

# Preliminary Privacy Impact Assessment

## ***Recommendation 12 of the Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain – a public reporting system for concerning behaviours and incidents***

Project Sponsor: Rachael Bambery, Executive Director – Service and Resolutions

Author: **s.9(2)(a) OIA** Senior Policy Advisor, National Security and International Policy

18 April 2023, Version 0.2

## Project Summary

1. Several government agencies including New Zealand Police (Police) currently have channels for the public to report concerning behaviours and incidents, including those related to terrorism or violent extremism. However, many people who want to share their concerns, whether that is speaking up about an incident or seeking assistance when someone they know is at risk of radicalisation, are unclear about where to go for help and who can respond.
2. The Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain (the RCOI) signalled the need for a more coordinated cross-agency response that removes these barriers for the public.
3. Specifically, Recommendation 12 of the RCOI is to: *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.*
4. As part of the Government’s response to the Recommendation 12 of the RCOI, Police is leading the development of a Business Case for a new reporting system for concerning behaviours and incidents related to terrorism or violent extremism (Recommendation 12 reporting system).
5. The purpose of the new Recommendation 12 reporting system is to:
  - improve current systems and processes for the public to report concerning behaviours and incidents related to terrorism or violent extremism to a single point within government
  - improve the system across government agencies, including Police, for joining up, triaging, and managing publicly reported information to:
    - address current gaps in how these agencies understand threats and remove information siloes
    - enable these agencies to better coordinate national responses, including undertaking prevention activities and monitoring and investigating reports of terrorism or violent extremism behaviours and incidents.
6. 9(2)(f)(iv) [REDACTED]

7. Police is currently leading the development of a cross-agency<sup>1</sup> Business Case and has not yet determined the final design of the Recommendation 12 reporting system.
8. As an initial step, Police has undertaken a preliminary Privacy Impact Assessment (PIA) to identify:
  - how the collection, use, and sharing of information through the Recommendation 12 reporting system may differ from 9(2)(f)(iv) [REDACTED] (i.e. status quo)
  - any additional privacy risks relating to the use, storage, and disposal, etc. of personal information collected through the Recommendation 12 reporting system that Police will need to address during the system design phase.
9. 9(2)(f)(iv) [REDACTED]  
[REDACTED]  
[REDACTED]
10. Police will complete a more detailed PIA after confirming the detailed system design for the Recommendation 12 reporting system. This will include a more detailed assessment of the specific controls that Police has incorporated into the final design to mitigate privacy risks.

---

<sup>1</sup> Police is working with the Department of the Prime Minister and Cabinet, New Zealand Security Intelligence Service, Department of Internal Affairs, and Ministry for Ethnic Communities.

# Project Detail

## 1. Purpose - collection, use, disclosure or sharing

### Purpose for new information collection

11. 9(2)(f)(iv) [Redacted]

[Redacted]

- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

9(2)(f)(iv) [Redacted]

[Redacted]

- [Redacted]
- [Redacted]
- [Redacted]

[Redacted]

16. 9(2)(f)(iv) [Redacted]

**Using currently held information for a new purpose**

17. 9(2)(f)(iv) [Redacted]

**Sharing information with, or disclosing information to other agencies**

19. The RCOI identified that while several agencies collect information from the public on concerning behaviours and incidents, this information is not always appropriately shared or shared in a timely way between these agencies. Information siloes can create vulnerabilities for identifying national security threats and barriers to effectively respond to these threats.

20. 9(2)(f)(iv) [Redacted]

9(2)(f)(iv) [Redacted]

[Redacted]

**Collaborating with others to gain insights**

- 23. 9(2)(f)(iv) [REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

**2. Transparency, technology and social expectations**

**Notifying individuals and communities**

- 24. 9(2)(f)(iv) [REDACTED] there will need to be clear communication with the public about what information they can be report through the Recommendation 12 reporting system. There will also need to be clear disclaimers when the public makes reports about what will happen with their information. 9(2)(f)(iv) [REDACTED].
- 25. Currently, Police explicitly sets out on the Police public website how we manage personal information that we receive (<https://www.police.govt.nz/about-us/how-we-manage-personal-information>). 9(2)(f)(iv) [REDACTED]
- 26. Police acknowledges that affected communities (and the RCOI) in relation to public reports about threats, have repeatedly called for agencies to notify those making reports about the value of the information they provide and what action has been taken. 9(2)(f)(iv) [REDACTED]  
[REDACTED]  
[REDACTED]

