Office of the Lead Coordination Minister for the Government's Response to the Royal Commission's Report into the Terrorist Attack on the Christchurch Mosques

Office of the Minister of Police

Cabinet Social Wellbeing Committee

Cross-agency business case for a public reporting system for concerning behaviours and incidents

Proposal

1 This paper seeks Cabinet's approval of a Single Stage Business Case (SSBC) for a new public reporting system for concerning behaviours and incidents related to terrorism and violent extremism.

Relation to government priorities

2 The SSBC was developed as part of the Government's response to Recommendation 12 of Ko tō tātou kāinga tēnei: the report of the Royal Commission of Inquiry (Royal Commission) into the terrorist attack on Christchurch masjidain on 15 March 2019 (the RCOI report): *Develop and promote an accessible reporting system that enables members of the public to easily and safely report concerning behaviours or incidents to a single contact point within government.*

3 In the Speech from the Throne, the Government committed to responding to the RCOI report by working to eradicate violent extremism and foster a truly inclusive society for people from every culture, faith, and background.

4 The Government's response to the Royal Commission supports our wider goals to lay the foundations for the future and create a fairer, more equitable Aotearoa New Zealand.

Executive Summary

5 Recommendation 12 of the Royal Commission sits under the countering terrorism and violent extremism pillar of the all of government response process. This relates to encouraging public reporting on issues of potential concern relating to terrorism and violent extremism – whatever its source – to enable agencies to act early in investigating threat issues, or to refer reporters to potential support services, as appropriate.

6 For impacted communities that are affected by violent extremism or who have been or may be the target of terrorism, progressing Recommendation 12 is also a priority. Currently, these communities are uncertain about where to go for assistance and which government agency has the mandate to respond.

7 We are seeking your approval of a SSBC which recommends a new reporting system that will address these challenges by:

- providing a safe, easy, and accessible way for the public to report concerning violent extremism and terrorism-related behaviours and incidents
- improving how agencies manage and share reports of these concerning behaviours and incidents to enable a more coordinated response to national security threats
- increasing public trust and confidence in government agencies being able to effectively respond to national security threats.

8 The in-scope violent extremism and terrorism-related behaviours and incidents the public can report through the new reporting system are behaviours and incidents that show mobilisation to violence, indicate radicalisation, or early radicalisation (which are discussed further below). We are seeking your endorsement of previous ministerial decisions to this scope of behaviours and incidents for the new public reporting system.

9 We are also seeking your agreement to delegate to the Minister of Police future decisions about the branding, promotion, and education to support public awareness and use of the new reporting system. These activities will include clearly communicating to the public about which concerning behaviours and incidents will be in-scope and out-of-scope of the new reporting system and how agencies will manage and respond to in-scope and out-of-scope reports.

10 We recommend a future evaluation of the new reporting system is completed no later than 24 months after the proposed implementation date. This will enable us to better understand future demand on the new public reporting system and to ensure ongoing effectiveness. We are seeking your direction for the Minister of Police to report back to Cabinet on the outcome of this review within this proposed timeframe.

11 In April 2022, Cabinet approved $13.500 million tagged contingency funding to develop a new public reporting system [CAB-22-MIN-0129 refers]. However, as noted in the June 2023 report back, this tagged contingency did not include capital expenditure. To support successful implementation and ongoing operation, officials have advised an additional capital injection of $3.977 million is required to implement the SSBC's recommended option, with an additional $3.031 million (FY 26/27) and $0.923 million (ongoing) in operating expenditure to fund the depreciation and capital charge.

12 We are currently considering funding options to cover the total implementation and operating costs for the new reporting system, and we will report back to Cabinet at a later date to seek necessary approval of required funding.

Cabinet approved funding to develop a public reporting system in response to Recommendation 12 of the Royal Commission

13 In April 2022, Cabinet approved a $13.500 million contingency initiative *Reporting System for Concerning Behaviours and Incidents* for Vote Police, for inclusion in the 2022 Budget package. Cabinet further agreed that:

- drawdown against the tagged contingency for FY2022/23 would be subject to Cabinet approval to develop a system for reporting concerning behaviours and incidents
- drawdown of funding from FY2023/24 is subject to Cabinet approval of an Implementation Business Case [CAB-22-MIN-0129 refers].

14 In August 2022, Cabinet's External Relations and Security (ERS) Committee made the decision to go forward with investment in the new reporting system when it approved the drawdown of $1.094 million in operating funding to develop a business case for the new system [ERS-22-MIN-0031 refers].

15 In June 2023, we reported back to Cabinet on progress on the SSBC [CAB-23-MIN-0226 refers]. At that time, we advised that:

- we considered Police is best placed as host agency for the new reporting system, under a cross-agency governance structure. The SSBC attached as Appendix A recommends this approach.
- the new reporting system should target reporting about behaviours and incidents that indicate mobilisation to violence and signs of radicalisation, but also accommodate reporting of early radicalisation behaviours. We are now seeking your endorsement of this scope.

16 At this time, Cabinet agreed to a further drawdown of $0.430 million against the tagged contingency to complete the SSBC.

The new reporting system will make it safer and easier for the public to report concerning behaviours and incidents and enhance New Zealand's response to violent extremism and terrorism

17 The key driver for this investment is improving the ability to manage the risk posed by terrorism and violent extremism behaviours and incidents. A new reporting system is aligned with and will contribute to New Zealand's Counter Terrorism and Violent Extremism Strategy, and the National Security Strategy, and Preventing and Countering Violent Extremism Strategic Framework.

