Office of the Minister for National Security and Intelligence
Office of the Minister Responsible for the GCSB
Office of the Minister in Charge of the NZSIS

Chair, Cabinet National Security Committee

Intelligence and Security in a Free Society: Report of the first Independent Review of Intelligence and Security in New Zealand

Paper Seven: Generic legislative issues and consequential amendments

Proposal

1. Cabinet is asked to make decisions on generic legislative issues necessary for the drafting of the Intelligence Services and Oversight Bill, including offences and transitional arrangements. The paper also addresses a number of consequential amendments that fall out of the package, including amendments to the protected disclosure regime, the advanced passenger processing provisions in the Immigration Act 2009, and the provisions enacted in 2014 to counter foreign terrorist fighters.

Executive summary

2. The paper proposes:

   2.1 Continuation of the legislative provisions put in place by the Countering Terrorist Fighters Legislation Bill in 2014;

   2.2 Amendments to the Immigration Act, including to provide for the mandatory collection of and systematic access to, outbound advance passenger processing information.

   2.3 A comprehensive and coherent set of offences to apply to security and intelligence information, including rationalisation of the existing offences in the New Zealand Security Intelligence Act 1969, the Government Communications Security Bureau Act 2003, the Inspector-General of Intelligence and Security Act 1996 and the Intelligence and Security Committee Act 1996;

   2.4 Amendments to the protected disclosure regime to ensure a clear and accessible pathway for would-be whistle blowers who work with security and intelligence agencies and/or handle classified information;

   2.5 Commencement and transitional provisions.

Background

3. The Countering Terrorist Fighters Legislation Bill was introduced and passed in late 2014 to respond to the threat posed by foreign terrorist fighters and in recognition of the United Nations Security Council's resolution urging states to restrict the movement of such people, amongst other things. The Bill was progressed urgently to ensure an

adequate response to the threat was in place in advance of the review of legislative settings that was anticipated would occur with the independent review of intelligence and security legislation in 2015. Some of the provisions were enacted with a sunset clause and are due to expire on 31 March 2017.

4. The Immigration Act requires carriers travelling to New Zealand to provide certain information on all passengers and crew to allow for advance passenger processing. The particular information is specified in regulations and includes personal information contained in the person's passport. Carriers must provide information about inbound passengers if directed to do so by the chief executive. The system does collect information about outbound passengers to the extent that that is required by destination countries for their inbound processing and because outbound advanced passenger processing is required to make SmartGate work in New Zealand. It is, however, not mandatory for carriers to provide outbound advanced passenger processing information and nor is Immigration New Zealand authorised to access outbound information.

5. The New Zealand Security Intelligence Service Act, the Government Communications Security Bureau Act, the Inspector-General of Intelligence and Security Act and the Intelligence and Security Committee Act all contain offences relating to the protection of sensitive information and/or proceedings. These are cast in different terms and have varying penalty levels. There are also offences in the general law that are intended to protect information that has implications for national security.

6. The Protected Disclosures Act 2000 contains a specific process for employees of the NZSIS and the GCSB to follow when making a protected disclosure that takes account of the fact that any disclosure is likely to have implications for national security.

Provisions put in place by the Countering Terrorist Fighters Legislation Bill

7. The Countering Terrorist Fighters Legislation Bill amended the Customs and Excise Act 1996, the New Zealand Security Intelligence Service Act and the Passports Act 1992. The provisions of the Bill were aimed at two objectives: monitoring and investigating foreign terrorist fighters, and restricting and disrupting the travel of such people.

Investigating foreign terrorist fighters

8. The amendments to the New Zealand Security Intelligence Service Act enabled the NZSIS to obtain visual surveillance warrants and to undertake warrantless surveillance (authorised by the Director of Security) for a period of up to 24 hours in situations of urgency or emergency. These powers made surveillance possible where it was necessary for the detection, investigation or prevention of an actual, potential or suspected terrorist act. The provisions put in place by the Bill were effectively a separate regime from the other warranted powers under that Act.

9. The Customs and Excise Act was also amended to enable Customs to provide direct access to Customs' information to the NZSIS and the Police for counter-terrorism purposes.

10. The reviewers concluded that there was a basis for continuing the NZSIS's ability to conduct visual surveillance. As a matter of principle, the reviewers did not see any reason to treat visual surveillance differently from other surveillance methods

authorised under the New Zealand Security Intelligence Service Act. They considered that the separate regime for visual surveillance was largely a product of the "targeted, temporary nature" of the Countering Terrorist Fighters Legislation Bill and the fact that it was passed under urgency.

11. The reviewers accept that visual surveillance could assist the agencies to perform their intelligence functions in other contexts and note that a visual surveillance device is treated the same as other types of surveillance devices under the Search and Surveillance Act 2012. They recommend that visual surveillance should be subject to the new authorisation regime they propose.