**Use of technology**

- 27. 9(2)(f)(iv) [REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

**Involving service users and meeting social expectations**

- 28. Police has externally engaged with affected communities and Kāpuia (the Ministerial Advisory Group on the Government’s response to the RCOI) on the response to Recommendation 12 of the RCOI. We have also convened a cross-agency Governance Group to provide support and guidance as Police develops the Business Case for the Recommendation 12 reporting system. This Group comprises senior officials from Police, the Department of the Prime Minister and Cabinet, Department of Internal Affairs, New Zealand Security Intelligence Service, and Ministry for Ethnic Communities. This Group is also supported by advisory group of officials from these agencies.
- 29. Police will continue to engage these stakeholders in the design and implementation phases of the Recommendation 12 reporting system.

### 3. Fairness and quality

#### Collecting, using, disclosing or sharing information respectfully and fairly

30. 9(2)(f)(iv) [Redacted]

[Redacted]

[Redacted]

#### Information sources, data quality and purpose

33. 9(2)(f)(iv) [Redacted]

[Redacted]

### 4. Systems and security

#### Describe the security and privacy features of the platform used to store information

35. 9(2)(f)(iv) [Redacted]

36. 9(2)(f)(iv) [Redacted]  
[Redacted]  
[Redacted]

[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]

[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]



**Privacy Risk Analysis**

Record any new or elevated privacy risks arising from the project. Consult with relevant subject matter experts as needed.

<p><b>Risk description</b> What could happen and how will this affect individuals or Police</p>	<p><b>Pre-existing Controls</b> What pre-existing controls are in place to reduce the impact and/or likelihood of the risk (briefly describe any existing practice, policy, or technical control)</p>	<p><b>Recommended controls</b> To reduce risk to an acceptable level</p>
<p><b>Purpose - collection, use, disclosure or sharing</b></p>		
<p>9(2)(f)(iv) [Redacted]</p>	<ul style="list-style-type: none"> <li>9(2)(f)(iv) [Redacted]</li> </ul>	<p>9(2)(f)(iv) [Redacted]</p>
<p>9(2)(f)(iv) [Redacted]</p>	<p>9(2)(f)(iv) [Redacted]</p>	<p>9(2)(f)(iv) [Redacted]</p>

**Privacy Risk Analysis**

Record any new or elevated privacy risks arising from the project. Consult with relevant subject matter experts as needed.

<p><b>Risk description</b> What could happen and how will this affect individuals or Police</p>	<p><b>Pre-existing Controls</b> What pre-existing controls are in place to reduce the impact and/or likelihood of the risk (briefly describe any existing practice, policy, or technical control)</p>	<p><b>Recommended controls</b> To reduce risk to an acceptable level</p>
<p>9(2)(f)(iv) [Redacted]</p>	<p>9(2)(f)(iv) [Redacted]</p>	<p>9(2)(f)(iv) [Redacted]</p>
<p>9(2)(f)(iv) [Redacted]</p> <ul style="list-style-type: none"> <li>■ [Redacted]</li> <li>■ [Redacted]</li> <li>■ 9(2)(f)(iv) [Redacted]</li> </ul>	<p>9(2)(f)(iv) [Redacted]</p> <ul style="list-style-type: none"> <li>■ [Redacted]</li> <li>■ [Redacted]</li> <li>■ [Redacted]</li> <li>■ [Redacted]</li> <li>■ [Redacted]</li> <li>■ [Redacted]</li> </ul>	<p>9(2)(f)(iv) [Redacted]</p> <ul style="list-style-type: none"> <li>■ [Redacted]</li> <li>■ [Redacted]</li> <li>■ [Redacted]</li> <li>■ [Redacted]</li> </ul>

**Privacy Risk Analysis**

Record any new or elevated privacy risks arising from the project. Consult with relevant subject matter experts as needed.

<p><b>Risk description</b> What could happen and how will this affect individuals or Police</p>	<p><b>Pre-existing Controls</b> What pre-existing controls are in place to reduce the impact and/or likelihood of the risk (briefly describe any existing practice, policy, or technical control)</p>	<p><b>Recommended controls</b> To reduce risk to an acceptable level</p>
<p><b>Transparency, participation, and social expectations</b></p>		
<p>9(2)(f)(iv) [Redacted]</p>	<p>9(2)(f)(iv) [Redacted]</p>	<p>9(2)(f)(iv) [Redacted]</p>
<p>9(2)(f)(iv) [Redacted]</p>	<p>9(2)(f)(iv) [Redacted]</p>	<p>9(2)(f)(iv) [Redacted]</p>
<p>9(2)(f)(iv) [Redacted]</p>	<p>• 9(2)(f)(iv) [Redacted]</p>	<p>• 9(2)(f)(iv) [Redacted]</p>

**Privacy Risk Analysis**

Record any new or elevated privacy risks arising from the project. Consult with relevant subject matter experts as needed.

