Departmental Disclosure Statement

New Zealand Intelligence and Security Bill

The departmental disclosure statement for a government Bill seeks to bring together in one place a range of information to support and enhance the Parliamentary and public scrutiny of that Bill.

It identifies:

- the general policy intent of the Bill and other background policy material;
- some of the key quality assurance products and processes used to develop and test the content of the Bill;
- the presence of certain significant powers or features in the Bill that might be of particular Parliamentary or public interest and warrant an explanation.

This disclosure statement was prepared by the Department of the Prime Minister and Cabinet.

The Department of the Prime Minister and Cabinet certifies that, to the best of its knowledge and understanding, the information provided is complete and accurate at the date of finalisation below.

10 August 2016

Contents

Part One: General Policy Statement

The New Zealand Intelligence and Security Bill implements the Government response to the Report of the First Independent Review of Intelligence and Security in New Zealand: Intelligence and Security in a Free Society (G.24a) (the **Review**).

The Review is the first that has been undertaken pursuant to amendments to the Intelligence and Security Committee Act 1996 that were made in 2013, and it has resulted in wide-ranging recommendations. In particular, the Review recommends that the Government Communications Security Bureau (the **GCSB**) and the New Zealand Security Intelligence Service (the **NZSIS**) and their oversight bodies be covered by a single, comprehensive piece of legislation. It emphasises the need to remove barriers to effective co-operation between the GCSB and the NZSIS and the need to improve transparency and oversight arrangements to give the public greater confidence that the agencies are acting lawfully and appropriately.

The Bill adopts the majority of the Review's recommendations. In developing its response to the Review, the Government has sought to ensure that the new legislation—

- is adaptable to changing circumstances and is technology-neutral; and
- reflects New Zealand's long-standing commitment to human rights, democracy, accountability, and the rule of law; and
- is effective, clear, and easy to understand; and
- promotes a joined-up and efficient New Zealand intelligence community that engages effectively with other domestic agencies, including law enforcement agencies; and
- facilitates effective engagement and co-operation with New Zealand's international security partners.

The Bill replaces the 4 Acts that currently apply to the GCSB, the NZSIS, and their oversight bodies (the Inspector-General of Intelligence and Security and the Intelligence and Security Committee). Having 1 piece of legislation will make the law much easier to understand and access.

The Bill continues existing protections around political neutrality, lawful advocacy, protest, and dissent and it requires the Director-General of an intelligence and security agency to regularly consult the Leader of the Opposition. Its purpose is expressly framed as to "protect New Zealand as a free, open, and democratic society", and a variety of provisions are included to increase transparency around the intelligence and security agencies' activities. For example, some activities carried out by the GCSB and the NZSIS as part of their functions will be acknowledged in legislation for the first time (for example, the use of assumed identities and human intelligence activities).

The Bill will bring the GCSB and the NZSIS more fully within the ambit of normal State sector arrangements. Specifically, it establishes the NZSIS as a public service department under the State Sector Act 1988 and makes the GCSB fully subject to that Act. The Director-General of each agency will be appointed by the State Services Commissioner, and their terms and conditions will be determined within the State Sector Act 1988 framework.

To remove artificial and confusing barriers to co-operation and to make clear the consistency of purpose and links within the New Zealand intelligence community, the Bill contains shared objectives, functions, and powers for the GCSB and the NZSIS. It contains a single authorisation regime applying to both agencies that covers their intelligence collection and protective security functions.

Warrants may authorise the intelligence and security agencies to carry out an otherwise unlawful activity where it contributes to 1 of the 3 shared objectives of the agencies. The proposed activity must be necessary and proportionate to the purpose for which it is sought to be carried out in order for a warrant to be issued. The authorisation regime also provides for the possibility of joint warrants being issued that enable the agencies to conduct joint operations using the specialist capabilities of both agencies, where this is judged to be appropriate.