12. For this reason, visual surveillance was included in the warranting regime we recommended in Cabinet paper two of this suite of papers. In that paper, we also recommended the adoption of the reviewers' recommendations for an urgent authorisation regime that applies to all of the powers able to be authorised under warrant [NSC-16-MIN-0008 refers].

13. The agencies' ability to access information held by other government agencies, including Customs, is dealt with in Cabinet paper six of this suite of papers.

Disruption of travel

14. The Countering Terrorist Fighters Legislation Bill also amended the Passports Act to allow the Minister of Internal Affairs to cancel or refuse to issue a travel document for up to three years (the previous maximum period was 12 months). This was to ensure that there was a sufficiently long period to account for the fact that travel and attack planning may extend over a period beyond 12 months.

15. The amendments also introduced a 10 working day temporary suspension period to prevent a person from travelling. As the reviewers noted this addressed an obvious gap in the law which meant that, if a suspected foreign terrorist fighter was seeking to travel and the NZSIS did not become aware until shortly before the person's departure, there was no ability to keep the person in New Zealand while the cancellation of their passport was processed.

16. The reviewers have recommended that the current maximum cancellation period of three years, and the ability to suspend for 10 working days while the process of cancellation is progressed, should both be retained.

17. In response to public submissions that decisions to cancel or to refuse to issue travel documents on national security grounds should be judicially reviewed, the reviewers have recommended:

    17.1 Any decision by the Minister of Internal Affairs to cancel or refuse to issue a travel document on security grounds should be referred to the Chief Commissioner of Intelligence Warrants; and

    17.2 A judicial commissioner should review the decision and have the ability to overturn if one of the grounds for judicial review is made out.

18. The reviewers note that the cancellation of, or refusal to issue, a travel document impinges on a person's right to leave New Zealand and can have a significant impact on the individual concerned. In addition, we note that it impacts on the person's right to

freedom of movement, which is protected under section 18 of the New Zealand Bill of Rights Act 1990. Section 18 reflects article 12 of the International Covenant on Civil and Political Rights, which recognises a person's right to leave a country and also to enter his or her own country. For this reason, we think that ensuring a readily accessible review mechanism is necessary.

19. We agree with the reviewers' recommendations and recommend that the provisions put in place by the Passports Amendment Act 2014 (which came out of the Countering Terrorist Fighters Legislation Bill) be continued with the recommended role for judicial commissioners discussed in the preceding paragraph. However, we do not accept one aspect of the reviewers' recommendation, namely that a commissioner should be able to "overturn" the Minister's decision. If the review decision is to proceed on judicial review grounds, commissioners should be able to refer a decision back to the Minister to reconsider, but will not be able to substitute their own decision (as is the case with judicial review).

Proposed requirements for outbound passengers, including advance passenger processing

20. In addition to the provisions put in place by the Countering Terrorist Fighters Legislation Bill, we propose a small number of amendments to the Immigration Act 2009 to provide for the mandatory collection of and systematic access to, outbound advance passenger processing information.

21. These proposals were not the subject of recommendations from the reviewers but we consider that the following proposals will complement existing measures to manage foreign fighters and other people posing a security threat. It would also allow for better management of the risks posed by other high risk travellers, including criminals sought for arrest, prisoners who have escaped or are on parole, travellers posing a risk to the safety of passengers, crew, or craft, and potential perpetrators or victims of people trafficking.

22. We note that Australia amended its legislation in 2014 to extend advance passenger processing requirements to departing air and maritime travellers as part of a suite of amendments in the Counter-Terrorism Legislation Amendment (Foreign Fighters) Act 2014 (Aus).

23. Specifically, we propose amendments to the Immigration Act in relation to advanced passenger processing for outbound travellers that:

    23.1 Allow for both the collection of information and for boarding directives;

    23.2 Are mandatory and apply an infringement and offence regime (in the same way as it does for inbound advance passenger processing information) so that the provision of information is assured and boarding directives are followed;

    23.3 Allow Immigration New Zealand to share outbound advance passenger processing information with Police, Customs, the Department of Corrections and the Aviation Security Service, or allow them direct access to the information (the ability of NZSIS to have direct access to Immigration New Zealand datasets is discussed in Cabinet paper six of this suite of papers).

24. A passenger name record is a record in an airlines' computer reservation system that contains a range of information including the itinerary for a passenger, ticket information, contact details and means of payment. In New Zealand, use of passenger name record data complements advance passenger processing as it is used to screen for risky travellers. Advance passenger processing is only used by seven countries whereas passenger name record is universally available. Accordingly, we also propose that the Immigration Act be amended in relation to passenger name record information for outbound travellers to:

    24.1 Provide clear legislative authority for Immigration New Zealand to use passenger name record information for outbound travellers, as is the case for inbound travellers;

    24.2 Make the provision of passenger name record information on outbound travellers mandatory and include an infringement offence regime, as is the case for inbound travellers.

25. The Immigration Act should also be amended to grant Immigration New Zealand an express power to direct a carrier not to carry a person out of New Zealand on a lost, stolen, invalidated or fraudulent travel document.

