigators from Maritime NZ had ruled out alternatives. The total value of the services was less than $5,000 and did not therefore require a contract for services under the financial delegation rules.

3.98 For these reasons the Inquiry does not find a breach of the Code of Conduct. However, as with MBIE's engagements referred to above, there should have been a written contract with appropriate safeguards.

Ministry of Health

The Ministry of Health did not breach the Code when contracting mystery shopper services. The day-to-day management of the contracts was appropriate, but the Ministry should consider reviewing its contracting arrangements as they are now outdated.

3.99 The Ministry of Health engaged external security consultants to undertake public health enforcement functions, including 'mystery shopping' to monitor compliance with the Sale and Supply of Alcohol Act 2012, the Smoke-free Environments Act 1990 and the Psychoactive Substances Act 2013. The element of subterfuge arguably makes this a form of surveillance, but in this context there was a relatively low likelihood of a privacy intrusion.

3.100 There have been three main providers of these services since contract arrangements were made in 1999. These include two independent consultants, and Thompson and Clark. The amounts involved per engagement were not large. In total, however, the contracts have amounted to more than a million dollars over approximately the last decade.

Application of the Code of Conduct

3.101 The Ministry of Health had contracts in place for these services. The contracts were detailed, and this included providing for how the suppliers should conduct themselves. The Inquiry's view is that the day-to-day management of the contracts was appropriate.

3.102 However, the agreements have now been in place for a significant period. During that time, there have been changes in investigative practices (including the introduction of the new licensing regime in 2013), in the legal environment related to the use of surveillance, and in the available providers of these types of service. The Inquiry's view is that the Ministry of Health should consider reviewing its current contracting arrangements. The review should include updating the Ministry's contracts to reflect current legal parameters, and also testing the continued need for such services and, if they are still required, developing a procurement process that goes to market to test the potential suppliers of these services.

Cyclops Monitoring

Various agencies' use of remote camera monitoring services by Cyclops Monitoring, a company associated with Thompson and Clark, did not breach the Code of Conduct. However, the area justifies further attention in any future engagements.

3.103 The Inquiry identified four instances of government agencies using the services of Cyclops Monitoring Ltd, a company associated with Thompson and Clark.[73] Cyclops Monitoring provides advanced security camera services, using internet-enabled security cameras. The cameras use motion-sensing technology to capture images and transmit them to Cyclops for real-time off-site monitoring and analysis, which enables an immediate response if

[73] Until 6 July 2018 Cyclops Monitoring Ltd and Thompson and Clark Investigations Ltd had the same two directors. The two companies have at all times had the same two shareholders.

appropriate. The service aims to enable proactive responses to security threats, rather than waiting to review security footage after a security incident. The technology used by Cyclops is in an early stage of development, and government agencies engagement with this company has been limited:

a The Ministry of Education trialled wireless monitored security cameras from Cyclops Monitoring in five schools in Auckland for six months, which enabled immediate responses to people on school sites after hours to deter vandalism.

b Land Information New Zealand and the Canterbury Earthquake Recovery Agency used Cyclops to monitor the security of properties in the Red Zone following the Canterbury earthquakes.

c Housing New Zealand Corporation participated in a short trial of the technology with the NZ Police, installing cameras in vacant properties to prevent theft and damage.

3.104 In addition, Cyclops Monitoring received a project grant of $225,000.80 (excl. GST) in 2014-15 from Callahan Innovation. This grant was to support the research and development of Cyclops Monitoring's remote monitoring technology. The grant related to the technology that allows Cyclops to connect to existing cameras.

3.105 There are a wide range of security camera and security guard providers that are properly engaged by government agencies to support safety and security of government property and facilities. The Inquiry found that the use of Cyclops Monitoring was limited and focused on relatively standard and low-risk security camera services, with reports of some benefit and efficiency from the ability to respond in real time to intrusions or security breaches. Thompson and Clark noted that CCTV cameras are common and typically positioned on private property to protect assets. They also pointed out that Police regularly review data from multiple cameras.

3.106 However, the engagement of external companies such as Cyclops to carry out 24-hour remote monitoring of security camera data could potentially become a high-risk activity. This is particularly so within the context of emerging data analysis technologies, connected data systems, and machine learning-assisted interrogation of 'big data'. If widely used by different public and private clients, there is potential for a single company to have the capability to track individual movements in an invasive way. This highlights the importance of government agencies fully considering the implications of engaging external providers and ensuring there are appropriate safeguards for the information that is provided and entrusted to those providers.

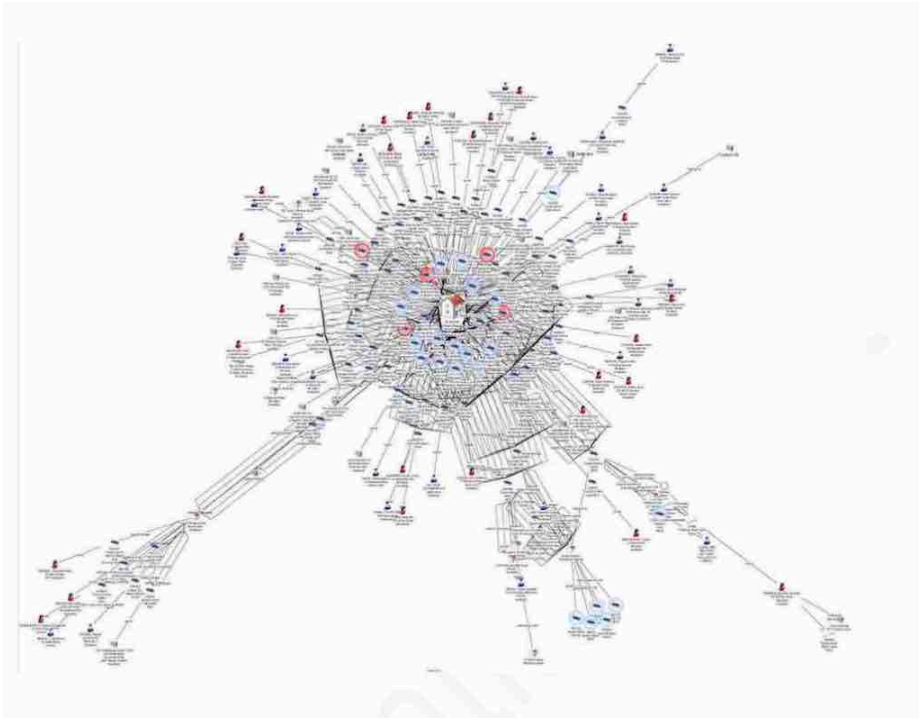
3.107 In our view, government agencies need to put privacy controls in place to ensure that their involvement in any network of that type is appropriate, and that there are appropriate safeguards around the information that is provided and entrusted to any provider. The Inquiry does not find a breach of the code, but this is an area that will justify attention by agencies in any further engagements.

Receiving information obtained or informed by surveillance

3.108 In addition to the agencies who engaged external security consultants directly to carry out surveillance as described above, several agencies received information from Thompson and Clark that in some cases may have been obtained or informed by surveillance. These agencies did not seek or endorse the surveillance, but the Inquiry considers care is necessary to ensure the receipt of such information does not create an impression of tacit endorsement.

3.109 Thompson and Clark obtained information from surveillance in at least two categories. The first was traditional surveillance. It was clear to the Inquiry that Thompson and Clark conducted large-scale surveillance of Greenpeace through close observation, supported by extensive searches of government databases – in particular the motor vehicle and driver licence databases. Thompson and Clark justified searching the motor vehicle database on the grounds that they were acting on behalf of MBIE and the Police, although those agencies categorically denied that this was the case. Thompson and Clark continue to dispute this, and the topic is considered further below in the section dealing with access to NZTA databases.

3.110 In 2012, an analyst for Thompson and Clark compiled a chart depicting hundreds of individuals, vehicles and addresses connected to Greenpeace. The information for this chart came largely from surveillance logs and motor vehicle checks. The image below is blurred to protect privacy, but the full chart contains details about people, companies, buildings and vehicle movements centred around Greenpeace's headquarters:



3.111 This chart came to the Inquiry's attention because it was created by Thompson and Clark's analyst while working for the Ministry of Agriculture and Forestry, using software licensed to

the Ministry. This is discussed further below in the secondary employment section. It is understood that the clients for the underlying surveillance were private oil and gas companies, not government agencies. Thompson and Clark states that the information in the chart was not provided to the oil and gas clients, and that the work was carried out in order to provide accurate information to MBIE and Police about threats to the oil and gas industry.

3.112 The second category of surveillance by Thompson and Clark was social media monitoring of closed groups under assumed identities. Thompson and Clark's social media monitoring was carried out under assumed identities, and the company told DOC that it monitored 'closed sources of information for analysis'.[74] This suggested Thompson and Clark had access to closed sources, and conducted social media monitoring in a way that may have constituted surveillance on the extended definition used in this report.[75] Despite its previous statement to DOC, Thompson and Clark denied that this was in fact the case.

3.113 The Inquiry was concerned about the risk that some government agencies may have received information – for example about the capabilities or plans of Greenpeace – that was informed by this surveillance information. While the surveillance was carried out for private clients in the oil and gas industry, government clients may have inadvertently received information informed by this surveillance.

3.114 Thompson and Clark's threat assessments, newsletters and situation reports about 'issue motivated groups' were potential vehicles for such information. While the information in the newsletters and situation reports was typically described as 'open source', derived from open web pages, in at least one case a threat assessment appears to have included information gathered through both forms of surveillance described above.[76] The agencies at greatest risk of receiving such information were MBIE and NIWA.

3.115 While the Inquiry did not see widespread examples of inappropriate surveillance information being received by government agencies, there is a need to be careful that receiving such information does not create a perception of tacit governmental approval of surveillance. The Inquiry does not suggest that MBIE or NIWA acted unreasonably in these circumstances, but in light of the information now available, care will be justified in any future engagements.

Engagements not involving surveillance

Overview

3.116 Government agencies also engage external security consultants for purposes not involving surveillance. These include comparatively low-risk activities such as serving documents, acting as security guards, and undertaking building security assessments. These are

74 Email from Director of Thompson and Clark to officials at DOC and other agencies, 21 September 2016.

75 In the Inquiry's view, it may be a breach of a reasonable expectation of privacy for a person to join a closed social media group under a covert or false identity. This type of conduct may therefore be a form of 'surveillance', requiring appropriate controls and management. Social media surveillance of this sort is not necessarily a breach of the Code of Conduct, as this depends on the purpose, context and management of the activity.

76 See the discussion of the Threat Assessment provided to NIWA from paragraph [3.153] below. The full list of government clients receiving such reports was Southern Response, the Department of Conservation, the Ministry of Agriculture and Forestry, MBIE, AgResearch, Scion, GNS and NIWA.

summarised in Appendix 4. The analysis below relates to other engagement with Thompson and Clark.

Department of Conservation

DOC's engagement of Thompson and Clark to carry out security risk assessments and related services did not breach the Code of Conduct.

Nature of the engagement

3.117 The Department of Conservation (DOC) engaged Thompson and Clark on two separate occasions.

3.118 The first was a short engagement in 2015 to undertake a security risk assessment ahead of the National Fieldays at Mystery Creek, where DOC intended to have a stand. This engagement was organised at a regional office and was small-scale. The employee concerned had previously engaged Thompson and Clark to provide similar advice when he worked at AgResearch. The Inquiry found this engagement to be unremarkable.

3.119 The second engagement is more relevant to the Inquiry. DOC regularly partners with other agencies to undertake 1080 operations as it is an effective means of controlling rats, possums and stoats, which are a threat to New Zealand's native birds. It is also biodegradable making it suitable for aerial application over rugged and inaccessible terrain.

3.120 DOC, OSPRI (TBfree NZ), Federated Farmers, Forest & Bird and the New Zealand branch of the Worldwide Fund for Nature all agree that 1080 is an effective, safe and valuable tool in the fight to protect New Zealand's native species. However, significant opposition remains.

3.121 The Inquiry received evidence in the form of departmental health and safety incident reports, including reports of specific incidents of harassment attributable to anti-1080 protests. Over the most recent two-year period (ending September 2018) departmental employees and contractors were subjected to 52 reported threats. These incidents included serious physical confrontations, threats of violence, vehicle tampering, and damage to departmental facilities.

3.122 DOC engaged Thompson and Clark in October 2016 through a standard contract for services, including security awareness services involving situational reports, first responders training, a security response plan, residential security reviews, and commercial security reviews. DOC was aware that Thompson and Clark provided services to other government agencies and also to OSPRI specifically around 1080 threats.

3.123 A second contract, entered into in May 2017, related to the development of a physical security policy, complete national threat assessments for DOC, visits to pilot sites, and security assessments of pilot sites. This second contract was also seen as relevant to the Government's Protective Security Requirements.

3.124 The Department of Conservation took steps to retain information provided to them by Thompson and Clark via the 'Slack' platform. The Inquiry reviewed this information and found no examples of closed source intelligence.

3.125 The contract with Thompson and Clark was terminated under the no-fault provision in July 2018.

Application of the Code of Conduct

3.126 To support the self-assurance processes offered by the Inquiry, DOC undertook an extensive forensic examination of its information holdings. In addition, it informed the Inquiry that it had focused discussions with Director Assurance, Director Safety, relevant solicitors and compliance officers, and other relevant DOC staff. This forensic search did not draw any material issues to the attention of the Inquiry.

3.127 The Inquiry noted that DOC put in place robust contracting arrangements with Thompson and Clark. These contracts included provisions relating to the application of the Code of Conduct, including that suppliers 'must, before commencement of a project with the Director General, read the Code of Conduct issued by the State Services Commission'. Clause 3.2 provided that the contract must be fair, impartial, responsible and trustworthy. Schedule 3 of the main contract also attached the Code of Conduct.

3.128 The Inquiry found nothing extraordinary about the engagement between DOC and Thompson and Clark.

AgResearch Limited

AgResearch's engagement of Thompson and Clark was adequately governed, responded to a specific set of threats, did not involve surveillance, and was not inconsistent with the Code of Conduct.

3.129 AgResearch Ltd is a Crown Research Institute whose purpose is to enhance the value, productivity and profitability of New Zealand's pastoral, agri-food and agri-technology sectors. Among its other functions, AgResearch is one of the country's leading researcher on the use of genetic modification technologies and also undertakes some research involving use of animals.

3.130 In 2001, there were incidents of threats and intimidation directed at AgResearch scientists who were involved in research at the Ruakura facility in Hamilton that included genetic modification of cows. These threats included a graffiti attack at a scientist's home and later a Molotov cocktail incident at the AgResearch headquarters. More stringent security measures including a new security system were put in place, and in June 2006 the National Manager of Resources and Facilities entered into a contractual relationship to receive a Risk Management Package and associated services from Thompson and Clark.

3.131 While the original term of the engagement was one year, Thompson and Clark continued to provide a Risk Management Package to AgResearch until 2016. In June 2007, at the same time as the 'Happy Valley' incident, AgResearch defended its use of Thompson and Clark to its responsible Minister, citing serious concern about the health, safety and security of its employees.

Nature of the engagement

3.132 Throughout the 10-year engagement, AgResearch received the following services from Thompson and Clark:

a Regular situational assessment reports that summarised reporting of activist or oppositional activity, including media activity, protests and other forms or organised opposition to animal testing and genetic modification activity

b Assistance with an investigation of an employee involving stolen lab equipment

c Site visits to assess security at individual sites

d Security advice and support for AgResearch's involvement in NZ Fashion Week (2009 and 2010)

e Security planning and support for a number of major events (particularly in 2009 and 2010).

3.133 The nature of the regular reporting received from Thompson and Clark changed over the course of the engagement. Early reports provided a regular monthly overview of 'National Extremism', which highlighted the protest activities of groups of different types, ranging from animal rights to anti-GE, anti-war/globalisation/racism and environmental. The reports grouped issues by theme and by categorizing domestic and interactional protest or activist activity. AgResearch was able to provide the Inquiry with a good history of this reporting, with the exception of 2009/10, where there were IT-related constraints. On reviewing the evidence, the Inquiry found that these early reports can best be described as akin to a moderately sophisticated media monitoring analysis. The main sources for the reporting were media outlets (newspaper, television and radio), political websites (including government websites), activist websites, and similar outlets overseas. As time progressed and technology matured, the Inquiry was able to see increased use of social media as a source for the reports.