All warrants require the approval of the Attorney-General. Where a warrant is sought to collect intelligence about a New Zealander, both the Attorney-General and a Commissioner of Intelligence Warrants will need to approve the activity that the authorisation is sought for. All warrants are subject to review and audit by the Inspector-General of Intelligence and Security.

To support the GCSB and the NZSIS to carry out their functions and to ensure clarity and transparency around their access to information, the Bill contains a comprehensive information-sharing regime. It also significantly increases the number of Privacy Act 1993 information privacy principles applying to the GCSB and the NZSIS, which will give individuals an avenue for making complaints in respect of certain actions taken by the GCSB and the NZSIS where none has previously existed.

The Bill also makes a number of significant enhancements to the oversight institutions and their roles. These include the removal of the current restriction on the Inspector-General of Intelligence and Security inquiring into operationally sensitive matters, and clarifying that the Inspector-General may review warrants on substantive, as well as procedural, grounds. The Intelligence and Security Committee will be able to request that the Inspector-General of Intelligence and Security inquire into any matter relating to the intelligence and security agencies' compliance with New Zealand law, including human rights law.

The Bill also continues, for an unlimited time, the provisions put in place by the Countering Terrorist Fighters Legislation Bill in 2014, including the amendments to the Passports Act 1992, which enable the refusal of applications for, or cancellation of, New Zealand travel documents of a person if there are reasonable grounds to believe that the person is a danger to national or international security. This Bill includes an additional protection that requires all such decisions regarding New Zealand travel documents to be subject to review by a Commissioner of Intelligence Warrants.

Part Two: Background Material and Policy Information

Published reviews or evaluations

2.1. Are there any publicly available inquiry, review or evaluation reports that have informed, or are relevant to, the policy to be given effect by this Bill?	**YES**
The title is 'Intelligence and Security in a Free Society: Report of the First independent review of Intelligence and Security in New Zealand'. Authored by Hon Sir Michael Cullen, and Dame Patsy Reddy, and dated: 29 February 2016. Available at : https://www.parliament.nz/en/pb/papers-presented/current-papers/document/51DBHOH_PAP68536_1/report-of-the-first-independent-review-of-intelligence	

Relevant international treaties

2.2. Does this Bill seek to give effect to New Zealand action in relation to an international treaty?	**NO**

Regulatory impact analysis

2.3. Were any regulatory impact statements provided to inform the policy decisions that led to this Bill?	**YES**
Regulatory Impact Statement: Intelligence Services and Oversight Bill, the Department of the Prime Minister and Cabinet, 5 April 2016. Addendum to Regulatory Impact Statement: Intelligence and Security Legislation, the Department of the Prime Minister and Cabinet, 11 August 2016. The regulatory impact statement can be found and downloaded at http://www.treasury.govt.nz/publications/informationreleases/ris.	

2.3.1. If so, did the RIA Team in the Treasury provide an independent opinion on the quality of any of these regulatory impact statements?	**NO**
The RIS identified above did not meet the threshold for receiving an independent opinion on the quality of the RIS from the RIA Team based in the Treasury.	

2.3.2. Are there aspects of the policy to be given effect by this Bill that were not addressed by, or that now vary materially from, the policy options analysed in these regulatory impact statements?	**NO**
The features of the RIS identified above correspond to the key policy features of this Bill with the exception of the definition of 'national security'. The definition in the Bill reflects the recommendation of the independent reviewers, while the proposed definition in the RIS is an alternative formulation proposed by officials and not agreed to.	

Extent of impact analysis available

2.4. Has further impact analysis become available for any aspects of the policy to be given effect by this Bill?	**NO**
A number of the problems faced by the intelligence and security agencies (as well as the issues that these give rise to) are difficult to discuss publicly or to quantify, because of the need to keep operational matters confidential. For this reason it has not been possible to provide significant analysis of the impacts (including of the costs and benefits) of the proposed changes. Instead, officials considered matters such as transparency and building public trust and confidence in the intelligence and security agencies, as keystone objectives in lieu of a fully developed cost/benefit analysis.	