Protection of intelligence and security information – a comprehensive set of offences and ensuring the most appropriate authority for purpose of protected disclosures involving national security information

Objectives

26. Preventing unauthorised disclosure of information with national security implications is important as unauthorised use or disclosure could have serious ramifications for New Zealand's national security and undermine New Zealand's reputation as an intelligence partner with the capabilities to protect classified information.

27. Replacing the current four Acts with a single piece of legislation necessitates consolidation and rationalisation of the existing offences in those Acts. It also presents an opportunity to simplify and strengthen the law around unauthorised use or disclosure of classified information. There are some gaps in the current law and some of the penalties applying to the current offences are out of date and no longer provide a realistic deterrent. Accordingly, we recommend the inclusion of a coherent and comprehensive set of offences relating to the protection of security and intelligence information in the Intelligence Services and Oversight Bill. The proposed offences should be consistent and have parity with similar and related offences across the statute book (e.g. Search and Surveillance Act).

28. We think that it is important to ensure that, alongside a comprehensive regime to protect classified information with enhanced penalties, there is a clear and accessible pathway to disclosure for those wishing to bring issues of concern forward for investigation. Accordingly, we recommend amendment of the Protected Disclosures Act so that protected disclosures pathway provided for employees outside of the security and intelligence agencies mirrors that of the agencies' employees where the disclosure involves classified information or relates to the work of the agencies.

Offences in current legislation

29. The reviewers propose carrying over and amalgamating offences in the existing four Acts in their proposed single new Act. All four of the current Acts have offences relating to unauthorised disclosure or use of information, although these are formulated differently and have different penalty levels applying.

30. The New Zealand Security Intelligence and Service Act and the Government Communication Security Bureau Act also contain offences relating to information obtained under warranted powers. These parallel offences contained elsewhere on the statute book which recognise the particular sensitivity relating to information obtained pursuant to intrusive State powers.

31. Additionally, the New Zealand Security Intelligence Service Act contains offences intended to protect the identity of employees and officers, and prohibiting personation of an officer or employee of the Service. The Inspector-General of Intelligence and Security Act makes obstructing, hindering or resisting the Inspector-General or anyone exercising powers under that Act an offence. Unauthorised publication of complaints, inquiries and decisions under the Inspector-General's legislation is also an offence.

32. The Crimes Act 1961 provides a graduated scale of offences "against the Sovereign and the State" with treason as the most serious and also including espionage and wrongful communication, retention, or copying of official information. These latter two offences are particularly relevant to any unauthorised use or disclosure occurring in relation to classified information. There is also a lower level offence in the Summary Offences Act 1981 relating to unauthorised disclosure of certain official information. The Armed Forces Discipline Act 1971 also makes unauthorised disclosure of information an offence in relation for members of the Armed Forces covered by the Act.

33. Given the overlap between the offences relating to unauthorised disclosure of information and offences in the Crimes Act and the Summary Offences Act, we have considered whether any changes to the general law are also necessary to ensure a coherent and comprehensive set of offences relating to the protection of security and intelligence information.

Offences relating to the protection of information

34. There are currently three categories of offences relating to the protection of information:

    34.1 Offences relating to the disclosure of information obtained in the course of employment, work with or assisting, or appearing before the agencies or the Inspector-General or the Intelligence and Security Committee (section 12A(1) New Zealand Security Intelligence Service Act; section 11 Government Communications Security Bureau Act; sections 28 and 29 Inspector-General of Intelligence and Security Act; section 20 Intelligence and Security Committee Act);

    34.2 Offences relating to information obtained through exercise of intrusive powers (section 23 Government Communications Security Bureau Act; sections 4G, 4IB, 4IE, 12A(2) and (3) New Zealand Security Intelligence Service Act); and

34.3 Offences relating to espionage and official information (sections 78 and 78A Crimes Act respectively; section 20A Summary Offences Act and section 25 Armed Forces Discipline Act in relation to the latter).

35. We propose that the offences in the current intelligence and security Acts which relate to unauthorised disclosure and use of information will be carried over and rationalised. These provisions:

35.1 Ensure that the secrecy of the work of the agencies is protected and are aimed at employees and former employees; and

35.2 Protect the proceedings of the Inspector-General and the Intelligence and Security Committee and apply to a range of people who participate or assist with those proceedings.

