Document 1

Excerpts from Status Reports to the Minister of Internal Affairs 8 October 2019 to 26 May 2021

8 October 2019

Countering Violent Extremism (CVE) Online

The CVE Cabinet paper was considered by the Cabinet Social Wellbeing Committee (SWC) on 25 September 2019. Cabinet confirmed the paper on 30 September 2019. The Prime Minister and you will be making announcements about CVE engagement in mid-October 2019, ahead of round table meetings with stakeholder groups. Officials will provide a further briefing to your office with advice about convening a ministerial group to coordinate the Whole-of-Government response to CVE.

15 October 2019

Countering Violent Extremism (CVE) Online

The CVE Cabinet paper was considered by the Cabinet Social Wellbeing Committee (SWC) on 25 September 2019. Cabinet confirmed the paper on 30 September 2019. The Prime Minister and you announced the funding and next steps for this project on 14 October 2019. Next week we will begin targeted consultation with industry, and civil society, with a particular focus on ethnic communities. Officials will provide a further briefing to your office with advice about convening a ministerial group to coordinate the Whole-of-Government response to CVE.

22 October 2019

Countering Violent Extremism (CVE) Online

The targeted engagement on Countering Violent Extremism will take place from 23 October to 4 November 2019. Registrations have opened and at this stage the sessions are attracting substantial and diverse attendance. We can provide you with further updates once the sessions have begun. Officials will provide a further briefing to your office about convening a ministerial group to coordinate the Whole-of-Government response to CVE.

29 October 2019

Countering Violent Extremism (CVE) Online

The targeted engagement on Countering Violent Extremism has begun and will run to 4 November 2019. At this stage the sessions are attracting substantial and diverse attendance. Initial feedback from the sessions confirms officials' assessment of harms resulting from exposure to CVE material, and general support for the proposals, subject to these groups seeing further detail on the final design. There has been some initial push back against the current timeframes. Officials' are looking to manage this and will provide you with advice and seek your direction on how to address this. Officials have recently provided a briefing to your office about convening a ministerial group to coordinate the Whole-of-Government response to CVE. The briefing included letters for you to sign and send, to ensure support and approval for early drafting of a CVE amendment Bill progressing legislative amendments to the Classification Act.

5 November 2019

Countering Violent Extremism (CVE) Online – update on consultation

Recent activities

Targeted engagement on CVE is continuing. Initial feedback confirms officials' assessment of harms resulting from exposure to CVE material, and general support for the proposals, subject to further engagement on the final design. There has been some push back against the current timeframe.

You recently approved a four-day extension of engagement timeframes, and a plan to supply an exposure draft Bill to certain stakeholder groups over the Christmas break.

On 23 October 2019, officials briefed your office about convening a ministerial group to coordinate the whole-of-government response to CVE. The briefing included letters for you to sign and send to ensure support and approval for early drafting of a CVE Amendment Bill to progress legislative amendments to the Films, Videos and Publications Classification Act 1993.

We understand that the Green Party and Rt Hon Winston Peters have indicated their support for early drafting of the amendment Bill.

Next steps

We will send you a draft Cabinet paper with the detailed policy proposals and a summary of the consultation feedback by 15 November 2019.

We will send you a proposed agenda and supporting papers for the Ministerial Group once a date is confirmed for the first meeting.

12 November 2019

Countering Violent Extremism (CVE) online

Targeted engagement on legislative fixes to strengthen our regulatory system to address violent extremist content online concluded on 8 November 2019.

Many stakeholders supported the policy intent and proposals, contingent on the proposals adhering to three key principles:

- government censorship should be transparent and open to public scrutiny;
- clear, inflexible definitions of what is censored; and
- material should only be censored if it can be demonstrated that it causes harm.

A recurring message was that more needs to be done to proactively address the drivers of violent extremist behaviour and provide protection for targeted groups.

To accommodate requests for additional detail on the proposals, you approved a four-day extension of engagement timeframes.

On 23 October 2019, officials briefed your office on the process for securing support and approval for early drafting of a CVE Amendment Bill to progress legislative amendments to the Films, Videos and Publications Classification Act 1993. The Attorney-General has approved early drafting of the Bill. We will provide drafting instructions to the PCO this week.

You are meeting the Chief Censor on 21 November 2019 to discuss the likely next steps on CVE work following recent engagement with internet service providers. We will provide your office with a briefing ahead of your meeting

Countering Violent Extremism (CVE) online work progress – verbal update

Recent activities

- Officials concluded targeted engagement through workshops across Hamilton, Christchurch, Auckland and Wellington.
- A briefing and draft Cabinet paper will be provided to your office 15 November 2019.

- The Attorney-General has approved early drafting of a Bill to enact proposed amendments.

Next steps

- We will update you on progress and next steps to deliver enactment of proposals to counter violent extremist content online.

We will also discuss the proposed agenda for the upcoming Ministerial CVE meeting on 2 December 2019 (5 – 5:30 pm). You will chair this meeting.

19 November 2019

Countering Violent Extremism (CVE) online

On 23 October 2019, officials briefed your office on the process for securing support and approval for early drafting of a CVE Amendment Bill to progress legislative amendments to the Films, Videos and Publications Classification Act 1993 (the Classification Act). The Attorney-General has approved early drafting of the Bill. We have provided drafting instructions to PCO this week.

We provided your office with a draft Cabinet paper setting out proposed changes to the Classification Act, for consultation with your ministerial colleagues.

You are meeting the Chief Censor on 21 November 2019 to discuss the likely next steps on CVE work following recent engagement with ISPs. We have provided your office with a briefing ahead of your meeting.

Countering Violent Extremism (CVE) online – verbal update

Recent activities

- We are meeting with relevant industry groups, including online content hosts and internet service providers (ISPs) to identify and address specific concerns raised during the recent targeted consultation.
- We have met with Spark and 2Degrees. These ISPs are broadly comfortable with the process and asked to continue to be involved. We outlined the plan for an exposure draft, and this alleviated most of their concerns around pace and the level of details available to date.
- We also met with Internet NZ as an important stakeholder in this work. They continue to have concerns about the pace of the work and the filtering proposal.

Next steps

You will be verbally updated on this work at this week's officials' meeting.

26 November 2019

Countering Violent Extremism (CVE) online

On 23 October 2019, officials briefed your office on the process for securing support and approval for early drafting of a CVE Amendment Bill to progress legislative amendments to the Films, Videos and Publications Classification Act 1993 (the Classification Act). The Attorney-General has approved early drafting of the Bill. PCO has advised they will commence drafting this week.

We provided your office with a draft Cabinet paper setting out proposed changes to the Classification Act, for consultation with your ministerial colleagues. Consultation closes on 2 December 2019.

We provided your office with a briefing ahead of the first Countering Violent Extremism Ministerial group meeting, scheduled for 2 December 2019. The briefing included a proposed agenda, and accompanying papers for your approval and distribution to ministerial colleagues prior to the meeting.

3 December 2019

Countering Violent Extremism (CVE) online

Recent activities

- We are working with the Parliamentary Counsel Office on the exposure draft of a CVE Amendment Bill for progressing legislative amendments to the Films, Videos and Publications Classification Act 1993 (the Classification Act).
- We provided your office with a final CVE Cabinet paper for your approval, following Ministerial and Departmental consultation on proposed changes to the Classification Act.
- The Department has also developed a draft of the Domestic Online Crisis Response Process in conjunction with other Government Departments, NGOs and industry.
- The process will be socialised with select group of industry and NGOs in New Zealand. We will finalise the process in January 2020.

Next steps:

If you agree, we will lodge the Cabinet paper on 5 December 2019, for consideration by the Cabinet Social Wellbeing Committee on 11 December 2019. Cabinet confirmation is expected on 16 December 2019.

10 December 2019

Countering Violent Extremism (CVE) online

Recent activities

- We are working with the Parliamentary Counsel Office on the exposure draft of a CVE Amendment Bill for progressing legislative amendments to the Films, Videos and Publications Classification Act 1993 (the Classification Act).
- The first CVE Ministerial Group meeting was on 2 December 2019. It included a presentation from Facebook and Google representatives on their work to date in the CVE area.
- On 5 December 2019 a final CVE Cabinet paper was lodged following ministerial and departmental consultation on proposed changes to the Classification Act.
- The Department developed a final draft of the Online Crisis Response Process in collaboration with other Government Departments, NGOs and industry. The final draft will be socialised with other relevant agencies in February. The next step for the crisis response is to plan scenario testing workshops.

Next steps:

The Cabinet Social Wellbeing Committee (SWC) will consider the CVE Cabinet paper on 11 December 2019. Cabinet confirmation is expected on 16 December 2019. We have provided your office with an aide memoire and talking points to assist you at SWC.

24 January 2020

Countering Violent Extremism (CVE) online

Recent activities

- We have worked with the Parliamentary Counsel Office on the exposure draft of a CVE Amendment Bill for progressing legislative amendments to the Films, Videos and Publications Classification Act 1993 (the Classification Act). The exposure draft is now ready for consultation with targeted industry stakeholders.
- On 23 January 2020, we provided you with a briefing seeking approval to proactively release Cabinet material related to the CVE workstream.

- The Preventing and Countering Violent Extremism online (PCVE) Programme has been established to provide coordination across the work streams, with a strong focus on the establishment of the new CVE team.
- The Department has also developed a draft of the Domestic Online Crisis Response Process in conjunction with other Government Departments, non-government organisations (NGOs), and industry. The process will be socialised with a select group of industry and NGOs in New Zealand. We will finalise the process this month.

Next steps

We will provide you with an update on feedback from stakeholders and subsequent changes to the Amendment Bill following targeted industry consultation.

4 February 2020

Countering Violent Extremism (CVE) online

The exposure draft of the CVE Amendment Bill to the Films, Videos and Publications Classification Act 1993 (the Classification Act) has been sent out for consultation with targeted industry stakeholders, as well as Government agencies and the Legislation Design and Advisory Committee.

On 30 January 2020, following your approval, Cabinet material related to the CVE workstream was uploaded on the Department's website. The material attracted media interest, including two Newsroom articles.

The Preventing and Countering Violent Extremism online (PCVE) Programme has been established to provide coordination across the work streams, with a strong focus on the establishment of the new CVE team.

Consultation on the exposure draft closes on 17 February 2020. We will provide you with an update on stakeholder feedback, any impact the feedback will have on the CVE Amendment Bill, and the timing for the introduction of the Bill.

11 February 2020

Countering Violent Extremism (CVE) online

The exposure draft of the CVE Amendment Bill to the Films, Videos and Publications Classification Act 1993 (the Classification Act) is with targeted industry stakeholders, as well as Government agencies and the Legislation Design and Advisory Committee, for consideration. Feedback is due by 17 February 2020. To date, we have received minor technical feedback from Spark, which spoke positively about the proposed changes.

We have developed a final draft of the Online Crisis Response Process in collaboration with other government departments, NGOs, and industry. The final draft will be socialised with relevant agencies in February 2020. The next step is to plan scenario testing workshops.

Work is continuing to establish the new CVE team as part of the broader Preventing and Countering Violent Extremism online (PCVE) Programme.