3.134 In 2014 the frequency and detail of Thompson and Clark's reporting increased and AgResearch began to receive regular weekly situational reports. This increase in regular reporting followed the adoption of a full risk management package from Thompson and Clark, which the Inquiry was told was partly in response to the protest activity and community opposition in response to the plan to relocate a number of roles at its Invermay campus, near Mosgiel, to other campuses (which would result in a reduction in AgResearch staff numbers and operations at Invermay). These situational reports were more closely aligned to issues related to animal rights and GE. The regular reports continued until AgResearch terminated the arrangement in April 2016 after an internal review, which assessed the benefit the briefing was bringing and the cost, and found that the risks were low.

Application of the Code of Conduct

3.135 Despite the longevity of the arrangement between AgResearch and Thompson and Clark, the level of activity was largely limited to regular reporting. The Inquiry heard evidence that the original decision to engage Thompson and Clark had been informed by concerns about the safety of AgResearch staff and the security of its facilities, and that the decision had been made by senior managers after discussion with members of the executive team.

3.136 Despite several attempts by Thompson and Clark to extend the engagement to include additional services, AgResearch kept the engagement linked to the original purpose. The reports enabled AgResearch to anticipate protest activity and organise an increased security presence in response. This security presence provided by Thompson and Clark was limited to a handful of specialised high-profile events.

3.137 Throughout the engagement the relationship was mainly managed by a single senior manager within the facilities part of AgResearch, who distributed regular reporting to site managers. Occasionally there were specific engagements to meet the particular needs of individual sites. The current Chief Executive was aware of the arrangement (including when and why it was terminated), but had no relationship with Thompson and Clark. All employees

interviewed by the Inquiry claimed to have no knowledge of any surveillance undertaken by Thompson and Clark, nor did financial statements indicate that any surveillance was likely to have occurred.

3.138 The Inquiry team fully reviewed the reporting provided by Thompson and Clark and could find no clear evidence that the material was sourced other than through open sources. However, given the volume of material and the potentially closed nature of some social media forums, it is difficult to provide a definitive view on this. The Inquiry noted above the broader concern that agencies may have inadvertently received information obtained or informed by surveillance.

3.139 Overall, the Inquiry found that AgResearch's engagement of Thompson and Clark was adequately governed, responded to a specific set of threats, did not involve surveillance, and was not inconsistent with the Code of Conduct.

Southern Response Earthquake Services Ltd

Southern Response acted reasonably in engaging Thomson and Clark to provide services other than surveillance, including threat assessments and security reviews. There was no breach of the Code.

Nature of the engagement

3.140 As well as engaging Thompson and Clark to attend meetings, Southern Response engaged external security consultants to undertake the following activities:

a **Perform overall threat assessments for Southern Response and its employees** – These high-level security assessments involved desk-top analysis and intelligence gathering from open source documents. A weekly monitoring report was provided to Southern Response from early 2014 until mid-2017. These weekly reports comprised information similar to a traditional media and social media report using open sources of information, and were not extraordinary in their content. The most common source of much of the social media analysis was open comments made by individuals and organisers on public Facebook pages, including *Southern No Response* and *Quake Outcasts*. The analysis enabled Southern Response to draw on an up-to-date threat assessment at short notice.

b **Security reviews of Southern Response's office and operations** – These reviews included an assessment of physical risk, staff training on de-escalation and personal safety, and advice on electronic communications risk. The reviews were consistent with reasonable expectations for the protection of employees, the general public and the security of Southern Response's physical environment, and were not extraordinary.

c **Security reviews of the private dwellings of those employees and Board members who were at risk or who were targeted in specific threats to Southern Response** – These reviews involved a qualified expert inspecting the private dwellings of individuals and making a series of recommendations to improve physical security (for example, locks and security cameras), as well as a review of publicly available identifying information (for example, personal social media settings, and phone number listings). These assessments seemed consistent with reasonable steps to protect individual employees and Board members and were not extraordinary.

d **Security advice to support Southern Response's annual meetings** – This included an update of the overall threat assessment; advice to Board members and employees involved in the meeting; and liaison with the NZ Police, a local security firm and the venue managers. This advice did include recommendations relating to the issuing of trespass notices to individual claimants where those claimants were considered to be disrupting the meetings, including threats of physical harm or harassing and disruptive behaviour. These services were consistent with a reasonable expectation that Southern Response should protect employees, Board members and the general public attending the meeting, and were not extraordinary.

e **Detailed security risk assessments of individual claimants who had made specific verbal or physical threats or whose behaviour was perceived as harassment of Southern Response's employees or its contractors** – This included advice to Southern Response about the nature of any threat, and recommendations for steps the company should take. The advice included recommendations on when and how to make a formal complaint to the NZ Police and associated support in making those complaints. In a limited number of cases external security consultants also undertook detailed open-source assessments of individuals perceived to be a threat to Southern Response. In some cases specific legal advice was also sought. There was no indication of surveillance of individuals, including any review of material over which the individuals could have had a reasonable expectation of privacy.

f **Fraud investigations.** Southern Response engaged an external consultant (not Thompson and Clark) to carry out relatively infrequent and small scale investigations into cases of alleged fraud, consistently with industry practice.

Application of the Code of Conduct

3.141 The Inquiry considers that Southern Response acted appropriately under the Code in seeking professional external security advice during a period of great stress to its clients and as the company was increasing in its maturity in relation to key aspects of managing its relationships with clients.

3.142 There were good reasons for Southern Response to engage Thompson and Clark for non-surveillance activities, but there would have been benefits in having a formal contract given the nature and amount of work. Overall, the process of engaging Thompson and Clark did not result in a misuse of Southern Response's resources.

The issue of the treatment of individuals

3.143 Southern Response had a duty to ensure that its employees, the Board and members of the public were safe from threat of harm from individuals. Throughout the period under review, there was also a step-change in this expectation as required by a change in health and safety legislation and the lessons from the tragic shootings in Ashburton. Southern Response engaged appropriate professional advice to assist it in determining this risk, and engaged professionally with the NZ Police where it felt that such a risk might give rise to a level of harm. They had in place a process for identifying individuals that enabled them to differentiate their approach in a transparent and objective manner. The Inquiry found that this process was fair and reasonable.

The issue of the overall threat, and threat arising from individuals

3.144 For the State Sector, care needs to be taken to carefully dissect the notion of 'threat'. Throughout the Inquiry we observed that the word 'threat' was used in different ways.

3.145 It was reasonable (and responsible) for Southern Response to commission expert advice to inform itself about individuals making direct threats of harm to employees and the general public.

3.146 What would be less reasonable, under the terms of the Code, is to apply different treatment to customers, clients or members of the public who express their dissatisfaction with an activity or decision of an organisation or state servant by exercising their democratic right to protest or by engaging with institutions set up to support fair democratic process such as the Ombudsmen or the Privacy Commissioner.

3.147 The Inquiry found that Southern Response's engagement of Thompson and Clark to conduct surveillance was inconsistent with and breached the Code. However, the Inquiry has found that in engaging Thompson and Clark to provide other services that did not involve surveillance, Southern Response acted reasonably in balancing concerns about individual customers against wider threats to the company.

NIWA

NIWA's direct engagement of Thompson and Clark did not give rise to concerns under the Code.

Nature of the engagement

3.148 NIWA is a Crown Research Institute that provides environmental science research to enable the sustainable management of natural resources.

3.149 The Chief Executive informed the Inquiry that to the best of his knowledge, NIWA did not use any external security consultants before 2014. From 2014, NIWA engaged Thompson and Clark on three occasions:

- A 2014 security threat assessment to support deployment of NIWA staff on a project requiring field operations in the Persian Gulf.
- Training in situational security awareness for staff of NIWA's research vessel *RV Tangaroa*, to enable them to manage encounters with someone illegally boarding the vessel, following a protest incident in 2015 when Greenpeace protestors boarded the vessel in port.
- A 2016 review of NIWA's standard Vessel Security Plan, a security threat assessment, and overseeing security operations while the vessel was in port, associated with an upcoming voyage of *RV Tangaroa* for a private-sector client in the oil and gas sector.

3.150 The material provided to the Inquiry included extensive email correspondence between Thompson and Clark and NIWA staff about safety, vessel risk plans, training, situation reports, invoices, minutes of meetings with Thompson and Clark and the crew of the vessel, and possible protests and alerts. Sometimes this correspondence included interactions with NIWA's clients from the oil and gas industry who also engaged Thompson and Clark to provide security advice.

Provision of regular situational reporting

3.151 NIWA received regular generic oil and gas sector situational reports from Thompson and Clark. These contained an overview of protest activity aimed at that sector. The Inquiry's review of these reports indicates that they were based on open-source information.

Security Threat Assessment

3.152 In 2016 NIWA received a threat assessment from Thompson and Clark to support a voyage where *RV Tangaroa* was contracted to a private-sector oil and gas client. The contract with Thompson and Clark was with the client rather than directly with NIWA, despite the fact that NIWA paid for services from Thompson and Clark.

3.153 The Inquiry received the Security Threat Assessment. It provided a more detailed situation report specific to mobilisation for that voyage. While the threat assessment included a caveat that it was based on open-source materials, there was also information that may have been derived from closed-source information. This included statements such as:

> *"… evidence that Greenpeace NZ is keeping its direct action protest teams in a state of readiness and training."*
>
> *"…sensitive information that Greenpeace has recently been training its direct action teams while suddenly increasing its rhetoric against [private sector company], which is one of its current primary targets."*

3.154 The Threat Assessment from February 2016 also made a number of observations about the assets used by Greenpeace and their level of readiness and placement. In several cases the document stated 'it is known …' in relation to Greenpeace, without saying how Thompson and Clark came to have this knowledge.

Application of the Code of Conduct

3.155 The Inquiry considers it was reasonable for NIWA to seek expert advice in responding to the various security issues that arose in its operations for the oil and gas industry. Thompson and Clark provided appropriate services to NIWA, and there was no evidence that NIWA engaged Thompson and Clark directly to undertake surveillance.

3.156 The Inquiry's view is that NIWA's direct engagement of Thompson and Clark did not give rise to concerns under the Code of Conduct.

Ministry of Health

The Ministry of Health's engagement of external security consultants to support enforcement functions did not give rise to concerns under the Code of Conduct. However, the arrangements have been in place for a number of years and should now be reviewed as they are outdated.

Nature of the engagement

3.157 The Ministry of Health engaged external security consultants to provide expert advice and field support to a number of DHBs in relation to enforcement and compliance functions. The contracts were centrally managed by a portfolio manager at the Ministry of Health, but individual DHB public health units could access the providers under contract.

3.158 The contracts included a number of non-surveillance activities, including training for DHB staff on regulatory compliance, and support for investigations into the sale of laser pointers

and into water quality concerns in Northland. In one engagement, security consultants were used by the Auckland Regional Public Health Service (ARPHS) to investigate the use of 1080 in the Hūnua ranges. This involved walking public tracks to ensure that a recent 1080 drop did not cause any public health concerns. The Inquiry received evidence that this was not a service that these external consultants ordinarily provided for the ARPHS, but in this instance it was agreed that they would provide these additional resources as the ARPHS was not able to undertake the full function itself.

Application of the Code of Conduct

3.159 The Inquiry did not consider that any of these engagements gave rise to concerns under the Code of Conduct. However, the arrangements have been in place for a number of years and should now be reviewed, given recent changes in the regulatory and legal environment.

Other agencies

Ōtākaro

Ōtākaro's engagement of Thompson and Clark for physical security reviews and related services did not give rise to any concerns under the Code of Conduct.

3.160 Ōtākaro is a Crown Company that is delivering Crown-led anchor projects in the Christchurch rebuild. The company engaged Thompson and Clark in 2016 to ensure that Ōtākaro met mandatory Protective Security Requirements (described further below) at the Ōtākaro office and bus interchange. These services included:

a Reviews of physical security of the Ōtākaro office

b A review of physical security of the Christchurch bus interchange, and advice on developing a process relating to trespassing (May–July 2016)

c A workshop for senior leadership in relation to the Protective Security Requirements, and follow-up work on the bus interchange (June–Dec 2016).

3.161 The Chief Executive informed the Inquiry that the contracts were not tendered because of their low value (in total less than $50,000). Thompson and Clark were engaged as they had a good reputation, and were known by both the Ōtākaro Chief Executive in previous roles and the Ōtākaro Chair in his role with Southern Response.

3.162 The Inquiry's view is that these engagements did not give rise to any concerns under the Code of Conduct.

MBIE

MBIE's engagement of Thompson and Clark to provide security services at a petroleum conference did not give rise to any concerns under the Code of Conduct.

3.163 In 2013 MBIE engaged Thompson and Clark to provide security services for a petroleum conference in Auckland.

3.164 The Inquiry did not consider that this engagement gave rise to any concerns under the Code of Conduct.

Ministry of Foreign Affairs and Trade (MFAT)

MFAT's involvement in a third-party engagement of Thompson and Clark in relation to a TPP protest did not give rise to any concerns under the Code of Conduct.

3.165 In 2012 a Thompson and Clark Director approached an MFAT employee asking for a contact involved in arranging a Trans-Pacific Partnership (TPP) meeting in Auckland. The MFAT employee redirected Thompson and Clark to a third party to act as a potential referee to manage any potential conflict of interest.

3.166 MFAT also received a copy of a 2015 threat assessment that was provided on behalf of the NZ-US Partnership Forum held from 29 June to 1 July 2015. This threat assessment was commissioned by a third party and included analysis of potential protest action and groups opposed to the TPP. However, it contained no indication of surveillance related to those groups.

3.167 In 2016 Thompson and Clark were engaged by a third party to provide security for a third party for a TPP event in Auckland. This appointment was approved by MFAT, which paid the invoice.

3.168 The Inquiry's view is that the information provided by MFAT did not give rise to any concerns under the Code of Conduct.

Te Papa

Te Papa's engagements of Thompson and Clark for security reviews were low-risk and short-term, and did not give rise to concerns under the Code of Conduct.

3.169 Te Papa engaged Thompson and Clark on two projects, in 2008 and 2009, to complete security reviews of Te Papa's two physical sites. The engagements were low-risk and short-term, and the Inquiry was not provided with any information that might give rise to concerns under the Code of Conduct.

Plant and Food

Engagements of Thompson and Clark by Plant and Food were low-risk and short-term, and the Inquiry was not provided with any information that might give rise to concerns under the Code of Conduct.

3.170 Plant and Food research reviewed contracts and financial records, and identified two engagements with Thompson and Clark, and one with Cyclops. Plant and Food twice contracted Thompson and Clark:

a First in 2015 to complete a high-level physical and operational security review of the Mt Albert Research campus

b Then in 2018 to investigate an ongoing asbestos removal project and the potential exposure of staff and contractors to airborne asbestos at the Plant and Food Mt Albert site.

3.171 Plant and Food also engaged Cyclops Monitoring to monitor the Mt Albert site while it was undergoing renovations, in response to indications that members of the public were trespassing on the building site and were climbing the contractor's scaffolding.

Protective Security Requirements

3.172 During the Inquiry, questions were raised in the media about the appropriateness of Thompson and Clark remaining on an All of Government sub-panel of providers for Protective Security Requirements. While this topic is not specifically within scope, the Inquiry thought it worthwhile to consider the appointment and management of this sub-panel, given the broader issues arising about how external security consultants are engaged and overseen.

3.173 On 8 December 2014, Cabinet approved Protective Security Requirements (PSR) setting out the Government's expectations for managing personnel, physical and information security, including what agencies both must and should consider to ensure they are managing security effectively and successfully protecting their people, information and assets.

3.174 Cabinet directed all public service departments and the Defence Force, Police, Security Intelligence Service and Parliamentary Counsel Office to implement the Protective Security Requirements. Some agencies sought support from external security consultants to provide the capacity and capability for carrying out these assessments.

3.175 In 2017, at the request of the lead security agencies, MBIE created an All of Government sub-panel (building on the existing 'Risk Management and Operations' All of Government contracting sub-category) to deliver Protective Security Consultancy Services, which include services such as:

- Threat assessments
- Risk assessments
- Security planning
- Security governance
- Security assurance
- Security design
- Security awareness.