36. Most of the offences relating to information obtained through the exercise of intrusive powers should also be carried over and rationalised. These offences, like the offence in section 179 of the Search and Surveillance Act 2012 (disclosure of information obtained through search or surveillance), recognise the particular sensitivity of information obtained through intrusive powers. In particular, we are recommending that the Bill contain the following offences in relation to information obtained pursuant to a tier 1 or tier 2 warrant:

36.1 Disclosure of information obtained pursuant to a warrant or disclosure of the existence of the warrant by a person who is authorised by the warrant or requested to give assistance in giving effect to the warrant, other than as authorised by the warrant or in accordance with a Ministerial authorisation;

36.2 Disclosure of information obtained pursuant to a warrant by any person who acquires knowledge of that information, knowing it have been obtained pursuant to a warrant, other than as authorised by the warrant or in accordance with a Ministerial authorisation;

36.3 Failure by a person who is authorised by the warrant to destroy irrelevant information obtained pursuant to the warrant, with "irrelevant information" meaning information that is not directly or indirectly relevant to the protection or advancement of one of the objectives of the agencies or otherwise able to be retained under the rules relating to incidentally obtained intelligence (see Cabinet paper 5B of this suite of papers);

36.4 Failure by a person who is authorised by an interim authorisation or an urgent Director authorisation (NSC-16-MIN-0008, paragraphs 42 and 44 refer) to destroy information obtained pursuant to that authority when no warrant is issued in relation to the same matter, except to the extent that information is able to be retained under the rules relating to incidentally obtained intelligence.

37. The exception is section 4IB of the New Zealand Security Intelligence Service Act. That provision was inserted in 2014 by the Countering Foreign Terrorist Fighters Legislation Bill and forms part of a specific regime providing for visual surveillance by the NZSIS. The reviewers have recommended that the power to carry out visual surveillance should be retained (discussed above in this paper) and saw no reason why it should continue to be treated separately from other intrusive powers exercised by the NZSIS.

Accordingly, they recommended that it ought to be dealt with under the same strengthened authorisation regime recommended more generally (dealt with in Cabinet paper two of this suite of papers). In light of the range of offences applying in relation to information obtained pursuant to a warrant, we do not see any particular need for a specific protection relating to visual surveillance.

38. In recognition of the fact that classified information is generated and held across Government (and sometimes in the private sector) and relates to matters beyond just the work of the intelligence and security agencies, we propose that a new offence applying to persons owing a specific obligation of confidence in relation to classified information be introduced in the Crimes Act. There is a gap in the suite of offences currently available. At the high end, espionage is available where there is specific intent to prejudice the security or defence of New Zealand and provide information or the like to a foreign country or organisation. There is an offence relating to wrongful communication, retention, or copying of official information, where the acts committed are likely to prejudice the security or defence of New Zealand. There is nothing, however, that is aimed simply at the protection of classified information by those who are entrusted with access to it.

39. Our proposed new offence would be based on the offence of wrongful communication, retention, or copying of official information in section 78A, with appropriate means rea (mental) elements. However, it would only apply to those persons who owe a specific obligation of confidence in relation to classified information, either because they hold a security clearance that entitles them to have access to and requires them to protect that information, or because the classified information has been provided to them on an in-confidence basis and in full knowledge of its classified nature.

40. We consider that "classified information" should be defined to mean information that is marked with a national security classification of "confidential" or higher, or which the person knows to be classified at such a level. In order to meet New Zealand's international obligations, classified information for this purpose should also cover information that has been classified by foreign partners at an equivalent level.

41. Given the potential harm associated with the wrongful communication, retention, or copying of classified security intelligence information, it is proposed that this offence will carry a maximum penalty of 5 years imprisonment (as opposed to the maximum penalty of 3 years imprisonment that applies to section 78A). As with section 78A and a charge of espionage pursuant to section 78, a prosecution under this new offence will require the consent of the Attorney-General.

42. We also propose that the warrantless search power in section 25 of the Search and Surveillance Act should also be amended so that it may be exercised to obtain evidence of the new proposed offence in relation to classified information. We believe that this power is justified given the information that is involved, which by its nature has potential impacts for national security and the ease with which some information can be removed from authorised areas and concealed or passed to third parties. Once such a disclosure has been made, the damage has effectively been done.

Offences to protect the identity of employees of the agencies

43. It is currently an offence to publish or broadcast the identity of a NZSIS employee other than the Director of Security (section 13A New Zealand Security Intelligence Service

Act). The reviewers noted the reasons for keeping the identity of employees' secret, namely carrying out of secret operations and preventing danger to sources.

44. We propose carrying over this offence and applying it to the GCSB.

Personation of an employee of the agencies

45. The offence of personation as an employee of NZSIS (section 13) will also be retained. While it is proposed that this offence will be extended to include personation as an employee of GCSB, the drafting should be updated, with the equivalent offence in the Policing Act 2008 providing a possible model.

Failure to comply with power of inquiry under Inspector-General of Intelligence and Security Act

46. The offence in section 23(8) of the Inspector-General of Intelligence and Security Act that relates to the exercise of powers under the Act by the Inspector-General or another person covers actions such as obstruction, non-compliance with a lawful requirement and making a false statement. This offence should be retained and carried over to the new legislation.