<p><b>Risk description</b> What could happen and how will this affect individuals or Police</p>	<p><b>Pre-existing Controls</b> What pre-existing controls are in place to reduce the impact and/or likelihood of the risk (briefly describe any existing practice, policy, or technical control)</p>	<p><b>Recommended controls</b> To reduce risk to an acceptable level</p>
<p><b>Fairness and quality</b></p>		
<p>9(2)(f)(iv) [Redacted]</p>	<p>9(2)(f)(iv) [Redacted]</p>	<p>9(2)(f)(iv) [Redacted]</p>
<p><b>Systems and security</b></p>		
<p>9(2)(f)(iv) [Redacted]</p>	<p>9(2)(f)(iv) [Redacted]</p>	<p>9(2)(f)(iv) [Redacted]</p>
<p>9(2)(f)(iv) [Redacted]</p>	<p>9(2)(f)(iv) [Redacted]</p>	<p>9(2)(f)(iv) [Redacted]</p>

**Privacy Risk Analysis**

Record any new or elevated privacy risks arising from the project. Consult with relevant subject matter experts as needed.

<p><b>Risk description</b> What could happen and how will this affect individuals or Police</p>	<p><b>Pre-existing Controls</b> What pre-existing controls are in place to reduce the impact and/or likelihood of the risk (briefly describe any existing practice, policy, or technical control)</p>	<p><b>Recommended controls</b> To reduce risk to an acceptable level</p>
<p>9(2)(f)(iv) [Redacted]</p> <p>[Redacted]</p> <ul style="list-style-type: none"> <li>[Redacted]</li> </ul>	<p>9(2)(f)(iv) [Redacted]</p> <ul style="list-style-type: none"> <li>[Redacted]</li> </ul>	<p>9(2)(f)(iv) [Redacted]</p> <ul style="list-style-type: none"> <li>[Redacted]</li> </ul>

## Summary of findings and recommendations

39. As highlighted throughout this preliminary PIA, Police will need to undertake further work to determine the final design of the Recommendation 12 reporting system. At this stage, as we do not know detailed design of specific aspects **s.9(2)(f)(iv)**, it is not possible to fully canvass privacy risks. Instead, this preliminary PIA notes areas for further consideration as part of the system design phase. **s.9(2)(f)(iv)**

- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

40. It will be necessary for Police to complete a more detailed PIA after confirming the detailed system design for the Recommendation 12 reporting mechanism. This will need to take into consideration the specific controls that have been incorporated into the final design to mitigate privacy risks.

### PIA Sign off

**Project Manager**

**s.9(2)(a) OIA**

14 April 2023

**Privacy Officer**

Colin Trotter

14 April 2023

**Senior or Executive Leader**

Rachael Bambery

17 April 2023

## Appendix A: Guiding principles

### Purpose - collection, use, disclosure or sharing

- ▶ Any collection, use or sharing of information is for a reasonable and well-defined purpose aligned to Police strategic priorities and values, or those of the agency we share with.
- ▶ Consider whether use of identifiable personal information is necessary, and only collect, use, or share the minimum information needed to achieve the outcome.
- ▶ Risks and potential negative outcomes should be assessed so it's clear how these balance against positive outcomes.

### Transparency, participation, and social expectations

- ▶ Tell people in a way that makes sense to them what information is collected about them, how it will be used, who it will be shared with and why, even if it will be used or shared in a way that does not and cannot be used to identify them.
- ▶ Even when there is no legal requirement to tell people, being open about what we do with information is important to maintain public trust and respect in Police.
- ▶ Consult with a diverse and representative group of community stakeholders to reflect the different perspectives, values, concerns and needs of individuals and communities. For example, when considering use of new technologies or processes such as artificial intelligence and automated decision making.

