GOVERNMENT COMMUNICATIONS SECURITY BUREAU
TE TIRA TIAKI

PO Box 12-209
Wellington 6144
P +64 4 472 6881
F +64 4 499 3701
www.gcsb.govt.nz

29 August 2022

Scott
fyi-request-19406-bf8bb336@requests.fyi.org.nz

Tēnā koe Scott

Official information request

Thank you for your Official Information Act 1982 (OIA) request of 20 May 2022 to the Government Communications Security Bureau (GCSB) seeking the following:

In the recently re-issued Ministerial Policy Statement – Publically available information, it is stated that:

> *"GCSB and NZSIS may collect large datasets which might include personal information relating to a number of individuals. GCSB and NZSIS must have a policy that provides guidance on the collection, use, retention and disposal of this type of information."*

I would like to request a copy of the Joint Policy Statement that provides the guidance referred to here.

You were advised on 17 June 2022 that the time limit for responding to your request had been extended to 1 August 2022 because the consultations necessary to make a decision on your request were such that a proper response could not reasonably be made within the original time limit. I apologise for the late response.

Response to your request

The GCSB policy *PS-138 Data Retention and Destruction* is in scope of your request. I am releasing a summary of this document to you, as provided for by section 16(1)(e) of the OIA.

Some information in the document has been withheld under section 6(a) of the OIA, as the release of this information would likely prejudice the security or defence of New Zealand, or the international relations of the Government of New Zealand.

I note on 2 June 2022, the NZSIS provided you with a summary of JPS-011 *Obtaining and Using Publicly Available Information*.

Review

If you wish to discuss this decision, please feel free to contact information@gcsb.govt.nz.

You have the right to seek an investigation and review by the Ombudsman of this decision. Information about how to make a complaint is available at www.ombudsman.parliament.nz or freephone 0800 802 602.

Ngā mihi

Andrew Hampton
Te Tumu Whakarae mō Te Tira Tiaki
Director-General of the GCSB

The following is summarised information from the Government Communications Security Bureau (GCSB) Data Retention and Destruction policy. Where possible, excerpts of the original document have been used. Some details are withheld under section 6(a) of the Official Information Act 1982 as release would prejudice national security.

GCSB Data Retention and Destruction

Purpose

- This policy specifies how GCSB will manage the retention and destruction of data obtained and created by GCSB when performing its intelligence collection and analysis, and protective security services, advice and assistance functions under sections 10 to 12 of the Intelligence and Security Act 2017 (ISA). This policy gives effect to the requirements of the ISA, the Public Records Act 2005 (PRA) and the Privacy Act 2020, particularly Information Privacy Principle 9 (IPP9).
- The Ministerial Policy Statement (MPS) on *The management of information obtained by the GCSB and NZSIS, including retention and disposal of that information* directs GCSB to provide guidance to assist employees to determine whether data is required for the performance of statutory functions, and specify the timeframes within which the determination must be made. This policy gives affect to that MPS.

Scope

- This policy applies to all data obtained or created by GCSB in the performance of the following functions, and which GCSB holds:
    - Intelligence collection and analysis (under section 10 of the ISA); and
    - Protective security services, advice and assistance, including information assurance and cybersecurity activities (under sections 11 and 12 of the ISA).
- This includes data obtained or created by GCSB in the performance of those functions where GCSB is also cooperating with the New Zealand Security Intelligence Service, New Zealand Police or New Zealand Defence Force under the cooperation function in section 13 (1)(a) of the ISA.
- This policy applies regardless of the sources or methods used by GCSB to obtain or create data. Data covered by the policy includes:
    - Data obtained by operations conducted under the authority of intelligence warrants or other authorisations, including data obtained by people or organisations assisting GCSB under a section 51 request for assistance;
    - Data obtained through requests under section 121, voluntary disclosures, open-source research, and other lawful activities;
    - Data obtained by consent;
    - Data obtained from partner agencies;
    - Data/knowledge generated by analysing other data; and
    - Working materials generated by analysts or other personnel.
- While section 103 of the ISA applies only to data obtained by GCSB within the scope of an authorised activity done under an intelligence warrant, this policy applies to all data collected to perform one of the functions of the agency listed above under the

ISA. This means that the concept of irrelevant information in section 103 is applied more broadly to data obtained and created by GCSB.

- This policy does not cover:
    - Data that GCSB holds or transports solely for other agencies;
    - Data obtained or created when co-operating with either the New Zealand Police of New Zealand Defence Force to facilitate their functions (under section 13(1)(b) of the ISA);
    - Data obtained or created when co-operating with other entities to respond to imminent threat (under section 14 of the ISA);
    - Incidentally obtained information (section 104 of the ISA);
    - Information and records created as part of GCSB's corporate functions including for example, finance, procurement, human resources and travel;
    - Legal advice and instructions;
    - Policy advice and policy development;
    - Ministerial briefings;
    - GCSB Senior Leadership Team papers and other governance materials;
    - Material related to oversight, including correspondence from and to the Inspector-General of Intelligence and Security; and
    - Personal data about employees.

Policy

- The retention and destruction of data by GCSB will be administered using the Data Retention and Destruction Framework (DRDF). The framework establishes four states for data and applies reasonable Retention Time Limits (RTLs) and/or justifications for retention of that data outside of RTLs.
- All GCSB data that is subject to this policy will be covered by one or more of the following four states of the DRDF and must be subject to the retention and destruction time limits, review periods, processes and rules applicable to the state. The four states are:
    - Unprocessed;
    - Unassessed;
    - Internal Analytic Product (IAP); and
    - Required.
- GCSB will consider necessity and proportionality (including privacy implications) when establishing RTLs and review periods.

Implementation of Data Retention and Destruction Framework

- This policy establishes a framework for the retention and destruction of information by GCSB. It is expected that it will be implemented progressively and that over time technology, business processes and practice will develop in response to the new Framework.

Unauthorised information

- Under section 102 of the ISA, the GCSB must immediately destroy information collected under a warrant that is unauthorised, unless a warrant is issued that authorises the collection, or the information is approved for retention as incidentally obtained information to disclose according to the provisions of section 104 of the ISA.

Audit

- This policy and any policy or process established under this policy is subject to audit.