Summary of proposed offences and proposed penalties

47. The penalties proposed in relation to our recommended offences are set out in the following table together with the current offences that relate to security and intelligence information:

Offence	**Offence will apply to**	**Proposed change**	**Penalty**
Espionage (section 78 Crimes Act)	Everyone "who owes allegiance to the Sovereign"	No change	Maximum 14 years imprisonment
Wrongful communication, retention, or copying of official information (section 78A Crimes Act)	Everyone "who owes allegiance to the Sovereign"	No change	Maximum 3 years imprisonment
Wrongful communication, retention, or copying of classified information (new)	Persons owing a specific obligation of confidence in relation to classified information	Based on section 78A but applying to classified information. It will attract a higher penalty and engage a warrantless search power.	Maximum 5 years imprisonment
Unauthorised disclosure of certain official information (section 20A Summary Offences Act)	Everyone	No change	Maximum 3 months imprisonment/ $2,000 fine

Offence	Offence will apply to	Proposed change	Penalty
Unauthorised disclosure of information (section 25 Armed Forces Discipline Act 1971)	Members of armed forces	No change	Maximum 2 years imprisonment
Unauthorised disclosure of information by employees/former employees of agencies (section 12A(1) New Zealand Security Intelligence Service Act; section 11 Government Communications Security Bureau Act)	NZSIS and GCSB employees and former employees	Rationalisation into a single offence.	Maximum 2 years imprisonment/ $10,000 fine
Protection of IGIS and ISC proceedings (including unauthorised disclosure/breach of secrecy/unauthorised publication as covered in section 28 and 29 of the Inspector-General of Intelligence and Security Act and section 19 of the Intelligence and Security Committee Act)	Everyone	Retain and carry over	Maximum 2 years imprisonment/ $10,000 fine
Failure to destroy irrelevant information obtained pursuant to warrant / failure to destroy information obtained pursuant to urgent authorisation where no warrant is issued (sections 4G, 4IB,4IE, 12A(2) and (3) New Zealand Security Intelligence Service Act; section 23 Government Communications Service Bureau Act)	NZSIS and GCSB employees authorised by warrant or urgent authorisation	Rationalisation	Maximum $10,000 fine
Personation (section 13 New Zealand Security Intelligence Service Act)	Everyone	Extend offence to GCSB and limit to circumstances where conduct	Maximum 12 months imprisonment/ $15,000 fine

Offence	Offence will apply to	Proposed change	Penalty
		likely to lead a person to believe the person is an employee	
Publication/broadcast of identity of employees (section 13A New Zealand Security Intelligence Service Act)	Everyone	Extend to GCSB	Maximum $20,000 fine (body corporate)/ $5,000 fine (individual)
Failure to comply with IGIS in relation to power of inquiry (section 23(8) Inspector-General of Intelligence and Security)	Everyone	Retain and carry over	Maximum $5,000 fine

48. The offences will contain appropriate mens rea (mental) elements.

Protected disclosures

49. The reviewers noted the importance of the Protected Disclosures Act, which allows employees of the agencies to report any serious wrongdoing to the Inspector-General of Intelligence and Security. They considered that the Inspector-General is the appropriate authority because of the highly secret nature of the work and the Inspector-General's wide powers of inquiry into the agencies' activities.

50. However, there is one aspect of the protected disclosures regime as it relates to classified matters and the work of the agencies, that was not considered by the reviewers but which we think could benefit from amendment. Specifically, staff from other agencies (such as the Ministry of Foreign Affairs and Trade, Immigration New Zealand or the Department of Internal Affairs) may also be in the position of needing to make a protected disclosure in respect of classified information and/or the work of the agencies.

51. Under the Protected Disclosures Act at present, New Zealand Defence Force, Ministry of Defence, Ministry of Foreign Affairs and Trade, and Department of the Prime Minister and Cabinet staff are required to complain to the Ombudsman if the disclosure relates to the "the international relations of the Government of New Zealand or intelligence and security matters".

52. There are a number of employees in these four organisations who hold top level security clearances and who routinely work with the intelligence and security agencies and/or highly classified information. We consider that the issues arising from protected disclosures by these classes of employees are largely the same as those of employees of the agencies. Further, the Inspector-General is a better fit for the "appropriate authority" role under the Protected Disclosures Act where any classified material or the work of the intelligence and security agencies is involved. We see no reason to limit this to the four organisations currently listed in section 13 – it should apply equally to all

employees who are in the position of wanting to make a protected disclosure in relation to classified information or the work of the agencies.

53. Accordingly, we consider that section 13 should be amended so that the protected disclosures pathway for any employee in relation to classified matters and/or work with the agencies mirrors what is provided for in relation to the two intelligence and security agencies.

54. The reviewers also recommended that the legislation should be amended to make clear that the relevant provisions of the Protected Disclosures Act apply in the event of a protected disclosure by an employee. We consider that this is apparent on the face of the Protected Disclosures Act, particularly in view of section 12. However, current section 18 of the Inspector-General of Intelligence and Security Act has the potential to cause confusion about its relationship with the Protected Disclosures Act. That provision states that where an employee of the GCSB or the NZSIS brings any matter to the attention of the IGIS, that employee should not be subjected by the agency to any penalty or discriminatory treatment unless the IGIS determines that the employee has acted otherwise than in good faith.

