



Proactive release of material

The following document has been proactively released by the Government Communications Security Bureau (GCSB):

| Date | Title |
|------------|--------------------|
| 3 May 2024 | Terms of reference |

This document is an unclassified version of the terms of reference. Some parts of the original document are not appropriate to release and have been withheld in accordance with the Official Information Act 1982 (the OIA). The full, classified version has been provided to the Inspector-General of Intelligence and Security.

The withheld information has been replaced with an unclassified summary of the material¹. This is marked in the document with square brackets and italics. Where information has been withheld under section 9 of the OIA, no public interest has been identified that would outweigh the reasons for withholding it.

The relevant sections of the OIA that apply to the withheld information are outlined below:

| OIA Section | Explanation |
|-------------|---|
| 6(a) | To avoid prejudice to the security or defence of New Zealand or the international relations of the Government of New Zealand |
| 6(b)(i) | To avoid prejudice to the entrusting of information to the Government of New Zealand on a basis of confidence by the Government of any other country or any agency of such a Government |
| 9(2)(ba)(i) | To protect information which is subject to an obligation of confidence, where the making available of the information would be likely to prejudice the supply of similar information, and it is in the public interest that such information should continue to be supplied |

¹ This information has been provided in summary form as allowed for under section 16(1)(e) of the OIA.



Te Tira Tiaki
Government Communications
Security Bureau

Terms of reference

Date: 3/05/2024
To: [Name withheld], Director Cyber Defence Operations, NCSC, GCSB
From: Lisa Fong, Deputy Director-General NCSC, GCSB
For: Action and initial report by 31 May 2024

Review of procedures where reports of malicious cyber activity concern foreign state sponsored targeting of identified New Zealand individuals

Purpose

1. This terms of reference establishes a review of the National Cyber Security Centre's (NCSC's) procedures where it receives reports of malicious cyber activity involving foreign state-sponsored actors targeting identified New Zealand individuals. It seeks to identify where procedures and practices need improvement and recommendations to give effect to those improvements.

Background

- 2-7 *[These paragraphs describe actions taken by NCSC between 2021 and 2024 related to reports of possible foreign state cyber activity targeted at New Zealand members of the Inter-Parliamentary Alliance on China (IPAC).*

Between 2021 and 2024, the NCSC responded to the reports of possible activity against New Zealand members of IPAC in accordance with its incident triage and response procedures.

NCSC's actions did not include engaging with individuals who had been the possible targets of the activity, or briefing the responsible Minister.]

Objectives of this review

8. In establishing a review, this terms of reference seeks to:
 - a. examine the NCSC's existing procedures and practices when responding to reports of malicious cyber activity indicating foreign state sponsored actors are targeting identified New Zealand individuals;
 - b. identify areas for improvement in the NCSC's procedures when responding to reports of malicious cyber activity indicating foreign state sponsored actors are targeting identified New Zealand individuals – including but not limited to the triage, response, support to the individuals or organisations concerned and engagement with the responsible Minister;
 - c. recommend ways to deliver those improvements, including but not limited to internal policy and procedure, and external engagement and guidance;
 - d. identify, based on these findings and recommendations, whether the NCSC's response to the *[reports of possible foreign state cyber activity targeted at New Zealand members of IPAC]* was sufficient based on the information to hand at the time; and
 - e. recommend any further steps that may need to be taken regarding *[current or former members of IPAC and associated organisations]*.

Scope of review and relationship to other activity and agencies

9. Operational activity is expected to continue during the course of the review. *[Summary of subject of ongoing operational activity]*. While the fact of the review or its developing insights may inform this activity, it is not intended to prevent or constrain timely operational decisions.
10. This review does not extend to the quality of the technical analysis related to the *[reported activity]*. This review does not seek to establish whether the *[reported activity]* was successful.
11. This review does not purport to assess any action or otherwise by other agencies, including *[foreign partners]*, New Zealand Police, the NZSIS or the Parliamentary Service. It will, however, consider the relationship with and supporting role of other agencies when examining the NCSC's activity and responsibilities.
12. This review does not extend to joint New Zealand Intelligence Community (NZIC) or organisational policies for intelligence reporting involving Sensitive Category Individuals.

Deliverable and timeframe

13. The Director Cyber Defence Operations will prepare a draft report and recommendations for DDG NCSC consideration by 31 May 2024. The draft report should indicate the anticipated timeframes to deliver any recommendations arising from the review.

14. The final report is due to the DDG NCSC by 14 June 2024, on the basis any consultation required can be completed within this timeframe.
15. The DDG NCSC will make the final report and any decisions on the recommendations available to the Director-General GCSB, Minister Responsible for the GCSB, and the Inspector-General of Intelligence and Security.
16. The report is to be accompanied by a summary with the intention this be offered to the New Zealand individuals, followed by public release.
17. The DDG NCSC may grant an extension of time, where justified. This must be provided in writing, and if granted, the DDG NCSC will notify the extension to the Director-General GCSB, Minister Responsible for the GCSB, and the Inspector-General of Intelligence and Security.

Roles and responsibilities

18. The Deputy Director-General NCSC is the sponsor of this review and is accountable for the work produced under this terms of reference.
19. The review will be led by the Director Cyber Defence Operations, supported where appropriate with staff and input from across the NCSC and the GCSB.
20. Where consultation is required to answer the terms of reference, this is to be conducted within the timeframes set for completion of the written report and recommendations.
21. In the event the review identifies any issues warranting urgent attention, these are to be brought to the sponsor's attention and prioritised for early response ahead of the date for submission of the final report.

Lisa Fong

Deputy Director-General NCSC, GCSB

Date: 03/05/2024