Countering Violent Extremism (CVE) verbal update

- We will provide you with a verbal update on the following areas of work:
  - industry feedback received so far on the exposure draft of the CVE Amendment Bill to the Films, Videos and Publications Classification Act 1993;
  - timing options for progressing the CVE Amendment Bill; and

  - the proposed agenda and approach for the CVE Ministerial Meeting that you are chairing on 20 February 2020.
- We will seek to discuss this at the officials' meeting on 13 February 2020.

18 February 2020

Countering Violent Extremism (CVE) online

Following decisions by Cabinet in December 2019, we are working with Parliamentary Counsel Office (PCO) on an updated draft Films, Videos, and Publications Classification (Urgent Interim Classification of Publications and Prevention of Online Harm) Amendment Bill for your consideration.

Please see page six of *'Updates for Discussion,'* for a summary of recent activities and next steps.

[Out of scope] & Classification Update

Recent activities

Countering Violent Extremism (CVE)

- On 17 February 2020, submissions closed on the exposure draft of the CVE Amendment Bill (CVE Bill). We received nine written submissions from industry stakeholders.
- Following your approval at the 13 February 2020 officials' meeting, we amended timeframes for passing the CVE Bill, to follow standard legislative timing with a six-month select committee process. The Bill is now expected to be enacted in early 2021.

Next Steps

CVE

- We will provide you with an update on the CVE Bill exposure draft feedback on 20 February 2020. You will receive the final draft Bill for approval on 27 February 2020, ahead of Ministerial and Departmental consultation.
- We have developed a final draft of the Online Crisis Response Process in collaboration with other government departments, NGOs, and industry. We will discuss this with you at the CVE Protocols Meeting on 24 February 2020.

25 February 2020

Countering Violent Extremism (CVE) online

Following decisions by Cabinet in December 2019, we are working with Parliamentary Counsel Office (PCO) on an updated draft Films, Videos, and Publications Classification (Urgent Interim Classification of Publications and Prevention of Online Harm) Amendment Bill for your consideration.

On 17 February 2020, submissions closed on the exposure draft of the CVE Amendment Bill (CVE Bill). We received eleven written submissions from industry and agency stakeholders. Stakeholders were generally supportive of changes, but sought greater clarity on how the filtering system would operate. Submitters also provided suggestions on operational changes.

You will receive the final draft Bill for approval by 27 February 2020, ahead of ministerial and departmental consultation. Timeframes for passing the CVE Bill were amended, to follow standard legislative timing with a six-month select committee process. The CVE Bill is now expected to be enacted in early 2021.

10 March 2020

Countering Violent Extremism (CVE) online

Following decisions by Cabinet in December 2019, we are working with Parliamentary Counsel Office (PCO) on an updated draft Films, Videos, and Publications Classification (Urgent Interim Classification of Publications and Prevention of Online Harm) Amendment Bill (the Bill) for your consideration.

Following your approval of a draft LEG Cabinet paper and draft Bill, we are now conducting departmental consultation, which closes on 13 March 2020. We understand that your office is conducting ministerial consultation on the same timeframe.

We will provide you with a finalised Cabinet paper and Bill for your approval, ahead of lodging on 2 April 2020 for LEG, with Cabinet Committee consideration on 7 April 2020. This allows time for PCO to update the Bill following the close of consultation. Introduction to Parliament is then anticipated following the April recess.

17 March 2020

Countering Violent Extremism (CVE) update

Recent activities

- Following decisions by Cabinet in December 2019, we are working with Parliamentary Counsel Office (PCO) on an updated draft Films, Videos, and Publications Classification (Urgent Interim Classification of Publications and Prevention of Online Harm) Amendment Bill (the Bill) for your consideration.
- Following your approval of a draft LEG Cabinet paper and draft Bill, we conducted departmental consultation, which closed on 13 March 2020. We understand your office conducted ministerial consultation which closed on 16 March 2020.
- Following consultation, minor amendments were made to both the LEG Cabinet paper and draft Bill, in line with the feedback received.
- Within the wider Preventing and Countering Violent Extremism (CVE) programme, we have been proactive in working with key agencies regarding the establishment of key roles.

Next steps

We will provide you with a finalised Cabinet paper and Bill for your approval on 19 March 2020, ahead of lodging on 2 April 2020 for LEG, with Cabinet Committee consideration on 7 April 2020. This allows time for PCO to update the Bill following consultation. Introduction to Parliament is then anticipated following the April 2020 recess.

24 March 2020

Countering Violent Extremism (CVE) online

With New Zealand moving to COVID-19 alert level 4, the timeline for this Bill will now be delayed as the Bill awaits key decisions from Cabinet and introduction to the House.

We provided you with a finalised Cabinet paper and near-final version of the Bill for your approval on 19 March 2020. We anticipated lodging on 2 April 2020 for LEG, with consideration on 7 April 2020. These timeframes are no longer possible. Consideration of the paper will be delayed until normal Cabinet business resumes and introduction will be delayed until Parliamentary business resumes.

We are preparing draft First Reading Speech notes, a question and answer resource and an initial briefing for the Select Committee, for your review and approval. We will provide you with these documents in due course once normal business resumes and the LEG pack is submitted to Cabinet Office for consideration.

Within the wider Preventing and Countering Violent Extremism (PCVE) programme, we are continuing to work with key agencies regarding the establishment of key roles.

31 March 2020

Countering Violent Extremism (CVE) online

With New Zealand moving to COVID-19 alert level 4, the timeline for this Bill will now be delayed. Consideration of the paper will be delayed until normal Cabinet business resumes, and introduction will be delayed until Parliamentary business resumes.

We will provide you with draft First Reading Speech notes, a question and answer resource, and an initial briefing for the Select Committee, once normal business resumes.

Within the wider Preventing and Countering Violent Extremism (PCVE) programme, we are continuing to work with key agencies regarding the establishment of key roles and scenario planning. With COVID-19 priorities, this work is continuing at a slower pace.

7 April 2020

Countering Violent Extremism (CVE) online

With New Zealand moving to COVID-19 alert level 4, the timeline for this Bill will now be delayed. Consideration of the paper will be delayed until normal Cabinet business resumes, and introduction will be delayed until Parliamentary business resumes.

We will provide you with draft First Reading Speech notes, a question and answer resource, and an initial briefing for the Select Committee, once normal business resumes.

Within the wider Preventing and Countering Violent Extremism (PCVE) programme, we are continuing to work with key agencies regarding the establishment of key roles and scenario planning. With COVID-19 priorities, this work is continuing at a slower pace.

There is a connection to the work on voluntary transparency reporting, detailed further in the section on "Other Updates".

Work on voluntary transparency reporting

Recent activities

- Following your trip to Washington DC in March 2020, you expressed an interest in the status of the OECD-led Voluntary Transparency Reporting Protocol (VTRP) project.
- The VTRP project is an important component of wider transparency-related work with industry, which brings together the industry, governments, civil society, and NGOs to create a common voluntary reporting framework. The reporting framework includes metrics for online platforms to implement regular and transparent public reporting on the prevalence of terrorist and violent extremist content on their platforms. It will also include the steps platforms are taking to prevent, detect, and remove this content.
- The Ministry of Foreign Affairs and Trade is substantially involved in the development and coordination of the project to date. Key government and industry partners include Australia, Canada, the United Kingdom, the United States, France, the European Union, Facebook, Microsoft, Twitter, Google, and Amazon.
- Australia suggested using the G20 to progress this project. However, this was not supported by a number of other countries (including the United States) and we understand that the OECD will continue to be the mechanism to progress this work internationally.

Next steps

The project is progressing at a slower pace due to re-prioritisation of governments' resources towards the COVID-19 response, but partners remain confident it will proceed to completion in 2020.

14 April 2020

Countering Violent Extremism (CVE) online

The timeline for this Bill is delayed.

We will provide you with an updated LEG pack and final Bill once normal Cabinet and Parliamentary business resumes. Work to establish key roles within the wider Preventing and Countering Violent Extremism (PCVE) programme is continuing, but at a slower pace owing to COVID-19 priorities.

Work has also progressed to identify a partner to support the PCVE Programme to conduct analysis, provide policy advice and risk prevention strategies to the Department of Internal Affairs. This situational awareness work will help us to better understand the New Zealand context, support the establishment of our new countering online violent extremism capability and help us develop prevention strategies for use both online and offline.

21 April 2020

Countering Violent Extremism (CVE) online

The timeline for this Bill is delayed until House business resumes.

We are working with the Parliamentary Counsel Office to finalise the Bill, and prepare it for lodgement with the Cabinet Legislation Committee (LEG). We will provide you with an updated LEG pack and final Bill when Cabinet and Parliamentary business resumes.

28 April 2020

Countering Violent Extremism (CVE) online (Legislation Phase on hold)

The timeline for this Bill is delayed until House business resumes.

On 24 April 2020, we provided you with an updated LEG pack and the final Bill.

We are aiming to lodge the Cabinet paper on 30 April 2020, for consideration at the LEG meeting on 5 May 2020.

The Preventing and Countering Violent Extremism (PCVE) Programme, including establishment of key roles, is continuing but at a slower pace.

We are identifying an external provider to support the PCVE Programme to conduct analysis, and provide risk prevention strategies. This will help us better understand the New Zealand context, and develop prevention strategies for both online and offline use.

5 May 2020

Countering Violent Extremism (CVE) online (Legislation Phase on hold)

The timeline for this Bill is delayed until House business resumes.

On 24 April 2020, we provided you with an updated LEG pack and the final Bill.

On 5 May 2020, the Bill was approved for introduction by LEG. We understand the Bill is scheduled for Cabinet confirmation on 11 May 2020.

12 May 2020

Countering Violent Extremism (CVE) online (Legislation Phase on hold)

On 24 April 2020, we provided you with an updated LEG pack and the final Bill.

On 5 May 2020, the Bill was approved for introduction by the Cabinet Legislation Committee (LEG). This was confirmed by Cabinet on 11 May 2020. We understand that the Bill will be introduced to the House when normal parliamentary business resumes.

19 May 2020

Countering Violent Extremism (CVE) online

On 5 May 2020, the final Bill was approved for introduction by the Cabinet Legislation Committee (LEG). This was confirmed by Cabinet on 11 May 2020.

We anticipate the Bill will be introduced to the House in the week beginning 25 May 2020. We will provide you with a draft briefing to the Select Committee, ahead of the Bill's referral to the Select Committee in early June 2020.

On 7 May 2020, the new Digital Safety structure was announced. This new structure reflects our regulatory responsibility for countering violent extremism.

We have selected an external provider to conduct research into the scale and nature of online violent extremism in New Zealand. This will help us to better understand the New Zealand context and will ensure our new capability for countering online violent extremism is fit for purpose.

26 May 2020

Countering Violent Extremism (CVE) online

On 5 May 2020, the final Bill was approved for introduction by the Cabinet Legislation Committee (LEG). This was confirmed by Cabinet on 11 May 2020.

The Bill was introduced to the House on 26 May 2020. As per the discussion at the 21 May 2020 Officials' meeting, the First Reading will be delayed until July 2020 to enable a focus on the Gambling, Racing and Community Funding work programme.

2 June 2020

Countering Violent Extremism (CVE) online

On 5 May 2020, the final Bill was approved for introduction by the Cabinet Legislation Committee (LEG). This was confirmed by Cabinet on 11 May 2020.