55. We consider that this provision is intended to provide a broader protection for employees of the agencies who have cause to make a disclosure to the IGIS, no matter the nature or circumstances of that disclosure. For example, this provision would mean that an employee who is required to provide evidence about a matter that is the subject of an inquiry by the IGIS cannot be subject to disciplinary action by their employer by reason of having given that evidence in good faith. It also applies to disclosures that would not be protected under the Protected Disclosures Act. We think that is appropriate. Officials should, however, work with Parliamentary Counsel to ensure that the drafting of this provision in the new legislation sits comfortably with the Protected Disclosures Act.

Commencement and transitional provisions

56. Cabinet paper one in this suite of papers proposed that the majority of the new legislation would come into force on 1 December 2017 [NSC-16-SUB-0007]. However, after further work by officials around the implementation issues, we now propose the following arrangements for commencement:

    56.1 The provisions of the Bill that will continue the amendments to the Passports Act put in place by the Countering Terrorist Fighters Legislation Bill will commence the day after the Bill receives Royal assent;

    56.2 Certain provisions giving the agencies access to datasets held by other government agencies (described in more detail in Cabinet paper six) will commence the day after the Bill receives Royal assent; and

    56.3 The remainder of the Bill come into force six months after the Bill receives Royal assent.

57. It will be necessary to include transitional provisions in the Bill that deal with the effect of the following:

    57.1 Warrants and authorisations under both the New Zealand Security Intelligence Service Act and the Government Communications Security

Bureau Act should be "grandfathered" consistent with the approach that was taken in the Search and Surveillance Act 2012. That Act provided that applications made prior to commencement but not determined were to be determined under and governed by the old provisions and warrants that were in force at the date of commencement were to continue in force with the old provisions applying to them. We note that this will enable the existing warrants and authorisations to be transitioned to the new legislative regime in a progressive fashion rather than requiring them all to be renewed in a short period, which would put pressure on the agencies and on the relevant Ministers and the judicial commissioners.

57.2 Cancellations and refusals to issue travel documents made under the temporary provisions in the Schedule to the Passports Amendment Act 2014 should be treated as if they had been made under the re-enacted provisions in the new Act so that timeframes are unaffected by the transition to the new provisions.

57.3 The Directors of the agencies at the time the legislation commences will continue in office, subject to the following conditions on the incumbents:

57.3.1 Acceptance of an offer of appointment and agreement of new employment arrangements with the State Services Commissioner;

57.3.2 Having a term expiry date that is after the date of enactment of the legislation; and

57.3.3 Not resigning or having been removed from office.

57.4 In addition to the conditions in the preceding paragraph being met, it will also be necessary to override the following provisions of the State Sector Act 1988 in these limited circumstances:

57.4.1 Section 35, which provides for appointment of chief executives, to make clear that the State Services Commissioner will not be required to commence a new appointment process;

57.4.2 Section 40(1A), providing for appointment of an acting chief executive when a new department is established (in relation to the NZSIS only).

57.5 The transitional provisions dealing with the position of the incumbent Directors should also make clear that, in the event of either Director not accepting the position offered or an employment agreement not being reached, no compensation will be available to them for loss of office (which aligns with the Directors' current terms of appointment).

57.6 The appointments of the Inspector-General of Intelligence and Security and the Deputy Inspector-General of Intelligence and Security should be treated as if they were made under the new Act meaning that the terms of both appointments continue as originally intended at the time of appointment.

57.7 The ability of the responsible Minister or the Prime Minister to agree to the findings of the Inspector-General of Intelligence and Security being referred

to the Intelligence and Security Committee (NSC-16-MIN-0009, paragraph 13 refers) should apply to any own-motion inquiry or an inquiry requested by one of those Ministers, regardless of whether the inquiry commenced prior to the commencement of the new Act.

Ongoing review mechanism

58. Finally, we recommend that the requirement for periodic reviews of the agencies, their legislation and their oversight legislation that was inserted into the Intelligence and Security Committee Act in 2013 should be retained. As noted in Cabinet paper one of this suite of papers, the threat environment has been fluid and there has been considerable legislative change in comparable jurisdictions in recent years [NSC-16-SUB-0007 refers]. We expect that this will continue to be the case in coming years.

