OFFICE OF THE INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY

WORK PROGRAMME 2018/2019

Each year the Inspector-General publishes a work programme to update the public about the inquiries and reviews she is undertaking to ensure the intelligence and security agencies are acting lawfully and properly.

The work programme has been provided to the intelligence and security agencies and the Minister responsible for the intelligence and security agencies. The Inspector-General consults the Minister on the work programme and must consider the Minister's comments, but the final decision on the work of the office rests with the Inspector-General. The Inspector-General also takes into account the agencies' comments on proposed work.

Matters relating to both NZSIS and GCSB

1. **Own initiative inquiry into the role of the GCSB and the NZSIS, if any, in relation to certain specific events in Afghanistan.** An inquiry into certain events in Afghanistan, some of which relate to the events described in *Hit and Run*, published by Nicky Hager and Jon Stephenson in 2017. Events relating to Operation Burnham are within the scope of this inquiry. Among other things, the inquiry will consider United Nations Assistance Mission in Afghanistan (UNAMA) reports and how various other agencies treated detainees. The inquiry is not considering the actions and conduct of the New Zealand Defence Force, although some specific events and questions of fact may be common to both this inquiry and the Government Inquiry announced by the Attorney-General on 11 April 2018. The terms of reference for this inquiry are available on the Inspector-General's website: www.igis.govt.nz/assets/Uploads/Inquiry-Terms-of-Reference.pdf

2. **Review of all new intelligence warrants issued to the GCSB and NZSIS.** Review of all warrants as they are granted and a deeper analysis of a selected few warrants, from formulation of the intelligence case to reporting obtained under the warrant ("deep dives").

3. **Report on warrants issued in first six to nine months of operation of the Intelligence and Security Act 2017: is the new Act achieving its objectives? What, if any, issues have arisen in interpreting and applying the Act?** The Intelligence and Security Act 2017 was described at the time as the most significant reform of the legislation governing the intelligence agencies and their oversight in New Zealand's history. The public were assured that the reforms would improve transparency around agency activity and accountability. The "triple lock" warrant system was said to be a core protection of the rights of New Zealanders against improper intrusion on their privacy. This report on the first warrants issued under the new Act will address compliance with the new Act.

4. **Regular reviews of permissions to access restricted information.** "Restricted information" is a term used in the Intelligence and Security Act 2017 to refer to certain private information held by government agencies that is especially sensitive. It includes information held by Inland Revenue, the Ministry of Education, the Registrar-General of Births, Deaths and Marriages, and driver licence photographs. This regular review will consider the applications for permissions for the agencies to access restricted information and whether the agencies act in accordance with the terms of those permissions.

5. **Regular reviews of business records approvals and directions.** "Business records" is a term used in the Intelligence and Security Act 2017 to refer to information produced and held by telecommunications network operators, such as a telcos, and financial service providers, such as banks. It includes information like subscriber and billing information, and bank statements and transaction histories. The agencies can obtain "business records approvals" which enable them to issue directions to telecommunications network operators and financial service providers requiring access to business records. The current approvals cover broad areas of operational activity, which can be the basis for particular directions in relation to specific information, e.g. a person's bank statement. This review will consider whether business records approvals and directions have been implemented lawfully and properly.

Matters relating to NZSIS

1. **Review a sample of adverse and qualified security clearance decisions**. In 2016 the Inspector-General published a report on procedural fairness in the security clearance vetting process. This new review will examine a sample of adverse and qualified security clearance decisions to assess the fairness of the process, including looking at the completeness and accuracy of the information put to the decision-maker and the opportunity for the candidate to know and answer any adverse information.

2. **Review how NZSIS's relationships at the border with other government agencies are governed and internally reviewed.** This new review will examine how NZSIS manages the relationship with a range of other government agencies responsible for activities at New Zealand's border. There are a number of cooperation and information sharing arrangements in place, and, as noted in the IGIS annual report of 30 June 2017, the Inspector-General has heard from some sections of the New Zealand Muslim community about their experiences at the border. This raises broader questions about how government agencies, including the NZSIS, cooperate at the border.

3. **Review of NZSIS "open source" activities. It is lawful for the NZSIS to obtain and use publicly available information.** The Ministerial Policy Statement on "Obtaining and using publicly available information" provides guidance on the conduct of this activity. Internationally, intelligence and law enforcement agencies are increasingly using specialised tools and methods. The Inspector-General has not previously examined NZSIS "open source" activities, which involve intelligence activity in relation to information which is publicly available, including on the internet. This review will examine how the NZSIS carries out open source activities and whether those activities are lawful and proper and in accordance with the Ministerial Policy Statement.

4. **Review of operation of direct access agreements.** The Intelligence and Security Act 2017 made specific provision for direct access agreements. Direct access agreements enable NZSIS to access databases and information held by other government agencies without having to make specific requests each time NZSIS wants to obtain information. This review will address how direct access agreements are operating in practice.

Matters relating to GCSB

1. **Review how GCSB's access operations are conducted.** To give effect to an intelligence warrant, GCSB may access an information infrastructure or class of infrastructures (s 69 of the Intelligence and Security Act 2017). Information infrastructures are defined in the Act to include information technology systems and networks and any communications carried on, contained in or relating to them. This review will examine how the Bureau conducts access operations for the purpose of intelligence collection and analysis, including how such operations are planned, recorded and internally reviewed.

2. **Review a selection of operations under warrant involving the GCSB sharing "raw" (unprocessed) data with partner agencies, to assess adequacy of conditions and checks on compliance.** GCSB may share lawfully collected "raw" (unprocessed) data with partner intelligence agencies. Such sharing is subject to conditions and compliance obligations. This review will consider whether the conditions and compliance obligations are adequate.

3. **Review of GCSB "open source" activities.** It is lawful for the GCSB to obtain and use publicly available information. The Ministerial Policy Statement on "Obtaining and using publicly available information" provides guidance on the conduct of this activity. Internationally, intelligence and law enforcement agencies are increasingly using specialised tools and methods. The Inspector-General has not previously examined GCSB "open source" activities, which involve intelligence activity in relation to information which is publicly available, including on the

internet. This review will examine how the GCSB carries out open source activities and whether those activities are lawful and proper and in accordance with the Ministerial Policy Statement.

4. **Review of access by GCSB staff to partner data.** GCSB may lawfully access intelligence data gathered by some partner agencies. Access to partner intelligence by GCSB staff is subject to compliance rules. This review will consider whether instances of access by GCSB staff to partner data met partner compliance requirements and were lawful, in particular, whether those instances of access were necessary and proportionate and involved the least incursion possible into privacy interests.