Ministerial Policy Statement

Providing information assurance and cybersecurity activities under section 11 of the Intelligence and Security Act 2017 with consent

Summary

It is lawful for the Government Communications Security Bureau (GCSB) to provide information assurance and cybersecurity activities with consent. This ministerial policy statement (MPS) provides guidance on conducting those activities. In making decisions related to the provision of information assurance and cybersecurity activities with consent, GCSB must have regard to the following principles: necessity, proportionality, legality, respect for privacy, confidentiality and oversight. This ministerial policy statement also specifies certain matters to be included in internal policy and procedures and establishes regular reporting for oversight purposes.

Definitions

The Act *means the Intelligence and Security Act 2017.*

GCSB *means the Government Communications Security Bureau.*

Information assurance and cybersecurity activities *means activities that are carried out proactively or reactively to ensure the availability, confidentiality, and integrity of communications and information infrastructures (as defined in section 4 of the Act).*

Consented information assurance and cybersecurity activities *means information assurance and cybersecurity activities provided to a public authority or other persons that are lawful because those activities are carried out with the lawful consent of the relevant authority or person.*

NCSC *means the National Cyber Security Centre, which is part of GCSB.*

Public authority *means a person or body that performs or exercises any public function, duty, or power conferred on that person or body by or under the law (see section 4 of the Act).*

Threat reports *means reports related to threats to, or interference with, communications or information infrastructures of importance to the Government of New Zealand (as may be produced under section 12(5)(b) of the Act).*

Purpose

1. This MPS is issued by the Minister Responsible for the GCSB pursuant to section 206(a) of the Act.
2. The purpose of this MPS is to provide guidance to GCSB on providing consented information assurance and cybersecurity activities under section 11 of the Act. The MPS comprises the Minister's expectations for how GCSB should properly perform its functions and establishes a framework for good decision-making and best practice conduct.
3. MPSs are also relevant to oversight of the agencies by the Inspector-General of Intelligence and Security in the exercise of their propriety jurisdiction (the Act requires the Inspector-General to take account of any relevant MPS and the extent to which an intelligence and security agency has had regard to it when conducting an inquiry or review).
4. Every employee making decisions or taking any action related to consented information assurance and cybersecurity activities must have regard to this MPS. Employees should be able to explain how they had regard to the MPS. This might amount to an explanation of their consideration of any relevant internal policy or procedures that reflect the MPS. The Director-General is responsible for ensuring the MPS is reflected in GCSB's internal policies and procedures. If any action or decision is taken that is inconsistent with the MPS, employees must be able to explain why the action was taken and how they had regard to the MPS.

Scope

5. This MPS only relates to consented information assurance and cybersecurity activities. It is intended to ensure that consented information assurance and cybersecurity activities are appropriately authorised and are carried out consistently with the privacy and confidentiality interests of individuals and organisations who might be affected.
6. Otherwise unlawful activities and information assurance or cybersecurity activities for which consent has not been given may only be carried out in accordance with an authorisation issued under Part 4 of the Act. Information assurance and cybersecurity activities conducted pursuant to an authorisation must be conducted in accordance with the terms of that authorisation, including any restrictions or conditions set out in the authorisation. They must, like all activities of GCSB, be conducted with propriety.
7. This MPS does not address activities that are carried out under an authorisation or that can be lawfully carried out without the consent of any person.

Context

8. GCSB's objectives are set out in the Act. GCSB contributes to:
    a) The protection of New Zealand's national security;
    b) The international relations and well-being of New Zealand; and
    c) The economic well-being of New Zealand.
9. GCSB does this through the performance of its statutory functions, which include:
    a) Intelligence collection and analysis; and
    b) The provision of protective security services, advice and assistance.