18 The RCOI report noted all New Zealanders have a role in making New Zealand safe and inclusive[1]. The National Security Strategy emphasises the importance of harnessing the power of public reporting, to alert government agencies to previously unknown or emerging issues, so they can 'act early' to prevent unwanted outcomes. The proposed investment provides an opportunity to holistically strengthen the entire system for the prevention of

[1] See RCOI Report pages 728 and 744.

terrorism and violent extremism across the spectrum of unknown, emerging and known issues.

19 Currently, members of the public may not know where, how, why, or what to report. They may not understand the importance of the information they hold or may think agencies are too busy to respond. People may report a single incident to multiple agencies due to a lack of clarity about the role of different agencies, or because they have not had feedback about their report. Conversely, they may choose not to report as they are uncertain about which agency to report to.

20 Some people may find reporting traumatic – because they have concerns for their personal safety, the report is about a close family or community member, or they may be re-traumatised by having to explain their concerns to different agencies (sometimes on multiple occasions). Often this is exacerbated if the agencies lack the expertise to recognise and appropriately respond to cultural or religious sensitivities.

21 The RCOI report also noted an opportunity to enhance New Zealand's counter-terrorism effort by improving relevant public sector agency systems and operational practices to ensure the prevention of terrorist attacks in the future[2].

22 Restrictions on the collection and sharing of data (e.g. legislative mandates, privacy concerns, security classifications, technology limitations) mean that information held by agencies may not be easily shared with other agencies.

23 Multiple silos of data and lack of a central analysis function mean that analysis and referencing of publicly reported information is mostly manual. Agencies have no easy way of systematically knowing whether incidents are connected – either with past incidents or with incidents that another agency has information about. This means that it is harder to gain a comprehensive understanding of the terrorism and violent extremism risk.

24 The proposed investment will result in a significant improvement in customer experience by providing a dedicated reporting channel that is safe, easy, and accessible for the public to use as a single point of contact within government. This will mean the public does not have to navigate a complex national security system to know where to make reports about concerning terrorism and violent extremism-related behaviours and incidents. However, under a 'no wrong door' approach, the public will still be able to report through other channels, should they choose to do so. Agencies will work together to ensure that relevant public reporting is appropriately shared.

25 Police will engage with community advisory groups and networks to help inform the final design of the public facing components of the reporting system, such as website design, training material (to enhance cultural

[2] RCOI report, page 21.

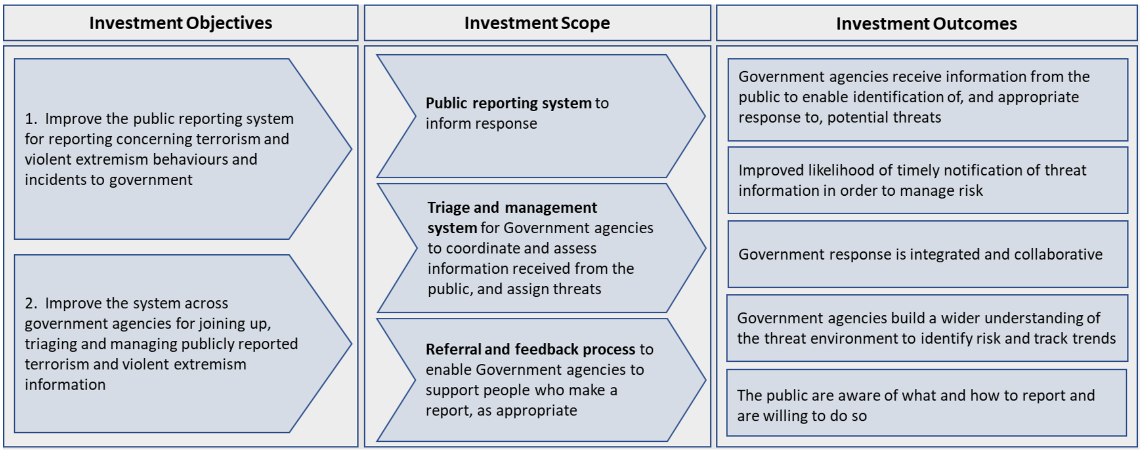
competence and diversity perspectives), the assessment process and referral process, and the content and tone of any promotional material.

26 The proposed investment will significantly improve the way that agencies manage information from public reports, by supporting intelligence discovery[3] to 'join the dots' that otherwise might not have been recognised.

Police has completed a Single Stage Business Case that recommends investment in a new reporting system

27 Police has led the development of a cross-agency business case[4], using the Treasury's Better Business Case model. As the project received a low risk profile rating and does not involve procurement, the Treasury advised the project could proceed with a SSBC. The Treasury also confirmed a Gateway review was not required for this business case.

28 The SSBC attached as Appendix A contains the Strategic Case for a new reporting system, including the case for change; the Economic Case, the recommended option for the new system; and the Commercial, Financial, and Management Cases. The table below summarises the investment objectives, deliverables and outcomes.



Investment Objectives

1. Improve the public reporting system for reporting concerning terrorism and violent extremism behaviours and incidents to government

2. Improve the system across government agencies for joining up, triaging and managing publicly reported terrorism and violent extremism information

Investment Scope

Public reporting system to inform response

Triage and management system for Government agencies to coordinate and assess information received from the public, and assign threats

Referral and feedback process to enable Government agencies to support people who make a report, as appropriate

Investment Outcomes

Government agencies receive information from the public to enable identification of, and appropriate response to, potential threats

Improved likelihood of timely notification of threat information in order to manage risk

Government response is integrated and collaborative

Government agencies build a wider understanding of the threat environment to identify risk and track trends

The public are aware of what and how to report and are willing to do so

29 The SSBC's recommended option will deliver against the investment objectives, scope, and outcomes. It will cost-effectively lift capability and capacity in the core functions of collection, triage, assessment, and assignment, and referrals (the recommended option and these functions are set out in further detail in Appendix B and Appendix C). The recommended option will achieve this for the most part by leveraging agencies' existing systems and processes and, therefore, does not require significant investment in new or advanced technologies.

