Te Tira Tiaki
Government Communications Security Bureau

Proactive release of material

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

Date	Title
14 June 2024	Review of NCSC Procedures and Practices: Malicious cyber activity involving foreign state-sponsored actors targeting identified New Zealand individuals

This document is an unclassified version of the review. 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 material[1]. 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.

National Cyber Security Centre

Te Tira Tiaki
Government Communications Security Bureau

Review of NCSC Procedures and Practices

Malicious cyber activity involving foreign state-sponsored actors targeting identified New Zealand individuals

14 June 2024

Table of Contents

Section 1 - Executive Summary

1.1 (U) This review has been conducted to meet objectives set out in Terms of Reference dated 3 May 2024, and reviews the National Cyber Security Centre's (NCSC's) procedures and practices where it receives reports of malicious cyber activity involving foreign state-sponsored actors targeting identified New Zealand individuals. The review was prompted by concerns regarding the NCSC's response to reports of [*malicious cyber activity*] targeting New Zealand members of the Inter-Parliamentary Alliance on China (IPAC).

1.2 (U) This review considers and describes the practices and processes that relate to the components of the NCSC that existed prior to the integration with CERT NZ, on 31 August 2023. The NCSC is continuing work to establish an operating model for the integrated agency, this includes aligning the currently distinct incident triage and response functions.

1.3 (U) Under the NCSC's pre-integration procedures and practice:

a. the NCSC receives and analyses a large amount of potential malicious cyber activity, and identifies a subset of this activity as "incidents" requiring response actions;

b. the NCSC triages and categorises all incidents, and responds to incidents with the objective of mitigating and remediating the threat posed by malicious cyber activity to the networks of nationally significant organisations or where there is potential for national level harm;

c. the NCSC's normal practice is to work with organisations that operate and administer the information technology systems or networks that are at risk due to malicious cyber activity;

d. the NCSC works alongside other New Zealand Government agencies where the incident relates to the functions of that agency;

e. the NCSC notifies the Minister Responsible for GCSB consistently with the "no surprises" principle;

f. the NCSC's procedures do not specifically address how to respond to reports indicating foreign state-sponsored actors that may be targeting identified New Zealand individuals.

1.4 (U) The review identifies the three following areas for improvement and related recommendations (set out in Section 6):

a. the NCSC's response to incidents needs to ensure due consideration is given to wider implications of cyber security incidents, and not focus solely on the technical response to such incidents;

b. where appropriate, the NCSC should consider some form of engagement with individuals in response to cyber targeting by foreign state-sponsored actors; and

c. identifying incidents that may be appropriate to brief to the Minister Responsible for the GCSB.

1.5 (U) The NCSC took actions related to reports of foreign state-sponsored malicious cyber activity against New Zealand members of IPAC in June 2021, April 2022, June 2022, and May 2024. Based on the actions taken in May 2024 and further engagement planned following the submission of this report, the review does not recommend any further actions need to be taken in response to this specific incident.

Section 2 - Background and Context

Terms of Reference

2.1 (U) This review has been conducted to meet objectives set out in the Terms of Reference dated 3 May 2024, and reviews 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. The Terms of Reference are attached in Appendix A.

Objectives

2.2 (U) The Terms of Reference established five objectives for this review:

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 regarding 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*].

2.3 (U) While this review considered the NCSC's response to reports of possible state-sponsored cyber activity targeting IPAC members, it did not focus on malicious cyber activity against a particular category of individuals, or conducted by a specific foreign state sponsored malicious cyber actor. This is consistent with the fact that a wide range of New Zealand individuals may be targeted by malicious cyber activity, and a range of foreign states conduct malicious cyber activity against New Zealand.

NCSC-CERT NZ integration

2.4 (U) On 31 August 2023, CERT NZ joined with the National Cyber Security Centre (NCSC) as a first step towards creating a lead operational cyber security agency. This consolidation of functions is intended to draw on the relative strengths of both agencies to deliver more effective and efficient cyber security outcomes for New Zealand.

2.5 (U) While the initial transfer of CERT NZ to the GCSB has been completed, work is ongoing to design and implement a new integrated operating model that aligns functions across both the NCSC and CERT NZ. One of the areas that has yet to be integrated are the separate incident triage and response functions provided by CERT NZ and the NCSC.