10. MPSs are an important component of the measures put in place by the Act to ensure the functions of GCSB are performed with propriety and in accordance with New Zealand law and all human rights obligations recognised by New Zealand law.
11. GCSB carries out information assurance and cybersecurity activities as part of performing its protective security services, advice and assistance function. Information assurance and cybersecurity activities are activities that are carried out proactively or reactively to ensure the availability, confidentiality, and integrity of communications and information infrastructures. Based on information obtained through consented information assurance and cybersecurity activities, GCSB may also produce threat reports that it can share with persons authorised by the Minister to receive them.
12. GCSB provides information and cybersecurity activities to public authorities and to any other persons when authorised by the Minister. This includes providing consented information assurance and cybersecurity activities to public and private sector organisations that the Government considers nationally significant. Such organisations include government departments, key economic generators, niche exporters, research institutions, operators of critical national infrastructure, and organisations or entities that are the victim of a cyber-borne threat where there are potential national security implications. Examples of the information assurance and cybersecurity activities GCSB provides to these organisations include malware detection and disruption services (such as the National Cyber Security Centre's computer network defence capabilities developed under Project CORTEX), cyber incident investigations and responses, and inspections to assess the security of communications and information infrastructures (including of locations where classified information is stored, processed or discussed).

New Zealand's cyber threat

New Zealand's public and private organisations have a wealth of information that is attractive to others, from intellectual property for a new technology innovation through to customer data, business and pricing strategies or government positions on sensitive topics.

Organisations are exposed to a wide range of attacks and attempts to steal information because of their connection to the Internet. The kinds of cyber incidents the National Cyber Security Centre (NCSC) detects and disrupts include:

- Foreign, likely state-sponsored actors attempting to gain access to networks.
- Personal details and system log-in information being stolen after users are tricked into entering those details into a fake website.
- Attempts to gain access to a network holding valuable intellectual property.
- Malicious code being inserted into a legitimate website in an attempt to gain access to the network of a user of that website.

If allowed to achieve their objective, these intrusions could result in substantial harm to important networks and the loss or manipulation of information important to the operation or future prosperity of New Zealand.

13. GCSB's specialist knowledge and skills, including in relation to advanced, foreign-sourced threats, means it has a unique ability in New Zealand to carry out these consented information assurance and cybersecurity activities. GCSB's information assurance and cybersecurity activities also play a part in supporting the Government's wider cybersecurity policy objectives.

Consented information assurance and cybersecurity activities

GCSB's activities will change over time and up to date information about them can be found on the GCSB website. The following are examples of the kinds of consented information assurance and cybersecurity activities the GCSB provides:

- Detection of malicious activity – through its cybersecurity capabilities NCSC may identify malicious activity on its customer's networks, such as the targeting of officials from a government agency through email and website exploits in an effort to get personal information and potentially compromise the agency's network. NCSC can detect such attacks and provide mitigation advice to prevent important information being lost or compromised.
- Analysis of cybersecurity incidents – organisations may report cybersecurity incidents to NCSC, and provide NCSC with information about an incident so that NCSC can analyse it and provide advice to the organisation to help it mitigate any threat posed.
- Assistance to check equipment and facilities - GCSB teams help government departments to check their equipment and facilities to ensure they are free from interception devices or other information security vulnerabilities.

Requirements relating to consent

14. Provision of GCSB's consented information assurance and cybersecurity activities is governed by the general law on consent. The consent of a recipient of activities makes otherwise unlawful activities lawful. For example, GCSB must receive explicit consent from a government department in order to access the department's computer systems to investigate any malware on that system. Without consent (or other lawful authority, such as a warrant), a GCSB employee accessing that computer system would be liable for the offence under section 252 of the Crimes Act 1961.
15. Consent to receive information assurance and cybersecurity activities from GCSB must be given by a person authorised to make a decision on behalf of the recipient, as determined by the recipient. GCSB must take reasonable steps to ensure a person purporting to grant consent to activities has the legal authority to grant such consent.
16. Before consenting to information assurance and cybersecurity activities undertaken by GCSB, the intended recipient should be informed of the nature and scale of the activities that will be carried out and the information and systems to which GCSB will have access. GCSB should be satisfied the proposed recipient has sufficient understanding of the range of activity, level of intrusion, and the possible implications of the activities to which they are consenting to.
17. There should always be a written record of consent (for example, in the form of a Memorandum of Understanding or Deed) in place. This should be updated if the nature of activities to be provided changes.