[3] Discovery is a process of analysing data to surface previously unknown trends, patterns, or anomalies for further investigation.

[4] Police was supported by a cross-agency Advisory Group made up of representatives from Police, the New Zealand Security Intelligence Service (NZSIS), the Department of the Prime Minister and Cabinet (DPMC), the Department of Internal Affairs (DIA), the Ministry for Ethnic Communities (MEC), and the Ministry for Business, Innovation and Employment (MBIE). The development of the business case was overseen by a Governance Group made up of senior officials from DPMC (Chair), Police, NZSIS, DIA and MEC.

30 Even with the existing demand pressures, the SSBC recommends that Police is the host agency, under a cross-agency governance structure. Under the draft operating model, Police will carry out the information collection and triage functions and refer the public for wellbeing support if appropriate. The discovery or 'join the dots' function will continue to be carried out by the New Zealand Security Intelligence Service (NZSIS), using some of the information gathered as part of the new reporting system.

31 The SSBC has been endorsed by the Commissioner of Police and the Chief Executives of the Department of the Prime Minister and Cabinet (DPMC), NZSIS, Department of Internal Affairs (DIA), and Ministry for Ethnic Communities (MEC).

Implementation of the new reporting system

Confirming the scope of behaviours the public can report through the new reporting system

32 In August 2022, Cabinet agreed the business case should, amongst other things, confirm "the range of national security harms, incidents and behaviours that are included in a new reporting system through engagement with communities and with national security agencies" [ERS-22-MIN-0031 refers].

33 National security harms can cover a range of issues (e.g. foreign interference, mis- and dis-information) and are much broader than the terrorism and violent extremism focus of the RCOI report.

34 In December 2022, the then Minister of Police provided direction on the scope of behaviours and incidents the public would be asked to report through the system. The SSBC proceeded on the basis that the focus of the reporting system should be on terrorism and violent extremism-related behaviours and incidents.

35 The current legislative and policy mandates of operational agencies (i.e. Police and NZSIS), discussed further below, define criminal thresholds and the parameters for operational activity that also constrain the scope of behaviours these agencies can respond to.

36 We are seeking Cabinet's endorsement of the following terrorism and violent extremism-related behaviours and incidents which will inform the scope of the new reporting service. These include:

- **behaviours and incidents that show mobilisation to violence:** these behaviours have reached the threshold for unlawful activity (and for action by agencies). Examples include physical assaults, arson, and Terrorism Suppression Act 2002 offences such as planning or preparing to carry out or carrying out or facilitating a terrorist act.

- **behaviours and incidents that indicate radicalisation:** these are the behaviours that are identified in the *Kia mataara ki ngā tohu Know the signs* indicators released by the NZSIS in October 2022. Examples include accessing violent extremist content, engaging with violent extremist individuals or groups, and declaring intent to conduct a terrorist or violent extremist act.

- **early radicalisation behaviours:** these are behaviours where an individual may be radicalising towards the use of violence or displaying indicators of hateful extremism – that normalises the use of threatening or violent behaviour as a 'legitimate' course of action to further their extreme beliefs. Examples include individuals with a hostile worldview (e.g. 'us versus them') who make dehumanising or violent statements against 'others' whom they perceive as 'the enemy'.

37 It is likely the public will use the new reporting system to report a wider range of harms and behaviours[5], that sit outside current agency response mandates and fall below the threshold of terrorism and violent extremism-related behaviours and incidents described above (out-of-scope reports).

38 As part of the system design, there will be specific processes for managing out-of-scope reports, including how Police will use and retain information, which is discussed further below. This will include acknowledgment when a report is received and high-level feedback on the outcome or actions taken on the basis of that report. Appendix C also sets out how information will flow through the reporting system – including how Police will collect, triage, assess, and action reports, and where and how long Police will retain information. Scenario 1 in Appendix C notes the processes for out-of-scope reports.

Police and NZSIS mandates for countering terrorism and violent extremism will determine the level of response and the use and retention of information

39 Police and NZSIS are the lead domestic agencies for counter terrorism and Police is often the lead agency for the operational response to a range of events that can occur with little or no warning, including terrorist incidents. Police works closely with its domestic and international partners, including sharing intelligence, to deliver our lawful functions set out under Section 9 of the Policing Act 2008, which include national security.

40 NZSIS's mandate in relation to countering terrorism and violent extremism is defined under Section 10 of the Intelligence and Security Act 2017 (ISA), which sets out the NZSIS functions to collect and analyse intelligence in accordance with New Zealand Government priorities. The NZSIS works closely with domestic agencies, in particular the Government Communications Security Bureau and Police. The NZSIS assists these agencies in matters

[5] For example, harms and behaviours identified in the RCOI report and are consistently reflected in the daily lived experience of members of impacted communities across New Zealand. This can include targeted mis/dis-information campaigns, religiously and/or ethnically motivated harassment and abuse, racism, and micro-aggressions.

relating to national security, conducting joint operational work, protective security, and threat mitigation.

41 DIA operates a Terrorist and Violent Extremist Content objectionable content removal regime which aligns and contributes to Police and NZSIS counter terrorism risk management measures and actions (refer Appendix C).