3.176 The sub-panel was established as part of the refresh of the All of Government panel for consultancy services in late 2017. To be eligible for appointment to the sub-panel, in addition to applying directly to the sub-panel, providers needed either to be already contracted to the Risk and Operations subcategory, or to be successful in the subcategory as part of the panel refresh. The All of Government panel agreement includes the following requirements of external security providers:

- The services must be provided in accordance with industry best practice (cl 4.8)
- Providers must act in the best interests of the participating agency (cl 4.8)
- Providers must comply with all privacy and other policies and guidelines issued by the participating agency and notified or made available to the provider (cl 7.1); notably, this would include the State Services Code of Conduct to the extent that it is notified or made available to the provider

- Providers must obtain, maintain and comply with any governmental, regulatory or other approvals, permissions, consents or requirements necessary to provide the services (cl 7.1)
- Providers must comply with all laws in so far as they relate to the provision of the services (cl 7.1)
- Providers must use all reasonable endeavours to avoid damaging or adversely affecting the reputation of the participating agency (cl 7.1).

3.177 The Inquiry did not identify any issues with the establishment or management of this panel. The panel includes a number of external security providers, who offer services to agencies that are specialised and may not be required regularly. Notably, the scope of the All of Government contract does not include private investigation or surveillance services.

The panel agreement and Thompson and Clark

3.178 The process for appointing providers to the All of Government panel appears to be robust. Eleven providers were appointed to the Protective Security Consultancy Services sub-panel, including Thompson and Clark, following a standard process for reviewing and moderating applications. The overarching contract refresh process for the Consultancy Services Panel included independent internal peer review.

3.179 The Inquiry therefore did not find any particular issues with how Thompson and Clark or any other external security provider was appointed to the sub-panel, and does not take a view on the composition of the panel. The Inquiry notes that the All of Government contracts have specific clauses (see above) that set out general expectations and requirements that MBIE or other agencies can draw on as needed.

Opportunities for MBIE to strengthen its support to other agencies

3.180 Given the Inquiry's broader findings relating to the engagement and oversight of external security consultants, the Inquiry would encourage greater use of the panel contract to ensure external providers are aware of the Code of Conduct and to ensure they adhere to it.

4 The relationship between government employees and agencies and Thompson and Clark

Overview

4.1 In the lead up to the Inquiry, Greenpeace raised particular concerns about MBIE's relationship with Thompson and Clark, including concerns that this relationship was too close; that MBIE officials actively assisted Thompson and Clark to expand their commercial activities in the oil and gas sector; and that MBIE officials also provided them with commercial or confidential information. Subsequent Official Information Act releases revealed further concerns about relationships between Thompson and Clark and other state servants, including the Ministry for Primary Industries and the Security Intelligence Service.

4.2 Government agencies and their employees must uphold appropriate standards of impartiality and objectivity in their dealings with private security consultants, in accordance with the Code of Conduct. This includes avoiding situations where personal interests or relationships are, or may appear to be, in conflict with the interests of the organisation. The perception of impartiality can also be impaired where a relationship with a private security consultant is particularly close and lacks professional distance.

4.3 The Inquiry found two areas of concern in this area:

a There were a number of instances where the relationship between agencies (including MBIE) or their employees and Thompson and Clark lacked the necessary professional distance.

b Two employees of the Ministry for Primary Industries and its predecessor undertook secondary employment with Thompson and Clark while still carrying out their role with the Ministry. At least two other government employees, one from MAF and one from Maritime New Zealand, discussed with Thompson and Clark the possibility of similar secondary employment with the company.

4.4 In addition, the Inquiry found some areas of concern in the relationship between NZTA and Thompson and Clark – in particular, with NZTA's management of Thompson and Clark's access to the motor vehicle register, and with Thompson and Clark apparently obtaining personal information from NZTA databases through an intermediary.

Professional distance

Ministry of Business, Innovation and Employment

MBIE's conduct considered as a whole breached the Code of Conduct, by failing to maintain the level of objectivity and impartiality that the Code requires.

Context

4.5 MBIE is responsible for administering the Crown Minerals Act 1991. While the purpose of the Act focuses on extracting value from the minerals estate, MBIE's policy focus is broader. The Ministry's Statement of Intent refers to promoting sustainable growth.[77] More specifically, New Zealand Petroleum & Minerals (NZP&M) states it is committed to the responsible management of resources, including working with other agencies and engaging with councils, iwi and communities about petroleum and minerals development.[78]

4.6 The Inquiry found that some interactions between NZP&M and Thompson and Clark lacked the impartiality, objectivity and professional distance required by the Code. Thompson and Clark were acting on behalf of the oil and gas industry, and MBIE failed to keep them at an appropriate arm's length from those MBIE staff who were administering the Act. Some emails between MBIE staff and Thompson and Clark supported an overall finding of a lack appropriate professional distance.

Relationship with Thompson and Clark

4.7 Thompson and Clark is engaged by a number of companies in the oil and gas sector, and the NZP&M part of MBIE had reason to engage with external security consultants as part of its role in ensuring that New Zealand's oil, gas, mineral, and coal resources are effectively managed.

4.8 In general, most MBIE employees maintained an appropriate professional distance in their relationship with Thompson and Clark:

a A review of MBIE's gift register confirmed that no employees received any corporate entertainment provided by Thompson and Clark.

b Senior MBIE executives who were interviewed by the Inquiry did not have a relationship with Thompson and Clark outside of attending infrequent meetings of the Minerals and Exploration Joint Intelligence Group and attending industry conferences where Thompson and Clark were present.

c The Chief Executive and former Chief Executive have no relationship with Thompson and Clark at all.

d There was email evidence of some MBIE employees refusing social events and reminding Thompson and Clark of boundaries put in place to protect against a perception of conflict of interest.

[77] Ministry of Business, Innovation and Employment *Statement of Intent 2013-2016*, which applied at the relevant time.

[78] < https://www.nzpam.govt.nz/about/purpose-and-role/>

4.9 However, in some cases, MBIE employees (particularly from NZP&M) demonstrated a degree of familiarity:

a Some emails revealed informal relationships between MBIE employees and Thompson and Clark.[79] These employees no longer work in NZP&M, and most of them are no longer employed by the state service.

b On several occasions, Thompson and Clark asked MBIE employees to provide contact details for executives of companies within the petroleum and minerals sector. In some cases these requests related to companies that were new entrants in the New Zealand market and that were therefore likely to be prospective clients for Thompson and Clark. On two occasions, MBIE employees responded to Thompson and Clark's requests and provided contact details. This was not private information and could have been found without great difficulty by other means, including searches of websites and Company Office records.

c On one occasion, in June 2015, an MBIE employee provided a map of potential exploration activity to Thompson and Clark. This email referred to the information as being confidential, although it appears that it was a consolidated map of otherwise publicly available information. It was provided to Thompson and Clark on the basis that Thompson and Clark was engaged by companies who held permits included in the map.

4.10 Other aspects of the relationship between MBIE and Thompson and Clark contributed to an overall close relationship:

a Thompson and Clark provided secretariat functions for the Taranaki Oil and Gas Security Group (TOGS), a group led by Thompson and Clark to bring together industry stakeholders and the NZ Police to enable a better understanding of wider security issues facing the sector in Taranaki. This group's terms of reference were provided to the Inquiry. Consistent with reasonable expectations of industry engagement, MBIE provided occasional guest speakers to the TOGS group, as did other state servants and NZ Police.[80]

b While Thompson and Clark did sometimes indicate to MBIE who in the sector had engaged them, this was not consistently the case. In some cases, MBIE officials engaged with Thompson and Clark without knowing the identity of Thompson and Clark's client. As a matter of good process, state servants should always clarify on whose behalf a given intermediary is acting, whether that intermediary is a security consultant, a public relations consultant, or a legal representative.

4.11 However, the most significant feature of the relationship between MBIE and Thompson and Clark related to 'Operation Exploration'. MBIE established and led Operation Exploration as the key interagency governance mechanism following an amendment to the Crown Minerals Act in 2013. This amendment created offences for damaging or interfering with structures or ships being used offshore in prospecting, exploration and mining activities – including

[79] For example emails supplied to the Inquiry dated 25 May 2014, 5 June 2014.

[80] A senior MBIE presented to the Taranaki Oil and Gas Security Group at Thompson and Clark's invitation in June 2014.

incursions into specified non-interference zones.[81] The design of Operation Exploration was influenced by the concept of 'issue motivated groups'. This framework distinguished those whose interests warranted protection under enforcement provisions of the Crown Minerals Act from those who would probably oppose exploration activity and therefore probably breach the non-interference zone in protest. The Inquiry found this 'issue motivated groups' construct problematic overall, and this is explored in para 4.35 below.

4.12 Operation Exploration established an Operational Planning Group and the Minerals Exploration Joint Intelligence Group (MEJIG), which was set up to coordinate intelligence provided to the various agencies involved in enforcing the laws regarding offshore petroleum and mineral exploration. MEJIG's role was to consider intelligence, and highlight activities that might potentially lead to interference with offshore petroleum and minerals exploration. The MEJIG part of Operation Exploration was led by the NZ Police; however, the operating tempo of when that group met was often determined by Thompson and Clark, as it related to when exploration activity occurred.

4.13 It was through these mechanisms that Thompson and Clark established a very close relationship with Operation Exploration. The firm attended meetings with officials as a key participant and regularly provided intelligence information to MEJIG.[82] The Inquiry did not review the primary information provided to the NZ Police as that was outside our Terms of Reference. However, from the information available to the Inquiry, it appears likely that some of the information provided to MEJIG agencies by Thompson and Clark was gathered through surveillance, particularly surveillance of Greenpeace. As noted above, it was clear to the Inquiry that Thompson and Clark has undertaken significant and sustained surveillance of Greenpeace, most likely paid for by private-sector petroleum and minerals interests.[83]

4.14 The close nature of this relationship can be compared to the limited evidence of any relationship between MBIE (including NZP&M) and environmental and other groups opposed to petroleum and minerals exploration over the same period.[84] MBIE told the Inquiry that it relied on those interests being represented in the policy process though agencies such as the Ministry for the Environment and the Department of Conservation. However, the Inquiry considers that this form of input does not absolve agencies of the responsibility to consider the interests of diverse stakeholders. It is with the benefit of hindsight that a failure to establish and maintain a relationship with diverse sector interests has been a misjudgement on MBIE's part. The Inquiry found that this lack of a relationship with environmental interests, particularly at a policy level, contributed to a perception of bias by some environmental groups, including Greenpeace.

4.15 The Inquiry also heard evidence that the organisation had concerns about potential poor regulatory practice. In 2013/14 MBIE became concerned about tensions between its promotional and regulatory responsibilities, particularly in relation to conflicts of interests. In this same period there were structural and leadership changes at MBIE, with the Ministry

81 At the time these amendments were passed, there was strong protest from groups opposed to oil and gas exploration, including Greenpeace. Those groups informally refer to the amendments as the 'Anadarko amendments', because they were passed around the same time as the arrival of the Anadarko oil drilling ship *Noble Bob Douglas*.

82 This included information used in support of a prosecution of Greenpeace for breaching a non-interference zone in April 2017. A contractor engaged by Thompson and Clark recorded video and still footage of Greenpeace's activities, and sent this to the NZ Police through a live online portal.

83 See further paragraph [4.71] below.

84 Leaving aside MBIE's prosecution of Greenpeace for breaching a non-interference zone.

appointing leaders who had more experience in regulatory systems, as opposed to those with industry connections and expertise. This step-change was characterised by senior executives in Inquiry interviews as a shift from valuing industry knowledge to placing greater value on the regulatory and compliance experience of career state servants. The Inquiry considers that this was an appropriate step.

4.16 Key to this change was a separation of promotional activity from functions related to the block offer process and MBIE's enforcement responsibilities, including oversight of the non-interference zone under the Crown Minerals Act. The structural changes were part of a broader programme to help resolve potential tensions between NZP&M's regulatory and promotional functions.

4.17 The Inquiry found that senior executives at MBIE were attuned to concerns about the perception of bias towards petroleum and minerals sector interests and had put some measures in place to manage those risks, including separation of conflicting functions within NZP&M.

4.18 While the policy, promotion and regulatory functions were split at the fourth-tier level, accountability was shared from the third tier up, including shared accountability to the Minister of Energy. There was, however, a continued perception of conflict and bias by stakeholder groups, like Greenpeace, who are opposed to petroleum and minerals exploration.

Application of the Code of Conduct

4.19 Looked at individually, the interactions between MBIE employees and Thompson and Clark were low-level and not sufficient to constitute a breach of the Code of Conduct. For example the Inquiry found that the informal emails did not constitute a continued or systematic relationship between NZP&M and Thompson and Clark employees that was improperly personal or close.

4.20 The Inquiry also found that MBIE was sensitive to a perception of an improper relationship and put in place a much more rigorous approach to conflicts of interest than was evident in 2013/14.

4.21 The Inquiry found that by providing Thompson and Clark with contact details for petroleum and minerals companies MBIE had not breached the Code. The information was not private, and could have been found without great difficulty by other means, including searches of websites and Company Office records. Although providing these contact details did not reach the material level necessary to constitute a breach, nonetheless it was inappropriate for MBIE to provide this information given the Code's requirement to treat information with care.

4.22 The Inquiry considered that, when assessing MBIE's conduct against the Code, the issue of MBIE's design of the interagency relationships in Operation Exploration was more challenging. Officials uncritically adopted the construct of 'issue motivated groups' to guide the design of their enforcement function in a manner that was problematic. The enforcement approach enabled Thompson and Clark to embed itself as a crucial participant within the regulatory and enforcement function, despite the fact they represented private economic interests. The Inquiry found this to be poor regulatory practice.

4.23 The closeness of this relationship was in contrast to the absence of a relationship with interests that opposed petroleum and minerals exploration. This had the further effect of fuelling a perception of bias.

4.24 As a result, the Inquiry was required to look at the cumulative effect of the relationship, the actions that were taken, and the role MBIE as an organisation had to play in that dynamic. Overall the Inquiry found that MBIE's conduct considered as a whole breached the Code of Conduct, by failing to maintain the level of objectivity and impartiality that the Code requires.

New Zealand Security Intelligence Service

The email contact between an NZSIS employee and a Thompson and Clark Director risked harming the reputation of the NZSIS and was therefore inconsistent with the Code. The Inquiry agrees with the conclusion of an internal NZSIS review that any breach was at the lower end of the scale.

Relationships between NZSIS and Thompson and Clark

4.25 In 2016, an employee of the NZSIS provided a Director from Thompson and Clark with unclassified information to support Thompson and Clark's business development. The employee gave advice on who to approach in different agencies and gave insight into the agencies' capability and approach to Protective Security Requirements (PSR). In one case the employee directly referred work to Thompson and Clark. This was during the period before there was a panel of suppliers, and the NZSIS did have a role in supporting agencies to understand providers of relevant services in the market.

4.26 In another case the employee attended a workshop with one of the company's clients (a government agency) and the Thompson and Clark Director to discuss the PSR requirements.

4.27 This workshop was consistent with the employee's job description. The interactions between the employee and the Director occurred before the appointment of a panel of providers of these services. The employee concerned had no subsequent involvement in the procurement process to appoint the panel.

4.28 Some of the communication was informal and provided evidence of a personal relationship. The Inquiry heard evidence that the employee and the Director had a relationship that was not close but friendly, and pre-dated the individual's employment within the New Zealand intelligence community. These informal communications related to catching up in a social setting.

4.29 The NZSIS conducted an investigation into the nature of that employee relationship. This was an appropriate step to take, particularly given that the NZSIS did not become subject to the Code of Conduct until 28 September 2017. This matter was resolved as an employment matter, and the NZSIS concluded that any breach of the principles in the Code was at the lower end of the scale.

4.30 The NZSIS then carried out a more substantial search of its holdings, going beyond the timeframe stipulated by the Official Information Act request that triggered the scrutiny. They began to analyse information going back to 2003, when Thompson and Clark was established. As a result the NZSIS informed the Inquiry that it has identified a handful of instances where Thompson and Clark contacted the NZSIS wanting to pass on information that the company believed raised security concerns. The SIS told the Inquiry that the

information was unsolicited and provided in the same way that any member of the public can give information to the NZSIS. The NZSIS supplied complete records of these interactions to the Office of the Inspector General of Intelligence and Security for it to review. The Inspector-General is considering these records separately.

Application of the Code of Conduct

4.31 The Inquiry considers that the NZSIS employee's email contact with the Thompson and Clark Director risked harming the reputation of the NZSIS and were therefore inconsistent with the Code.[85] We agree with the conclusion of an internal NZSIS review that any breach was at the lower end of the scale.