Focus of activities

18. The focus of GCSB in carrying out its protective security function is on the protection of information infrastructures of importance to the Government of New Zealand. Generally, the focus of the consented information assurance and cybersecurity activities carried out by GCSB will tend to be on activities that have some or all of the following features:
    - to protect nationally-significant information infrastructures against the risks that arise due to being connected to the Internet (such as malicious software, or "malware"), and which are generally not adequately mitigated by commercially-available tools;
    - to address threats that have implications for New Zealand's national security, and cyber incidents that potentially have been perpetrated by an Advanced Persistent Threat actor;
    - to detect or prevent a malicious actor from intercepting communications or causing significant harm (such as loss of customer data or intellectual property, damage to IT networks);
    - to be assured that important communications or information infrastructures are secure;
    - to analyse and share information about techniques used by malicious actors to compromise communications and information infrastructures; and
    - to test or develop methods of ensuring the availability, confidentiality or integrity of communications and information infrastructures.
19. However, the particular consented information assurance and cybersecurity activities carried out by GCSB will be determined having regard to all of the circumstances, including potential impacts, consequences and harm arising from risks.

Principles

20. The following principles constitute a framework for good decision-making and must be taken into account by GCSB when planning and providing consented information assurance and cybersecurity activities. All consented information assurance and cybersecurity activities should be subject to ongoing review as to whether the services continue to be consistent with these principles.

Necessity

21. Consented information assurance and cybersecurity activities should only be provided to a recipient to the extent necessary for a purpose that is consistent with the GCSB performing its protective security function, which includes producing threat reports.
22. Factors that are relevant to assessing the purpose of carrying out the activity include: the importance to the Government of New Zealand of the communications and information infrastructures that are the subject of the activities, and the anticipated effectiveness and benefits of the activities to be carried out.
23. While the recipient of activities grants consent to GCSB to carry out those activities, GCSB must only carry out activities within the scope of that consent to the extent necessary for that purpose.
24. Activities that will not be necessary for a purpose consistent with the performance of GCSB's protective security services, advice and assistance function (including the production of threat reports) include where an activity would not do anything to ensure the availability, confidentiality or integrity of any communications or information infrastructures.

Proportionality

25. Necessary activities must be carried in a manner that is rationally and proportionately connected to their purpose. Information assurance and cybersecurity activities necessarily involve a degree of intrusion in order to provide the desired protective service, but should be carried out in a way that, as far as possible, limits the impact of that intrusiveness.
26. The impact of a consented information assurance and cybersecurity activity should be proportionate to its purpose, namely the requirement for the activity and the anticipated benefit of it. Where an activity is made up of several parts, the impact of each part should be proportionate to its purpose. Factors that are relevant in assessing the impact of an activity include:
    - The amount of information involved;
    - How much of that is personal information or particularly sensitive information (e.g. commercially sensitive information);
    - The duration of the activity; and
    - Any risks posed to communications or information infrastructures as a result of carrying out the activity.
27. The impacts of an activity should be limited to what is necessary in order to achieve the purpose of the activity. For example, when analysing a cybersecurity incident the GCSB should only have access to the information that is necessary to complete that analysis.

Legality

28. GCSB must ensure that consented information assurance and cybersecurity activities are provided in accordance with the law. This includes adherence to any additional specific legal obligations owed in respect of certain types of privileged and protected information or data that GCSB may gain access to during the course of those activities. Where appropriate, legal advice should be sought during the planning and conduct of consented information assurance and cybersecurity activities.

Respect for privacy

29. GCSB is subject to the Privacy Act 1993 and information privacy principles 1, 4(a), and 5 to 12 will apply where GCSB has access to personal information. GCSB should take special care in relation to any personal information, which will entail taking reasonable steps to mitigate any privacy impacts of consented information assurance and cybersecurity activities.
30. GCSB should conduct Privacy Impact Assessments when developing significant new projects or cybersecurity activities that have a significant implications for the privacy of individuals.
31. Steps to mitigate the privacy impacts of activities may include applying technical measures so that personal information obtained as a result of activities is only able to be viewed by GCSB employees where that information is required to perform the consented activities, subjecting such information to dissemination controls, or taking reasonable steps to inform affected persons about how personal information might be affected (taking into account GCSB's security requirements).