42 Police acknowledges there may be concerns about potential overreach of its mandate. This is especially with regards to the collection and storage of information that, while it may not immediately relate to criminal activity, may be useful for intelligence purposes.

43 Police intends to only use information collected through the new reporting system to:

- assess and identify national security threats and detect and help prevent harm from terrorism and violent extremism
- assist those making reports and people at risk of radicalisation to access appropriate support
- support the intelligence discovery function of the NZSIS – to retain information under the intelligence collection and analysis provisions of the ISA - so that agencies can better 'join the dots' to prevent and respond to emerging national security threats.

44 Police will design a rigorous process to comply with the Privacy Act 2020 – including ensuring information is collected for a lawful purpose connected with a function of Police, and collection is necessary for that purpose. Police has completed a preliminary Privacy Impact Assessment (PIA) to inform the system design phase, including developing sufficient controls to mitigate privacy risks (e.g. information retention processes for out-of-scope reports). Police will continue to engage with the Office of the Privacy Commissioner to manage privacy risks and complete a more detailed PIA after confirming detailed system design.

45 Fundamental to the design of the system will be a measured and proportionate approach. This will include verifying and quality checking the nature, strength and validity of reports for **criticality** (to assess whether an immediate response is required), **relevance** (whether the behaviour or incident in the report falls within the scope of the reporting system), **credibility** (the report is not false, vexatious, or malicious) and **actionability** (the report meets the threshold for agency response).

46 Only reports that meet this acceptance criteria will be accepted as in-scope and entered into a system of record. Biographical detail will be entered into the National Intelligence Application (NIA) used by Police, but access to the context and background information of the report will be restricted. For example, information reported that is assessed to be malicious (subject to review for any other relevant circumstances) will not be entered into NIA, retained or shared with other agencies.

47 Appendix C provides further detail about how Police will collect, triage, assess, and action reports, including where these checks will occur in the process and when Police will share and retain information.

48 Reports that are not assigned for further action (out-of-scope reports) may be referred to wellbeing support providers for general assistance or closed. Police may also refer out-of-scope reports to other agencies and reporting channels where appropriate. For example, referring out-of-scope reports about harmful online content to DIA.

49 Some information (i.e. reports that meet the criteria to be triaged in) will be shared with NZSIS, as NZSIS will continue to carry out the discovery or 'join the dots' function, as it does now under current functions. This requires information to be retained as reference data, until such time when it is surfaced if it is matched with another piece of relevant information.

Branding, promotion, and education to support public awareness and use of the new reporting system

50 Subject to approval of the SSBC, the project will develop a brand, and communications and educational material as part of the implementation phase. This work will be guided by the following principles.

- The audience for the messaging is everyone in New Zealand, as everyone has a role to play in preventing terrorism and violent extremism.
- Communications will be clear about the types of behaviour and incidents that are in scope, and which are out of scope.
- Explicit reference will be made to the system's consideration of human rights and privacy principles.
- Communications collateral will include information about what agencies will do with the reports (e.g. how long information will be kept and why).
- To ensure equity of access for communities, the project may target some engagement and resources (e.g. collateral in various languages).
- Communications will leverage existing arrangements across government as much as possible (e.g. the counter-terrorism hui, engagement on the National Security Strategy).
- Promotion should be proportionate to the threat level.
- The reporting system will use all of government branding (i.e. a '.govt.nz' web address), to reflect the cross-agency nature of the service.

51 We are seeking your agreement to delegate any future decisions about the final branding, launch, and ongoing promotion of the new reporting system to the Minister of Police following further decisions by Cabinet about any source of additional funding necessary to launch the project.

There is uncertainty about the future level of demand for the new reporting system

52 The RCOI report identified the need for a single point of contact for the public to report concerning behaviours and incidents. Agencies that currently receive these types of reports have different approaches to capturing data, which means there is no consistent data about current levels of demand, or trend data that might help with projecting demand in future.

53 Current reporting rates suggest the public makes around 110 reports per week across agencies regarding issues relating to extremist harm. However, looking at other like-minded jurisdictions (e.g. England and Wales), where discriminatory and hate crimes are recorded, shows that they have significant under-reporting of these issues, with only five to 15 percent of behaviours related to extremist harms likely to be reported.

54 Assuming our reporting rates are similar, officials anticipate the design of an easy, safe, and accessible channel, and promotion and education to the public about what and how to report could increase the number of reports to 220 to 275 reports per week. This would result in reporting rates of about 20 to 25 percent, which reflects overall rates of crime reporting in New Zealand[6].

55 Police will build a level of service to respond to this level of reporting demand, adjusting the level of service if rates are higher. This may result in, for example, a backlog in assessing reports, or tighter prioritisation in the triage process.

56 Police will leverage existing Police technology as much as possible. Consequently, the SSBC identifies a minimal investment in basic workflow and case management technology, subject to testing workflow and subsequently adjusting these process technologies so that they are fit to meet future demand.

Implementation timeline

57 Pending approval of the SSBC now and approval of required funding in future, the project is expected to take 12 months to implement the new reporting system.

Transparency

58 Over time, the new reporting system will generate an important evidence-base of the number and types of incidents New Zealanders witness or experience relating to extremism. This aggregated information will be of value to academic researchers (including He Whenua Taurikura, New Zealand’s Centre of Research Excellence for Preventing and Countering Violent Extremism) and communities, to inform our understanding of the impact and any changes in terrorism and violent extremism in New Zealand. An annual report will also be published, outlining details on the use and performance of the new reporting system.