Department of Conservation

Aspects of emails between a DOC employee and Thompson and Clark were overly familiar, but the Inquiry does not consider that they involved a breach of the Code of Conduct.

Relationship between a DOC employee and Thompson and Clark

4.32 In 2015, an employee of the Department of Conservation (DOC) had an email exchange with a Director of Thompson and Clark in which the employee responded to Thompson and Clark's desire to offer services to DOC. The employee's emails set out the general nature of DOC's concerns about emerging health and safety risks related to 1080 protests. The information the employee provided included the names, roles and contact details of DOC employees who could have functional oversight over such an engagement should it be required. Alongside this exchange of information, there were also some personal exchanges of a minor nature.

4.33 The employee had a past professional relationship with Thompson and Clark, which had been established when the employee had been employed at another agency. In the employee's time at the previous agency, Thompson and Clark had provided the agency with advice on event security. The employee had then subsequently engaged Thompson and Clark to provide a desktop security assessment in support of DOC activities at the National Fieldays. The employee did not have a personal relationship with the Director or any other individual at Thompson and Clark.

Application of the Code of Conduct

4.34 While aspects of the emails between the employee and Thompson and Clark were, in hindsight, overly familiar, the Inquiry does not consider that they involved a breach of the Code of Conduct.

The construct of 'issue motivated groups'

4.35 Thompson and Clark's newsletters received by agencies including MBIE, AgResearch, NIWA and DOC regularly used the concept of 'issue motivated groups'. Thompson and Clark

[85] The NZSIS did not become part of the Public Service until 28 September 2017: State Sector Act 1988, Schedule 1.

applied this label to various groups, including Save Animals from Exploitation (SAFE), Oil Free Otago, Climate Justice Taranaki, Farmwatch, the Green Party, the Mana Movement, Greenpeace and some iwi groups.[86]

4.36 'Issue motivated groups' is a concept traditionally used by intelligence and risk management bodies to refer to coalitions of people drawn together by a common interest, such as a protest or petition. The cause is most often a political reaction to a government or official body, an industrial venture, or private commercial interests. This broad definition, of a coalition with a common interest, would capture many New Zealanders who find themselves, from time to time, expressing strong personal views on issues, at protest events or online. The State Services Code of Conduct recognises the rights of state servants to freely express their personal opinions where this does not conflict with their professional interests, so highly is this freedom valued in New Zealand society.

4.37 Issue motivated groups have historically been associated with environmental activists, animal rights activists, and 'hacktivists' – groups that, while inherently political, are not officially connected to or represented by a political party. On any number of public policy issues, these groups are also stakeholders whose contributions will be critical to a rounded consideration of the relevant issue.

4.38 The Inquiry found that the construct of 'issue motivated groups' may be unhelpful for government agencies if used in an uncritical way, particularly agencies without sophisticated in-house intelligence functions such as the New Zealand Police. Furthermore, receiving information, for example in the form of a regular newsletter, that aggregates the views of minor groups within a protest movement with more extreme elements (often lone individuals) can further perpetuate an 'us and them' mentality that is unhelpful to state servants as it can lead to an overstatement of risk. The State Services should usually consider constructive relationships with the non-governmental sector, including NGO activists who oppose government policy, to be part of their role as neutral state servants.

4.39 In applying the Code of Conduct to the evidence, the Inquiry considered the New Zealand Bill of Rights Act 1990, including the requirement that state servants must not interfere with the right of private individuals to freedom of expression. Where there is a serious threat to national security or a risk of criminal activity, state servants can get support from appropriate expert agencies, including the NZSIS and NZ Police, to assess this risk. In those cases where expert agencies are involved, there will be proper oversight from the Inspector General of Security and Intelligence and the Independent Police Conduct Authority, and any surveillance will be conducted as warranted activity.

4.40 In short, government agencies should not use the concept of 'issue motivated groups' uncritically to determine their relationship with non-governmental organisations and groups.

[86] The Inquiry did not see any evidence that Thompson and Clark undertook surveillance of iwi groups. Iwi groups were included in newsletters where media or social media posts included coverage of protest activity. This was often in regions were exploration activity occurred such as Northland, the East Coast and Taranaki.

Secondary employment

Overview

4.41 The Inquiry found four instances where state sector employees employed in enforcement, compliance and intelligence functions within government agencies were engaged, or considered engaging, in a secondary employment relationship with Thompson and Clark. In at least two cases state servants did undertake that secondary employment with Thompson and Clark:

a Two employees of MAF and MPI undertook secondary employment with Thompson and Clark while carrying out their primary role with the government agency. The work they did appears to have included compiling or accessing (directly or indirectly) government-held information for the purpose of their work for Thompson and Clark. Their actions are currently the subject of investigations by the Serious Fraud Office (SFO).

b One further employee of MAF/MPI was also approached to undertake secondary employment by Thompson and Clark, but there is no evidence that this person took up that employment.

c One employee of a justice sector agency approached Thompson and Clark and was offered a role after moving to Maritime New Zealand. He or she obtained approval from the Chief Executive on the recommendation of lower-tier managers to carry out 'open source research on issue motivated groups' for Thompson and Clark. However, the proposed secondary employment did not occur.

4.42 The Inquiry also received evidence of employees of the NZ Customs Service entering into secondary employment with other external security consultants. The Inquiry considered that this fell outside its Terms of Reference (which was specific to relationships with Thompson and Clark) and referred this issue separately to the State Services Commissioner.

4.43 Undertaking secondary employment is not of itself a breach of the Code of Conduct. State sector employees are entitled to participate in secondary employment if they have authorisation, there is no conflict of interest, and the secondary employment does not affect their ability to undertake their duties for their primary employer.

4.44 The State Services Commission's *Guide to Understanding the Code of Conduct*[87] states that additional employment may create a conflict if it involves (among other things):

a Work in a business that has or is developing a contractual relationship with any government organisation

b A business that lobbies Ministers, or Members of Parliament, or government organisations

c A business that is regulated by the organisation the state servant works for

d A business that has an interest in the privileged, private or confidential information that the state servant can access.

87 http://www.ssc.govt.nz/sites/all/files/UnderstandingtheCode-April2010.pdf

4.45 Secondary employment with Thompson and Clark or other external security consultants has the potential to create a conflict of interest or a perception of such a conflict, which could breach the Code's requirement to act responsibly and harm the reputation of the organisation. Where state sector employees have access to private information it is particularly important that they treat the information with care and use it only for its intended purpose. Similarly, where employees have an enforcement or compliance role, it is important that they do not use that role improperly for personal gain in secondary employment. The employment may cause a perception of conflict, even if the state servant is not acting improperly.

4.46 Secondary employment is increasingly common as employment trends change. The future of work will also mean that secondary employment or flexible employment arrangements are more common, particularly as the workforce ages. Many people have more than one job, and state servants, particularly those in regional areas, may often have multiple employers. With these developing trends, it will be important that government agencies ensure they have appropriate internal policies and procedures to manage potential conflicts of interest.

Ministry for Primary Industries

Two employees of MAF carried out secondary employment with Thompson and Clark in breach of the Code of Conduct.

MAF did not have adequate measures in place at the time to ensure that all employees respected individual privacy, complied with the Code of Conduct, and avoided secondary employment involving risks of a conflict of interest. The organisational culture in the relevant MAF division provided weak protection against abuse.

Context

4.47 The current Ministry for Primary Industries (MPI) is the product of a series of mergers that brought together a number of separate departments from across the primary sector. Most relevant is the merger of the Ministry of Agriculture and Forestry and the Ministry of Fisheries in 2011.

4.48 The Ministry of Agriculture and Forestry (MAF) had an enforcement and compliance function primarily in relation to the Biosecurity Act 1993 and Animal Welfare Act 1999. This included the power to undertake investigations related to prosecutions for ill-treatment or neglect of animals, and the importing and exporting of live animals. The Inquiry heard evidence that the unit was small and closely knit, but geographically isolated from the rest of the organisation. They had historically (before 2008) engaged Thompson and Clark to assist with these functions (see above). Although this relationship ended in 2008, some individual relationships had been established.

Instances of secondary employment

4.49 Two MAF employees undertook secondary employment[88] with Thompson and Clark in breach of the Code of Conduct, one from 2011 to 2012 and the other from 2013 to 2014. Both have since left the state sector.

[88] We used the term 'secondary employment' to encompass both employment and contracting relationships.

4.50 In December 2010, immediately following a round of restructuring within MAF, the first employee approached a Thompson and Clark Director to ascertain whether they had any employment opportunities available, and followed up using work email. Between April 2011 and April 2012, the employee carried out work for Thompson and Clark as a contractor, while still continuing in a substantive role at MAF, before ultimately leaving MAF to join Thompson and Clark as a permanent employee in April 2012. In particular:

a During those 12 months, the employee invoiced for hours worked, which involved collecting and analysing information and developing that information into intelligence products using specific software programs. The Inquiry saw invoices totalling approximately 45 hours work over this period.

b There was no record of any formal approval given for this secondary employment.

c Some of the work was undertaken after-hours. However, the employee used an MPI laptop, specialist software and email, and contemporaneous emails indicated that some of the work was carried out during work hours.

d The information analysed was in general provided by Thompson and Clark, and included:

i Information obtained through surveillance of Greenpeace or individuals associated with Greenpeace on behalf of private-sector petroleum and minerals interests

ii Information relating to an investigation into the hacking of a Solid Energy website in 2011 (Solid Energy's actions are outside of the scope of this Inquiry)

iii A timeline related to the Pike River mine disaster, created in support of Thompson and Clark's engagement for Pike River and in particular its Chief Executive.

4.51 In March 2013, an MPI employee was engaged as a contractor by Thompson and Clark while also employed at MPI. There was no evidence that he sought or obtained approval for this secondary employment, which continued until 2014. He had a close working relationship with the MAF employee whose secondary employment is referred to above.

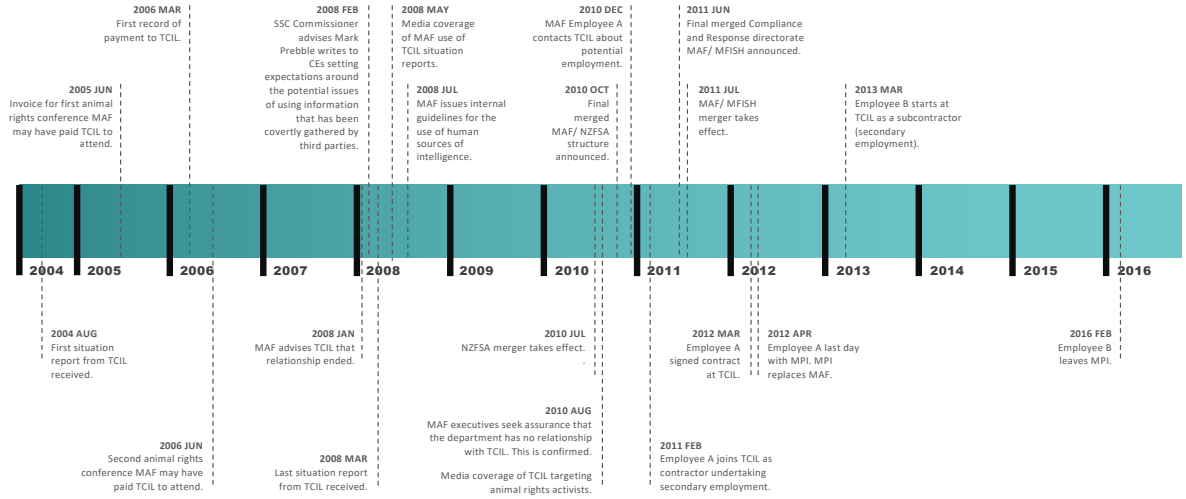
4.52 There was evidence that the MPI employee obtained information from NZTA databases in support of Thompson and Clark investigations in 2011 when he worked for MAF. This was personal information from the motor vehicle and driver licence databases that Thompson and Clark would not have been authorised to receive, including telephone numbers, dates of birth and driver licence numbers. The information also appears to have been made available by searching names and addresses, rather than by searching a licence plate, which is the only form of search a private investigator with authorised access is entitled to carry out.[89] The MPI employee was able to access this information by using an NZTA contact in the Combined Law Agency Group (CLAG), discussed further below.

4.53 Matters related to this work are among the issues currently being investigated by the Serious Fraud Office.

4.54 During the course of this second employee's work for Thompson and Clark, a third employee was approached by a Director of Thompson and Clark to work for the company. There is no indication that this resulted in any work being undertaken.

[89] Land Transport Act, s 241.

4.55 The timeline below sets out the key dates associated with the relationship between MAF (and individual employees) and Thompson and Clark.



Application of the Code of Conduct

4.56 Secondary employment of the type described above presents a serious breach of the State Services Code of Conduct. This Inquiry does not seek to make any findings of civil or criminal liability, particularly during an ongoing investigation.

4.57 The Inquiry spoke to a number of people who worked in the former MAF and who described a culture heavily influenced by restructuring processes and prolonged periods of job uncertainty. The Inquiry was told that the first employee, in particular, had been affected by these change processes, and felt disillusioned. Over the relevant period the employee had several managers, two of whom were based in a different city.

4.58 The Inquiry also heard evidence that the capability within MAF's enforcement and compliance function was not strong and had been impacted by challenges related to scale (it was a small unit), personnel (there had been challenging dynamics within the team), and resourcing throughout a period of change. The unit was also geographically isolated, which further compounded the difficulty of ensuring proper oversight.

4.59 Overall, the Inquiry found that MPI's predecessor agency MAF did not have adequate measures in place to ensure that all employees respected individual privacy, complied with the Code of Conduct, and avoided secondary employment involving risks of a conflict of interest. The organisational culture in the relevant MAF division provided weak protection against abuse.

4.60 MPI has recently commissioned work to assess its fraud and corruption risks, including its open information environment. This remains a work in progress. The Ministry has also taken a number of other steps to protect the management of information, including establishing a Security and Privacy Directorate led by a Chief Security Officer.

Maritime New Zealand

The Chief Executive of Maritime NZ gave approval for an employee to undertake secondary employment with Thompson and Clark. Given the nature of the employee's work as an intelligence analyst and the risk of conflict of interest, the application should not have been approved. In the circumstances this fell just short of breaching the Code of Conduct.

Secondary employment not undertaken

4.61 In early 2014, an employee from a justice sector agency approached Thompson and Clark by email to see whether there were any work opportunities available. Some time went by, and that employee took up an intelligence analyst role at Maritime New Zealand. A Director of Thompson and Clark then re-engaged with the employee and offered work described as an 'open source research project'. The employee met with the Director to discuss the nature of that work and sought approval from an immediate manager, a senior manager, and subsequently the Chief Executive. The employee clearly set out for management the nature of that work, which was documented as 'open source research project with [Thompson and Clark] on Issue Motivated Groups'.

4.62 The employee received written approval for this secondary employment, both from the general manager and the Chief Executive of Maritime New Zealand. However, for unrelated reasons, the employee did not ultimately provide those services to Thompson and Clark.

Application of the Code of Conduct

4.63 The Inquiry considers that the employee took appropriate steps, consistent with the expectations of a state servant under the Code of Conduct.

4.64 It is potentially problematic for any intelligence, enforcement or compliance state servant to work in secondary employment as an external security consultant. This is because the secondary employment has the potential for improper use of specialist knowledge, access to privileged information, and specialist skill. This has the potential to create a conflict, or the perception of a conflict, that may result in the misuse of information and/or bring the organisation into disrepute.

4.65 Given the nature of the employee's work within Maritime NZ as an intelligence analyst and the risk of conflict of interest, the application should not have been approved. In the circumstances this fell just short of a breach of the Code of Conduct.

Access to NZTA databases

The Inquiry found that NZTA's prior lack of oversight of authorised access to the motor vehicle register, and the lack of formality and care in information sharing through the Combined Law Agency Group (CLAG), left both those forms of access open to exploitation, and breached the Code of Conduct requirement to treat information with the level of care expected by the public.

Two MAF employees who accessed NZTA information on behalf of Thompson and Clark, directly or indirectly, breached individual privacy and were in breach of the Code of Conduct requirement to treat information with the level of care expected by the public.