2.6 (U) This review focused on the practices and process that relate to the pre-integration NCSC incident triage and response function. This function focuses on identifying and responding to malicious cyber activity impacting nationally significant organisations or that otherwise has

national level harm. CERT NZ has traditionally focused on malicious cyber activity affecting individuals and small to medium sized businesses.

2.7 (U) The recommendations produced as a result of this review should be used as an input to the future design considerations for an integrated CERT NZ and pre-integration NCSC incident triage and response function.

Process

2.8 (U) In the course of conducting the review and preparing this report, the Cyber Defence Operations branch of the NCSC:

a. reviewed written NCSC procedures and guidance related to incident detection and response;

b. spoke to NCSC staff involved in responding to incidents;

c. sought the views of the NZSIS and New Zealand Police on roles and responsibilities related to reports indicating foreign state-sponsored actors may be targeting identified New Zealand individuals;

d. reviewed documentation related to the NCSC's response to reports of malicious cyber activity targeted at members of IPAC; and

e. spoke to NCSC staff involved in responding to the incidents of reported targeting of members of IPAC.

2.9 (U) As required by the Terms of Reference, a draft version of this report was delivered to the Deputy Director-General, NCSC on 31 May 2024.

2.10 (U) The NCSC consulted the following agencies on the draft report:

a. the NZSIS;

b. New Zealand Police; and

c. the Parliamentary Service.

2.11 (U) The NCSC also provided a copy of the draft report to selected NCSC staff, including who were involved in responding to the incidents of reported targeting of members of IPAC, for their comment.

Section 3 - Current Procedures and Practice

3.1 (U) This section sets out the NCSC's current approach to the identification, triage, and response to cyber security incidents, including those that relate to reports indicating foreign state-sponsored actors that may be targeting identified New Zealand individuals.

Identification

3.2 (U) The NCSC becomes aware of malicious cyber activity affecting New Zealand in a variety of ways. This includes through the operation of its technical cyber security services (for example CORTEX and Malware Free Networks), victims of incidents reporting activity directly to the NCSC, and information or referrals provided by international partners, other New Zealand Government agencies, and private sector organisations.

3.3 (U) NCSC staff conduct preliminary analysis of these indications of malicious cyber activity. If the activity is of sufficient seriousness to require further investigation or follow on action, NCSC staff will create a formal incident[2] record in the NCSC's incident management tool. The incident is then tracked through a standard workflow process until it has been resolved and closed out. In the 2023/24 financial year, the NCSC recorded 316 incidents of this type.

3.4 (U) The NCSC becomes aware of a large volume of potential malicious cyber activity, however, the vast majority of these events do not reach the threshold for escalation to a formal incident record. A significant amount of malicious cyber activity affecting New Zealand is not targeted, and is instead part of opportunistic exploitation of vulnerable systems and often global in nature. This includes most email-based phishing campaigns. The NCSC's staff prioritise escalation of activity judged most likely to cause significant harm to New Zealand's nationally significant organisations or cause a high national harm.[3]

Triage

3.5 (U) The NCSC formally triages all incident records to assess the level of significance and determine what actions to take to investigate and respond to the malicious cyber activity.

3.6 (U) As part of this process, the NCSC assigns each incident a category that considers the known or likely impact of the incident, the type of victim affected, and any exceptional circumstances that may warrant flagging the incident for particular attention. Incidents range from "C6 – Minor Incident" to "C1 – National Cyber Emergency".

3.7 (U) The triage and categorisation of incidents is intended to support timely decision making to enable response actions to prevent harm. Triage decisions often need to be made based on incomplete information and using the technical subject matter expertise and operational experience of NCSC staff.

[2] (U) The NCSC defines cyber security incidents as, occurrences or activity that appears to have degraded the confidentiality, integrity, or availability of a data system or network.
[3] (U) In April 2024, one of the NCSC's suite of detection services identified over 350,000 alerts of potential malicious activity affecting New Zealand, that were triaged by NCSC analysts. From these alerts, five incidents were raised.

Response

3.8 (U) The objective of the NCSC's response is to mitigate and remediate the threat posed by malicious cyber activity. The NCSC will conclude its response and close an incident ticket once it has exhausted options for taking actions that will support mitigation and remediation; or where any remaining actions would be disproportionate to the threat posed by the malicious cyber activity.