The Bill was introduced to the House on 26 May 2020. As per the discussion at the 21 May 2020 Officials' meeting, the First Reading will be delayed until July 2020 to enable a focus on the Gambling, Racing and Community Funding work programme.

9 June 2020

Countering Violent Extremism (CVE) online

On 5 May 2020, the final Bill was approved for introduction by the Cabinet Legislation Committee (LEG). This was confirmed by Cabinet on 11 May 2020.

The Bill was introduced to the House on 26 May 2020. As per the discussion at the 21 May 2020 Officials' meeting, the First Reading will be delayed until July 2020 to enable a focus on the Gambling, Racing and Community Funding work programme.

16 June 2020

Countering Violent Extremism (CVE) online

The Bill was introduced to the House on 26 May 2020. The First Reading is delayed until July 2020 to enable a focus on the Gambling, Racing and Community Funding work programme.

On 5 June 2020, we resumed face-to-face engagement with key agency partners. This will help us support the countering violent extremism eco-system.

Our external research provider has initiated conversations with key stakeholders to better understand the scale and nature of online violent extremism in New Zealand. This work will help us develop a "map" of online extremism in New Zealand, which will also support the ongoing development of prevention strategies for both online and offline use. This is expected to take four weeks.

23 June 2020

Countering Violent Extremism (CVE) online

On 26 May 2020, the Bill was introduced to the House, with the First Reading anticipated in July 2020. Please also see the 'Updates for Discussion' item, *Establishing the Preventing and Countering Violent Extremism function*.

Establishing the Preventing and Countering Violent Extremism function

Recent activities

- We are ensuring that the online elements of countering violent extremism are integrated into the broader frameworks of agencies working on these issues. To do this, we are working closely with the New Zealand Police, New Zealand Security Intelligence Service, Department of the Prime Minister and Cabinet, and other CounterTerrorism Coordination Committee agencies.
- A new Director and Deputy Director Digital Safety have been appointed. Recruitment for other key PCVE roles is underway.
- We have signed a contract with a private provider to conduct research into the scale and nature of online violent extremism in New Zealand. This work is expected to take four weeks, and will help us develop a "map" of online extremism in New Zealand, which will also support the ongoing development of prevention strategies for both online and offline use.

Next steps

We will provide you with a verbal update on the progress of this work at the next officials' meeting.

30 June 2020

Countering Violent Extremism (CVE) online

On 26 May 2020, the Bill was introduced to the House, with the First Reading anticipated in July 2020.

7 July 2020

Countering Violent Extremism (CVE) Online

On 26 May 2020, the Bill was introduced to the House. The timing of the First Reading is to be confirmed.

In June 2020, we resumed engagement with key agency partners to ensure they integrate the online elements of countering violent extremism into their frameworks. This engagement is bringing real value to our understanding of the work.

We have received initial insights from our external research provider into the scale and nature of online violent extremism in New Zealand. These early findings will help frame the next phase of our research and identify any gaps as we develop a "map" of online extremism in New Zealand.

Recruitment to extend our capability is underway. We have received significant interest, and anticipate people starting from late-August 2020.

28 July 2020

Countering Violent Extremism (CVE) Online

On 26 May 2020, the Bill was introduced to the House. The timing of the First Reading is to be confirmed.

Recruitment to extend our capability is underway. We have received significant interest, and anticipate people starting by September 2020.

1 September 2020

Preventing and Countering Violent Extremism Online.

Recent activities

- We continue to progress our long-term thinking through a series of workshops with key agencies, building on the insights we have received from our external research partner into the scale and nature of online violent extremism in New Zealand.
- Appointments have been made to several senior positions in the Digital Violent Extremism team.
- We have received further insights from our external research partner into the scale and nature of online violent extremism in New Zealand. These have shown that there is substantive online far-right and hate speech activity in New Zealand, but by a relatively small group of people. We await more detailed insights over the coming weeks.

Next steps

A detailed workshop is scheduled for this week about the next steps for the longer-term strategy for harm prevention and minimisation strategies in New Zealand.

15 September 2020

Countering Violent Extremism (CVE) Online

We continue to work with key agencies to build on the external research into the scale and nature of online violent extremism in New Zealand, and to progress our planning.

13 October 2020

Countering Violent Extremism (CVE) Online

We continue to work with key agencies to build on the external research into the scale and nature of online violent extremism in New Zealand, and to progress our longer-term planning. We anticipate further insights from our external research partner in November 2020.

Work on the Preventing and Countering Violent Extremism framework, including key priorities, is progressing well.

The Manager Digital Violent Extremism, the Principal Advisor for Countering Violent Extremism, and the Manager Intelligence and Insights, have started. Appointments have also been made to the remaining senior and key leadership positions, completing the Digital Safety senior leadership team. These appointments will enable the Department to extend its focus on online violent extremist content.

27 October 2020

Countering Violent Extremism (CVE) Online

We continue to work with key agencies to build on the external research into the scale and nature of online violent extremism in New Zealand, and to progress our longer-term planning. We anticipate further insights from our external research partner in November 2020.

Work on the Preventing and Countering Violent Extremism framework, including key priorities, is progressing well.

Work on the Preventing and Harm framework and Cabinet paper are progressing well with contributions from key agencies.

20 January 2021

Increase to New Zealand's Online Crisis Response level

Recent activities

We have activated New Zealand's Online Crisis Response to the level of "Increased Monitoring" leading up to the Inauguration of the President of the United States of America, and following the recent violence and unrest in the United States.

This response is currently in place from the evening of 20 January to 22 January 2021 (NZT). Platforms, such as Twitter and Facebook, and media sites will be monitored continuously over this period.

Next steps

We will continue to monitor the situation and will advise if the response level changes from the current setting. Preparations have been made should a New Zealand crisis response become necessary.

We will provide you with a briefing following the conclusion of this response.

Document 2

Te Tari Taiwhenua
Internal Affairs

Preventing Countering Violent Extremism Programme

Scope Document

IN-CONFIDENCE

Cohesion: https://dia.cohesion.net.nz/Sites/RGL/PCVE/_layouts/15/WopiFrame.aspx?sourcedoc={a77d8d14-f4b3-4118-a34b-924db16db17e}&action=default&DefaultItemOpen=1

Document control

Project ID/Name	
Author	9(2)(a)
Title	Preventing and Countering Violent Extremism
File name	
Cohesion reference	

Revision history

Version	Date	Author	Description of changes
0.1	19/12/2019	9(2)(a)	First Draft
0.4	17/02/2020	9(2)(a)	Changes to document to include Programme Scope
0.6	02/03/2020	Amanda Duncan	Programme Team feedback
0.7	05/03/2020	9(2)(a)	Programme Manager feedback
0.8	12/03/2020	9(2)(a)	Final for Board approval

Distribution list

Name	Role	Business Unit
Carmel Ali	Programme Manager, PCVE Programme	Policy, Regulation and Communities
Marilyn Little	Deputy Chief Executive	Policy, Regulation and Communities
Raj Krishnan	General Manager, Policy	Policy, Regulation and Communities
Michael Woodside	Director, Policy	Policy, Regulation and Communities
Maarten Quivooy	General Manager Regulatory Services	Policy, Regulation and Communities
Jolene Armadoros	Director, Digital Safety	Policy, Regulation and Communities
Caroline Bridgland	Director, Office of Ethnic Communities	Policy, Regulation and Communities
Orsola Del Sante-Bland	Finance Business Partner	Organisational Capability and Services
Meredith Atkinson	Human Resources Business Partner	Organisational Capability and Services
Cristina Samson	Principal Communications Advisor—External	Organisational Capability and Services

Contents

Background

Under the Films, Videos, and Publications Classification Act 1993, (FVPC) the Department of Internal Affairs (the Department) has the powers to identify, seek the removal of and prosecute those sharing or possessing "objectionable material".

The definition of "objectionable material" includes content that deals with matters such as sex, horror, crime, cruelty or violence in such a manner that the publication is likely to be injurious to the public good (section 3 of the Films, Videos, and Publications Classification Act 1993). Specifically relating to violent extremist content, sections 3(d) and (e) state that particular weight should be given if the publication promotes acts of terrorism or infers particular groups are inherently inferior to other groups.

On 15 March 2019 during the aftermath of the Christchurch attacks the Department's Digital Safety Group took the lead working with technology companies and other agencies to reduce the spread of the attack video and manifesto. This was largely done through the relationships they had built with tech companies, non-government organisations (NGO's) and law enforcement agencies through the child exploitation and spam work.

As a direct result of the Christchurch attacks, the New Zealand Government alongside the French Government set up the Christchurch Call. The Christchurch Call is a commitment by Governments and tech companies to eliminate terrorist and violent extremist content online.

At the same time, the Department started a review into policy changes of Films, Videos, and Publications Classification Act 1993 that could strengthen New Zealand's position surrounding the censorship of live streaming and objectionable content to prevent online harm.

The Government approved several initiatives within the countering violent extremism and counter terrorism eco-system, one of which was to extend the work of the Department to focus on violent extremist online content.

Context

Preventing and countering violent extremism is both a domestic and global problem. It can manifest itself both physically and online within communities. The Department has a number of roles to play in the wider eco-system including:

- our work in the Digital Safety Group countering violent extremism online through the regulation and censorship of online content through the Films, Videos, and Publications Classification Act 1993
- contributing our operational expertise and thought leadership to the Christchurch Call work programme and the wider counter terrorism eco-system
- our regulation of aspects of the Anti-Money Laundering and Countering Financing of Terrorism Act 2009, which places obligations on New Zealand's financial institutions and casinos to detect and deter money laundering and terrorism financing

- our regulation of the New Zealand charitable sector
- our management of New Zealand's passport, citizenship and identity systems
- our policy work within New Zealand
- supporting New Zealand communities through the Office of Ethnic Communities, the Safer Communities Fund and the Ethnic Communities Development Fund.

The Department's operating context in the broader counter terrorism eco-system is complex and there are unique operational requirements to participate in this environment.

The Department is also supporting the independent inquiry, the Royal Commission of Inquiry into the Attack on Christchurch Mosques on 15 March 2019.

Programme Mandate

The Department received funding for four years to focus on minimising the harm from violent extremist and terrorist content online. There are three core components to the CVE uplift for DIA:

- Policy and legislative changes – FVPCA review and longer-term planning for a broader Media Content Regulatory Review
- Operational capability – establishing a new team dedicated to protecting people and communities from online violent extremism
- Considering long term strategy including how DIA can contribute to the prevention of violent extremism in New Zealand (for instance, thinking about community engagement, Office of Ethnic Communities opportunities etc)

Programme Outcomes

The programme will:

- ensure coordinated leadership of PCVE capability within the Department
- ensure a joined-up approach and key partnerships are in place to deliver PCVE across key government agencies
- embedded DIA in the current PCVE New Zealand eco-system
- deliver and embed a CVE function into the Department
- enable DIA to work alongside agencies to assist in the prevention of online violent extremism events in New Zealand
- facilitate the legal framework to allow services providers to do the right thing
- help to create safer, more resilient, thriving communities across New Zealand.
- operationalise a successful web filter for CVE content
- work across the system to deliver the prevention and engagement strategy for DIA
- ensure the Department understands and fulfils its obligations under the Christchurch Call

- collaboration and co-ordination across government organisation, non-government organisations and industry
- the right measures are in place to demonstrate the effectiveness of the new capability and prevention work.