Overview

4.66 Since late 2012 NZTA has been the delegate of the Secretary for Transport for the purposes of administering authorised access to certain Motor Vehicle Register information. This includes administering a statutory process of access by authorised persons, some of whom are private investigators. Approvals for authorised access are made by the Secretary for Transport (or his or her delegate) after consulting with the Privacy Commissioner, the Chief Ombudsman, and the Commissioner of Police. NZTA also administers the driver licence register.

4.67 Thompson and Clark was at times able to access information from the motor vehicle and driver licence databases in the following ways:

a Thompson and Clark had authorised access under s 241 of the Land Transport Act 1998, which allows authorised individuals, including authorised private investigators, to access names and addresses from the motor vehicle register.[90]

b On a number of occasions, one of the MAF employees referred to above[91] accessed information from the databases, including through the Combined Law Agency Group (CLAG), and provided it to Thompson and Clark.

Authorised access to the Motor Vehicle Register under s 241 of the Land Transport Act

4.68 The Motor Vehicle Register is a list of all motor vehicles for which registration plates have been issued, and includes information about the vehicle, as well as personal information about the person registered or previously registered against that vehicle, including the name, address, date of birth, and driver licence number. Since 2011, access to the personal information on the register has been restricted. However, under s 241 of the Land Transport Act, a person can be authorised to have access to the names and addresses on the register for specified purposes.[92]

4.69 Authorised access under this section is commonly granted to individuals from industries such as private investigators, motor vehicle traders, financial service providers, and petrol retailers, who are typically granted access for purposes specified for each industry.

90 Initial access was granted by the Secretary for Transport on 12 April 2012.

91 See the MPI section under 'Secondary employment', above.

92 However, they can access only the names and addresses of the person currently registered against the vehicle, and not if that person has notified the register that they want their name to be confidential.

4.70 Between 2012 and 2017, Thompson and Clark, along with other private investigators, were granted authorisation under s 241 to access the register for the following purposes:[93]

a Preparing evidence related to criminal offences

b The detection and investigation of suspected fraud

c Enforcing Court orders and judgments

d When acting as a contracted agent on behalf of government agencies with law enforcement functions, to assist in carrying out those functions.

4.71 Thompson and Clark used this register access heavily, carrying out over 4,000 searches between 2011 and 2017. NZTA told the Inquiry this was high in comparison to the use by other private investigation companies and individual private investigators for a similar period. In particular, Thompson and Clark ran thousands of number plates linked to Greenpeace and various oil and gas protest actions such as a Kaikōura swim protest in 2014, a protest against Todd Energy, and an Oil Free Seas Summit protest.

4.72 Generally, Thompson and Clark claimed this access was for the purpose of 'assisting govt agency to enforce Crown Minerals Act'. Thompson and Clark told the Inquiry the access related to threats against oil and gas people, assets and operations, and that the information was provided to the Minerals Exploration Joint Intelligence Group (MEJIG), 'for situational awareness of upcoming threats as part of Operation Exploration'. Thompson and Clark stated they were working for private clients from the oil and gas industry who had exploration and mining permits, which constituted contracts with the government. They were registered informants for the Police in relation to MEJIG activities from Jun 2013, and argued that such status is akin to an implied contract with Police. They had a designated police officer within the National Threat Assessment Unit to communicate with them, and provided information over a seven-year period. In two cases, information they provided was used in court proceedings.

4.73 On that basis, they argued that their access to the NZTA databases was on behalf of the Police and MBIE, who were 'unqualified ... unable … or under-resourced' to carry out the work themselves, and it was necessary 'to look at the bigger picture to determine where the risk was coming from'. In response to the Inquiry, they further claimed that in any event their searches also fell within the authorised purpose of 'preparing evidence related to criminal offences'.

4.74 Thompson and Clark said the high volume of searches was due to their practice of casting a wide net of searches in order to rule out individuals as persons of interest. They explained that only the information assessed as relevant, which was a small subset of the total information obtained, was passed onto the Police and MEJIG, and none of the information was shared with their clients.

[93] Access was granted initially on 12 April 2012 for 12 months, for the four purposes listed and the following additional purpose: 'to identify registered persons of motor vehicles within Solid Energy New Zealand Limited's West Coast industrial site that Thompson and Clark Investigations Limited provide security for, where the vehicles are unattended or have not been able to be stopped or, where vehicles are stopped, to confirm that details supplied are accurate.' On 25 July 2013, they were granted renewed access for just the four purposes listed for a further four years, along with five other investigation companies.

4.75 The Police and MBIE categorically denied that Thompson and Clark acted on their behalf as claimed. Thompson and Clark dispute this response by the Police. In any event, the Inquiry was not able to reconcile the thousands of searches of plates connected to Greenpeace with the authorised purposes under the Act. Taking into account the responses from Police and MBIE, and Thompson and Clark's explanations, the Inquiry considers that some, or more likely most, of Thompson and Clark's access fell outside the permitted purposes under the Act.

4.76 NZTA provided very little oversight of this access by Thompson and Clark. Like other private investigators, Thompson and Clark accessed through a portal provider rather than directly through NZTA, and NZTA did not hold records of what had been accessed, unless it specifically requested this information from the portal. NZTA carried out a limited audit on a one-month sample of Thompson and Clark's access in 2013, and at that stage no issues were raised. No further audits were carried out to check whether the purposes and conditions of access were being adhered to until Thompson and Clark applied for renewed access in 2017.

4.77 When Thompson and Clark applied to renew access in 2017, they sought access for broader purposes than those previously allowed.[94] At that point, the NZTA staff who considered the application appropriately raised questions about their access to date, and after further investigation rejected their application for further access. As part of this process, NZTA called for and considered further information from Thompson and Clark about their access between 2014 and 2017. Ultimately, NZTA was not satisfied with the response, or that Thompson and Clark would act within the purposes, terms and conditions of any future authorisation.[95] Thompson and Clark currently do not have authorised access to the motor vehicle register.[96]

4.78 In 2017, NZTA commissioned an external review of third party access (via portals) to the motor vehicle register, which has led to access and oversight being tightened up, including more frequent auditing.

Access through NZTA employees

4.79 As noted above in relation to secondary employment, on at least one occasion in 2011, NZTA employees provided personal information from the driver licence database to a MAF employee, who in turn provided it to a MAF colleague working in secondary employment for Thompson and Clark. The information related to a Greenpeace employee of interest to Thompson and Clark, and it is clear the information was sought on behalf of Thompson and Clark in support of its work for the oil and gas industry. The relevant NZTA and MAF employees were participants in the Combined Law Agency Group (CLAG) in Auckland, which is a group from across 20 government agencies with law enforcement and regulatory and intelligence responsibilities. These agencies have a primary objective of sharing

94 Thompson and Clark wanted access to "identify registered persons of motor vehicles involved in activity likely to impact assets and facilities of Thompson and Clark clients involved in lawful, permitted activity in the oil and gas, energy sector and food supply chain industries." There is an available inference that Thompson and Clark's previous access was at least in part for this purpose.

95 NZTA to Thompson and Clark, 22 June 2018.

96 Thompson and Clark, like any member of the public, can make an application for personal information against a registration plate which will be considered against criteria contained in the Official Information Act. The timeframe for an Official Information Act request involves a wait of up to 20 working days.

information and resources between the agencies. The Inquiry heard evidence that during the relevant period, CLAG operated in a high-trust environment, and ad hoc requests of this nature between CLAG members were common. Information was freely shared between members in different agencies, with a general trust that requests would be for legitimate purposes.

4.80 At the relevant time, NZTA had no guidance for its CLAG members as to when information should be shared or what protocols should be followed, and there were no records kept of information shared in this way. However, in April this year NZTA issued a protocol dealing with information shared through CLAG. The protocol includes a detailed process, and indicates who the key decision makers should be, what should be taken into account to ensure the information sharing is lawful, and how records should be kept.

Application of the Code of Conduct

4.81 The actions of the two MAF employees breached individual privacy and the Code of Conduct requirement to treat information with care. In light of the current investigation by the Serious Fraud Office, the Inquiry makes no findings of civil or criminal liability.

4.82 NZTA's low-level of oversight of authorised access to the motor vehicle register, and the lack of formality and care in information sharing through CLAG, left both those forms of access open to exploitation, and breached the Code of Conduct requirement to treat information with the level of care expected by the public.

4.83 However, in NZTA's recent interactions with Thompson and Clark NZTA employees appropriately raised concerns and sought to uphold the integrity of the motor vehicle registration and driver licence systems.

4.84 In addition, NZTA has taken significant steps over the last two years to improve oversight and tighten up access through both channels, to ensure that both the motor vehicle and the driver licence registers are appropriately protected.

4.85 This Inquiry has found there still appears to be a lack of clarity and monitoring by NZTA and other agencies as to how and on what basis these registers are accessed, particularly as between government agencies. There is benefit in achieving better oversight here, both within NZTA and within the individual agencies accessing the databases.

APPENDIX 1: TERMS OF REFERENCE

Consolidated Terms of Reference for Inquiry into the use of external security consultants

29 October 2018

This document consolidates the Terms of Reference previously issued on 27 March 2018 and 19 June 2018, in light of the request by the Minister of Research, Science and Innovation under s 11(4) of the State Sector Act 1988 dated 3 October 2018.

For the avoidance of doubt, the State Services Commissioner has delegated his statutory powers of investigation (including the powers in ss 8, 9, 10, 11, 25 and 57 57C of the State Sector Act) to Doug Martin and Simon Mount QC for the purposes of this Inquiry.

Definition

"Crown Agencies" means the agencies listed in Appendix One of the Terms of Reference.

The Inquiry will identify and report on:

1 the circumstances of, and reasons for, any engagement by Crown Agencies of external security consultants including but not limited to Thompson & Clark Investigations Limited (TCIL) and its associated companies and entities;

2 the nature and outcomes of any such engagement; and

3 the nature of the relationship between current and former employees of Crown Agencies and TCIL and its associated companies and entities.

Without limiting its scope, the Inquiry will specifically report on:

4 whether external security consultants have carried out surveillance activities directly or indirectly on behalf of any Crown Agencies and, if so:

- a the nature of any such surveillance, either generally or relating to specific individuals;
- b the extent to which Crown agencies requested that surveillance, and/or received information relating to that surveillance;
- c any actions undertaken as a result of information received;

5 any internal or external advice to Crown Agencies relating to or produced as a result of engaging external security consultants and/or any monitoring undertaken, including but not limited to advice relating to potential disclosure of the existence, nature or circumstances of any surveillance undertaken;

6 governance and reporting mechanisms (or lack thereof) relating to the engagement of security consultants; and

7 whether or not, and the extent to which, any matters identified by the Inquiry amounted to a breach of the State Services' Standards of Integrity and Conduct (Standards) or would have amounted to a breach if the Standards had applied.

The Inquiry may also make recommendations in relation to any matter contained in its report. The Inquiry will not consider, report on, or make recommendations relating to:

- any individual entitlement or complaint, such as those relating to a specific insurance claimant;
- actions taken to resolve specific insurance claims, except insofar as those actions related to the use of external security consultants;
- general operational performance or governance arrangements.

APPENDIX 2: INQUIRY METHOD

Powers under delegation

1 The Inquiry has been undertaken using the Commissioner's functions and powers under the State Sector Act 1988. The Act permits the Commissioner to delegate the extensive powers of inquiry, which include the power to require the production of any records, files or other information, to require government employees to answer questions, and to enter government premises.

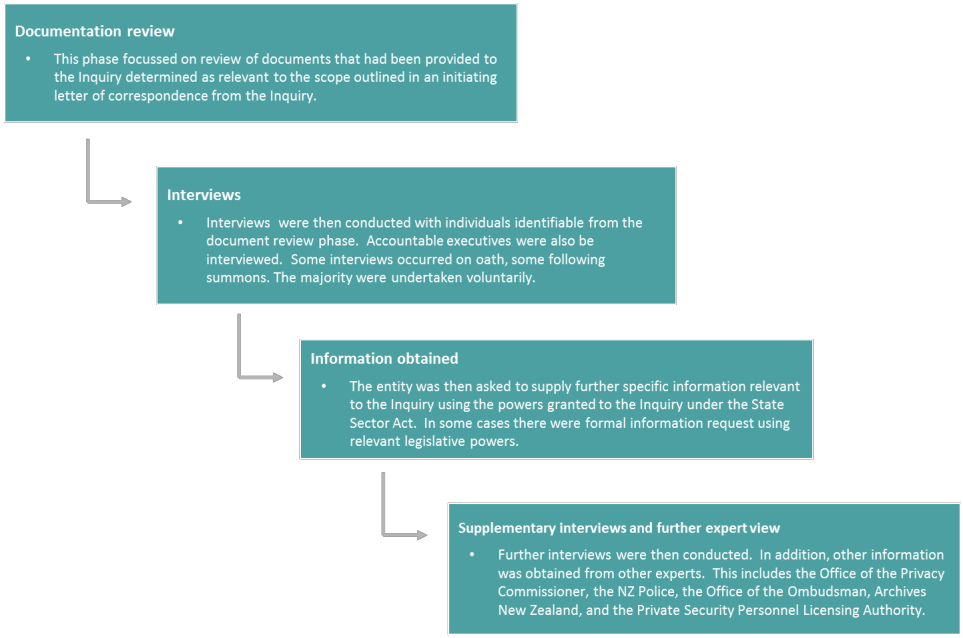
Three categories of entities

2 The Inquiry considered entities in three categories:

- **Category 1** – Entities whose activities had been brought to the attention of the Inquiry. This included Southern Response, MBIE, NZSIS, DOC, and MPI.
- **Category 2 –** Entities whose activities the Inquiry decided warranted further consideration on the basis of a review of other information and/or a self-assessment undertaken by the entity's Chief Executive. These included the Ministry of Health, MFAT, AgResearch, NIWA, Plant and Food, DIA, Crown Law, and MSD. With each of these entities the Inquiry carried out a full review of documents and a number of interviews, where these were warranted.
- **Category 3** – Other entities who were required to undertake a guided self-assessment that was then interrogated by the Inquiry. Some were required to undertake further work. A summary of these assessments is included as Appendix 3.

3 The Inquiry then undertook a deep inquiry into each of the Category 1 entities. This followed four key phases:

Figure 2: Phases of the Inquiry



APPENDIX 3: CODE OF CONDUCT

A code of conduct issued by the State Services Commissioner under the State Sector Act 1988, section 57

We must be fair, impartial, responsible & trustworthy

The State Services is made up of many organisations with powers to carry out the work of New Zealand's democratically elected governments.

Whether we work in a department or in a Crown entity, we must act with a spirit of service to the community and meet the same high standards of integrity and conduct in everything we do.

We must comply with the standards of integrity and conduct set out in this code. As part of complying with this code, our organisations must maintain policies and procedures that are consistent with it.

For further information see **www.ssc.govt.nz/code**

Fair

We must:

– treat everyone fairly and with respect

– be professional and responsive

– work to make government services accessible and effective

– strive to make a difference to the well-being of New Zealand and all its people.

Impartial

We must:

– maintain the political neutrality required to enable us to work with current and future governments

– carry out the functions of our organisation, unaffected by our personal beliefs

– support our organisation to provide robust and unbiased advice

– respect the authority of the government of the day.

Responsible

We must:

– act lawfully and objectively

– use our organisation's resources carefully and only for intended purposes

– treat information with care and use it only for proper purposes

– work to improve the performance and efficiency of our organisation.

Trustworthy

We must:

– be honest

– work to the best of our abilities

– ensure our actions are not affected by our personal interests or relationships

– never misuse our position for personal gain

– decline gifts or benefits that place us under any obligation or perceived influence

– avoid any activities, work or non-work, that may harm the reputation of our organisation or of the State Services.