[6] New Zealand Crime and Victims Survey 2021.

Future review of the new reporting system

59 There are several unknowns with establishing a new reporting system. Previously, when Police launched the 105 non-emergency reporting channel, instead of diverting demand from the existing 111 emergency channel, there was an overall increase in demand on Police reporting. As discussed above, the future level of demand for the new reporting system is uncertain, and based on several assumptions, and there is also uncertainty about the proportion of in-scope and out-of-scope reports, and value of reports Police will receive. The current costs for the new reporting system do not include contingency for a significant increase in demand above current predictions.

60 Given the level of uncertainty around a new reporting system, we recommend an evaluation and review of the system be completed no later than 24 months from the start of operation. This will provide an evidence base to support future planning and any additional funding requirements. This review should consider:

- the number of reports received by the reporting service
- the scope of behaviours and incidents the public has reported
- level of public awareness of what and how to report
- the effectiveness of privacy and human rights considerations
- feedback from the public on customer experience when using the service
- the number and significance of cases assigned to the national security system for further investigation and the prevention of extremist harm
- the number of referrals to well-being providers and dis-engagement services
- the evolving information environment (e.g. the use of Artificial Intelligence in reports)
- any additional resources that may be required so agencies can adequately respond to reports that are assigned to them for response.

61 The review will inform any necessary modifications to the service in terms of technology enhancements and resource needs (e.g. a case management system that spans multiple agencies and is integrated with current systems).

62 Following the evaluation, agencies (including but not limited to Police) may seek additional funding for investment in resources to operate the reporting system and for agency response activities.

Cost-of-living Implications

63 There are no cost-of-living implications for the proposals in this paper.

Financial Implications

64 Operating costs for the new reporting system fall within the remaining tagged contingency. However, as signalled in our report back in June 2023, the total $13.500 million tagged contingency did not include any provision for capital expenditure.

65 Additional capital funding of $3.977 million will be required to implement the recommended option in the SSBC. This funding will be used for investment in workflow and case management systems.

66 The impact of the capital expenditure on the ongoing operating costs will also require an uplift of $3.031 million (FY 26/27) and $0.923 million (ongoing) to fund the depreciation and capital charge.

67 We note Police is unable to absorb these additional costs into existing baseline due to existing demand pressures. We are currently considering funding options to cover the total implementation and operating costs for the new reporting system, and we will report back to Cabinet at a later date to seek necessary approval of required funding.

Legislative Implications and impact analysis

68 There are no legislative implications for the proposals in this paper.

69 A regulatory impact statement is not required to support the proposals in this paper.

70 A Climate Implications of Policy Assessment is not required for the proposals in this paper.

Treaty of Waitangi implications

71 We acknowledge the Crown’s Treaty responsibilities and the importance of the Māori Crown relationship. This includes the duty to act reasonably and in good faith and for the Crown to actively protect the interests of overlapping groups.

72 The new reporting system will contribute to the Crown’s delivery on these responsibilities in a way that supports tikanga and cultural values. This includes providing a mechanism to acknowledge the harm experienced by Māori and other ethnic and minority groups disproportionately affected by violent extremism and terrorism, empower them to safely report concerning behaviours and incidents, and provide pathways to support services. The proposed agency triage process will also include specific controls that will mitigate the risk of undue public surveillance and false or malicious reporting on Māori.

73 In addition, He Ara Waiora[7] provides an opportunity to consider more broadly the investment in a new public reporting system will contribute to the wellbeing concepts of mana tuku iho (mana deriving from a strong base of identity and belonging) and manu tauutuutu (mana found in knowing and fulfilling one's rights and responsibilities to the community, and in the participation and connectedness of an individual in their community). He Ara Waiora principles will be purposefully incorporated in the system design.

74 Police has engaged with Iwi Chairs Forum representatives on the response to Recommendation 12 and will continue to engage with Māori on the detailed design of the reporting system, including controls to mitigate risks of discrimination and stigmatisation.

Population Implications

75 The new reporting system will provide a safe, easy, and accessible point of contact for members of the public to report concerning incidents and behaviours.

76 It will offer benefits for all New Zealanders through improved public safety and reduced risk of harm, and by improving the likelihood that agencies will receive timely notification of threat information.

77 In particular, the new system will offer benefits to members of religious, ethnic, and other impacted communities (e.g. Rainbow communities) across New Zealand who may be disproportionately affected by incitement of hateful extremism, or who may be the target of violent extremism. These communities see the RCOI report as responding to an environment where – due to tightly defined agency operating models – these communities may find it difficult, confusing, or intimidating to report concerning behaviours and incidents they experience in their everyday lives.

78 The new reporting system may have the potential to securitise or stigmatise some communities. To counter this, as indicated above under discussion of agency mandates and Treaty of Waitangi implications, the new reporting system will be designed in such a way as to be sensitive to and minimise the impact of any biased, vexatious, and inappropriate 'over-reporting' of some communities. As part of the triage process, agencies will consider the nature of any report, including assessing for any explicit or implicit bias, organised or systemic reporting or advocacy for a particular agenda, and ill-defined or vexatious intent.

79 Police will continue to work with stakeholder groups – including those from impacted communities – to ensure that public concerns and aspirations are consistently understood and considered in the design and implementation phases of the new system.

[7] He Ara Waiora is a waiora (wellbeing) framework developed by Treasury, built on te ao Māori knowledge and perspectives of wellbeing.