3.9 (U) NCSC incident response staff determine the response actions to pursue based on their technical knowledge and previous experience, taking into account:

a. the category assigned to the incident, which is based on the scale and impact of the activity;

b. the extent to which the incident has implications for nationally significant organisations and national security. This includes consideration of the nature of the malicious cyber actor[4] (where this is known or suspected);

c. the ability of the victim organisation of the malicious cyber activity to independently mitigate or remediate the threat, including through commercial service providers;

d. the willingness and ability of the victim organisation to work with the NCSC; and

e. the resources and capability that the NCSC has available to respond.

3.10 (U) The NCSC's response actions could include:

a. passing information to a possible victim organisation to enable them to take action;

b. referring the incident to another agency to respond;

c. engaging with potential victim organisations to provide incident response support;

d. making use of the NCSC's capabilities to disrupt the potential malicious cyber activity; and

e. using the insights from the incident to support the development advice, guidance and broader commentary on the cyber threat landscape to help inform and protect a wider range of potential victim organisations.

3.11 (U) The NCSC may be limited in the information that it can use or disclose when responding to an incident due to restrictions related to classified or otherwise confidential information.

Prioritising engagement with those best placed to mitigate the threat

3.12 (U) The NCSC's response actions have typically prioritised engagement with the organisations and entities who are best placed to undertake the technical actions needed to investigate, mitigate, remediate malicious cyber activity, and undertake direct engagement with individual users of their systems.

Working alongside other New Zealand government agencies

3.13 (U) The NCSC works with other New Zealand government agencies where the incident relates to the functions of that agency, and where it may be appropriate for that agency to either take the lead, or work alongside the NCSC in responding to the incident.

[4] (U) Of the 316 incidents recorded by the NCSC in the 2022/23 financial year, 23% of these had links to suspected state-sponsored actors.

3.14 (U) The NCSC may engage with Police if there is evidence of criminal offending that can be investigated. Police may engage with any affected individuals in the course of conducting such an investigation.

3.15 (U) The NCSC may engage with the NZSIS where malicious cyber activity may represent a wider counter-intelligence or foreign interference threat, *[text deleted*], or where there is no imminent risk to information or systems.

3.16 (U) To support this engagement, the NCSC leads a weekly interagency operational meeting which includes representatives from government agencies that have a role in the triage and response to cyber security incidents[5]. The intent of this forum is to identify areas where another agency may be able to support the response to a specific threat or incident.

3.17 (U) For all incidents that are categorised as a "C3 – Significant" or above, the NCSC considers whether or not it is appropriate to escalate the incident as part of an activation of New Zealand's National Security System. This system is led by the Department of Prime Minister and Cabinet's Strategic Crisis Management Unit. The protocol and considerations around escalation are detailed in New Zealand's Cyber Security Emergency Response Plan (CSERP).[6]

Wider actions to address the threat of malicious cyber activity

3.18 (U) Alongside the direct response to incidents through engagement with victim organisations, the NCSC takes a wide range of other actions to protect New Zealand against malicious cyber activity. These include:

a. operating capabilities to disrupt malicious cyber activity, such as the "Malware Free Networks" (MFN) service;

b. hosting security information exchanges to support information sharing and collaboration on cyber security matters amongst New Zealand organisations;

c. setting standards and producing advice and guidance to support New Zealand public sector and wider organisations to protect themselves against malicious cyber activity; and

d. providing bespoke briefings about cyber threats and cyber security measures to key individuals and groups.

3.19 (U) These wider actions are informed by the NCSC's understanding of cyber threats to New Zealand – including the NCSC's experience responding to incidents of malicious cyber activity. Many of these activities are able to be carried out at scale, protect a wide range of potential victims, and are more scalable than incident response and engagement. These measures intend to avoid, prevent and mitigate incidents before they can cause harm.

The NCSC's approach to triaging and responding to malicious cyber activity related to foreign state-sponsored actors targeting New Zealand individuals

3.20 (U) The NCSC's current procedures do not specifically prescribe the actions the NCSC will take to respond to reports indicating foreign state-sponsored actors that may be targeting identified New Zealand individuals.

3.21 (U) Instead, the fact that activity may be conducted by a foreign state-sponsored actor, or may be targeted at an identified New Zealand individual are factors that are considered in the

[5] (U) This includes representatives from New Zealand Police, the New Zealand Security Intelligence Service, the Department of Internal Affairs, and the NCSC and CERT NZ.
[6] (U) Available at www.dpmc.govt.nz/publications/new-zealands-cyber-security-emergency-response-plan

course of NCSC's normal triage and response actions. No single factor related to an incident determines the NCSC's categorisation or response actions, the NCSC's approach aims to consider all relevant dimensions of an incident based on the information it has.