APPENDIX 4: SUMMARY OF DECLARATIONS BY GOVERNMENT AGENCIES

Entity Name	Identified engagement of (or with) External Security Consultants	Provider(s)	Purpose(s)	Summary
Public Service Department				
State Services Commission (SSC)	Yes	Icaras	Physical Security Threat Assessment	SSC informed the Inquiry that they had engaged Icaras between November 2016 and February 2017 to carry out a Physical Security Threat Assessment relating to the Public Service Chief Executive roles.
Ministry of Business, Innovation and Employment (MBIE)		Multiple providers		Key issues related to MBIE's use of external security consultants is covered in the body of the report. MBIE also engaged external security consultants to carry out the following activities: • Security services for MBIE and employees across its national and international offices • Reviews of MBIE's physical and environmental security standards. These reviews focused on improving the design of worksites, including balancing the customer experience with the safety and security of employees and visitors. These engagements were not extraordinary. • Security consultants were engaged to provide staff security training, including de-escalation, duress and first responder training, and situational safety and tactical communications training. • Computer Emergency Response Team (CERT) is an organisation within MBIE that receives cyber incident reports, tracks cyber security incidents or attacks, and provides alerts and advice to its customers on how to respond to and prevent further attacks. CERT engaged security specialists to provide services related to its physical environment, and consistent with reasonable expectations given CERT's functions. • Training designed to support MBIE's in-house intelligence capability in advanced social media investigations. • The Insolvency and Trustee Service uses private investigators as process servers. This work includes tracking and securing assets and collecting business records. Occasionally this work also includes interviews for a statement of affairs, which is a statement made by directors related to a company's liquidation. • The services for which Insolvency and Trustee Service uses private investigators include: as process servers; to track, secure and collect assets and business records; and to provide general assistance to the Official Assignee in complex insolvent estates. Occasionally this work also includes interviews for a statement of affairs from company directors or bankrupts. • Immigration NZ engaged forensic auditors to carry out activities falling under the broad definition of investigative practices, to examine whether individuals were complying with the employment requirements for their particular immigration status.
Department of Conservation (DOC)	Yes	TCIL	Threat assessment	DOC's use of external security consultants is covered in the main body of this report.

Entity Name	Identified engagement of (or with) External Security Consultants	Provider(s)	Purpose(s)	Summary
Department of Corrections	No	N/A	N/A	The Department of Corrections undertook an internal review, including: • Enquiries to the Executive leadership team and other appropriate senior managers • Enquiries to major outsource contract providers • Examination of financial systems for contracts and payments to TCIL, associated entities, or other external security consultants • Examination of emails for interactions with TCIL and related entities • Examination of the document management system for records relating to TCIL and related entities • Examination of the procurement system for vendor records. The Department informed the Inquiry that it found nothing to suggest there has been any inappropriate engagement of, or interaction with, TCIL, its shareholders or related entities, or with other external security providers.
Crown Law Office	Yes	Peter Ward & Associates Nicholas Perry ICIL	Process serving	Crown Law reviewed its use of external security consultants through a review of email and document management systems and financial management systems. This review identified that Crown Law has used and continues to use the services of external security consultants in limited circumstances, mainly to serve documents and in limited instances to provide litigation support, including contacting witnesses and supporting the briefing and cross-examination of witnesses. Crown Law had a relationship with an external security consultant relevant to a civil case involving MSD – this is explored further in the main body of this report.
Ministry for Culture and Heritage (MCH)	No	N/A	N/A	MCH carried out a review across the matters identified and confirmed that it did not identify any interactions related to the matters.
New Zealand Customs Service (NZ Customs)	Yes		Secondary employment	NZ Customs maintains dedicated investigative and intelligence capabilities to prosecute serious crime such as drug trafficking, as enabled by legislation such as the Customs and Excise Act 1996, the Misuse of Drugs Act 1975 and the Search and Surveillance Act 2012. Customs therefore does not typically seek external providers for this type of activity. Based on the criteria provided, Customs undertook a review of the years 2008 to 2018, and of some financial records back to 1998, and an email search using key words relating to TCIL and its identified subsidiaries. Customs identified some contact with TCIL, where Customs was copied into emails between TCIL and other parties such as port companies. Customs also identified that a small number of staff sought secondary employment with external security consultants. In July 2018, Customs approved new policies to better address secondary employment and conflicts of interest.

Entity Name	Identified engagement of (or with) External Security Consultants	Provider(s)	Purpose(s)	Summary
Ministry of Defence	Yes	Employrite	Employee vetting	The Ministry of Defence confirmed that it has not engaged TCIL or its associated entities. This was based on a review of its financial and email records. It identified the use of an external vetting agency to vet new employees while full NZSIS-vetted clearances are being processed. The process involves a database and credit check/analysis, a qualifications check, and a Ministry of Justice criminal history check. The checks are always done with the knowledge and consent of the particular individual.
Ministry of Education	Yes	Corporate Risks Ltd Cyclops Monitoring	Review fire damage Trial of managed camera solutions	The Ministry of Education reviewed records for the past 10 years based on the guidance in the Inquiry's letter. The only two entities engaged over this period were Corporate Risks Ltd and Cyclops Monitoring ltd. Both were engaged by the property division to review fire damage to schools. Engagements related to Cyclops Monitoring are included within the main body of this report.
Education Review Office (ERO)	Yes – out of scope	Not stated	Building security advice	The ERO identified one engagement of an external security consultant for building security advice, which the ERO noted was not within the scope of the inquiry. The ERO provided assurance that it had not had dealings with TCIL or its associated entities.
Ministry for the Environment (MFE)	No	N/A	N/A	MFE confirmed that it has not had any interactions with TCIL or any of its associated entities, nor has it engaged any security consultants in the manner specified in the Inquiry letter. The details of the internal review process were not provided.
Ministry of Foreign Affairs and Trade (MFAT)	Indirect	TCIL	Security services Threat assessments	MFAT completed an internal review and analysis of the years from 2008 on the use of external security consultants, and confirmed: • It has not used external security consultants for any services related to high-level security assessments and private investigations of individuals or groups • It has not engaged third parties to gather intelligence from open source documents, using surveillance on individuals or groups, and has not conducted any threat assessments on individuals or groups. Issues related to indirect engagement with TCIL are covered in the main body of this report.
Government Communications and Security Bureau (GCSB)	Nil	N/A	N/A	The GCSB confirmed that it has had no interactions with TCIL or its associated entities. It confirmed that after a review of its current financial management system as far as records allow, it could not identify any contracts or payments, or any use of or interactions with, external security consultants as defined in the letter from the Inquiry.
Ministry of Health (MOH)	Yes	TCIL Marie Scott Tanya McCall	Enforcement of public health legislation	MOH's use of external security consultants is covered in the main body of this report.

Entity Name	Identified engagement of (or with) External Security Consultants	Provider(s)	Purpose(s)	Summary
Inland Revenue Department	Yes – out of scope	Not stated	Process serving	Inland Revenue confirmed that it completed a self-evaluation based on the recommended search parameters. IRD's financial records indicate that it has used external security consultants for a variety of business reasons, the majority of which can be excluded as out of scope. Further detailed analysis of 1,762 line items, excluding activities such as process serving, found no concerns. IRD informed the Inquiry that it has not used the services of TCIL or its associated entities.
Department of Internal Affairs (DIA)	Yes	Paragon NZ	Process serving (deprivation of citizenship)	DIA undertook an internal review including: • A request to Deputy Chief Executives that they provide information about any business functions in their Branch that may have engaged external security consultants at any time in the 10 ten years • A company name and key word search of financial and document management system records since 2008, and further investigation of any matches, to determine whether the documentation indicated interaction with external security consultant services. DIA has used, and continues to use, external security consultants (as defined in the Inquiry's letter) to serve notices of deprivation of citizenship. These are examined in the main body of this report. DIA's Complaints, Investigations and Prosecutions Unit has contact with external security consultants as part of its role in investigating complaints received by the Private Security Personnel Licensing Authority (hosted by Ministry of Justice). In addition: • The Gambling Compliance team used an external security consultant as a process server, but this did not involve surveillance. • For censorship prosecutions, the Crown Solicitor may engage private investigation companies as a process server. • The Weathertight Homes Resolution Service, hosted by DIA in the early 2000s, did employ private investigation firms, although given the timeframe this has not been investigated in detail.
Ministry of Justice	Yes	TCIL Others not named	Investigate on behalf of defendants Building security Risk assessments Threat assessments Advice on risk analysis	Based on a review of financial and contract management systems, the Ministry of Justice identified that TCIL had been used on two occasions by the Public Defence Service, once in 2011 and once in 2012, to investigate on behalf of defendants in criminal cases funded through legal aid. The Ministry is comfortable that this is a standard use of investigators in serious criminal cases. The Ministry's review of these instances raised no cause for concern. Other use of external security consultants involved advice on the security of Ministry sites (such as the newly constructed Christchurch Justice and Emergency Services Precinct); risk assessments of other Ministry sites; a threat assessment of the Ministry; and advice on its risk analysis tools. None of these consultants engaged with the public.
Land Information New Zealand (LINZ)	Yes	Cyclops Monitoring	Monitoring	LINZ identified one contract related to Cyclops Monitoring, which is covered in the main body of this report.

Entity Name	Identified engagement of (or with) External Security Consultants	Provider(s)	Purpose(s)	Summary
Te Puni Kōkiri / Ministry of Māori Development (TPK)	No	N/A	N/A	TPK searched its financial, contract, email and document management systems to confirm that it has no record of using external security consultants for the past 10 years. TPK excluded its use of Māori Wardens, who from time to time support routine or special engagements and events, but which would fit the exclusion in the Inquiry's letter for security guard services.
Ministry for Pacific Peoples	No	N/A	N/A	The Ministry carried out the following activities: • Searched supplier listings in their financial system • Reviewed its contracts database and clarified the nature of those contracts • Completed a search of its electronic files, including its email system • Made inquiries with longstanding staff members as well as senior staff members • Verified that it has not used and does not use platforms such as Wordpress or Slack to exchange information with security consultants. As a result, the Ministry confirmed that it has not engaged TCIL or any other external security consultant.
Ministry for Primary Industries (MPI)	Yes	TCIL		MPI's use of external security consultants is covered in the main body of this report. MPI undertook the assurance recommended by the Inquiry focusing on the last 10 years and did not identify any further evidence that it had any interactions with TCIL, its associated entities, or any other providers beyond those the Ministry had already informed the Inquiry about.
Department of Prime Minister and Cabinet (DPMC)	Yes	Cyclops (CERA)	Security camera monitoring	DPMC undertook a search of its information systems and financial records, including accounts payable and its general ledger for the period since 2008, and confirmed that to the best of its knowledge no external security consultants have been used to provide investigative or surveillance services. DPMC inherited some financial records and functions from CERA, and identified that CERA had some transactions with Cyclops Monitoring for security camera monitoring.
Serious Fraud Office (SFO)	Yes	Icarus	Security framework review	The SFO searched its records and found no relationship with TCIL or its associated entities. The SFO engaged an external security consultant in November 2017 to review the SFO's overall security framework.
Ministry of Social Development (MSD)	Yes	Paragon ICIL Avon Investigations Scope Investigations Ltd	Surveillance (specific cases of suspected fraud) Security camera monitoring Audits, trespass, process serving	MSD's use of external security consultants is covered in the main body of this report.

Entity Name	Identified engagement of (or with) External Security Consultants	Provider(s)	Purpose(s)	Summary
Statistics New Zealand	No	N/A	N/A	Statistics NZ reviewed its HR records and found no reference to the use of external security consultants. It also reviewed its contracts database, and vendors on the finance system for the companies listed.
Ministry of Transport (MOT)	No	N/A	N/A	MOT reviewed its systems and records and found no indication that it had engaged TCIL, its associated entities, or any other security consultants as defined by the Inquiry's letter. In 2011, the Ministry considered an application from TCIL to access the Motor Vehicle Register. These issues are discussed in the main body of this report.
The Treasury	Yes	Icarus	IT security Protective Security Requirements	The Treasury carried out a self-evaluation and found no matters to bring to the attention of the Inquiry. Specifically, Treasury has had no interactions with TCIL or any of its associated entities, and the Treasury does not use the services of 'external security consultants' as defined by the Inquiry. The Treasury sought advice on information technology using members of the GCDO Security and Related Services All of Government panel, and an external security consultant provided advice on meeting the Protective Security Requirements mandated by Cabinet. Treasury is comfortable that all interactions with external security providers have been appropriate and entirely consistent with the professional expectations of the public service as expressed in the Code of Conduct for the State Services.
Ministry for Women	No	N/A	N/A	The Ministry for Women reviewed financial and contractual records and confirmed that it has not had any interactions with security consultants, including TCIL, over the last seven years.
Oranga Tamariki – Ministry for Children	Yes	Not specified	Process serving Locating people	As MSD hosts key systems under a shared service arrangement, the Ministry performed a system search on Oranga Tamariki's behalf, including a forensic email search and a search of financial records. Based on this review, Oranga Tamariki and the former CYFS have not contracted with TCIL or its associated companies. The search did find some minor personal correspondence. Both Oranga Tamariki and CYFS have contracted with external security consultants a number of times, in most cases to serve court documents. In two cases, services were sought to assist in assessing whether a restraining order had been breached and in locating children after other avenues had been exhausted. MSD informed the Inquiry that it would carry out a further review of its document management system regarding other external security providers, and inform the Inquiry if any matters arose. The Inquiry has not been notified of any further issues.
New Zealand Security Intelligence Service (NZSIS)	Yes	TCIL	N/A	The NZSIS reviewed its current financial management system as far as records allow for any contracts or payments to 'like' companies. It did not identify any use of, or interactions with, external security consultants as described by the Inquiry's letter. The NZSIS relationship with external security consultants is covered in the main body of this report.
Te Kāhui Whakamana Rua Tekau mā Iwa—Pike River Recovery Agency	No	N/A	N/A	Provided a nil response.

Entity Name	Identified engagement of (or with) External Security Consultants	Provider(s)	Purpose(s)	Summary
Departmental Agencies				
Social Investment Agency	No	N/A	N/A	Provided a nil response.
Non-Public Service Department				
Parliamentary Counsel Office (PCO)	No	N/A	N/A	The PCO's Director of Corporate Services confirmed that the organisation had never used any firm to undertake the services described in the Inquiry letter since they had started in their role in 2008.

Entity Name	Identified engagement of (or with) External Security Consultants	Provider(s)	Purpose(s)	Summary
Crown Agents				
Accident Compensation Corporation (ACC)	Yes	Advance Investigation Ltd Beattie Varley & Associates Ltd Investigation Services Ltd Limestone Risk Management Ltd Paragon NZ Ltd Sole Trader TAG Investigations Ltd Complete Protection Services Ltd Darren Gray Security NZ Ltd Scope Investigations Ltd Tasman Investigations Ltd Westland Investigations Ltd Maurice J Kerrigan & Associates Paradigm Investigations Ltd DG Solutions Ltd Nelson Investigations Ltd ICIL Group Zavest Ltd	Visual surveillance Photographic and video surveillance Static observation Obtaining witness statements Investigative assistance, including interviewing Other, including forensic accounting and pixilation.	ACC's use of external security consultants is covered in the main body of this report.

Entity Name	Identified engagement of (or with) External Security Consultants	Provider(s)	Purpose(s)	Summary
Callaghan Innovation	No	N/A	N/A	Callaghan undertook a self-evaluation and identified no interactions with TCIL, its associated entities, or other providers that fell within the description of the Inquiry's letter. Callaghan's relationship with Cyclops Monitoring Ltd is covered in the main body of this report.
Civil Aviation Authority (CAA)	Yes	Insurance and Commercial Investigators Ltd Others not specified	Carry out or assist with investigations under s15A of the Civil Aviation Act Serve documents	Until 2010, the Personnel and Flight Training Unit of the CAA engaged a number of individuals from Insurance and Commercial Investigators Ltd to assist staff to conduct investigations under s 15A of the Civil Aviation Act. The aim of a s 15A investigation is to determine whether an aviation participant is meeting its regulatory responsibilities. Private investigators were required because the CAA Personnel Licensing Unit employed aviation technical specialists who did not have extensive investigation expertise. Private investigators were given delegations under s 23B of the Civil Aviation Act to conduct s 15A investigations. The CAA employed a specialist s 15A investigator in 2012, after which the services of private investigators were no longer required. Other than the above, the CAA has on a small number of occasions used private investigators to serve documents on people in remote areas of New Zealand.
Auckland District Health Board (ADHB)	Yes	TCIL	Employee investigation	Auckland District Health Board identified two contracts with TCIL, both in 2015. ADHB contacted TCIL to investigate an employee suspected of misappropriating DHB property. This is an internal employment matter and outside the scope of the Inquiry. For the other, see the MOH section of the main body of this report. The DHB noted that the two instances did not include specialist investigative or security services as defined in the Inquiry letter, and that ADHB does not engage external security consultants for those purposes.
Bay of Plenty District Health Board (BOPDHB)	Yes	Not specified	IT security / cyber security audits	BOPDHB noted that there are occasions where it would use external security consultants for IT-related security exercises or cyber security audits, although these are excluded from the scope of the Inquiry. It would not typically use the services of external security consultants for specialist investigative or security services that would fall within the Inquiry. The organisation reviewed systems and records and could not find evidence of any interactions with TCIL or its associated entities.
Canterbury District Health Board (Canterbury DHB)	Yes – out of scope	Not specified	Security guards Audit	Canterbury DHB and West Coast DHB provided a joint response (from their joint CEO) confirming that neither had a relationship with external security consultants other than for security guard and associated services or, on occasion, for audits. The DHBs specifically confirmed that they had not had any interactions with TCIL or its associated companies. Neither of the DHB's two subsidiary companies, Canterbury Linen Services Ltd and Brackenridge, have had a relationship with external security consultants.
Capital and Coast District Health Board (CCDHB)	No	N/A	N/A	CCDHB confirmed that it has no record of engaging external security consultants for the services noted in the Inquiry's letter. It also confirmed it has no record of engaging TCIL or its associated entities.