Human Rights

80 Police will be engaging with the Human Rights Commission (HRC) to develop appropriate controls to address any human rights implications, including meeting legislative requirements under the Human Rights Act 1993 and New Zealand Bill of Rights Act 1990 (NZBORA), as part of the detailed design of the new reporting system. This includes balancing the right to freedom of expression protected under NZBORA and the right to freedom from discrimination by providing mechanisms to filter out-of-scope reports while also ensuring protection from over-reporting for certain – especially impacted – communities.

81 Police and HRC will also work together on how they might share information about appropriately responding to advocacy campaigns or vexatious reporting issues once the new system is operating.

Privacy implications

82 We acknowledge the following Privacy Commissioner statement that expresses concerns about the privacy implications of the new reporting system and how agencies will appropriately manage information.

> *A public reporting system that facilitates the collection and recording of sensitive personal information by Police to be shared with an intelligence agency carries significant privacy risk. I have not seen sufficient evidence to show that this would be the most effective and proportionate solution to the problem identified. Officials at Police have worked with my Office to understand and mitigate some of these risks and an evaluation of this system at 24 months would appear to be appropriate given a number of identified uncertainties about reporting demand, the value of the reports to Police / intelligence agencies, and the number of out-of-scope reports. However, I still have concerns about the design of this reporting system, in particular, the scope of behaviours to be reported through the system appears to be over-broad. Police have not demonstrated that the collection of lower-level behaviours is necessary to address the policy problem this reporting system is intended to address. I recommend that further work is undertaken before the scope of behaviours to be reported on is endorsed by Cabinet, to avoid unnecessary overcollection of very sensitive personal information, and the harm to personal privacy and public trust this may entail.*

83 We are satisfied the scope of behaviours we are seeking your endorsement of is clear about the types of behaviours and incidents that agencies can action and is narrow enough to mitigate the risks highlighted by the Privacy Commissioner. We are confident the proposed triage process and controls that Police will be building into the system to manage out-of-scope reports, along with proposed public communications will reduce the risk of overcollection and retention of personal information that agencies do not need to hold or use. Furthermore, this activity is essentially no different to the processes already applied in Police where public reporting is received, assessed and responded to on a daily basis.

84 We also note that delaying Cabinet endorsement of the scope of behaviours and incidents will likely require a re-working of the SSBC, thereby significantly delaying implementation of the new reporting system. We understand impacted communities, through Police engagement with community representatives, have indicated progressing the response to Recommendation 12 and having a safe, easy, and accessible reporting channel is a priority. There is likely to be frustration and concern if there are further delays.

Use of external resources

85 The development of the SSBC utilised the following external contractor and consultant resource:

Qty	Duration	Type	Service Provided	Reason
1	9 months	Contractor	Project delivery expertise	
1	12 months	Contractor	Policy advice; business case writer	
1	6 months	Contractor	Change management and communications	
1	4 months	Contractor	ICT project delivery expertise	
1	2 weeks	Consultant	Quality assurance on demand analysis and cost model for SSBC	Independent quality assurance; expertise

86 For the project implementation phase, Police will leverage the existing workforce capacity and capability as much as possible, but some use of contractors in specialist service roles may be necessary. The below table highlights where external resources may be required. Due to the project start date and short-term duration, some roles may not be fulfilled by Police resources due to prior commitments on resources.

Qty	Duration	Type	Service Provided	Reason
1	12 months	Contractor	Project delivery expertise	External contractors to be sought should the project requirement exceed internal capacity / capability – to be confirmed at project set up phase
1	12 months	Contractor	Senior business analysis	
1	12 months	Contractor	Project coordination	
1	10 months	Contractor	Change management and communications	
2	12 months	Contractor	Workstream Lead Engagement and Workstream Lead Service Design	
1	3 months	Contractor	Recruitment coordination	
1	3 months	Contractor	Organisational design	
1-3	12 months	Contractor	Community input to service design	Part of community engagement activities
1	6 months	Contractor	Diversity and cultural subject matter expertise	

1-2	3-6 months	Consultant / Contractor	Content development and graphic design creation	Likely to be short term Statement of Work for specialist input / products
1	4-6 months	Consultant / Contractor	User experience (UX) design	
1	TBC	Consultant	Brand design / website development	
1	TBC	Consultant	Training and translation material development	
Var-ious	TBC	Vendor	Design and configuration of workflow technologies	Amendment to existing Police Master Service Agreement
1	4 weeks	Consultant	Independent quality assurance; expertise	External service

Consultation

87 The Department of the Prime Minister and Cabinet (DPMC); The Treasury; the New Zealand Security Intelligence Service (NZSIS); the Department of Internal Affairs (DIA); the Ministry of Business, Innovation and Employment (MBIE); Ministry of Justice, Ministry of Social Development; Ministry for Ethnic Communities (MEC); Ministry for Pacific Peoples; Te Puni Kōkiri; the Human Rights Commission, and the Office of the Privacy Commissioner have been consulted on this paper.

88 Most agencies have indicated support for progressing the new reporting system in response to Recommendation 12 of the Royal Commission. We acknowledge some agencies have expressed interest or concerns about specific aspects of the final design of the reporting system. In addition to our response to the Privacy Commissioner's concerns noted above, we understand that Police will continue engaging with agencies as part of the system design phase to manage these concerns and mitigate identified risks.

89 Developing the SSBC has been a cross-agency project, with input and advice from an Advisory Group made up of representatives from Police, NZSIS, DPMC, DIA, MEC and MBIE. A wide range of stakeholders with interest in the expected outcome is detailed in the SSBC stakeholder map. As well as the cross-agency representatives, a subset of key stakeholders informed the development of the SSBC. This group includes the Kāpuia Ministerial Advisory Group; Iwi Chairs Forum Advisory Panel; Police Commissioner's Muslim Reference Group and Ethnic Focus Forum; impacted cultural, ethnic, and faith-based communities; CERT NZ; Crimestoppers; Netsafe; and victim support and wellbeing providers.