3.22 (U) The fact that activity is targeted at an individual is unlikely to lift the NCSC's overall categorisation of an incident; an incident would need to affect a large number of individuals or relate to a significant compromise of a high-profile individual (such as a government minister) to result in a higher categorisation. The NCSC may consider the identity of an affected individual and the implications of the incident for them as part of deciding what response actions to take.

Notifying the Minister Responsible for the GCSB

3.23 (U) The NCSC currently considers notifying the Minister Responsible for the GCSB of incidents on a "no-surprises" basis, and expects staff and leaders to identify and escalate situations where a notification may be required as part of the obligations of accountable public officials.

3.24 (U) Examples of circumstances when the NCSC has notified the Minister Responsible for the GCSB of cyber security incidents are:

a. publicly known incidents where the Minister may be asked to confirm whether the NCSC is involved in the response;

b. the compromise of networks of significant government agencies by a state-sponsored actor;

c. the compromise of a database held by a private sector company containing a large volume of personal information of New Zealanders;

d. major public incidents of ransomware of New Zealand systems; and

e. in the early stages of responding to an incident where there may be a significant compromise or need for a major NCSC response.

Section 4 - Areas for Improvement

4.1 (U) This section sets out observations and areas for improvement related to the NCSC's current approach for responding to reports of malicious cyber activity involving foreign state-sponsored actors targeting identified New Zealand individuals. It provides a number of recommendations where procedures and practices can be improved.

4.2 (U) The NCSC should look to make improvements in the following three areas.

a. The NCSC's response to incidents needs to ensure due consideration is given to wider implications of cyber security incidents, and not focus solely on the technical response to such incidents.

b. Where appropriate, the NCSC should consider some form of engagement with individuals in response to cyber targeting by foreign state-sponsored actors.

c. Identifying incidents that may be appropriate to brief to the Minister Responsible for the GCSB.

The NCSC's response to incidents needs to ensure due consideration is given to wider implications of cyber security incidents, and not focus solely on the technical response to such incidents

4.3 (U) The NCSC's current policies, practices and standard operating procedures relating to the identification, triage, and response to cyber security incidents focus on understanding and responding to the technical cyber security threat posed by malicious cyber activity. This focus aligns with the NCSC's expertise and pre-integration mandate.

4.4 (U) The NCSC generally brings incidents to the attention of NZSIS or Police if an incident has wider national security implications or form the basis for a criminal investigation and, in the past, CERT NZ where they were not related to nationally significant organisations or high impact malicious cyber activity. The NCSC has also previously co-ordinated with other agencies who have led the non-technical response to a cyber incident, such on privacy or business continuity consequences of the incident.

4.5 (U) There are some mechanisms for the NCSC to regularly co-ordinate with other agencies, such as the regular interagency operational meeting and, in the past, by other agencies seconding staff into the NCSC. However, any information exchange and co-ordination typically occurs because of the initiative, experience and judgement of NCSC staff, rather than because they are required as a part of clear procedures or practice.

4.6 (U) Recommendation 1: The NCSC, in consultation with other key New Zealand Government agencies, should develop guidance for NCSC staff on bringing incidents to the attention of those agencies in circumstances where the incident may have wider implications for New Zealand's interests.

4.7 (U) Most individuals will have an interest in knowing that a state-sponsored actor has targeted them with malicious cyber activity. Malicious cyber activity targeted at an individual may also reflect a wider threat to the safety or security of an individual. The NCSC's pre-integration focus on the response to malicious cyber activity affecting nationally significant organisations' network security means the consequences for any individual targeted have not been prominent considerations in the incident triage and response process.

4.8 (U) Recommendation 2: The NCSC should amend its procedures to ensure that, when responding to incidents where state-sponsored malicious cyber activity is targeted at

individuals, implications of that activity for the affected individuals is factored into the NCSC's response to the incident.

Where appropriate, the NCSC should consider some form of engagement with individuals in response to cyber targeting by foreign state-sponsored actors

4.9 (U) The NCSC's traditional remit and corresponding procedures and practice meant it has prioritised engagement with nationally significant organisations in response to incidents. This includes where individuals have been targeted, in which case the NCSC prioritises engagement with the organisation that administers the IT systems or networks that may have been affected by malicious cyber activity[7]. While the NCSC has a range of policies, practices and guidance documents for the identification, triage, and response to cyber security incidents and engaging with nationally significant organisations, these do not point the NCSC towards engaging directly with individuals who are targeted by foreign state-sponsored cyber actors. This means the NCSC rarely takes action to engage directly with such individuals.