Scope

The Preventing and Countering Violent Extremism (PCVE) Programme has been established to lead the:

- design and implementation of a new operational capability within the Department to focus on countering violent extremist content online and that is embedded in the broader eco-system in New Zealand
- policy and legislative changes to address gaps in current censorship regulatory system
- the proposed media content regulatory review to include online content hosts
- Christchurch Call commitments and resourcing within the Department
- design and development of a web filter tool to counter violent extremist content
- development of a long-term strategy for the Department in PCVE (including, but not limited to, additional prevention and community engagement opportunities).

The PCVE Programme is also responsible for the success of navigating and embedding the Department within the broader domestic and international countering violent extremist content online eco-systems. This includes:

- thought leadership
- oversight of how the Department shares its expertise and collaborates with the other agencies working in this space
- support of the different agencies working in this space
- working to prevent a siloed approach ensuring greater unity across the complex counter terrorism eco-system for Years 1 and 2 and beyond.

The PCVE Programme is responsible for, will oversee, and provide resources and reporting for the various phases of the programme workstreams.

In addition, the PCVE Programme is responsible for linking the New Zealand Online Crisis Response Process into the broader and already established infrastructure both internally and externally. The Programme will also provide coordination and secretarial support to the Senior Officials group and the Countering Violent Extremism Ministerial Group.

In Scope

The table below outlines what is in scope for the Programme.

Item	Details	Workstream
Establishing the new function within the Department, including any new structure, recruitment, training and health and safety.	The aim is to add approx. 17 new FTE across PRC to support the new function. Two FTE allocated to Policy and 15 FTE allocated to Digital Safety. Decisions on the structure will be made by the GM Regulatory Services as part of existing delegation.	CVE Build- Change stream
Extending the current Property portfolio to house the new function including making any changes to existing buildings to meet new security requirements, looking at co-location options and preparing a long-term property strategy.	Currently the Digital Safety Group is spread over three locations.	CVE Build-ICT/Property/Process streams
Extending the current technology infrastructure to include any new requirements for tooling and information sharing tools and protocols for CVE.	The Digital Safety IT infrastructure that sits outside of the DIA infrastructure.	CVE Build – ICT/Property/process streams
Embedding new security (ICT and Physical, Personal) requirements across the Digital Safety Group and any impacts on the wider DIA.	It is expected that the new function will be required to work at a classified level. The impacts of this will need to be understood across all aspects of the work.	Programme
Define the operating model under which the function will operate and how it will integrate into the wider CVE eco-system.	This will be done in collaboration with sector partners and overseas research and experience.	CVE Build – Change/process streams
Changes to the legislation and development of new regulations to the Films, Videos and Publications Classification Act.	Changes relate to gaps identified following the Christchurch attacks that would strength the current legislation.	Policy
Implementing any required regulatory changes resulting from changes in the FVPC Act.	The legislative changes are now expected to be enforce in early 2021.	Programme

Collaboration with relevant domestic agencies to develop appropriate process, information sharing and response protocols.	The effective operation of the new function in DIA is dependent on positive engagement and relationships with sector partners working in the current eco-system.	Programme
Christchurch Call operational obligations and relevant crisis response (including engagement with the Global Internet Forum to Counter Terrorism GIFCT).	DIA's role in the Christchurch Call will need to be considered as it requires resource from PRC, DS and Policy.	Prevention and Strategy – Christchurch Call
Wider Christchurch Call impacts.	Christchurch Call activities and discovery to understand the wider contributions and potential involvement from DIA.	Prevention and Strategy – Christchurch Call
Design and development of web filter options for CVE content.	Work through all aspects of the ability to create and manage the filtering of web content relating to CVE.	Prevention and Strategy - Filter
Administrative, secretarial and communications support for the Senior Officials group and the countering violent extremism Ministers group.	This allows greater coordination and oversight of what is happening across the sector.	Programme/ Communication and Engagement
Research, design and development of the prevention strategy for DIA.	The prevention strategy will set the future direction for CVE across the Department.	Prevention and Strategy
Budget Bids for out years for prevention.	PCVE to also be reviewed once function is operational.	Prevention and Strategy
Communication and Engagement.	Communications and engagement – provider the overarching communications strategy and messaging for the PCVE programme and lead co-ordination of communications across the sector partners.	Communication and Engagement

Out of Scope

The table below outlines what is currently considered out of scope for the programme.

Item	Notes
Budapest Convention and Cloud Act implementation.	These are slow burning initiatives that will have impacts on the operations of the new function. It is not expected to impact the initial set up.
Leadership of broader Christchurch Call work programme.	This is led by the Ministry for Foreign Affairs and Trade.

Programme Eco-System

There are multiple agencies involved in both the prevention and countering of violence extremism. The programme must embed this work into the wider eco-system which currently exists in New Zealand and is also undergoing a significant work programme as a result of the terrorist attacks.

The global nature of the work will require work both domestically and international through both engagements in international forums, working with international tech companies to working on international operations.

The Christchurch Call is the international component of the Government's work to eliminate terrorist and violent extremist content online. It is a commitment to work together with international partners to eliminate the content off the Internet. The spread of this content is a global problem and cannot be addressed within a global response.

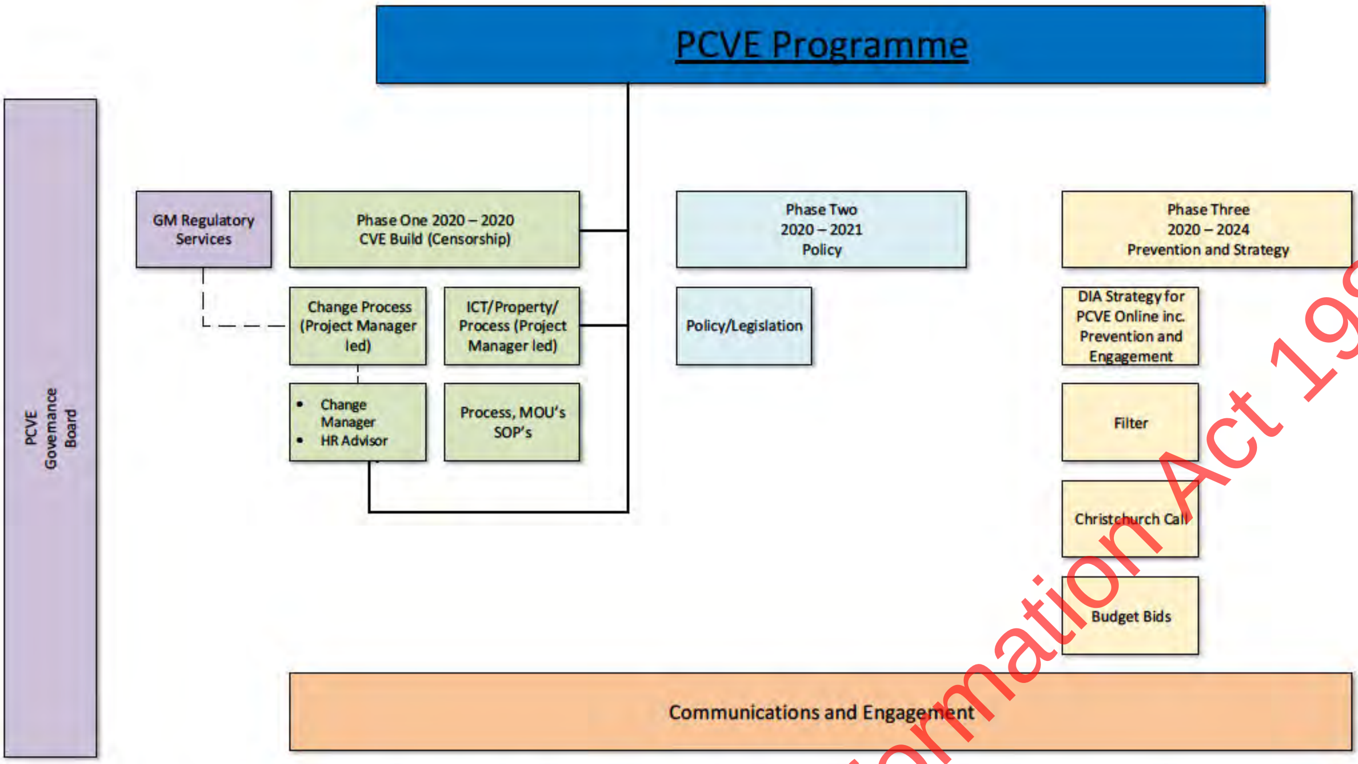
There is also a broader Government programme which includes the:

- Hate speech review (led by the Ministry of Justice),
- Budapest convention on cybercrime (jointly led by the Department of the Prime Minister and Cabinet and the Ministry of Justice),
- Social Cohesion (led by Ministry of Social Development
- Crowded Places (led by Police)

Approach

The programme work will be managed within phase. Each phase will have multiple workstreams and have a responsible business owner. The programme will seek guidance from the PCVE governance board, but decision making will sit with the Business Owners and Programme Sponsor.

The programme is will be responsible for the direction and co-ordination of activities across the phases in the programme.



Critical to the approach will be the need to work across the sector and with stakeholders to build the operational capability, policy and the prevention strategy. Given the importance of stakeholder engagement and communications, it has been called out as separate workstream that will work across all other workstreams.

The security considerations for this work programme will need to occur across the programme. They will be managed at the programme level and will filter down into all the phases.

Phases

The programme will include the following phases:

- CVE Build (Censorship)
- Policy
- Prevention and Strategy

Under each phase there are multiple workstreams. 'Communication and engagement' is a supporting function that runs across all phases.

CVE Build (Censorship)

CVE Build will include all aspects of operationalising CVE into the Censorship function with the Digital Safety group. This will include a technology capability, operating model, property and change/structure.

- The technology capability will deliver the technology strategy for the CVE function, as well as identify and implement technologies and tooling that will be required to support the function.
- The operating procedures capability will design the operating model for which the function will operate under. This will include a high-level outline of the framework for operation and move down to operating processes and procedures to support the day to day operations of the function.
- Change and structure will drive the change and care for existing people and new people coming into DS. This will include new structure and roles for CVE including management of the change consultation process; and the recruitment strategy
- Property will involve extending the property profile to include the new CVE function and any new security requirements for the function.

Policy

Policy includes

- The legislative changes required to support operationalising CVE and support the broader CVE workplan
- The media content review
- The Films, Videos, and Publications Classification (Urgent Interim Classification of Publications and Prevention of Online Harm) Amendment Bill, to be enacted in 2021, will make changes to New Zealand's media classification legislation to prevent harm from objectionable, illegal material.
- The Bill provides additional regulatory tools to manage harms caused by content that is live streamed, and/or hosted by online content hosts. The Bill also facilitates the establishment of a Government backed (either mandatory or voluntary) internet filter, if one was desired in the future. It provides Government with explicit statutory authority to explore and implement such mechanisms through regulations, following consultation.
- Wider work to reform the media content regulatory framework

On 16 December, Cabinet agreed to Ministers Martin and Faafoi to report back to it in 2020 with their proposed terms of reference, engagement approach for a comprehensive review to modernise New Zealand's media content regulation system.