2.5. For the policy to be given effect by this Bill, is there analysis available on:	
(a) the size of the potential costs and benefits?	**NO**
(b) the potential for any group of persons to suffer a substantial unavoidable loss of income or wealth?	**NO**
The policy which this Bill gives effect to is not expected to cause any group of persons to suffer a loss of income or wealth.	

2.6. For the policy to be given effect by this Bill, are the potential costs or benefits likely to be impacted by:	
(a) the level of effective compliance or non-compliance with applicable obligations or standards?	**YES**
(b) the nature and level of regulator effort put into encouraging or securing compliance?	**YES**
The exercise of the intrusive powers will inevitably impact on individual privacy. Compliance with the Bill's provisions is necessary to ensure any individual privacy impacts are mitigated. Effective compliance is supported by increased oversight, accountability and transparency around the use of powers. This is particularly relevant for the structure of the authorisation of intelligence warrants (Part 4 of the Bill) and the involvement of both the Attorney-General and a retired High Court Judge when a New Zealander is targeted. The Bill sets out the responsibilities and powers of oversight bodies. The roles of the Inspector-General of Intelligence and Security and the Intelligence and Security Committee are strengthened by the Bill. Under clause 92 a panel of judicial commissioners will be set up to increase capability to manage the work load (RIS paragraphs 133 – 167). The addendum to the RIS covers the implications of changes to the Privacy Act 1993 by the Bill. Individuals may complain to the Privacy Commissioner if they consider that the intelligence and security agencies (the GCSB or the NZSIS) have interfered with their privacy – noting that this right only applies to actions that engage information privacy principles that apply to the GCSB and the NZSIS. Increased application of the principles gives individuals an avenue of complaint in respect of certain actions taken by the NZSIS and GCSB where none has existed previously. On the changes to the Immigration Act 2009, an infringement and offence regime already operates effectively for carriers providing Advance Passenger Processing information and Passenger Name Records information on passengers planning to arrive in New Zealand. Ministry of Business, Innovation and Employment officials have not identified any reason why it would not operate as effectively when extended to passengers leaving New Zealand.	

Part Three: Testing of Legislative Content

Consistency with New Zealand's international obligations

3.1. What steps have been taken to determine whether the policy to be given effect by this Bill is consistent with New Zealand's international obligations?
The Ministry of Foreign Affairs and Trade and Crown Law were consulted on the development of the policy proposals in order to determine compliance with relevant international obligations.

Consistency with the government's Treaty of Waitangi obligations

3.2. What steps have been taken to determine whether the policy to be given effect by this Bill is consistent with the principles of the Treaty of Waitangi?
No specific steps were taken as it was considered that the provisions do not affect the general principle that New Zealand legislation is to be interpreted consistently with the principles of the Treaty of Waitangi.

Consistency with the New Zealand Bill of Rights Act 1990

3.3. Has advice been provided to the Attorney-General on whether any provisions of this Bill appear to limit any of the rights and freedoms affirmed in the New Zealand Bill of Rights Act 1990?	**YES**
Advice provided to the Attorney-General by the Ministry of Justice, or a section 7 report of the Attorney-General, is generally expected to be available on the Ministry of Justice's website upon introduction of a Bill. Such advice, or reports, will be accessible on the Ministry's website at http://www.justice.govt.nz/policy/constitutional-law-and-human-rights/human-rights/bill-of-rights/	