Recommendations

The Minister for National Security and Intelligence and the Minister Responsible for the GCSB and in Charge of the NZSIS recommend that the National Security Committee:

Countering foreign terrorist fighters

1. **note** that the Countering Terrorist Fighters Legislation Bill amended the Customs and Excise Act 1996, the New Zealand Security Intelligence Service Act 1969 and the Passports Act 1992;

2. **note** that the Countering Terrorist Fighters Legislation Bill had the objectives of monitoring and investigating foreign terrorist fighters and restricting and disrupting the travel of such people;

3. **note** that the amendments to the New Zealand Security Intelligence Service Act enabled the NZSIS to obtain visual surveillance device warrants and to undertake warrantless surveillance for a period of up to 24 hours in situations of urgency or emergency;

4. **note** that the reviewers recommended that:

    4.1 visual surveillance be dealt with under the new authorisation regime they have recommended; and

    4.2 an urgent authorisation regime be included in the proposed legislation that applies to all of the powers able to be authorised under warrant;

5. **note** that the recommendations referred to in paragraph 4 above were both addressed by the Committee at its April 2016 meeting [NSC-16-MIN-0008 refers];

6. **note** that the Customs and Excise Act was amended by the Countering Terrorist Fighters Legislation Bill to enable Customs to provide direct access to Customs' information to the Police and the NZSIS for counter-terrorism purposes;

7. **note** that the agencies' ability to access information held by other government agencies, including Customs, is dealt with in Cabinet paper six of this suite of papers;

8. **note** that the amendments to the Passports Act made by the Countering Terrorist Fighters Legislation Bill;

8.1 allowed the Minister of Internal Affairs to cancel or refuse to issue a travel document for up to three years;

8.2 introduced a 10 working day temporary suspension period to prevent a person from travelling while cancellation of the person's passport is processed;

9. **agree** that the maximum cancellation period of three years and the ability to temporarily suspend for 10 working days while the process of cancellation is progressed be retained;

10. **agree** that any decision by the Minister of Internal Affairs to cancel or refuse to issue a travel document on security grounds:

10.1 should be referred to the Chief Commissioner of Intelligence Warrants; and

10.2 a judicial commissioner should review the decision and have the ability to refer the decision back to the Minister of Internal Affairs if one of the grounds for judicial review is made out;

Proposed requirements for outbound travellers, including advance passenger processing

11. **agree** to amend the Immigration Act 2009 providing for advance passenger processing for outbound passengers by:

12. allowing for the collection of information and for boarding directives;

12.1 making it mandatory and applying an infringement and offence regime (in the same way as it does for inbound advance passenger processing information) so that the provision of information is assured and boarding directives are followed;

12.2 allowing Immigration New Zealand to share outbound advance passenger processing information with Police, Customs, the Department of Corrections and the Aviation Security Service or allow them direct access to the information;

13. **agree** to amend the Immigration Act to:

13.1 provide clear legislative authority for Immigration New Zealand to use passenger name record information for outbound travellers, as is the case for inbound travellers;

13.2 make the provision of passenger name record information on outbound travellers mandatory and include an infringement offence regime, as is the case for inbound travellers;

14. **agree** to amend the Immigration Act to grant Immigration New Zealand an express power to direct a carrier not to carry a person out of New Zealand on a lost, stolen, invalidated or fraudulent travel document;

Protection of intelligence and security information

15. **note** that preventing unauthorised disclosure of intelligence and security information is important as unauthorised use or disclosure could have serious ramifications for New Zealand's national security and undermine New Zealand's reputation with intelligence partners;

16. **note** that the New Zealand Security Intelligence Service Act 1969, the Government Communications Security Bureau Act 2003, the Inspector-General of Intelligence and Security Act 1996 and the Intelligence and Security Committee Act 1996 all contain offences relating to the protection of sensitive information and/or proceedings, which are cast in different terms and have varying penalty levels;

17. **note** that there are also offences in the general law that are intended to protect information that has implications for national security;

18. **agree** that the following offences, containing appropriate mens rea elements, will protect intelligence and security information:

Offence	**Offence will apply to**	**Proposed change**	**Penalty**
Espionage (section 78 Crimes Act)	Everyone "who owes allegiance to the Sovereign"	No change	Maximum 14 years imprisonment
Wrongful communication, retention, or copying of official information (section 78A Crimes Act)	Everyone "who owes allegiance to the Sovereign"	No change	Maximum 3 years imprisonment
Wrongful communication, retention, or copying of classified information (new)	Persons owing a specific obligation of confidence in relation to classified information	Based on section 78A but applying to classified information. It will attract a higher penalty and engage a warrantless search power.	Maximum 5 years imprisonment
Unauthorised disclosure of certain official information (section 20A Summary Offences Act)	Everyone	No change	Maximum 3 months imprisonment/ $2,000 fine
Unauthorised disclosure of information (section 25 Armed Forces	Members of armed forces	No change	Maximum 2 years imprisonment