The review is intended to be far reaching including consideration of the definition of media and providers that are regulated, and the values and standards underpinning the regime, as well as reviewing our existing regulatory model and legislative framework. Ministers will likely consider the inclusion of regulation of content on social media within the scope of the review when they report to Cabinet.

DIA and MCH officials are currently preparing advice to Ministers' on next steps for the review. Timelines for the review are yet to be determined.

Prevention and Strategy

Prevention and strategy will include:

- the design and implementation of a new web filter for CVE online content. This will need to provide policy, operational and technical advice to support the legislation provisions for the proposed filter as well as, the design and development of the filter if approved.
- Christchurch call ongoing commitments. The impact of the Christchurch call has changed the landscape for the Department and introduced an international and ambassador/leadership role for the Department in the global work to combat violent extremism online. The requirements and resourcing impacts for DIA will be managed within the programme.
- Budget bids process for ongoing years including any changes required to the CVE Censorship funding, Prevention Strategy and web filter work
- The DIA PCVE strategy including prevention, engagement and research

Communications and Engagement

Communications and engagement is central to the success of this programme and will need to occur at every level of this programme. As such the programme will be responsible for the secretarial support to the Senior Officials Group and the countering violent extremism Ministers group.

The communications and engagement will include:

- the development and ongoing tweaking of key messages for both internal (DS staff and the wider Department) and external audiences (both domestic and international) to support the ongoing narrative of the work programme and the wider CVE work
- involvement in an across government communications group to facilitate the sharing of information and agreed key messages within the eco-system

Assumptions

The following assumptions have been made in relation to the programme.

Assumption	Impact
The Christchurch Call will be an ongoing part of DIA's work programme	The impact and resourcing requirements will need to be understood and expectations managed across DIA and MFAT

The security classification for the team is expected to be at least to "Secret". There will be some work required at "Top Secret". Advice from partner agencies is that to fully participate in the eco-system both domestically and internationally, "Top Secret" classification will be required.	This may require a greater level of security around the property, technology and recruitment that is currently required within the CVE Build.
There is an existing eco-system in which DIA will need to work with partner agencies to confirm scope of role within the eco-system.	DIA does not lead or need to create – DIA will be guided by existing practice in other agencies.

Linkages

The table below outlines the linkages with other Groups or programmes.

Royal Commission of Inquiry into the Attack on Christchurch Mosques	Recommendations from the Royal Commission may need to be considered as a part of the operating model for the CVE function and how this team will operate in the CVE eco-system.
DIA Anti-Money Laundering (AML) Group	The AML Group works across anti-money laundering and countering financing of terrorism. They work within the same eco-system with a focus on financing of terrorism.

Glossary

Term	Definition
Countering Violent Extremism (CVE)	Preventing, responding and investigating violent extremism
Violent Extremism	**Violent extremism** refers to the justification of violence with the aim of radically changing the nature of government, religion or society. This violence is often targeted against groups that are seen as threatening violent extremists' success or survival (or those seen to support them) and to undermine violent extremists' world-view. This definition is in the Counter Terrorism Strategy approved by Cabinet on 16 September 2019 [CAB-19-MIN-0467 refers].
Terrorist Act	As defined in the Terrorism Suppression Act 2002, includes serious action, which includes causing death with an ideological, religious or political motivation and the intention to instil terror in a civilian population or to induce; or to compel the government to do or not do certain things. This definition is in the Counter-Terrorism Strategy approved by Cabinet on 16 September 2019 [CAB-19-MIN-0467 refers].
Objectionable Content	Under the Films, Videos, and Publications Classification Act 1993, "a publication is objectionable if it describes, depicts, expresses, or otherwise deals with matters such as sex, horror, crime, cruelty, or violence in such a manner that the availability of the publication is likely to be injurious to the public good...promotes or supports...acts of torture or the infliction of extreme violence or extreme cruelty...degrades or dehumanises or demeans any person, and/or promotes or encourages criminal acts or acts of terrorism.
Global Internet Forum to Counter Terrorism (GIFCT)	The Global Internet Forum to Counter Terrorism (GIFCT) was formally established in July 2017 as a group of companies, dedicated to disrupting terrorist abuse of members' digital platforms.
Christchurch Call	The Christchurch Call is a commitment by Governments and tech companies to eliminate terrorist and violent extremist content online.
Crisis Response	Refers to a critical incident where (1) the dissemination of content is linked to, or suspected as being carried out in, the context of terrorism or violent extremism; and (2) where there is an anticipated potential for viral dissemination across multiple online content hosts. This definition follows the European Union's Crisis Protocol for a collective response to viral spread of terrorist and violent extremist content online.

Digital Safety Operating Model

September 2020

Version 1.0

Te Tari Taiwhenua
Internal Affairs

New Zealand Government

Foreword

Whether you are new to the work of the Digital Safety team here at Te Tari Taiwhenua or whether you are already familiar with our journey, this document is intended to provide a helpful overview of our work. This operating model sets out:

- The digital safety environment in which we operate;
- The different roles of the digital safety team within that environment and the outcomes of our work;
- The various operational approaches and tools that we use to support our different roles; and
- Where we plan to take the next steps in our operational development.

If you are working as part of the Digital Safety team, or if you work with us to improve online safety for New Zealanders, you will hopefully see your contribution reflected in this document, or at least be able to see how your work helps create a safer online experience for all New Zealanders as part of the wider digital safety environment.

The Digital Safety team works in a fast-paced world where advancing technology and shifting social trends can create new challenges and opportunities seemingly overnight. As a result, we must adopt a flexible operational approach. So – the operating model set out in this document is version 1.0. It's our first, complete version. It gets us started and guides us – while providing a base for further fast-paced learning and development.

Thank you for all that you do to improve online safety for New Zealanders. This is purpose-driven work that addresses an area of modern life where there is huge potential for learning and connection – but also a huge potential for harm. This is particularly the case for our families, children and young people as well as our social structures and institutions.

Jared Mullen
Director of Digital Safety

6 September 2020

Contents

Executive Summary

Digital Safety within DIA operates in an environment characterised by complex and rapidly evolving technology and fractured, out of date legislation. The network of agencies who contribute to digital safety outcomes have overlapping and sometimes unclear regulatory roles – but work collaboratively overall to try and improve the online safety of New Zealanders.

In recent years DIA has operated in two main areas of the wider digital safety environment. The Department detects, deters and prosecutes those responsible for creating and sharing child exploitation material online – as well as assisting other local and international enforcement agencies in similar efforts. Our main tool for prevention is the digital child exploitation filter which blocks access to known child exploitation sites for users of those internet services who voluntarily subscribe to the filter. These operational activities have, until recently formed the basis of the Department's regulatory response to the Films, Videos and Publications Classification Act 1993 (FVPCA).

DIA also combats the harms arising from unsolicited electronic messages – spam and scams – providing an avenue of complaint for affected New Zealanders and working with New Zealand online businesses and agencies to help them comply with the law. Digital Safety administers a civil enforcement regime for those who choose not to comply. These operational activities form the basis of the Department's regulatory response to the Unsolicited Electronic Messages Act 2007.

Digital safety is strengthening operations in our traditional areas by:

- Making better use of our enhanced intelligence and insights capability to ensure that valuable investigative resource is targeted to the areas that will have greatest overall effect.
- Using up-to-date expert knowledge of child exploitation pathways to develop and execute a series of trials of preventative online techniques.
- Contributing our operational expertise in combating harmful digital messaging to create a better case for reform of outdated legislation.

The digital safety environment is both a product of wider societal change and a driver of it. One such societal change has been the rise of online extremism culminating in the distribution of online material as part of the terrorist attack in Christchurch on 15 March 2019 and subsequent copycat attacks.

The efforts of Digital Safety in co-ordinating the wide response to the viral, online spread of the Christchurch attacker's promotional video and propaganda have led to increased Government investment to help DIA to better address online violent extremism. In the short term, we are strengthening our operational capability by:

- Establishing and operating a highly capable intelligence and insights function to better understand and be prepared for the spread of extremist material online;
- Strengthening our collaboration and coordination with partner agencies in responding to online extremism; and

- Developing an ability to detect, investigate and if necessary enforce breaches of the FVPCA in relation to violent extremist material online.

After these first steps, Digital Safety will expand our operational capability to encompass preventative approaches that are informed by intelligence, insight, experience and research.

Another large societal shift occurred as New Zealand responded in an unprecedented way to the COVID 19 virus. The increased risk of digital harm, particularly for families and young people was acknowledged by Government and DIA was given responsibility for a major, highly successful digital safety campaign.

The campaign is ongoing and phase 2 has begun. Although the risk from COVID 19 will hopefully diminish, the risks to young people and families arising from the digital environment will likely continue to increase. Digital Safety will build its knowledge of both the science and practice of digital harm prevention and apply this to a full range of targeted, harm prevention approaches. We will continue to play a connecting role – ensuring that the best use is made of the shared expertise of all agencies who provide harm prevention services.

The knowledge and experience of Digital Safety will be helpful in assisting DIA’s effort to lead a comprehensive reform of media regulation in New Zealand.

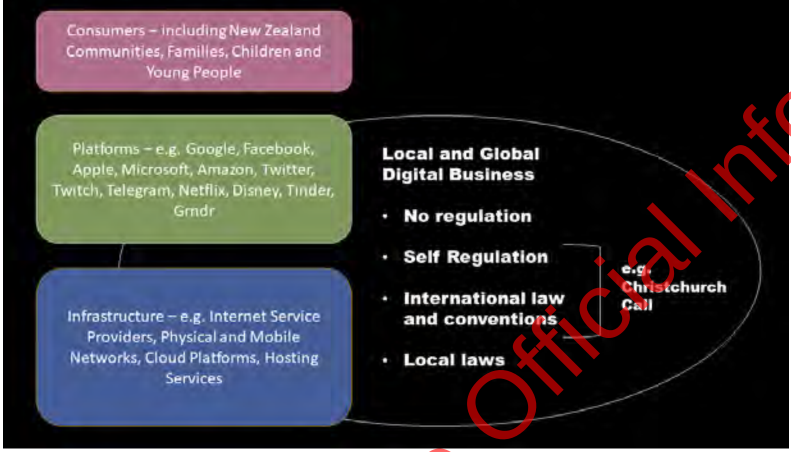
The Digital Safety Environment

The concept of Digital Safety is all about the people who use online services. New Zealanders online should be psychologically and physically safe. New Zealanders should feel free to participate online and express themselves regardless of their gender, race, sexual orientation or religious background. Their property and money should also be safe from illegal activity while they are online.

Although the concept of digital safety for New Zealanders might be simple, there are many aspects of a highly dynamic environment that impact on the actual level of digital safety experienced by New Zealand families, young people, children and communities.

Figure 1 shows a view of layers of the online environment.

Figure 1: The Digital Safety Environment


Consumers – including New Zealand Communities, Families, Children and Young People
Platforms – e.g. Google, Facebook, Apple, Microsoft, Amazon, Twitter, Twitch, Telegram, Netflix, Disney, Tinder, Grndr
Infrastructure – e.g. Internet Service Providers, Physical and Mobile Networks, Cloud Platforms, Hosting Services
Local and Global Digital Business
No regulation
Self Regulation
International law and conventions
Local laws
e.g. Christchurch Call

Most important are the Consumers (end users) and level of online safety they experience.