Entity Name	Identified engagement of (or with) External Security Consultants	Provider(s)	Purpose(s)	Summary
Counties Manukau District Health Board (CMDHB)	No	N/A	N/A	CMDHB undertook a search of its payment and contract management system, using search terms related to the legal entity names for TCIL and its associated companies, as well as a number of other relevant key words, and this resulted in 51 hits. CMDHB concluded that these hits were related to standard security arrangements (for example, building security arrangements) and therefore outside the scope of the Inquiry's letter. It reached that conclusion by reviewing the last invoice from each supplier (where available), conducting an internet search of suppliers, and reviewing cost codes.
Hawke's Bay District Health Board (HBDHB)	Yes – out of scope	Not specified	Investigations of suspected fraud	HBDHB reviewed and assessed the use of external security consultants, and found that it has used investigation services twice in the stated period for purposes outside the scope of the Inquiry, namely investigations of suspected fraud. In particular, HBDHB found no evidence of contracting TCIL or its associated entities. HBDHB's subsidiary companies, Allied Laundry Services Ltd and Technical Advisory Services, did not use external security consultants.
Health Promotion Agency	No	N/A	N/A	The Health Promotion Agency confirmed that it had had no interactions with external security consultants falling within the definition in the Inquiry's letter, including TCIL or its associated entities.
Hutt Valley District Health Board (Hutt Valley DHB)	Yes	Not specified	PSR Framework and Self-Assessment Report	Hutt Valley DHB identified one use of a security consultant, which was in order to develop a framework and self-assessment report for the Protective Security Requirements, supported by the South Island Alliance Programme Office. The DHB confirmed that it had not engaged TCIL or its associated entities.
Lakes District Health Board (LDHB)	No	N/A	N/A	LDHB completed an internal review and found no interactions with external security consultants (including TCIL and its associated entities) that fell within the definition in the Inquiry's letter. LDHB also confirmed that its subsidiary company, Spectrum Healthcare, found no interactions with external security providers falling within the definition in the Inquiry's letter, including TCIL and its associated entities.
MidCentral District Health Board (MDHB)	No	N/A	N/A	MDHB followed a number of lines of inquiry and found no known relationships with TCIL or associated entities. MDHB searched its financial records in relation to security services and investigations and did not find any matters that should be brought to the attention of the Inquiry.
Nelson Marlborough District Health Board (NMDHB)	No	N/A	N/A	NMDHB confirmed that it has not had any interactions with any external security consultants falling within the definition in the Inquiry's letter, including TCIL and its associated entities.
Northland District Health Board (NDHB)	No	N/A	N/A	NDHB confirmed that it has not accessed the services of external security consultants, including TCIL or associated companies, from 2008 to the present.
South Canterbury District Health Board	No	N/A	N/A	South Canterbury DHB stated that it does not use and has not used any external security consultants.
Southern District Health Board	No	N/A	N/A	Southern DHB confirmed that it had not had any interaction with TCIL from 2008 to the present, and that it could find no record of interactions with any other external security consultants in the same period.

Entity Name	Identified engagement of (or with) External Security Consultants	Provider(s)	Purpose(s)	Summary
Tairawhiti District Health Board	No	N/A	N/A	Hauora Tairawhiti confirmed that it has not had any contact, relationships or contracts as described in the Inquiry's letter, in particular with TCIL. Hauora Tairawhiti has three subsidiary companies, Tairawhiti Laundry Services Ltd (100% owned), Healthshare Ltd (20% interest), and TLab (50% interest), none of which, to the best of Tairawhiti DHB's knowledge, has had any interactions with external security providers, including TCIL and its associated entities.
Taranaki District Health Board	No	N/A	N/A	Taranaki DHB confirmed that it has taken the steps set out in the Inquiry's letter to provide the assurance required, and confirmed that it had not contracted any company or individual to provide specialist investigative or security services over the past 10 years. Taranaki DHB had three subsidiary companies over the period (HIQ, Fulford Radiology, and Allied Laundry).
Waikato District Health Board	Yes	Not specified	Specific case of fraud	Waikato DHB did not identify any interactions with TCIL, its associated entities, or other providers falling within the definition in the Inquiry's letter. The DHB undertook a comprehensive review of its financial, contracts, and email records for references to TCIL and its associated entities, and spoke to senior executives who have been with the DHB for more than 10 and up to 20 years. The DHB identified that specialist investigative staff had been engaged to address a specific case of fraud, which is outside the scope of the Inquiry. Waikato DHB's subsidiary HealthShare Ltd (a shared services organisation for the Midland region) has never used external security consultants.
Wairarapa District Health Board	No	N/A	N/A	Wairarapa DHB reviewed its transaction history to 2014 and their contracts register, and did not identify any contracts with or payments to the specified companies or other providers of security-related advice as defined by the Inquiry's letter.
Waitemata District Health Board	No	N/A	N/A	Waitematā DHB carried out an internal review and confirmed that it has had no interactions with TCIL or any of its associated entities, and is not aware of any use of other consultants who provide services described in the Inquiry's letter.
West Coast District Health Board	Yes – outside scope	Not specified	Security guards Audit	Canterbury DHB and West Coast DHB provided a joint response (from their joint CEO) confirming that neither had a relationship with external security consultants other than for security guard and associated services or, on occasion, for audits. The DHBs specifically confirmed that they had not had any interactions with TCIL or its associated companies.
Whanganui District Health Board	No	N/A	N/A	Wanganui DHB confirmed that it has satisfied itself as required by the Inquiry's letter. It checked its supplier list and payment system and confirmed that it has not used TCIL or any of its associated entities since the system was installed in 2009.
Earthquake Commission (EQC)	Yes	Avon Investigations Neill Group	Investigations related to litigation	EQC undertook a self-evaluation, including a review of its financial payment system and email records, and a keyword search. It confirmed that it had made no payments to TCIL or its associated entities, and provided the Inquiry with assurance that the companies identified by the keyword search were not delivering services within the scope of the Inquiry. EQC engaged private investigators twice in the previous three years, to assist with their response to separate litigation claims. These were the only instances of private investigators for litigation purposes over the past 10 years.

Entity Name	Identified engagement of (or with) External Security Consultants	Provider(s)	Purpose(s)	Summary
Education New Zealand (ENZ)	No	N/A	N/A	ENZ confirmed that it had not used any external security consultants, including private investigators, since it was established in 2012.
Energy Efficiency and Conservation Authority (EECA)	No	N/A	N/A	EECA reviewed financial systems, contract registries, and searched its email archive for any emails to or from anyone at the companies listed in the appendix and found no association with the companies in question, and has undertaken no business with TCIL.
Environmental Protection Authority (EPA)	Yes	Zavest Ltd	Investigation	EPA reviewed its records, including keyword searches of financial records for the past 20 years, searched the EPA Contract Register, and ran a centralised search of email and all electronic records. It also inquired with staff whether they have any knowledge of the use of security consultants falling within the terms of inquiry. The EPA found no record of having formally or informally engaged TCIL or its associated entities to provide services. In 2012, the EPA contracted an external security consultant to assist with an investigation into an alleged release of an ozone-depleting substance. The EPA identified some interactions with TCIL or its associated entities, including email correspondence with other agencies who had included TCIL or copied TCIL into the original message, and involvement in multi-agency exercises, including MEJIG (see body of the report), considering how the Government may respond to risks posed to offshore operations. TCIL is mentioned in the exercise brief as a security consultant.
Health Quality and Safety Commission	No	N/A	N/A	The Commission confirmed that it had not used any of the external security consultants referred to in the Inquiry's letter since it was established in 2010.
Health Research Council of New Zealand	No	N/A	N/A	The Health Research Council confirmed that it had not contracted with or used any company or individual to provide specialist or investigative or security services as defined in the Inquiry's letter. The Council reviewed its finance system back to 2005 for evidence that it had engaged external security consultants to deliver high-level security assessments and private investigations of individuals or groups, or engaged third parties to gather intelligence. The Council also reviewed its IT systems for any platforms used to exchange information with external security consultants.

Entity Name	Identified engagement of (or with) External Security Consultants	Provider(s)	Purpose(s)	Summary
Housing New Zealand Corporation (HNZC)	Yes	Not specified	ICT security Risk assessment and advice (personal security and home security) Personal security advice (conflict resolution) Security guards Security systems (incl cameras and monitoring)	HNZC sourced a variety of services from external security consultants, largely to do with providing specific security systems and personnel (ICT, cameras, and security guards), and risk assessment and personal security advice for staff. HNZC carried out an email search and confirmed that it had not had any interaction with TCIL. HNZC participated in a trial of the Cyclops Monitoring system, which is covered in the main body of this report.
Maritime New Zealand	Yes	Investigation Services Paradigm Investigations Private Investigations Ltd Jeff Gunn Ltd	Investigate 'fit and proper' Assist with prosecution Investigate matters relating to the grounding of the Rena Surveillance (of a ferry operator - enforcement of regulatory responsibilities)	Maritime New Zealand's use of, and relationship with, external security consultants is covered in the main body of this report.
New Zealand Antarctic Institute (Antartica NZ)	No	N/A	N/A	Antarctica NZ confirmed that, following an internal review, it found no interactions with TCIL, its associated entities, or other external security consultants as defined in the Inquiry letter.
New Zealand Blood Service	No	N/A	N/A	The New Zealand Blood Service reviewed its records and found no interactions with TCIL or its associated companies from 2008 to the present. The CE stated that to the best of their knowledge, the Service has not engaged any other external security consultants during this time.

Entity Name	Identified engagement of (or with) External Security Consultants	Provider(s)	Purpose(s)	Summary
Fire and Emergency New Zealand	No	N/A	N/A	FENZ was formed on 1 July 2017, as an amalgamation of 40 organisations throughout NZ. FENZ holds robust records for two organisations, the NZ Fire Service and the National Rural Fire Authority; the information for the other 38 organisations is held by local government. FENZ made enquiries of the records available, including and searching accounts payable and procurement databases, and was not able to find records of any contact with the organisations specified in the Inquiry's letter. The CFO also made enquiries of the leadership team, and confirmed that the organisation is not aware of the use of any external security consultants.
New Zealand Qualifications Authority (NZQA)	No	N/A	N/A	NZQA reviewed its procurement and contract systems, financial management information system, and email system, to confirm that NZQA has not engaged the services of external security consultants for the purposes referred to in the Inquiry's letter. NZQA noted that a number of services were excluded from scope. NZQA also confirmed that it has not engaged TCIL or its associated entities.
New Zealand Tourism Board	Yes	The Investigators New Zealand Ltd	Compliance enforcement	The Board reviewed its financial records for any interaction with external security consultants. The Board uses the services of an external security consultant to monitor the Approved Destination Status (ADS) programme in support of Tourism New Zealand's China Market Development Unit. This includes spot checks of ADS tours, as described in section 9 of the ADS Code of Conduct. The individuals carrying out the checks identify themselves as working for Tourism NZ, and are supplied with photographic identity cards to validate their status.
New Zealand Trade and Enterprise (NZTE)	No	N/A	N/A	NZTE searched its contracts database and financial records, and discussed the issue with its leaders. It found no records of engaging services covered by the Inquiry, and specifically identified that no payments were made to TCIL.
New Zealand Transport Agency (NZTA)	Yes	Corporate Risks Ltd	Regulatory assessment	NZTA carried out a review, including direct contact enquiries from the senior leadership team to their business groups, and a search of investment, finance, and business records. NZTA engaged the services of a private investigator from 21 November 2016 to 24 February 2017 to assess Uber's on-boarding process in Christchurch, Wellington and Auckland. NZTA has not contracted TCIL or its associated entities to provide specialist investigative or security services. The relationship between NZTA and TCIL is covered in the main body of this report.
New Zealand Walking Access Commission	No	N/A	N/A	The Commission confirmed that it had not engaged any external security consultants (as defined in the Inquiry's letter) since it was established in 2009 until the present.
Pharmaceutical Management Agency (PHARMAC)	Yes	Icaras Security Risk Management Ltd	Security assessments	Following an internal review, PHARMAC identified two instances in the past 10 years where it has engaged external security consultants, both relating to high-level security assessments of building security. PHARMAC has also sought a range of security advice that is outside the scope of this review, including IT security, security monitoring, security access management, and security guards. PHARMAC has not engaged TCIL or its associated entities from 2008 to the present.

Entity Name	Identified engagement of (or with) External Security Consultants	Provider(s)	Purpose(s)	Summary
Real Estate Authority	Yes	D'Urville Solutions Ltd Corporate Risks Ltd	Investigative functions Process serving	The Real Estate Authority carried out an internal review, and found that its interactions with external security providers were appropriate. The REA did not identify any interactions with TCIL or its associated providers. The Inquiry sought additional information about the REA's use of external security providers. The Authority occasionally uses external investigators to support it in investigating allegations about the conduct of licensees. It employs a team to conduct investigations either on REA's own motion or as a result of a decision of a Complaints Assessment Committee (appointed under statute). Investigators contact and interview witnesses, liaise with parties, obtain relevant documents from the parties and prepare reports for the Complaints Assessment Committee to consider. The companies are instructed and monitored by, and report to the REA investigations manager. Between 2009 and 2017, two private investigation companies were used. Since 2017, external investigators have only been used to serve documents in Disciplinary Tribunal proceedings.
Social Workers Registration Board	No	N/A	N/A	The Social Workers Registration Board did not identify any interactions with TCIL, its associated entities, or other providers that fell within the definition set out in the Inquiry letter.
Sport New Zealand	No	N/A	N/A	Sport NZ confirmed that it had not engaged any external security consultants from 2008 to the present.
WorkSafe New Zealand	Yes	Icaras Ltd Corporate Risks Ltd Axcenic (ICT) Insomnia (ICT) Wellington Investigations Ltd West Document & Investigation Tony Lowe Investigations Ltd Trademark Investigations	Physical and site security Process serving Locating witnesses	Worksafe reviewed financial transactions since it was established in 2014, and engaged with relevant employees. It identified the use of a variety of security firms, including for: • security guard services, alarm monitoring, and site assessments and audits • serving legal documents • investigating the location of witnesses. As part of due diligence before Worksafe lodged a trademark application, Trademark Investigations were engaged to carry out electronic investigation into the organisation SafePlus, to find out if they operated any products or services that used the name 'SafePlus'. Worksafe did not identify any interactions with TCIL or its associated entities.
Tertiary Education Commission (TEC)	No	N/A	N/A	TEC staff reviewed records back to 2004 and found no records relating to external security consultants. TEC's emphasis was on looking for the entities listed in the Inquiry's letter, as a well as an overall review to see if there were any other transactions that fit into the Inquiry's definition of external security consultant.