4.10 (U) As noted above, individuals are likely to have an interest in knowing that a state-sponsored actor has targeted them with malicious cyber activity. Notifying individuals that they have been targeted by malicious cyber activity may help those individuals to more tangibly understand the threat posed by malicious cyber activity, assess the implications that it may have for them personally, and take actions to reduce the risk or impact of malicious cyber activity against them. Individuals may also have information to share with the NCSC.

4.11 (U) Recommendation 3: The NCSC should adjust its procedures for responding to cyber security incidents so consideration is given to the NCSC or another agency undertaking some form of engagement with individuals who may have been targeted by foreign state-sponsored malicious cyber actors.

4.12 (U) That engagement may be carried out by the NCSC, or the NCSC may recommend that it be conducted by, or alongside, another organisation (such as the NZSIS or the organisations that administer or secure the individuals' IT systems).

4.13 (U) This does not mean the NCSC or another agency should directly engage with all affected individuals on every occasion, nor in pre-defined circumstances, or in relation to particular classes of people. Instead, the decision on whether or not to engage with an individual needs to be made on a case-by-case basis, weighing the reasons for engagement against the NCSC's capacity and capability to undertake direct individual engagement.

4.14 (U) There may be classification or practical constraints that determine what information the NCSC or another agency may share with an individual.

4.15 (U) The NCSC does, alongside other agencies, undertake protective cyber security briefings for specific individuals who may be at higher risk of malicious cyber activity. The NCSC does not currently have any publicly available guidance specifically for individuals who may be at increased risk of targeting by state-sponsored actors as part of its wider work to protect

[7] (U) The vast majority of these incidents relate to targeting of email addresses associated with individuals. These accounts are typically provided and administered by a separate organisation and not administered and directly owned by the individual. For example, email accounts provided and administered by their place of work.

against malicious cyber activity.[8] This means these individuals may not be able to easily access information about the actions they can take to protect themselves against such activity.

4.16 (U) Recommendation 4: The NCSC should publish specific guidance for individuals who may consider themselves to be at risk of targeting by foreign state-sponsored cyber actors.

Identifying incidents that may be appropriate to brief to the Minister Responsible for the GCSB

4.17 (U) While it is outside the scope of this review to consider the full range of circumstances in which GCSB briefs the Minister, the review did look at the circumstances in which the NCSC provides to the Minister about cyber security incidents.

4.18 (U) It is not possible to prescribe all of the circumstances in which it may be appropriate for the NCSC to brief the Minister about incidents. As public servants, staff within the NCSC must have sufficient awareness and exercise judgment about the issues it may be appropriate to brief the Minister about, and must be able to escalate those matters to leadership.

4.19 (U) The NCSC and the wider GCSB performs its operational functions independently and impartially,[9] with briefings to the Minister provided under the "no surprises" principle,[10] and as otherwise needed to support effective democratic oversight of the GCSB.[11] The Minister may also express expectations about when the GCSB will provide briefings.

4.20 (U) Recommendation 5: The NCSC should re-confirm its approach to briefing the Minister Responsible for the GCSB about cyber security incidents, incorporating the Minister's expectations about when incidents should be escalated to her office.

[8] (U) The NZSIS does produce a range of guidance related to protection against foreign interference, available at www.protectivesecurity.govt.nz/campaigns/protection-against-foreign-interference
[9] (U) Intelligence and Security Act 2017, s 17(b).
[10] (U) Cabinet Manual 2023, at [3.26].
[11] (U) See Intelligence and Security Act 2017, s 17(d).

Section 5 - Sufficiency of the NCSC's Response to [*reported activity*]

5.1 (U) The following section sets out a timeline overview of the NCSC's response to [*reports of possible foreign state cyber activity targeted at New Zealand members of IPAC]*, and observations about whether this was sufficient based on the information to hand at the time and the recommendations in Section 4.

5.2 (U) As noted at paragraph 2.8, the timeline below is based on the NCSC's written records of its response to incidents and discussions with staff who were involved in response actions.

June 2021 – concerns are raised via Parliamentary Service to the NCSC

5.3 (U) In June 2021, the Parliamentary Service advised the NCSC that a Member of Parliament who was also a member of IPAC had raised concerns about possible malicious cyber activity against IPAC members. The NCSC opened an incident ticket related to the matter.

