Ministerial Policy Statement

Information assurance and cybersecurity activities

Summary

It is lawful for GCSB to provide information assurance and cybersecurity activities with consent. This 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, 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

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.*

GCSB *means the Government Communications Security Bureau*

NCSC *means the National Cyber Security Centre, which is a business unit of GCSB.*

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).*

Context

1. GCSB carries out information assurance and cybersecurity activities as part of performing its protective security services, advice and assistance function. These activities are carried out proactively or reactively to ensure the availability, confidentiality, and integrity of communications and information infrastructures.
2. Through the NCSC, GCSB provides information assurance and cybersecurity services to organisations of national significance (which includes government agencies, key economic generators, niche exporters, research institutions and operators of critical national infrastructure), and responds to high-impact cyber incidents at a national level.
3. Examples of the information assurance and cybersecurity activities the GCSB carries out include:
    - cyber threat detection and disruption services (**CORTEX**) to prevent harm from advanced threats;
    - a malware detection and disruption service, which involves the NCSC generating and sharing cyber threat intelligence with consenting organisations;
    - supporting organisations to respond to cyber incidents;
    - providing advice and support to help improve cyber resilience;
    - producing cyber threat reporting;
    - managing the government's information security standards.
4. GCSB's activities change over time and up to date information on their information assurance and cybersecurity activities can be accessed on the GCSB website (**GCSB - Information Assurance**).

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, to customer data, business and pricing strategies, or government positions on sensitive topics.

Organisations are exposed to a wide range of cyber attacks and attempts to steal online information. The kinds of cyber incidents the NCSC detects and disrupts include:

- foreign actors attempting to gain access to networks;
- malicious cyber actors exploiting known, unpatched vulnerabilities in networks, technologies and devices to perform unauthorised actions on a system;
- use of techniques such as phishing to gain personal details and login information;
- data breaches of personally identifiable information or user credentials, which poses a risk to nationally significant organisations; and
- deployment of malicious code onto a network through a vulnerable website to attempt to allow future access for the actor.

If allowed to achieve their objective, these intrusions could result in substantial harm to important networks and the loss or manipulation of information. Maintaining the integrity and availability of information and communications networks is critical to New Zealanders and New Zealand organisations maintain a secure and prosperous society and economy.

Guidance for GCSB

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 permitted 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.
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.

Requirements relating to consent

8. 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.
9. 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.
10. 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 which they are consenting to.
11. There should always be a written record of consent in place (for example, in the form of a Memorandum of Understanding or Deed or exchange of letters or emails). This should be updated if the nature of activities to be provided changes.

Principles

12. The following principles constitute a framework for good decision-making and sets out best practice conduct 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

13. 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.
14. 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.
15. 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.

Proportionality

16. 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.
17. 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.
18. 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.

Respect for privacy

19. GCSB is subject to the Privacy Act 2020 and 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.
20. GCSB should conduct Privacy Impact Assessments when developing significant new projects or cybersecurity activities that have significant implications for the privacy of individuals.
21. 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

22. 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). 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.

Legal obligations

23. GCSB must adhere to any additional specific legal obligations in respect of certain types of privileged and protected information or data that GCSB may gain access to during the course of those activities. As appropriate, legal advice should be sought during the planning and conduct of consented information assurance and cybersecurity activities.

Oversight

24. GCSB must carry out all activities in a manner that facilitates effective oversight, including through keeping appropriate records about the planning, approval, conduct and reporting on the provision of information assurance and cybersecurity activities.

Matters to be reflected in internal policies and procedures

25. As a public service agency GCSB must comply with policies and procedures common to all New Zealand public service agencies.[1]
26. In addition, GCSB must have, and act in compliance with, internal policies and procedures that are consistent with the requirements and principles of this MPS and have systems in place to support and monitor compliance.
27. These policies and procedures must also address the following additional matters set out below.

Sharing data

28. 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. The MPS on *Cooperating with overseas public authorities* provides guidance on sharing information with overseas public authorities. GCSB must have in place a policy that addresses the use and disclosure of

[1] *This includes the Public Service Act 2020 and the Health and Safety at Work Act 2015.*

information collected in the course of providing consented information assurance and cybersecurity activities.

Information management

29. 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 *Information management* will also apply in relation to this information.

Compliance with information privacy principles

30. GCSB is subject to information privacy principles 1, 4(a), and 5 to 12 of the privacy principles in the Privacy Act 2020. 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.

Training

31. 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.

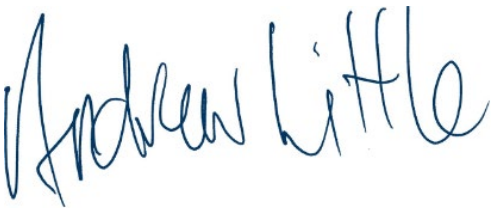
Authorisation procedures

32. The consent of those receiving services from GCSB provides authority for the carrying out of activities covered by this MPS.
33. 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

34. This MPS will take effect from 01 March 2022 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
01 March 2022