Offences, penalties and court jurisdictions

3.4. Does this Bill create, amend, or remove:	
(a) offences or penalties (including infringement offences or penalties and civil pecuniary penalty regimes)?	**YES**
(b) the jurisdiction of a court or tribunal (including rights to judicial review or rights of appeal)?	**YES**
(a)The Bill creates a number of offences and penalties. Some are carried over from existing legislation covering the intelligence and security agencies, while others are new. See Appendix one for details of the offences and related penalties. (b)Clause **9(3)** makes the NZSIS a public service department and as a result the Employment Relations Act 2000 will apply to its employees for the first time, bringing NZSIS within the jurisdiction of the Employment Relations Authority and the Employment Court. Clause 227 amends section 349 of the Immigration Act 2009 to extend an infringement and offences regime (currently covering Advance Passenger Processing information and Passenger Name Record information for travellers to New Zealand) to also cover the new clauses inserted by the Bill and passengers leaving New Zealand. Carriers who fail to comply with their obligations to collect Advance Passenger Processing information and Passenger Name Record information and to send that information to the Chief Executive of the Ministry of Business Innovation and Employment may be the subject of criminal charges or infringement fees. Carriers who allow a person to board a craft contrary to a directive or who allow a person to board a craft before the Chief Executive has made a decision will also be subject to criminal charges or infringement fees.	

3.4.1. Was the Ministry of Justice consulted about these provisions?	YES
The Ministry of Justice was consulted on the development of Bill, which included commenting on versions of the Bill and discussion with Ministry of Justice officials.	

Privacy issues

3.5. Does this Bill create, amend or remove any provisions relating to the collection, storage, access to, correction of, use or disclosure of personal information?	YES
The Bill sets up a warranting regime in Part 4 that authorises activity that would otherwise be unlawful—for example, conducting surveillance and intercepting private communications (clause 64). Provisions include tests for ensuring an intelligence warrant is necessary, and an authorisation regime that will impose restrictions on both intelligence and security agencies when they propose exercise of their powers in respect of a New Zealander. The agencies will only be able to take actions for the purpose of collecting intelligence about a New Zealander if they obtain the approval of both the Attorney-General and a Commissioner of Intelligence Warrants (a judicial commissioner). Part 5 of the Bill provides for the intelligence and security agencies to access information held by other agencies. Schedule 2 includes a list of data bases which the agencies are potentially able to access directly, following consultation and agreement between Ministers. For ad hoc information requests clause 101(3) clarifies that restrictions to disclosure from other Acts still apply (e.g. application of the Privacy Act 1993). Clause 112 provides the intelligence and security agencies with access to restricted personal information. But, the access is conditional on permission being granted by the Attorney-General and (if a New Zealander is involved) a Commissioner of Intelligence Warrants. Under clauses 263 and 264 of the Bill further Privacy Act 1993 information privacy principles are applied to the GCSB and NZSIS. It is possible to apply a broader range of principles to the agencies without undermining their ability to protect New Zealand and its interests through inclusion of bespoke exemptions to certain principles to enable performance of their statutory functions. The 'information sharing arrangements' section of the addendum of the RIS covers proposed changes to the Privacy Act. Clause 220 amends the Immigration Act 2009 to require carriers and persons in charge of commercial craft to collect personal information about travellers leaving New Zealand and supply that information to the Chief Executive of the Ministry of Business Innovation and Employment. The information (passport information collected through Advance Passenger Processing and details, such as when and where the travel was booked and how paid for, collected as part of Passenger Name Records) is already collected on people intending to travel to New Zealand. The provisions allow the Chief Executive to share outbound Advance Passenger Processing information (including by way of direct access) with specified agencies for the purposes of law enforcement, counter-terrorism and security (clause 226). There must be an agreement with the specified agency concerned, after consultation with the Privacy Commissioner, before information is shared. Agreements must detail limitations on disclosure of information by the specified agency and the Privacy Commissioner can require reviews and reports. New section 303B specifies the safeguards that must be covered by an agreement which allows direct access (for example, the position of the person in the specified agency who may access the database and data storage and disposal requirements).	