Communications

90 Following Cabinet decisions on the SSBC, Police will communicate with key agencies, groups, and impacted communities to inform them of next steps, including engagement on detailed design of the reporting system. We also propose to publicly announce the funding, timing, and process for implementing the new reporting system.

Proactive Release

91 We propose to proactively release this paper in whole, subject to redactions as appropriate under the *Official Information Act 1982*, in September 2023.

Recommendations

The Lead Coordination Minister for the Government's Response to the Royal Commission's Report into the Terrorist Attack on the Christchurch Mosques and the Minister of Police recommend that the Committee:

1 **note** in April 2022, Cabinet approved a $13.500 million contingency initiative *Reporting System for Concerning Behaviours and Incidents* for Vote Police, for inclusion in the 2022 Budget package [CAB-22-MIN-0129 refers];

2 **note** in August 2022, the Cabinet External Relations and Security Committee made the decision to go forward with investment in the new reporting system when it approved the drawdown of $1.094 million in operating funding against the tagged contingency to develop a business case for the new system [ERS-22-MIN-0031 refers];

3 **note** in June 2023, Cabinet approved a further drawdown of $0.430 million in operating funding against the tagged contingency to complete the business case for the new system [CAB-23-MIN-0226 refers];

4 **note** following the adjustments detailed in recommendations 1 to 3, the remaining balance of the *Reporting System for Concerning Behaviours and Incidents* tagged operating contingency is:

	$m – increase/(decrease)				
Vote Police	**2023/24**	**2024/25**	**2025/26**	**2026/27**	**2027/28 & Outyears**
Reporting System for Concerning Behaviours and Incidents – Tagged Operating Contingency	2.190	4.802	4.984	4.984	4.984

Business Case and implementation

5 **approve** the attached Single Stage Business Case: *Implementing Recommendation 12 of the Royal Commission of Inquiry into the Terrorist Attack on Christchurch Masjidain on 15 March 2019;*

6 **note** the Single Stage Business Case confirms New Zealand Police as the host agency for the new reporting system for concerning behaviours and incidents;

7 **endorse** the following scope of behaviours and incidents that the public will be asked to report through the new reporting system:

7.1 behaviours related to terrorism and violent extremism;

7.2 behaviours that indicate mobilisation to violence and signs of radicalisation (the *'Kia mataara ki ngā tohu Know the signs'* indicators);

7.3 early radicalisation behaviours;

8 **note** the new reporting system will use All-of-Government branding;

9 **delegate** to the Minister of Police any future decisions around the final branding, launch and ongoing promotion of the new reporting system;

Review of the new reporting system

10 **direct** the Minister of Police to report back to Cabinet on an evaluation of the new reporting system no later than 24 months after its launch;

Financial

11 **note** the proposed Single Stage Business Case estimates a required investment of $19.992 million operating from FY2023/24 to FY2026/27, an on-going operating requirement of $5.907 per annum from FY2027/28, and a capital injection of $3.977 million across FY2023/24 and FY2024/25;

12 **note** that the remaining balance of the tagged operating contingency, as set out in recommendation 4, is insufficient to cover the required funding for the new reporting system;

13 **note** that we are currently considering funding options to cover the total implementation and operating costs to deliver the proposed new reporting system over the four-year forecast period and we will report back to Cabinet at a later date to seek necessary approval of required funding.

Authorised for lodgement

Hon Andrew Little
Lead Coordination Minister for the Government's Response to the Royal Commission's Report into the Terrorist Attack on the Christchurch Mosques

Hon Ginny Andersen
Minister of Police

Appendices

Appendix A: Single Stage Business Case *Implementing Recommendation 12 of the Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain on 15 March 2019*

Appendix B: Detailed description of recommended option for new reporting system

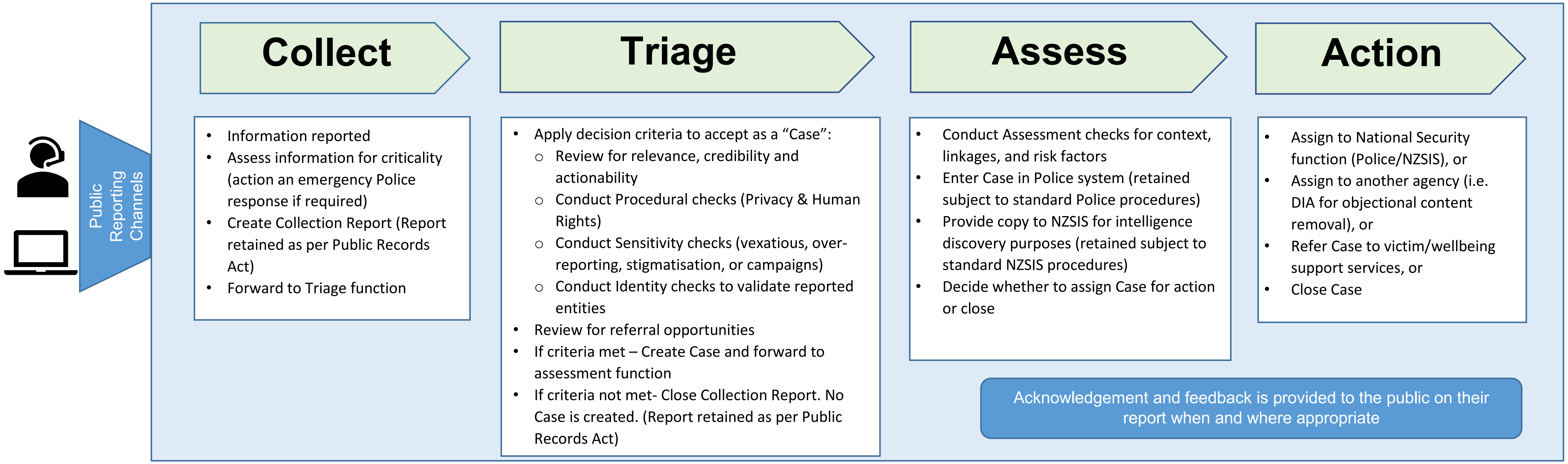
Appendix C: Scenarios for Public Reporting workflow and data retention