Whether connecting with each other, searching for and receiving/storing information or accessing entertainment, New Zealanders will have contact with some of the platforms that are mentioned in the green box of figure 1.

Of course, these are just examples of the galaxy of apps and environments that provide access to services online.

Platforms are in turn supported by online infrastructure. For example, information flows over physical and mobile networks, platforms can be hosted on cloud-based services, and connection between the platform and the customers is provided by Internet Service Providers.

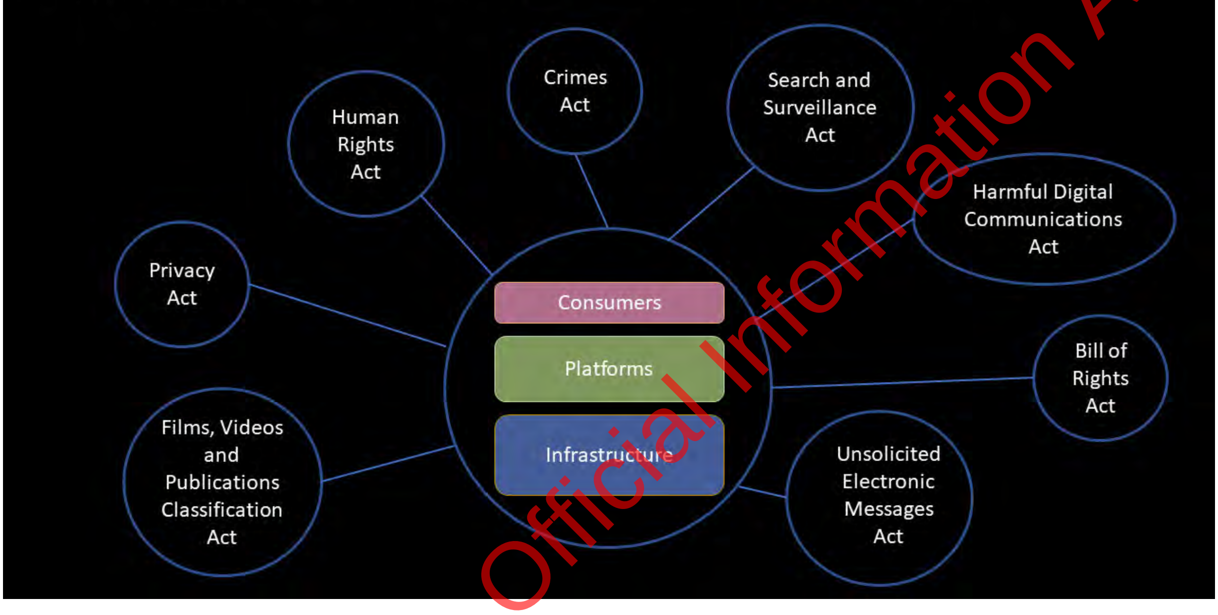
Platforms and some aspects of online infrastructure are increasingly dominated by large international corporations who deliver services around the globe. Consequently, the regulatory environment that governs how the whole system operates and affects the level of safety experienced by end users is a mixture of:

- Local laws (to the extent that these apply);
- International Law and Conventions (such as the Budapest convention on cyber-crime);
- Industry self-regulation through organisations such as the Global Internet Forum to Counter Terrorism (GIFCT), or voluntary participation in agreements such as the Christchurch Call; and
- No regulation at all.

New Zealand Regulation is Complicated – But Not Comprehensive

As Figure 2 shows, there are a number of different, local laws that influence the online safety of New Zealanders – many of which are out of date and conceived at a time well before the reality of today's online world was imagined. The many and varied frameworks can also create confusion on the part of consumers and industry. The application of New Zealand law to our online environment is patchy – especially where global corporations are concerned.

Figure 2: New Zealand Legislation Relating to Digital Safety


Crimes Act
Search and Surveillance Act
Human Rights Act
Harmful Digital Communications Act
Privacy Act
Consumers
Platforms
Infrastructure
Bill of Rights Act
Films, Videos and Publications Classification Act
Unsolicited Electronic Messages Act

Rights based legislation such as the Human Rights Act and the Bill of Rights Act protects New Zealanders from discrimination and preserves their right to freedom of expression. New Zealand criminal law applies to aspects of our online lives as does the search and surveillance legislation that supports the evidence gathering activity of local enforcement agencies.

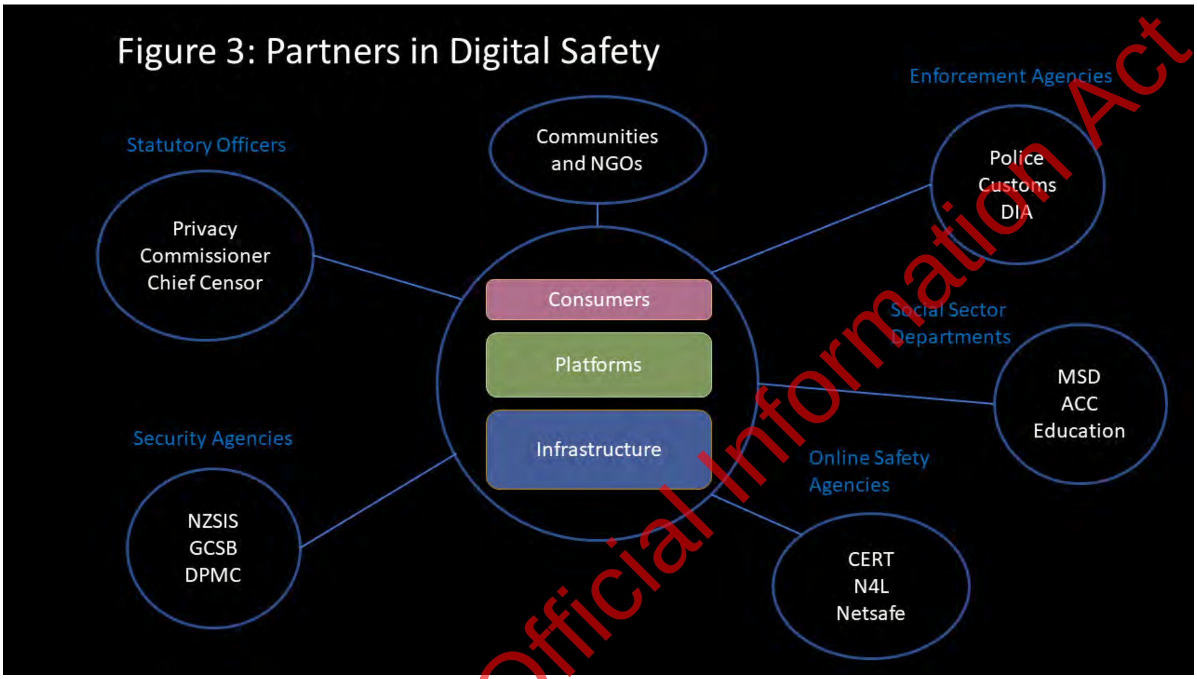
The Privacy Act protects New Zealanders' privacy and aims to ensure that our private information is only used for lawful purposes. The Films, Videos and Publications Classification Act is intended to restrict access to harmful content, prevent access to banned content and ensure that commercial films and streaming services display adequate consumer information.

The Harmful Digital Communications Act exists to protect individual users from certain types of online harm caused by other users. The Unsolicited Electronic Messages Act was passed to provide a level of protection from "Spam" (electronic junk mail).

The Department of Internal Affairs is responsible for operationalising only two of these pieces of legislation. The Films Videos and Publications Classification Act and the Unsolicited Electronic Messages Act.

New Zealand Digital Safety Partners Form a Complex Network

As you would expect, with such a wide array of laws applying to the online space, there is a correspondingly large number of individual agencies with a role to play in administering and applying the laws that help keep New Zealanders safer online. Figure 3 shows many of the agencies that play important roles in the online environment.



Enforcement agencies including Police, Customs and Internal Affairs work together to detect, investigate and, if necessary, prosecute breaches of the Films, Videos and Publications Classification Act. NZSIS, GCSB and DPMC form the core of our National Security community and are concerned with online behaviour that can pose a security risk to our country and our people.

Independent Crown Entities such as the Privacy Commissioner and the Chief Censor act to apply and interpret their respective legislation and increasingly provide public information and education. Non-government organisation Netsafe has a statutory role as the responsible agency for the Harmful Digital Communications Act and also has public education and advisory functions. Internet New Zealand is a sector body that champions internet freedoms.

New Zealand's Computer Emergency Response Team (CERT) has a role in helping New Zealand organisations remain secure online and Network for Learning (N4L) provides safe and secure network services for New Zealand schools. Social agencies such as Oranga Tamariki, the Ministry of Social Development, the Ministry of Education and ACC are also concerned with aspects of New Zealanders' online safety because of the link between digital harm and real-world outcomes.

Given the dispersed nature of regulatory authority and operational expertise across the system, agencies will often need to work collaboratively. In the aftermath of the Christchurch terror attacks for example, DIA worked with Police, New Zealand Internet Service Providers, large platforms such as Google and Facebook, and the Office of Film and Literature Classification to deal with the significant harm caused by the killer's video and his manifesto.

DIA cannot effectively regulate for digital safety on our own. It will take most online users, partner agencies, communities and industry partners working together to make a real difference.

Sometimes the work will have formal working arrangements, such as Memorandums of Understanding and operating procedures. Sometimes Digital Safety will lead and sometimes we will support or follow.

Our Digital Safety Operational Roles and Outcomes

DIA's role in the Digital Safety system derives from its responsibility for two of the many pieces of legislation described in Figure 2 above: The Films, Videos and Publications Classification Act (FVPCA); and the Unsolicited Electronic Messages Act (UEMA).