3.5.1. Was the Privacy Commissioner consulted about these provisions?	YES
The Privacy Commissioner, John Edwards, met with the authors of the independent review. Also, as part of seeking Cabinet policy decisions, the Commissioner was consulted by Department of the Prime Minister and Cabinet officials on the relevant policy matters, particularly information sharing proposals (Part 5 of the Bill) and the application of the information privacy principles (Clauses 263 and 264). Staff of the Office of the Privacy Commissioner were consulted on the broad policy underlining the Immigration Act 2009 amendments relating to information on travellers leaving New Zealand (Advance Passenger Processing information and Passenger Name Record information) and provided with a general outline of the approach likely to be adopted for the sharing of outbound Advance Passenger Processing information with specified agencies.	

External consultation

3.6. Has there been any external consultation on the policy to be given effect by this Bill, or on a draft of this Bill?	YES
Consultation on the Government's policy only occurred within Government. However, the independent review referenced above called for, and considered, public submissions.	

Other testing of proposals

3.7. Have the policy details to be given effect by this Bill been otherwise tested or assessed in any way to ensure the Bill's provisions are workable and complete?	YES
The operational agencies were consulted during the development of the policy and the legislation to ensure that the changes can be successfully operationalised.	

Part Four: Significant Legislative Features

Compulsory acquisition of private property

4.1. Does this Bill contain any provisions that could result in the compulsory acquisition of private property?	**NO**
The provisions in the Bill that provide for seizure of private property under an intelligence warrant (for example, an activity under clause 63(d)) does not change or transfer the owner's rights over that property.	

Charges in the nature of a tax

4.2. Does this Bill create or amend a power to impose a fee, levy or charge in the nature of a tax?	**NO**

Retrospective effect

4.3. Does this Bill affect rights, freedoms, or impose obligations, retrospectively?	**NO**

Strict liability or reversal of the usual burden of proof for offences

4.4. Does this Bill:	
(a) create or amend a strict or absolute liability offence?	**YES**
(b) reverse or modify the usual burden of proof for an offence or a civil pecuniary penalty proceeding?	**NO**
Clause 227 amends section 349(1)(b) of the Immigration Act 2009 which currently provides for a strict liability offence for circumstances where the carrier has allowed a person to board a craft for the purpose of travelling to New Zealand without receiving a decision from the Chief Executive as to whether or not that person is allowed to board the craft. The amendment will extend this provision to cover situations where the carrier has allowed a person to board a craft for the purpose of travelling from New Zealand before the Chief Executive has made a decision under new section 97A(1). The amendment of this offence extends its application, and is limited to situations where the person to whom the directive relates is attempting to travel on a passport or certificate of identity that is lost, stolen, invalid, forged, false, fraudulently obtained, or improperly altered, or the passport does not relate to the person who is attempting to travel on it. The offence contributes to the important goal of reducing the use of false travel documents for travel by making sure that a carrier does not allow a person to board a craft before the Chief Executive has confirmed that person may board a craft. The offence is committed by the carrier or person in charge of a commercial craft in a commercial or regulatory environment which involves a high number of individual transactions. Further, it is only committed if the Chief Executive has previously notified the carrier that they must obtain Advance Passenger Processing information from a traveller and provide it to the Chief Executive before the craft departs. Persons involved in the airline industry are already familiar with such obligations and the consequences of non-compliance in respect of inbound travellers. They can, therefore, be expected to have in place suitable procedures and safeguards to ensure compliance. The penalties have not been increased from the current level and contraventions of the new obligation will be punishable by an infringement penalty of $1000 for an owner, charterer or agent, or $500 for a person in charge of the craft. In serious cases of non-compliance a carrier may be prosecuted and face a maximum penalty of 3 months imprisonment or a fine of $50,000 (3 months imprisonment and $25,000 for a person in charge of a craft).	

Civil or criminal immunity

4.5. Does this Bill create or amend a civil or criminal immunity for any person?	**YES**
The Bill creates a number of immunities and/or exceptions. Some are carried over from existing legislation covering the intelligence and security agencies, while others are new. See Appendix two for details of the immunities, exceptions and the limitations.	