5.4 (U) The incident was triaged as a "C5 – Routine Incident" given it related to scanning, reconnaissance or a potential threat. Following some initial clarifying discussions with the Parliamentary Service, the NCSC engaged with the NZSIS about the matter, in response to which the NZSIS provided the NCSC with classified intelligence reporting from [*an international partner agency*]. The NCSC understood that NZSIS would provide the same classified reporting to the Parliamentary Service, which occurred in early July 2021.

5.5 (U) Based on the classified intelligence reporting, the NCSC undertook analysis to assess the likelihood of malicious cyber activity against New Zealand, or identify any such activity. This resulted in no indications justifying further investigation.

5.6 (U) In late June 2021, the NCSC advised the Parliamentary Service that the NCSC did not have any material information to update. At this time, the Parliamentary Service confirmed that they were not expecting any further assistance from the NCSC, and noted that the Parliamentary Service raised the matter only for the NCSC's awareness.

5.7 (U) The NCSC closed the incident ticket in mid-July 2021.

April 2022 – the NZSIS provides the NCSC with a classified report from an international partner agency

5.8 (U) In April 2022, the NZSIS passed the NCSC a classified intelligence report from [*an international partner agency related to possible malicious cyber activity against IPAC members*]. It did not explicitly reference any targeting of New Zealand individuals.

5.9 (U) The NCSC undertook analysis to identify whether any of the reported activity affected New Zealand, which resulted in no indications justifying further investigation. The NCSC did not open an incident ticket and took no further actions.

June 2022 – an international partner agency provides information to New Zealand Police and the NZSIS

5.10 (U) In June 2022, [*an international partner agency*] informed Police and the NZSIS [*about possible foreign state cyber activity that may have affected New Zealand members of IPAC*].

5.11 (U) NZSIS passed the information to the NCSC to lead on incident response actions. When doing so, the NZSIS asked to be kept updated on the NCSC's actions [*text deleted*].

5.12 (U) The NCSC opened an incident ticket on the basis of the information, and triaged the incident as a "C5 – Routine Incident" given it related to scanning, reconnaissance or a potential threat.

5.13 (U) [*The NCSC engaged with the Parliamentary Service about the reported malicious cyber activity]*. The NCSC prioritised [*engagement with the Parliamentary Service*] due to the NCSC's pre-existing relationship with the Parliamentary Service.

5.14 (U) Based on engagement with the Parliamentary Service, the NCSC assessed that [*the reported activity was likely to have been prevented by existing Parliamentary Service security arrangements*].

5.15 (U) The NCSC carried out open source research into [*another system that may have been affected by the reported cyber activity*] and assessed that [*any such activity was unlikely to have been successful*].

5.16 (U) The NCSC considered taking actions in relation to [*one individual who may have been affected by the reported cyber activity*]. NCSC staff assumed the individual was likely aware of the risk of targeting by foreign state-sponsored actors and would already be taking appropriate security measures.

5.17 (U) The NCSC briefed this incident and the response actions being taken at two inter-agency meetings in July 2022 and August 2022. This briefing included representatives from the NZSIS and Police. No concerns were raised about the approach being taken.

5.18 (U) The NCSC closed the incident ticket in early August 2022.

August 2022 international partner corrects information provided

5.19 (U) In August 2022, the [*international partner agency that provided information in June 2022*] corrected the information they had provided to the NZSIS and Police [*text deleted*].

5.20 (U) The NCSC did not re-open the previously closed incident and took no further actions based on the corrected information.

May 2024 correspondence, media coverage and the NCSC response

5.21 (U) In May 2024, the NCSC received correspondence [*from an international partner agency*]. This coincided with media coverage in New Zealand about the reported targeting of New Zealand members of IPAC.

5.22 (U) In response to the correspondence and concerns raised through the media coverage, the NCSC engaged with the affected individuals and the organisations responsible for administering the affected individuals' email accounts. This included further engagement with the Parliamentary Service to [*provide the corrected information about the malicious cyber activity reported in June 2022*]. The NCSC's engagement with all of the individuals occurred alongside the NZSIS.

5.23 (U) The NCSC engaged with the affected individuals and shared the information it had related to the reported activity. The NCSC also provided advice on steps the affected individuals could take to protect themselves from this type of activity.