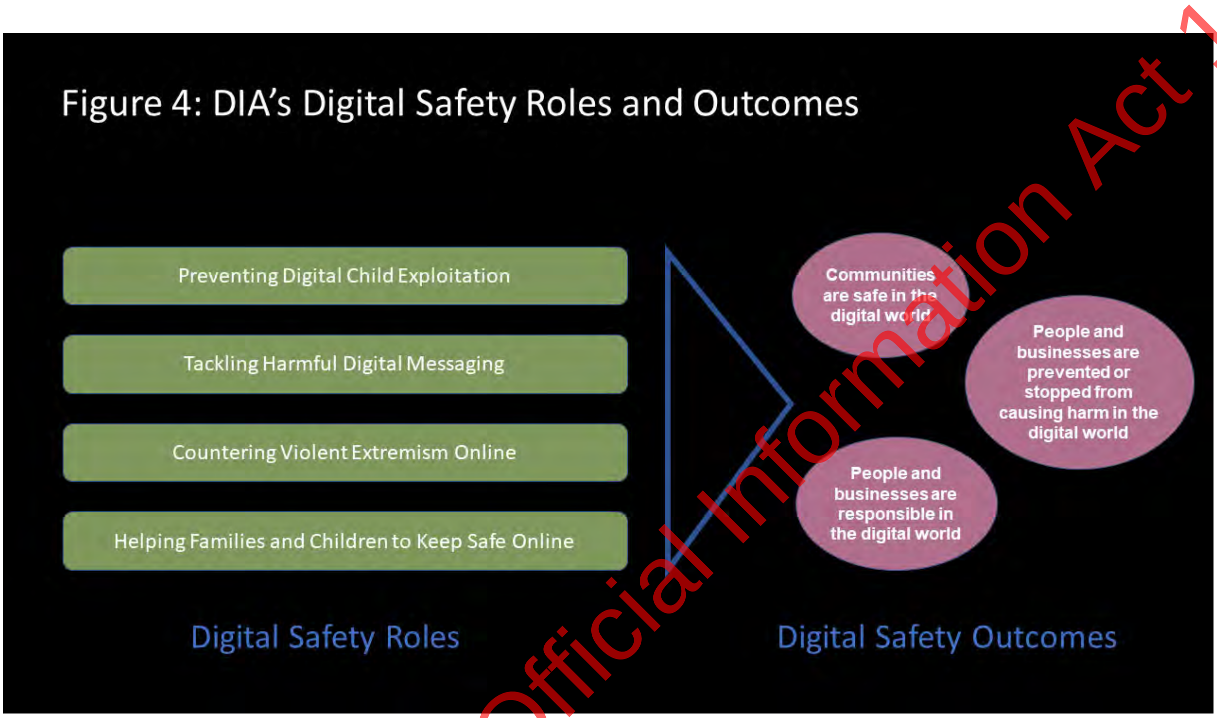


Figure 4: DIA's Digital Safety Roles and Outcomes

Preventing Digital Child Exploitation

Tackling Harmful Digital Messaging

Countering Violent Extremism Online

Helping Families and Children to Keep Safe Online

Digital Safety Roles

Communities are safe in the digital world

People and businesses are prevented or stopped from causing harm in the digital world

People and businesses are responsible in the digital world

Digital Safety Outcomes

On the face of things, the two pieces of legislation appear relatively straightforward. The UEMA attempts to ease the online burden for consumers and businesses by prohibiting unsolicited commercial electronic messages with a New Zealand link from being sent. The FVPCA is intended to restrict access to harmful content, prevent access to banned content and ensure that commercial films and streaming services display adequate consumer information. The FVPCA seeks to balance the harm arising from content with the right to freedom of expression set out in the Bill of Rights Act (BORA).

In practice – the responsible application of these two pieces of legislation often ensures that DIA's Digital Safety Team often has a larger, central role to play in ensuring that the online space is made safer for New Zealanders.

Our Traditional Regulatory Roles and Responses

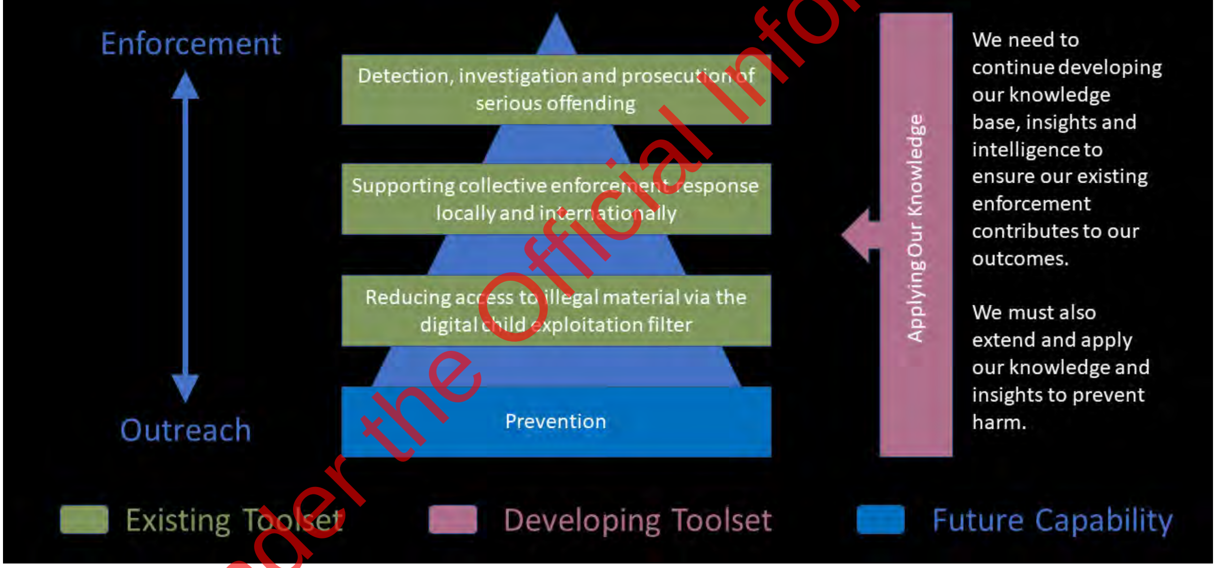
The FVPCA confers authority on the Secretary of Internal Affairs that is exercised under delegation by the Digital Safety Team. The Act also grants authority to Inspectors of Publications in administration and enforcement of the law. Similarly, the UEMA confers functions and powers on the enforcement Department (DIA) and on Enforcement Officers acting on delegated authority within the Department.

Combatting Digital Child Exploitation

Prior to March 2019, faced with very limited resources and high demand, DIA had chosen to focus the majority of its operational and regulatory effort towards addressing the significant individual and societal harm arising from online child abuse. The exploitation of children online continues to be a significant and growing problem.

Figure 5 shows how the Department currently approaches the prevention of digital child exploitation. The majority of our current efforts continue to be directed at detecting, investigating and prosecuting those that produce, distribute and possess illegal child sexual abuse and other illegal child abuse content. This is a significant collaborative effort with local and international law enforcement agencies - with whom the Digital Safety team have cultivated collaborative, close and productive relationships.

Figure 5: Preventing Digital Child Exploitation



Enforcement

Outreach

Detection, investigation and prosecution of serious offending

Supporting collective enforcement response locally and internationally

Reducing access to illegal material via the digital child exploitation filter

Prevention

Applying Our Knowledge

We need to continue developing our knowledge base, insights and intelligence to ensure our existing enforcement contributes to our outcomes.

We must also extend and apply our knowledge and insights to prevent harm.

🟩 Existing Toolset 🟪 Developing Toolset 🟦 Future Capability

We also provide a filtering service on a voluntary basis to New Zealand Internet Service Providers. The filtering service blocks access by New Zealand based internet users to sites found to contain child abuse and/or exploitation material. The filter directs the user to a page that provides information on how to seek help and presents information on how to question the decision made by DIA to filter the particular site. The operation of the filter is overseen by an independent reference group with external representation.

Developing Our Regulatory Capability to Prevent Child Exploitation

We are investing in an enhanced intelligence and insights capability to better understand and direct our scarce resources to the areas that will have the greatest impact. We currently prioritise our investigative efforts towards cases that present a high risk of real world harm to children – but we do not yet understand the extent to which this targeting of cases is consistent with the long-term prevention of harm.

We are also investing in a programme of trials of prevention activity to assess what works, and what can be rolled out quickly and efficiently.

Reducing Harmful Digital Messaging

Although current in 2007, the UEMA has since fallen behind the times in its coverage of the use and abuse of personal information to intrusively market both legal and illegal goods and services to New Zealanders online, and to prevent the increasing spread of scam messages and emails.

Figure 6 illustrates how the Department has focused the resources of a small, dedicated Digital Messaging team who work within the UEMA on dealing with cases that pose the greatest online risk to New Zealand consumers. This has been achieved through effective analysis and triage of the high volume of incoming complaints to determine cases where unwanted electronic messaging also intersects with other unethical or illegal behaviour (such as selling non-existent or overpriced personal protective equipment during COVID 19 for example).

The team also works with entities to ensure that they comply with the law. For example, charities who were looking to raise funds during COVID 19 were provided with advice on how to do this lawfully.

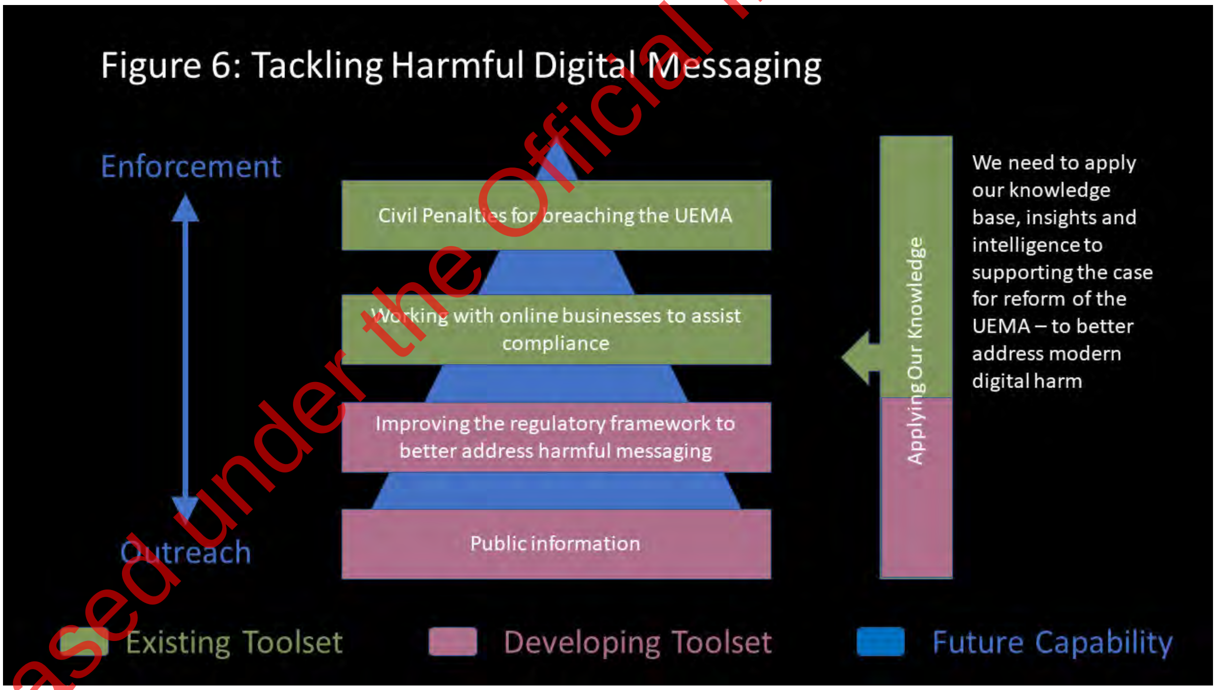


Figure 6: Tackling Harmful Digital Messaging

Enforcement

Outreach

Civil Penalties for breaching the UEMA

Working with online businesses to assist compliance

Improving the regulatory framework to better address harmful messaging

Public information

Applying Our Knowledge

We need to apply our knowledge base, insights and intelligence to supporting the case for reform of the UEMA – to better address modern digital harm

🟩 Existing Toolset 🟥 Developing Toolset 🟦 Future Capability

Improving Our Capability to Tackle Harmful Digital Messaging

Given the aged, porous legislation, one of the most effective approaches we have is to join up with others who are also active in the online protection space – Netsafe for example – to contribute to effective public messaging that builds public awareness of, and resilience to, spam and scams.