Significant decision-making powers

4.6. Does this Bill create or amend a decision-making power to make a determination about a person's rights, obligations, or interests protected or recognised by law, and that could have a significant impact on those rights, obligations, or interests?	**YES**
The Bill creates or amends a number of decision-making powers including, amongst other matters, the authorisation of intelligence warrants. See Appendix two for details.	

Powers to make delegated legislation

4.7. Does this Bill create or amend a power to make delegated legislation that could amend an Act, define the meaning of a term in an Act, or grant an exemption from an Act or delegated legislation?	**YES**
Under clause **109** the Governor-General may by Order in Council, and on the recommendation of the relevant Minister, amend Schedule 2 which lists databases to which direct access by the intelligence and security agencies may be provided. This allows for such matters as databases being reconfigured or the holder agency changing. The listing of the database in Schedule **2** does not, in itself, provide for direct access. The Order in Council process only changes the list of databases for which direct access may be available. Prior to any direct database access under the Bill (Part 5 subpart 2) there must also be an agreement between the relevant Ministers, as described above in question 4.6 (Appendix two). Before recommending an amendment to Schedule 2, the Minister must consult the Intelligence and Security Committee. Clause 229 amends section 402(a) of the Immigration Act 2009 to extend the scope of the regulations that prescribe the information to be obtained on travellers leaving New Zealand. This is a consequential change of including new sections in the Immigration Act. The current regulations are the Immigration (Carriers' Information Obligations) Regulations 2010.	

4.8. Does this Bill create or amend any other powers to make delegated legislation?	**NO**
The Bill creates ministerial policy statements but they are not legislative or disallowable instruments for the purposes of the Legislation Act 2012. As paragraphs 116 - 118 of the RIS explain they are a mechanism to enable the responsible Minister to direct the appropriate conduct of the lawful activities of the intelligence and security agencies.	

Any other unusual provisions or features

4.9. Does this Bill contain any provisions (other than those noted above) that are unusual or call for special comment?	**YES**
Clause 17 gives the intelligence and security agencies the additional function of providing assistance to another entity. The agencies require a specific legislative provision if they are to use their knowledge and capabilities to help organisations such as Maritime New Zealand or the Royal New Zealand Coastguard and assist with search and rescue operations. The assumption is that the searchers would benefit from information obtained from intercepting communications. The function may only be performed where there is an imminent threat to a person's life and safety and the agency could not obtain a warrant for the action in question. Clause 26 provides for the Director-General of an intelligence and security agency to authorise the acquiring, use and maintenance of an assumed identity. Safeguards include the requirement for a ministerial policy statement or statements to be issued addressing such matters as the circumstances in which such authorisations are appropriate. Limitations on the immunities associated with use of an assumed identity are covered in response to question 4.5 (see Appendix two). Clause 63(1)(g) explicitly identifies the use of human intelligence as an activity that may be authorised by an intelligence warrant for the first time in legislation. It is appropriate to transparently identify the use of employees or human sources as a means to collect intelligence. The usual safeguards inherent in the intelligence warranting process will apply.	

Appendix One: Further Information Relating to Part Three

Offences or penalties – question 3.4 (a)

The Bill creates offences and penalties related to unauthorised disclosure of information for persons associated with the New Zealand intelligence community. Maximum penalties are a term of imprisonment not exceeding 2 years or a fine not exceeding $10,000.

- Clause 153 creates offences in relation to publishing information about complaints or inquiries before, or considered by, the Inspector-General of Intelligence and Security.
- Clause 164 covers persons who have been appointed to assist, or appear before, the Intelligence and Security Committee.
- Clause 177 creates an offence for certain people to breach confidentiality requirements in regard to information they had knowledge of as part of their functions and duties. Named position include the Inspector-General, appointed reviewers, Director-Generals of the intelligence and security agencies and their employees.