Appendix A: Single Stage Business Case *Implementing Recommendation 12 of the Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain on 15 March 2019*

Appendix B: Detailed description of recommended option for new reporting system

Investment scope	The recommended option will deliver:
New public reporting system to inform response	• New dedicated 24/7 telephony (0800 number) and online (website) channels, providing a single point of contact for the public • Website meets government accessibility standards and has shielding capability • Anonymity option for people who are reporting • All of Government branding • Education and awareness programmes so that the public are aware of what, where, and how to report • Investment in the capacity and cultural competency of call takers • Ability to take reports in multiple languages • Ability to receive most file types and content regardless of source • Criticality check at point of receipt to determine whether immediate response is required • Cloud-based workflow system
Triage and management system for government agencies to coordinate and assess information received from the public, and assign threats	• Investment in dedicated capacity to triage and assess reports against security indicators to identify threat/risk • Integrated entity, knowledge, and information management processes • Procedural (privacy and human rights) and sensitivity (vexatious / overreporting) checks • Pattern and trend analysis • Delivery of a standardised and strengthened end-to-end process for assessing national security lead information • Triage function operational up to 8hrs/7 days per week • Investment in basic case management technology • Cross-agency governance structure to provide a coordinated, shared agency response and system accountability
Referral and feedback process to enable government agencies to support people who make a report, as appropriate	• Coordinated referral to wellbeing service providers • Partnering with Department of Prime Minister and Cabinet's (DPMC's) Preventing and Countering Violent Extremism framework to access disengagement services • Acknowledgement and feedback to public on their report

Appendix C: Scenarios for Public Reporting workflow and data retention



Public Reporting Channels

Collect

- Information reported
- Assess information for criticality (action an emergency Police response if required)
- Create Collection Report (Report retained as per Public Records Act)
- Forward to Triage function

Triage

- Apply decision criteria to accept as a "Case":
  - Review for relevance, credibility and actionability
  - Conduct Procedural checks (Privacy & Human Rights)
  - Conduct Sensitivity checks (vexatious, over-reporting, stigmatisation, or campaigns)
  - Conduct Identity checks to validate reported entities
- Review for referral opportunities
- If criteria met – Create Case and forward to assessment function
- If criteria not met- Close Collection Report. No Case is created. (Report retained as per Public Records Act)

Assess

- Conduct Assessment checks for context, linkages, and risk factors
- Enter Case in Police system (retained subject to standard Police procedures)
- Provide copy to NZSIS for intelligence discovery purposes (retained subject to standard NZSIS procedures)
- Decide whether to assign Case for action or close

Action

- Assign to National Security function (Police/NZSIS), or
- Assign to another agency (i.e. DIA for objectional content removal), or
- Refer Case to victim/wellbeing support services, or
- Close Case

Acknowledgement and feedback is provided to the public on their report when and where appropriate

Scenario 1: Information received, but no Case created

Context: Reporter has experienced a racist comment (e.g. 'go back to where you came from') OR someone has expressed an offensive viewpoint in a public space (e.g. 'all immigration should be banned') OR the report is misdirected/incomplete/nonsensical. Some identifying details provided, but no indication of wider extremist context.

Outcome: The report does not meet the decision criteria (freedom of expression, no other relevant context). Collection Report closed. No case is created. Referral to wellbeing services where appropriate.

About 80% of reports are expected to not meet the decision criteria and be closed. Records only retained for Public Record Act purposes.

Scenario 2: Information received, Case created, but discontinued at assessment stage

Context: Reporter has experienced an instance of aggressive or threatening behaviour, directed at them or their whanau or community, online or in person and they feel unsafe. Some identifying particulars provided. Some unconfirmed indications of concerning/extremist behaviours.

Outcome: The report initially meets the triage criteria. A Case is opened in the public reporting system and forwarded to the Assessment function. On further assessment, a decision is made not to proceed with the Case (information not credible or confirmed out of scope). The Collection Report and Case are closed, but the data is retained. Referral to wellbeing services where appropriate.

About 10% of reports are not expected to meet the criteria for further action and be closed. Records retained for intelligence (i.e., 'join the dots') purposes under existing NZP and NZSIS protocols.

Scenario 3: Information received, Case created and actioned

Context: Reporter has been the victim of, or is aware of, a significant act of extremist harm, including the instance or threat of physical violence that is driven by an extremist ideology or concerning behaviours, as articulated in the 'Know the Signs' publication OR a reporter holds concerns that a whanau or community member has been radicalised or is potentially mobilising to an act of violent extremism or terrorism.

Outcome: The report meets the triage criteria, a Case is created and assessed as requiring further action. The Case is assigned to agencies for action and/or referred to wellbeing services.

About 10% of reports are actioned and the records retained indefinitely.