5.24 (U) Following the NCSC's further engagement, the Parliamentary Service identified a number of phishing emails dating back to January 2021 received by parliamentary email addresses, and not blocked by [*Parliamentary Service security arrangements*] as previously assessed was the case. The NCSC has provided the other organisations responsible for administering the affected individuals' email accounts with technical details to enable them to identify any similar phishing emails.

5.25 (U) As it stands, the NCSC has not identified any information to indicate the phishing emails resulted in a successful compromise of any email addresses, devices, or networks. The NCSC will re-engage with organisations if they seek support in relation to any further information they discover.

5.26 (U) The NCSC briefed the Minister Responsible for the GCSB and the Inspector-General of Intelligence and Security about its planned actions in early May 2024.

Observations on the sufficiency of the NCSC's response

5.27 (U) The NCSC worked alongside the NZSIS in 2021 in relation to the [*international partner agency's*] classified report, and became aware of the 2022 [*report and correspondence from international partners*] from the NZSIS. The NZSIS asked to be kept updated on the NCSC's actions in response to the June 2022 [*correspondence from an international partner*]. The NCSC provided updates to the NZSIS and other agencies through briefings at an interagency operational meeting. Implementing the guidance in recommendation 1 will support this ongoing engagement between the NCSC and other agencies in future.

5.28 (U) The NCSC did not re-open the June 2022 ticket following the receipt of corrected information in August 2022. The review has been unable to determine whether consideration was given to re-opening the incident, or what reasons may have existed for not doing so. Re-opening the ticket and providing the [*corrected information*] to the Parliamentary Service may have resulted in the Parliamentary Service identifying the phishing emails that it subsequently identified in May 2024.

5.29 (U) The NCSC considered direct engagement with the one affected individual who the NCSC understood to have a good understanding of the threat and was assessed to likely have reasonable security arrangements in place. Therefore, the NCSC concluded additional engagement would add little value. The NCSC did not consider engagement with the other individuals until 2024.

5.30 (U) Through the NCSC's engagement with the affected individuals, each provided feedback that they would have seen value in being made aware of this activity. Once implemented, recommendations 2 and 3 will require NCSC staff to consider the implications for individuals as part of responding to incidents, and consider engagement with individuals in similar situations in the future. The action in recommendation 4 will ensure guidance is available to such individuals, even in absence of direct engagement by the NCSC.

5.31 (U) There is no record of the NCSC considering briefing the Minister Responsible for the GCSB until May 2024. Recommendation 5 will refresh the parameters for briefing the Minister about cyber security incidents, which will guide staff in the future.

No further actions recommended

5.32 (U) Under the Terms of Reference, the outcome of this review will be shared with the affected individuals.

5.33 (U) Given the further analysis and engagement that occurred in May 2024 and the intention to share the outcomes of this review with the affected individuals, no further actions are recommended at this time.

5.34 (U) If the NCSC becomes aware of further information indicating a successful compromise as a result of the reported activity, the NCSC will consider further action, including briefing the affected individuals.

Section 6 - Recommendations

(U) The recommendations in Section 4 of this report are set out below for reference.

1. (U) The NCSC, in consultation with other key New Zealand Government agencies, should develop guidance for NCSC staff on bringing incidents to the attention of those agencies in circumstances where the incident may have wider implications for New Zealand's interests.

   Anticipated timeframe for delivery: by 31 December 2024

2. (U) The NCSC should amend its procedures to ensure that, when responding to incidents where state-sponsored malicious cyber activity is targeted at individuals, implications of that activity for the affected individuals is factored into the NCSC's response to the incident.

   Anticipated timeframe for delivery: by 31 July 2024

3. (U) The NCSC should adjust its procedures for responding to cyber security incidents so consideration is given to the NCSC or another agency undertaking some form of engagement with individuals who may have been targeted by foreign state-sponsored malicious cyber actors.

   Anticipated timeframe for delivery: by 31 July 2024

4. (U) The NCSC should publish specific guidance for individuals who may consider themselves to be at risk of targeting by foreign state-sponsored cyber actors.

   Anticipated timeframe for delivery: by 30 September 2024

5. (U) The NCSC should re-confirm its approach to briefing the Minister Responsible for the GCSB about cyber security incidents, incorporating the Minister's expectations about when incidents should be escalated to her office.

   Anticipated timeframe for delivery: by 31 July 2024

Appendix A - Terms of Reference

Attached separately.