The clauses generally align with existing offences from Acts repealed by the Bill. The amalgamation of offences means some alterations to penalties. The maximum fine for NZSIS employees increases from $2,000 to $10,000. For GCSB employees the maximum jail term reduces from 3 to 2 years and the fine increases from $5,000 to $10,000. For clause 153 offences the maximum imprisonment term increases from 1 to 2 years.

Clause 183 carries over a current provision and makes it an offence to obstruct, hinder, resist or deceive the Inspector-General with a maximum penalty of $5,000.

Clause 207 creates a new offence in the Crimes Act 1961 of wrongful communication, retention or copying of classified information by someone who has a government security clearance (or someone who receives such information in confidence through an authorised disclosure). The penalty is up to 5 years imprisonment.

Clause 84 rationalises the current offences for failure to destroy information obtained and covers information which is not able to be otherwise retained under the Bill's warrant and authorisation provisions. The maximum fine is $10,000. As a result of the rationalisation for some offences there is an increase in the maximum penalty. Clause 85 makes it an offence for a person carrying out an authorised activity (defined under Part 4 of the Bill) to disclose or use certain information. Clause 86 covers someone disclosing information knowing it came from an authorised activity.

Clause 185 extends the current offence of publicising the identity of NZSIS employees to also include GCSB employees. The maximum fine is $5,000 for an individual and $20,000 for a body corporate.

Clause 184 extends offences regarding impersonating an NZSIS employee to also include GCSB employees with an associated maximum fine and jail term (based on the Policing Act 2008 section 72 – $15,000 fine and/or 12 months imprisonment).

Clause 253 amends the Passports Act 1992. Clauses from Schedule 2 are moved into the body of the Act with no sunset clause. The sections relate to Ministerial decisions to refuse to issue, cancel or retain travel documents (new section 27GA). The Schedule 2 provisions were temporary provisions added by the *Countering Terrorist Fighters Legislation Bill*. They expire 31 March 2017. The Bill provides for a new review process. Under new section 27GF the Chief Commissioner of Intelligence Warrants is notified of any decision to issue, cancel or retain travel documents under 27GA.(Also refer paragraphs 238 -246 in the RIS.)

Appendix Two: Further Information Relating to Part Four

Civil or criminal immunities- question 4.5

Clause 33 provides immunity for a person who assists in the establishment and maintenance of an assumed identity taken by an employee of an intelligence and security agency.

Clause 34 provides civil and criminal immunity for an action done (or omitted to be done) by the person who is authorised to have the assumed identity.

Clause 26(3) allows an intelligence and security agency to make a false document (as defined by the Crimes Act 1961 section 255) to support an assumed identify. The production and use of such documents is included within the immunities provided by clauses 33 and 34. The power to produce false documents is limited to those that are not ordinarily issued or given by a Minister or government agency.

These immunities are necessary to enable the intelligence and security agencies to carry out their activities covertly, including protecting the identity of employees and others authorised by the agencies to carry out activities.

These are also limited. They do not apply if the action is not done in good faith and with reasonable care. Also, the immunity of employees and other authorised persons does not cover breaches of contractual arrangements that are not a necessary part of maintaining the assumed identity. Nor does it allow for something to be done that the authorised person is not qualified to do (for example, fly a plane without a licence).

Equivalent clauses, with appropriate amendments, provide civil or criminal immunities related to the establishment, maintenance and use of a corporate identity by intelligence and security agencies (clauses 44 and 45).

The Bill puts in place comprehensive immunities for the intelligence and security agencies and their employees with some amendments. There is immunity from criminal liability for acts done in good faith (as long as specified conditions are met)—when obtaining an intelligence warrant (clause 87) and assisting the Police and NZ Defence Force (clause 16(4)). Clause 88 provides a general immunity in relation to the carrying out of authorised activity (ie activities authorised by a warrant) with the conditions being the act was necessary and done in a reasonable manner.