Confidentiality

32. GCSB must, to the extent agreed with a recipient, keep confidential the fact that consented information assurance and cybersecurity activities have been provided. Any information obtained

by GCSB in the course of providing consented information assurance and cybersecurity activities can only be used by approved staff to perform GCSB's protective security functions or to produce threat reports (unless authorised by an authorisation under Part 4 of the Act). Threat reports may only be shared with parties authorised by the Minister to receive them. GCSB should not disclose the identity of a recipient who has been affected by a particular threat unless it is necessary to achieve GCSB's statutory functions, in accordance with its internal policies on minimising identities.

Oversight

33. GCSB must carry out all activities in a manner that facilitates effective oversight, including through the keeping of appropriate records about the planning, approval, conduct and reporting on the provision of information assurance and cybersecurity activities. This will include the provision of six monthly reports to the Inspector-General of Intelligence and Security, copied to the responsible Minister. These reports should provide an overview of consented information assurance and cybersecurity activities during the period in question with particular emphasis on any new developments. The purpose of these reports is to ensure the Inspector-General and the responsible Minister have a broad understanding of the nature and scope of GCSB's activities in this area, and to facilitate the Inspector-General's oversight function.
34. GCSB must ensure consent granted by recipients of information assurance and cybersecurity activities is appropriately recorded in writing (through a Memorandum of Understanding, or Deed, or similar document).

Matters to be reflected in internal policies and procedures

35. GCSB must have, and act in compliance with, internal policies and procedures that are consistent with the requirements and principles above, and must have systems in place to support and monitor compliance. GCSB must also have policies and procedures that address the following matters:

Sharing of data

Information obtained by GCSB through the carrying out of information assurance and cybersecurity activities may only be used for the purpose of performing its protective security function and to produce threat reports, unless a warrant is obtained authorising its use for another purpose. GCSB may only share threat reports with persons or classes or persons authorised by the Minister to receive that information (see MPS on *Cooperation with overseas public authorities*). GCSB must have in place a policy that addresses the use and disclosure of information collected in the course of providing consented information assurance and cybersecurity activities.

Information management

Information held as a result of the provision of consented information assurance and cybersecurity services must be handled and stored in accordance with clear access controls that correspond to the sensitivity of the information. The MPS on *Management of information obtained by GCSB and NZSIS* will also apply in relation to this information.

Compliance with information privacy principles

GCSB is subject to information privacy principles 1, 4(a), and 5 to 12 of the information privacy principles in the Privacy Act 1993. All policies relating to consented information assurance and cybersecurity services and the handling of any information accessed or held as a result of such

activity must incorporate guidance about compliance with the relevant information privacy principles.

Compliance with public service minimum standards of integrity and conduct
The Director-General of GCSB must issue policies and procedures that reflect GCSB's obligations under the Public Service Act 2020.

Health and safety
All consented information assurance and cybersecurity activities must be undertaken consistently with GCSB's obligations under the Health and Safety at Work Act 2015.

Training
GCSB employees may only participate in providing consented information assurance and cybersecurity activities if they have been trained on the relevant law, policies and procedures.

Authorisation procedures

36. The consent of those receiving services from GCSB provides authority for the carrying out of activities covered by this MPS.
37. The Minister responsible for the GCSB will authorise the sharing of threat reports that are produced as a result of carrying out information assurance and cybersecurity activities with any person or class of persons, in New Zealand or overseas.

Duration of ministerial policy statement

38. This MPS will take effect from 28 September 2020 for a period of three years. The Minister who issued an MPS may, at any time, amend, revoke or replace the MPS.

Ministerial Policy Statement issued by:

Hon Andrew Little
Minister Responsible for the Government Communications Security Bureau
Minister Responsible for the New Zealand Security Intelligence Service

September 2020