Offence	Offence will apply to	Proposed change	Penalty
Discipline Act 1971)			
Unauthorised disclosure of information by employees/former employees of agencies (section 12A(1) New Zealand Security Intelligence Service Act; section 11 Government Communications Security Bureau Act)	NZSIS and GCSB employees and former employees	Rationalisation into a single offence.	Maximum 2 years imprisonment/ $10,000 fine
Protection of IGIS and ISC proceedings (including unauthorised disclosure/breach of secrecy/unauthorised publication as covered in section 28 and 29 of the Inspector-General of Intelligence and Security Act and section 19 of the Intelligence and Security Committee Act)	Everyone	Retain and carry over	Maximum 2 years imprisonment/ $10,000 fine
Failure to destroy irrelevant information obtained pursuant to warrant / failure to destroy information obtained pursuant to urgent authorisation where no warrant is issued (sections 4G, 4IB,4IE, 12A(2) and (3) New Zealand Security Intelligence Service Act; section 23 Government Communications Service Bureau Act)	NZSIS and GCSB employees authorised by warrant or urgent authorisation	Rationalisation	Maximum $10,000 fine
Personation (section 13 New Zealand Security Intelligence Service Act)	Everyone	Extend offence to GCSB and limit to circumstances where conduct likely to lead a person to believe	Maximum 12 months imprisonment/ $15,000 fine

Offence	Offence will apply to	Proposed change	Penalty
		the person is an employee	
Publication/broadcast of identity of employees (section 13A New Zealand Security Intelligence Service Act)	Everyone	Extend to GCSB	Maximum $20,000 fine (body corporate)/ $5,000 fine (individual)
Failure to comply with IGIS in relation to power of inquiry (section 23(8) Inspector-General of Intelligence and Security)	Everyone	Retain and carry over	Maximum $5,000 fine

Protected disclosures

19. **note** that under the Protected Disclosures Act 2000 at present, New Zealand Defence Force, Ministry of Defence, Ministry of Foreign Affairs and Trade, and Department of the Prime Minister and Cabinet staff are required to complain to the Ombudsmen if the disclosure relates to "the international relations of the Government of New Zealand or intelligence and security matters";

20. **agree** that section 13 of the Protected Disclosures Act be amended so that it mirrors what is provided for in relation to the security and intelligence agencies for all employees who are in the position of wanting to make a protected disclosure in relation to classified information or the work of the agencies;

21. **direct** officials work with Parliamentary Counsel to ensure that the redraft of section 18 of the Inspector-General of Intelligence and Security Act in the new legislation sits comfortably with the Protected Disclosures Act;

Transitional provisions

22. **agree** that the Bill be commenced in the following manner:

    22.1 the provisions of the Bill that will continue the amendments to the Passports Act put in place by the Countering Terrorist Fighters Legislation Bill will commence the day after the Bill receives Royal assent;

    22.2 certain provisions giving the agencies access to datasets held by other government agencies (described in more detail in Cabinet paper six) will commence the day after the Bill receives Royal assent; and

    22.3 the remainder of the Bill will come into force six months after the Bill receives Royal assent.

23. **agree** that the following transitional provisions be included in the Bill:

23.1 warrants and authorisations under both the New Zealand Security Intelligence Service Act and the Government Communications Security Bureau Act should be "grandfathered" consistent with the approach that was taken in the Search and Surveillance Act 2012

23.2 cancellations and refusals to issue travel documents made under the temporary provisions in the Schedule to the Passports Amendment Act 2014 should be treated as if they had been made under the re-enacted provisions in the new Act so that timeframes are unaffected by the transition to the new provisions;

23.3 the Directors of the agencies in office at the time the legislation commences will continue in office, subject to the incumbents:

23.3.1 Accepting an offer of appointment and agreeing new employment arrangements with the State Services Commissioner;

23.3.2 Having a term expiry date that is after the date of enactment of the legislation; and

23.3.3 Not resigning or having been removed from office.

23.4 where these conditions are met, the following provisions of the State Sector Act 1988 will be overridden:

23.4.1 section 35, which provides for appointment of chief executives, to make clear that the State Services Commissioner will not be required to commence a new appointment process;

23.4.2 section 40(1A), providing for appointment of an acting chief executive when a new department is established, in relation to the NZSIS only.

23.5 in the event of either Director not accepting the position offered or an employment agreement not being reached, no compensation will be available to them for loss of office (which aligns with the Directors' current terms of appointment).

23.6 the appointments of the Inspector-General of Intelligence and Security and the Deputy Inspector-General of Intelligence and Security should be treated as if they were made under the new Act meaning that the terms of both appointments continue as originally intended at the time of appointment;

23.7 the ability of the responsible Minister or the Prime Minister to agree to the findings of the Inspector-General of Intelligence and Security being referred to the Intelligence and Security Committee [NSC-16-MIN-0009, paragraph 13 refers] should apply to any own-motion inquiry or an inquiry requested by one of those Ministers, regardless of whether the inquiry commenced prior to the commencement of the new Act.

Ongoing review mechanism

24. **agree** that the requirement for periodic reviews of the agencies, their legislation and their oversight legislation that was inserted into the Intelligence and Security Committee Act in 2013 be retained and carried over to the new legislation.

Authorised for lodgement

Rt Hon John Key
Minister for National Security and Intelligence

Hon Christopher Finlayson
Minister Responsible for the GCSB
Minister in Charge of the NZSIS