Clause 68(4) provides immunity for someone (the police, any individual or other organisation) who assists an intelligence and security organisation in giving effect to an intelligence warrant. The immunity is the same as that available to an employee of an agency in relation to the execution of a warrant.

An employee or entity wishing to rely on an immunity must establish on the balance of probabilities that the immunity applies.

An exception with conditions, rather than an immunity, is provided for employees in regard to specific offences that may be committed in the course of performing an investigation. This includes a new exception for breaches of certain Road User Rules (clause 189) while conducting visual surveillance from a vehicle on a public road. A second exception relates to section 246 of the Crimes Act 1961 for receiving unsolicited information in circumstances that would otherwise constitute the offence of receiving stolen property– clause 188.

The immunities and exceptions in the Bill do not prevent the Crown being held directly liable for breaches of the New Zealand Bill of Rights Act 1990 by public officials.

Decision-making powers - question 4.6

Clauses 55 and 56 set out the decision-making power to authorise an intelligence warrant – authorisation to carry out an unlawful activity. Changes are proposed to the existing legislative powers.

- An intelligence warrant can be a purpose-based warrant, for specific operational purposes (clause 64). The approach taken by the Bill means that the GCSB and NZSIS will not always need to identify the particular details of an intelligence target. A safeguard against misuse of a purpose-based warrant is the need to demonstrate why the result could not be reasonably achieved through a warrant against an identified person, place or thing.
- The Bill removes the current prohibition on the GCSB targeting New Zealanders when performing its foreign intelligence function.
- Any intelligence warrant targeting New Zealanders would be restricted. It would need to be on the grounds of national security (rather than on broader grounds of international relations and wellbeing). Alternatively, the grounds could be that the New Zealander was an agent of a foreign power (working for a foreign state or organisation). This restriction applies to both agencies. There is currently no restriction for the NZSIS.

The decision-making power to authorise an intelligence warrant is given solely to the Attorney-General when there is no New Zealander targeted (a Type 2 warrant). The decision to authorise an intelligence warrant must be joint, with a Commissioner of Intelligence Warrants, when a New Zealander is targeted (Type 1). The Bill sets out criteria (clause 57 in particular) that must be met before any intelligence warrant can be authorised.

In special cases of a 'situation of urgency' a streamlined process under clause 69 can be used. But, an imminent threat to life and safety, or a material implication for New Zealand's national security, must be involved.

Clause 77 gives the Directors-General of the intelligence and security agencies the power to authorise an activity for which an intelligence warrant is required, on two conditions: firstly that a delay in applying for an intelligence warrant would defeat the purpose of obtaining the warrant and secondly it is a 'situation of urgency'. In this situation an intelligence warrant must still be applied for within 24 hours. If that warrant is not authorised all information collected under the clause 77 authorisation would need to be destroyed as soon as practicable.

Clauses 102 -109 give the relevant Ministers the power to grant the intelligence and security agencies direct access to certain databases (for an example, births, deaths and marriages). The Ministers (including the Minister with responsibility for the database) must be satisfied that direct access is 'necessary'; privacy of individuals is adequately protected and appropriate procedures for access will be put in place. There must also be consultation with the Privacy Commissioner and the Inspector-General of Intelligence and Security.

The functions of the Inspector-General of Intelligence and Security also include conducting reviews of the compliance systems of each intelligence and security agency relating to information management, and conducting unscheduled audits of such compliance systems.

Clause 221 introduces a new power to direct that a person not be permitted to board a craft to leave New Zealand (new section s97A of the Immigration Act 2009). The decision-making power is given to the Chief Executive of the Ministry of Business Innovation and Employment and he or she must have reason to believe a person is attempting to travel on a passport or certificate of identity that is lost, stolen, invalid, forged, fraudulently obtained or improperly altered. The power can also apply if the passport or certificate of identity does not relate to the person who is attempting to travel on it.