Entity Name	Identified engagement of (or with) External Security Consultants	Provider(s)	Purpose(s)	Summary
Crown Research Institutes				
AgResearch	Yes	TCIL	Security and threat assessment	AgResearch's use of external security consultants is covered in the main body of this report.
Institute of Environmental Science Research (ESR)	No	N/A	N/A	ESR carried out a self-evaluation and confirmed that neither ESR nor any of its subsidiaries had engaged external security consultants as set out in the Inquiry's letter. In particular, ESR confirmed that it had not made any payment to nor received any services from TCIL or its associated entities. ESR identified a number of interactions with TCIL, including: • ESR carrying out a forensic analysis of a garment for TCIL, at a cost of $600, invoiced to and settled by TCIL • References to TCIL in documents or TCIL being copied into emails by other agencies or entities, including in relation to Public Health Statutory Offices, Environmental Health Analysis, Advice Services Guide, 1080 testing, and a request to test herbal cigarettes • General business development approaches from TCIL, including an offer for security risk management services (no action was taken by ESR) and a presentation to CRI Property Managers on lessons from the Pike River disaster • A spam email from a TCIL domain.
GNS Science	No	N/A	N/A	GNS reviewed its financial records and email system (for tiers 1–3) for interactions with TCIL and its associated entities. It identified no payments to TCIL or its associated entities. GNS identified emails from TCIL between June 2016 and August 2017, for general business development (for security planning, vessel port call support, and security response to operation), providing example Security Situation Reports from other agencies and a risk assessment framework. TCIL provided two specific business proposals to provide security awareness and security risk management for the integrated ocean drilling programme; GNS did not proceed with these proposals. TCIL also sought information from GNS (and was directed to publicly available information on the GNS website), and asked to be added to a distribution list.
Landcare Research	No	N/A	N/A	Landcare interrogated finance and contracts databases and found no mention of TCIL or related parties. The CEO also has no knowledge of using security contractors for anything other than routine security after-hours and ICT security advice, both of which are outside the definition in the Inquiry's letter.
National Institute of Water and Atmospheric Research (NIWA)	Yes	TCIL	Security and threat assessment	NIWA's use of external security consultants is covered in the main body of this report.

Entity Name	Identified engagement of (or with) External Security Consultants	Provider(s)	Purpose(s)	Summary
Plant and Food Research	Yes	TCIL Cyclops Monitoring	Physical and operational security review Investigation into asbestos removal Building security monitoring	Plant and Food's use of external security consultants is covered in the main body of this report.
Scion	Yes	Concord Security / Advanced Security TCIL	Premises security Security and Threat Assessment	Scion engaged an external security provider in 2015 to provide security services for its Genetically Modified Organism trial. This is ongoing. TCIL supplied Situation Reports to Scion unsolicited and free of charge from July 2015 to May 2018. Scion searched its financial systems, contracts database, and IT system for the listed organisations and associated keywords ad did not identify any engagements of other external security providers.
Autonomous Crown Entities				
Arts Council of New Zealand Toi Aotearoa	No	N/A	N/A	The Arts Council of New Zealand confirmed that it has not entered into any contracts for services with external security consultants, nor has it engaged in discussions to procure these services.
NZ on Air (Broadcasting Commission)	No	N/A	N/A	NZ on Air confirmed that it did not identify any interactions with TCIL, its associated entities, or other providers that fell within the definition provided in the Inquiry's letter.
Government Superannuation Fund Authority	No	N/A	N/A	The Government Superannuation Fund Authority confirmed that it has not used the services of any external security consultants, including TCIL, in the last 10 years.
Guardians of New Zealand Superannuation	Yes	RisQ Chivalry Security First Advantage Pinnacle Security	Personal and premises security Event security Due diligence Employee vetting	The Guardians of NZ Superannuation identified the use of a variety of security consultants, to: • provide advice on premises security and personal security training for staff • assist with security management for the 8th Annual Meeting of the International Forum of Sovereign Wealth Funds, which it hosted in Auckland in November 2016 • do background checks on key individuals who were prospective or existing external investment managers, as part of the organisation's standard due diligence procedures • undertake routine criminal and credit pre-employment checks. The organisation has not engaged the services of TCIL. The NZ Super Fund has a number of subsidiaries, which are a combination of passive holding companies and active investment vehicles – they are not operating companies, and are therefore low-risk in relation to the Inquiry.

Entity Name	Identified engagement of (or with) External Security Consultants	Provider(s)	Purpose(s)	Summary
Museum of New Zealand Te Papa Tongarewa	Yes	TCIL Others not specified	Premises security Security assessments Technical experts across procurement	Te Papa's use of external security consultants is covered in the main body of this report.
New Zealand Artificial Limb Service	No	N/A	N/A	The NZALS reviewed its records and found no interactions and no cause for concern regarding the issues set out in the Inquiry letter.
New Zealand Film Commission	No	N/A	N/A	The Film Commission discussed the request internally, and reviewed its records. It confirmed that it did not believe it had any matters that should be brought to the attention of the Inquiry.
Heritage New Zealand (Pouhere Taonga)	No	N/A	N/A	Heritage NZ reviewed all contracts, financial transactions and email systems and confirmed there were no records of any interaction with TCIL or its associated entities. It also confirmed that it has not engaged security services (as specified in the Inquiry's letter) from any provider.
New Zealand Lotteries Commission	Yes	Paragon Investigations OPSEC Solutions	Premises security Conflict training Robbery training	Lotto NZ reviewed its use of external security consultants from 2008. It has used external security consultants for the following activities: • Review of retail (Lotto outlets) physical security risks (annual/biennial review) • Review of new office physical security (2014) • Conflict training – internal staff (2016) • Ad hoc investigation of retail incidents (outside the scope of the Inquiry) • Robbery training for Lotto outlets (2018 – in progress at time of response) • Robbery training for Lotto outlets (2018 – in progress at time of response).
New Zealand Symphony Orchestra (NZSO)	No	N/A	N/A	NZSO informed the Inquiry that it has had no interactions with TCIL, its associated entities or other providers falling within the Inquiry's definition of 'external security consultants'.
Public Trust	Yes	Not specified	Locating people Risk assessments Security advice	Public Trust reviewed its use of external security consultants over the past 10 years. Public Trust, including its operating subsidiary New Zealand Permanent Trustees Ltd, engages external security consultants for the primary purpose of locating missing clients, beneficiaries or other family members that it needs to contact in order to fulfil its fiduciary obligations. External security consultants are also occasionally engaged to conduct risk assessments and provide security advice and support for dealing with an aggressive client, to protect the health and safety of Public Trust staff. Public Trust did not identify any interactions with TCIL or its associated entities. Public Trust operates a number of additional subsidiaries, including three non-trading companies and many nominee companies. It did not identify any use of external security consultants by these subsidiaries.

Entity Name	Identified engagement of (or with) External Security Consultants	Provider(s)	Purpose(s)	Summary
Commission for Financial Literacy and Retirement Income	No	N/A	N/A	The Commission carried out an internal audit of financial records and contract registries from 2008 to the present. It did not identify any interactions with TCIL, its associated entities, or other providers.
Te Taura Whiri I Te Reo Maori (Maori Language Commission)	No	N/A	N/A	The Commission informed the Inquiry that it undertook all reasonable steps to ascertain that it had not engaged the use of external security consultants. It noted it had engaged routine services that are outside of the scope of the Inquiry, such as alarm monitoring, waste management document disposal, and audits.
Te Māngai Pāho	No	N/A	N/A	Te Māngai Pāho confirmed that it has not engaged any external security consultant during the period of interest, including TCIL.
Testing Laboratory Registration Council / Accreditation Council (IANZ)	No	N/A	N/A	The Accreditation Council confirmed that neither it, nor its subsidiary Telarc Ltd, has had dealings with external security agencies, including TCIL and its associated entities, since 2008, either in a formal or informal manner.
Independent Crown Entities				
Broadcasting Standards Authority	Yes – out of scope	Ruffel and Associates Protect Self Defense	Staff training	The Broadcasting Standards Authority conducted a self-evaluation with respect to the use of external security consultants and confirmed that it did not identify any interactions that fall within the scope of the Inquiry. It consulted with long serving staff and undertook a review of correspondence, physical and virtual files and financial records. It has not engaged any security consultants to provide specialist investigative or security services as defined in the Inquiry letter. The Authority engaged security consultants in 2017 to provide staff training to de-escalate potential physical harm scenarios and establish physical security procedures, and in 2016 to provide self-defence training for staff.
Children's Commissioner	No	N/A	N/A	The Children's Commissioner confirmed that it has not had any relationship with external security consultants, including TCIL.
Commerce Commission	Yes	Not specified	Process serving Location of debtors	The Commerce Commission undertook a review of its contract, information and finance systems, and questioned staff. The Commission identified that it engaged external security consultants fewer than 20 times over 10 years, relating to personal service, process services, exhibit returns, location of debtors, information provided in relation to cases undertaken. The Commission has not engaged TCIL or any of the associated entities within the period of the review. They did have some interactions in 2014 where TCIL provided evidence connected to an investigation into a potential breach of an Act the Commission enforces. The CE has assessed these interactions as appropriate and no cause for concern. The CE considers that the use of external security consultants has been appropriate, subject to appropriate oversight and controls in place, and consistent with Code and the professional expectations of the public sector.

Entity Name	Identified engagement of (or with) External Security Consultants	Provider(s)	Purpose(s)	Summary
Drug Free Sport New Zealand (DFSNZ)	Yes	Omega Investigations Lisa Grace	Investigations	DFSNZ is responsible for implementing the world anti-doping code in New Zealand. It is necessary, from time to time, to engage investigators to support DFSNZ's pursuit of individuals where there has been credible evidence or information that a breach of the Sports Anti-Doping Rules has occurred. DFSNZ have had little or no in-house expertise to perform this work. The organisation does not engage investigators for any other purposes. Each engagement is in relation to a specific athlete. DFSNZ undertook a comprehensive internal review of their engagement of external security consultants, and found: • engagement of external security consultants to support 6-8 cases between 2013-2017, including investigative work spanning several years, and which, where appropriate, culminated in the Sports Tribunal in a banning an athlete(s) for breaching the anti-doping Code. • an independent contractor was engaged to support investigation into the website, NZ Clenbuterol. The engagement included direct weekly oversight. DFSNZ found no references to TCIL or its associated entities.
Electoral Commission	No	N/A	N/A	The Electoral Commission confirmed that it has had no interactions with any external consultants falling within the definition covered by the State Services Inquiry, including TCIL and its associated entities.
Electricity Authority	Yes	Security Risk Management Ltd	Employment issues	The Electricity Authority (Authority) consulted its records from establishment in 2010, and those of the Electricity Commission (Commission) prior to this date, to determine the use by both organisations of external security consultants and identified two investigations related to employees. Both engagements were short term, the consultant was appropriately licensed, and the Authority is satisfied with how they were governed. Neither the Commission nor the Authority has engaged TCIL or its associated entities.
External Reporting Board	No	N/A	N/A	The External Reporting Board reviewed its records from inception in July 2011 to 30 June 2018 and confirmed that it has not used any external security consultants falling within the definitions provided in the Inquiry letter, including TCIL and its associated entities.
Financial Markets Authority (FMA)	No	N/A	N/A	The FMA confirmed that it undertook the reviews requested, and did not identify an instance where it engaged such services since its establishment in 2011.
Health and Disability Commission (HDC)	No	N/A	N/A	HDC confirmed that it has not engaged any external security consultants, including TCIL and its associated entities.
Human Rights Commission	No	N/A	N/A	The Human Rights Commission: • reviewed its finance system back to 2005 for evidence of any relationship with external security consultants delivering high level security assessments and private investigations of individuals or groups or the engagement of third parties to gather intelligence, and • reviewed IT systems for platforms to exchange information with external security consultants. The Commission found no evidence of any relationship of this nature.

Entity Name	Identified engagement of (or with) External Security Consultants	Provider(s)	Purpose(s)	Summary
Law Commission	No	N/A	N/A	The Law Commission advised that in the absence of a law reform project relating in some way to "external security consultants" the Commission would not in the normal course of performing its statutory functions and powers use or have any interactions or relationships with external security consultants. The Commission searched its online and archived records for 2008/09-2017/18 and found no record of TCIL or payment to any TCIL company. To the best of their knowledge and belief, there is no reason to expect the Commission has had any relationship with external security consultants for any purpose.
New Zealand Productivity Commission	No	N/A	N/A	The Productivity Commission confirmed that it undertook the self-evaluation and sought assurance as requested by the Inquiry. The Commission has not identified any interactions with TCIL, its associated entities, or other providers, falling within the definition(s) of security consultancy as set out in the Inquiry letter.
Office of Film and Literature Classification (OFLC)	Yes	Not specified		The OFLC undertook a review of financial and email records exceeding the 10 year period requested. The OFLC identified one case in 2014 where external security consultants were contracted by the Office in a manner which meets the definition provided. The CE assured themselves that this engagement was consistent with the professional expectations of the public service as well as internal policies. The Inquiry team has explored the context of this engagement and found no cause for concern. OFLC can confirm that it has no knowledge of, and can find no record of, any interactions with TCIL or its associated entities.
Privacy Commissioner	No	N/A	N/A	The Privacy Commissioner undertook an internal review of interactions with external security consultants as defined in the Inquiry letter, and found no interactions that give the CE cause for concern.
Takeovers Panel	No	N/A	N/A	The Takeovers Panel undertook an internal review of the use of external security consultants as defined in the Inquiry letter. The panel confirmed that it has not identified any interactions with TCIL, its associated entities, or other providers.
Transport Accident Investigation Commission	No	N/A	N/A	The Commission confirmed that it has not hired any security services, except for on occasion security guards to guard accident sites or evidence. It confirms that it has not had any interactions with TCIL or its associated entities.
Crown Entity Companies				
New Zealand Venture Investment Fund Limited (NZVIF)	No	N/A	N/A	NZVIF confirmed that it has not contracted any specialist investigative or security services or engaged in any third parties for the purposes as outlined in the Inquiry letter since the company was incorporated in 2002.
Crown Irrigation Investment Limited	No	N/A	N/A	Crown Irrigation Ltd confirmed that it has not had any interactions with TCIL, its associated entities, or other providers falling within the definition outlined in the Inquiry letter.
Radio New Zealand Limited (RNZ)	No	N/A	N/A	RNZ confirmed that it has not use any external security consultants.

Entity Name	Identified engagement of (or with) External Security Consultants	Provider(s)	Purpose(s)	Summary
Television New Zealand Limited (TVNZ)	Yes	First Security Zero Risk The Investigators Michael Savage and Associates	Premises security High risk deployment training Staff security Fraud investigations Process serving	TVNZ, including all subsidiaries, has engaged the following security consultants and private investigators during the last seven years for the following services: • premises security (mainly after hours), front desk relief • high risk deployment training for News employees • security for News staff, external fraud investigation • document serving, internal fraud investigation. TVNZ confirmed that it has not engaged TCIL or its associated companies within the past eight years.
Crown Asset Management Limited	No	N/A	N/A	Crown Asset Management Limited confirmed that the company had not engaged any external security consultants or had cause to engage such consultants during the time of its operation.
Crown Infrastructure Partners	No	N/A	N/A	Crown Infrastructure Partners confirmed that it has not had any interactions with TCIL, its associated entities, or other providers falling within the definition outlined in the Inquiry letter.
Education Payroll Ltd	No	N/A	N/A	Education Payroll reviewed records back to the establishment of the company in 2014, and spoke with key managers. Based on this review, it did not identify any evidence of EPL having engaged external security consultants or investigators from 2014 to present (noting that this excludes standard security guard services and IT security related services). EPL further confirmed that it has had no commercial relationship with TCIL or associated entities.
Network for Learning (N4L)	No	N/A	N/A	Network for Learning confirmed that it has not engaged any organisation for the provision of investigative or surveillance services. It has also never engaged TCIL or its associated entities. N4L provides security services to schools in NZ, and engages with vendors of online security products both within NZ and internationally.
Ōtākaro Limited	Yes	TCIL	Premises security	Ōtākaro's engagement of TCIL is covered in the main report.
Predator Free 2050 Limited	No	N/A	N/A	Predator Free 2050 confirmed that it had found no interactions and/or no cause for concern.
Research and Education Advanced Network New Zealand Limited (REANNZ)	No	N/A	N/A	REANNZ confirmed that it has not used the services of any private investigator, nor any services from TCIL and its associated entities.
Southern Response				Southern Response's use of external security consultants is covered in the main body of this report.
Tamaki Redevelopment Company Limited	No	N/A	N/A	Tāmaki Regeneration Company confirmed that it has not undertaken any external security work.

Entity Name	Identified engagement of (or with) External Security Consultants	Provider(s)	Purpose(s)	Summary
Reserve Bank of New Zealand				
Reserve Bank of New Zealand (RBNZ)	Yes	IRisk	Security assessments	RBNZ engaged a provider to undertake high-level security assessments, which included the gathering of intelligence from open source documents on security related issues, following review by the legal team of the provider and of the contract terms. RBNZ has not engaged TCIL or its associated entities.