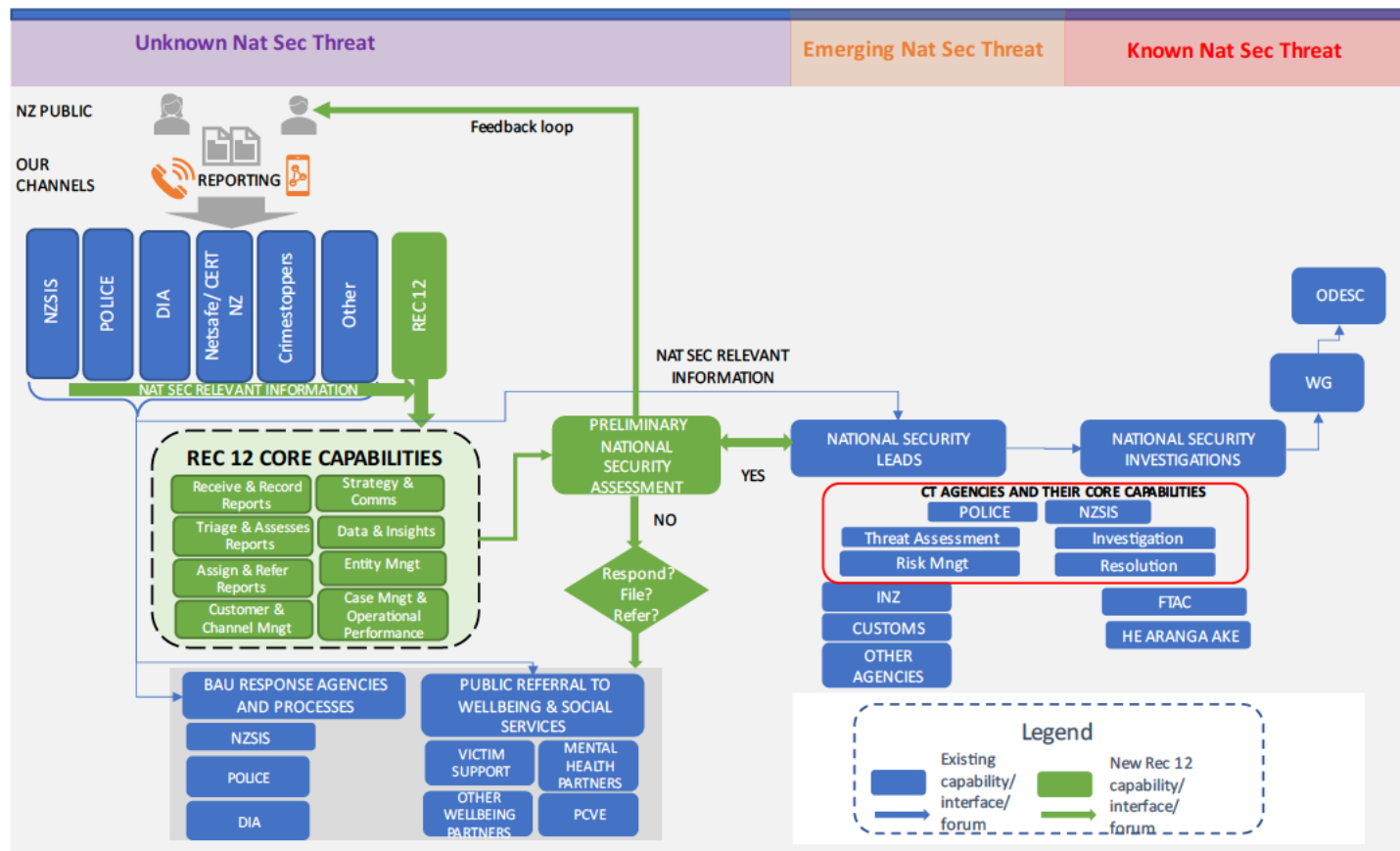
### Fairness and quality

- ▶ Collect and use information in ways that are proportionate in scope and scale, respectful of individuals and communities and does not unreasonably intrude on the privacy interests of individuals or groups.
- ▶ Ensure the accuracy and quality of information is fit for purpose for its intended use or to share with others.
- ▶ Information is a strategic asset and maintaining its accuracy through its lifecycle is a key component in delivering policing services.

### Systems and security

- ▶ Apply information management practices that align with security standards. Consider the sensitivity of the information being collected, used, shared, and reported.
- ▶ Store and maintain information so that it is accessible and reliable, and only keep it for as long as it is necessary and relevant.
- ▶ If a privacy breach occurs, address it quickly, and be accountable for it.

9(2)(f)(iv)





9(2)(f)(iv)