We must also work to build the case for more modern, comprehensive regulation that tackles intrusive, predatory and deceptive online commercial behaviour.

Our Changing Regulatory Role in Rapidly Changing Times

In addition to our traditional regulatory roles in the digital safety system described above, we have had to adapt and change to accept new responsibilities in response to a rapidly changing environment. The impact of online violent extremism and the impact on New Zealand households of COVID 19 have both given rise to expanded roles and responsibilities for the Digital Safety Team.

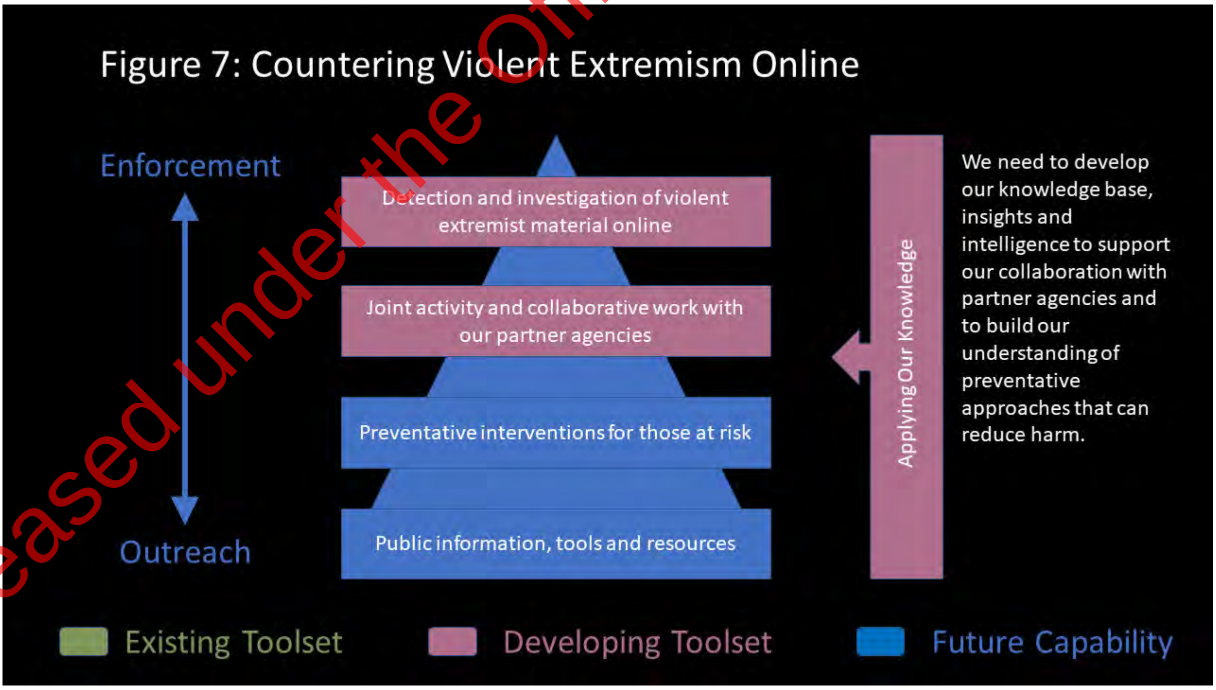
The Rise of Online Extremism

Since the September 11, 2001 Terrorist attacks in the United States, online extremism has been an increasing problem. Advancing technology, connectivity and the emergence of omnipresent social media has provided the ideal opportunity for violent extremists to spread their message and gain participation (both on and offline) for their cause.

Although the existence of objectionable (illegal) violent extremist material online is not new, the regulatory response was largely provided by Police and Customs who sought classification of, and conducted enforcement relating to objectionable content made available by terrorist organisations such as Islamic State and Al Qaeda. As discussed earlier, DIA concentrated its scarce resource on limiting the availability of illegal child exploitation material.

However, in the aftermath of the March 15, 2019 attacks on two Christchurch Mosques, the Department led the co-ordination and response to the viral availability of the online promotional material produced by the far-right terrorist.

Figure 7: Countering Violent Extremism Online


Enforcement
Outreach
Detection and investigation of violent extremist material online
Joint activity and collaborative work with our partner agencies
Preventative interventions for those at risk
Public information, tools and resources
Applying Our Knowledge
We need to develop our knowledge base, insights and intelligence to support our collaboration with partner agencies and to build our understanding of preventative approaches that can reduce harm.
Existing Toolset
Developing Toolset
Future Capability

Our efforts led to a significant additional investment by Government in DIA's capability to respond to online violent extremism. The department established a programme to embed the new capability into the department and has been implementing new roles and systems in the Digital Safety directorate to operationalise the new approaches.

As Figure 7 shows, the initial focus is on three areas:

1. The establishment of a highly capable intelligence and insights function so that New Zealand can be aware of and understand the spread of extremist material online, and be better prepared for any adverse online or offline consequences;
2. Sharing this information with our partner agencies so that we can collaborate and coordinate our responses to online extremism; and
3. An ability to detect, investigate and if necessary enforce breaches of the FVPCA in relation to violent extremist material online.

However, Figure 7 also shows that Digital Safety will need to develop and contribute to better prevention initiatives in relation to online extremism which may include relevant, targeted public information and tools that support New Zealanders to keep themselves safer online. Our prevention approach will be informed not only by our investigation, intelligence and insights work, but also by our engagement with communities and experts in the field.

A Safer Family Online Environment During COVID 19 Restrictions

As the COVID 19 pandemic spread worldwide, and made its way to New Zealand, Government implemented a level 4 alert, effectively confining New Zealanders to their homes, in order to contain the spread of the virus. Expert advice to Government highlighted the risks posed by increased exposure of young people to the online environment during level 3 and level 4 restrictions.

As a result, DIA was funded to lead a large scale public information campaign to improve awareness of online risks for children and young people and to provide practical tools and approaches to support families to keep themselves safer online. *Keep it Real Online* is highly successful and has involved the collaboration of DIA's Communications and Digital Safety teams as well as Netsafe, OFLC, Education and Police.

Phase 2 of the campaign continues this collaborative approach but also draws in a slightly wider group of agencies and young people in the design of approaches to appeal directly to younger age groups.

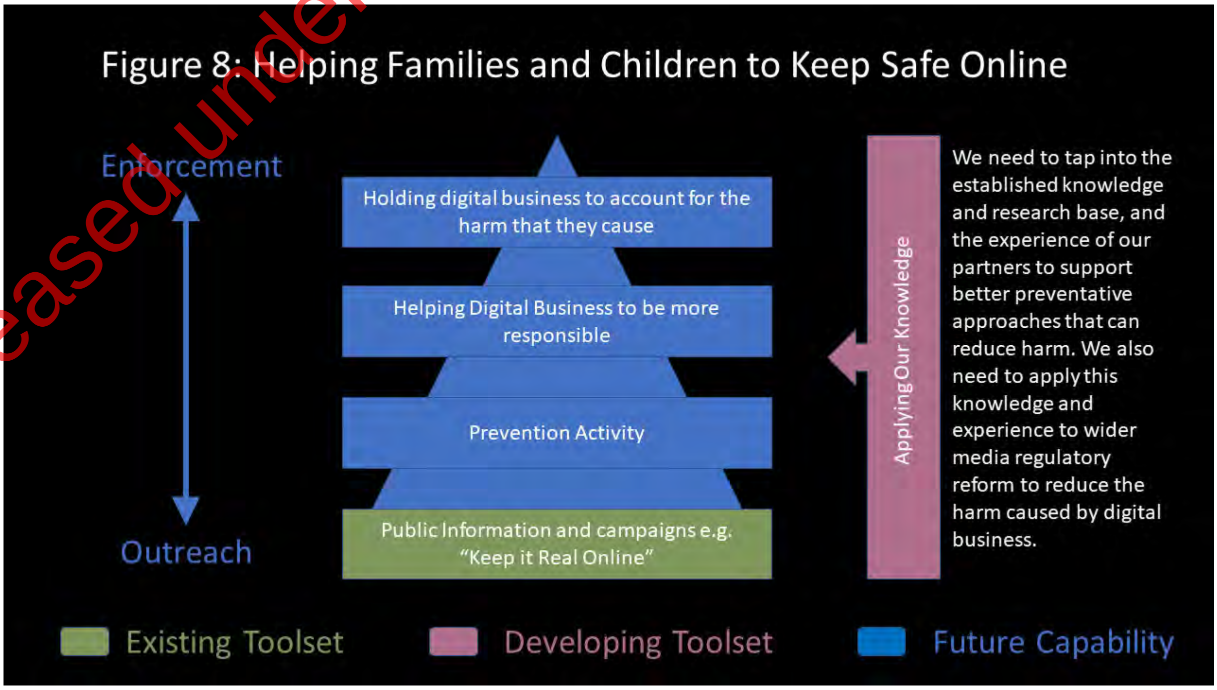


Figure 8: Helping Families and Children to Keep Safe Online

Enforcement
Outreach
Holding digital business to account for the harm that they cause
Helping Digital Business to be more responsible
Prevention Activity
Public Information and campaigns e.g. "Keep it Real Online"
Applying Our Knowledge

We need to tap into the established knowledge and research base, and the experience of our partners to support better preventative approaches that can reduce harm. We also need to apply this knowledge and experience to wider media regulatory reform to reduce the harm caused by digital business.

🟩 Existing Toolset 🟪 Developing Toolset 🟦 Future Capability

Keep it Real Online has shown that DIA is uniquely placed as a government Department to connect the various strands of existing work to better protect children and young people online. Although COVID 19 may eventually diminish, the risk of harm to children and young people posed by the worst aspects of the online environment will likely endure – and increase.

As a result, as shown in Figure 8, it is vital that DIA builds its knowledge of both the science and practice of digital harm prevention and applies this to a full range of targeted, preventative approaches that support the public information and widely available tools for parents and young people. There are many non-government and community organisations, in addition to Government agencies, with expertise and knowledge in this area. Digital Safety will continue to play a connecting role – ensuring that the best use is made of the knowledge and information available to New Zealanders.

DIA is also poised to lead a wider review of media content regulation in New Zealand and the operational knowledge and experience of the Digital Safety directorate will be a helpful in assisting this effort.

Document 4

New Zealand Online Crisis Response Process

Te Tari Taiwhenua
Internal Affairs

New Zealand Government

Contents

Introduction

On 15 March 2019 a terrorist opened fire in two mosques in Christchurch killing 51 and wounding 49 others. This unprecedented attack was live streamed on social media. The video was then copied and hundreds of variations of it were identified across multiple platforms in the coming days. In addition to the video, the shooter also released a manifesto outlining his motivations for the attack. Both the video and the manifesto were classified as 'objectionable'.

This attack, the lessons learned through the response to mitigating the harm of the online content of this attack and others, have highlighted the need to put in place a domestic response process. Government, non-government (NGO's) and Online Service Providers (OSP's) must work together in a co-ordinated way to mitigate harm to New Zealanders of online content associated with terrorist and violent extremist acts. The nature of the internet is such that response must be swift to disrupt the spread and potential for harm in such circumstances.

This document outlines the agreed voluntary Crisis Response Process for organisations in New Zealand to adopt in the event of a future online crisis. Furthermore, it details the roles and responsibilities of the agencies involved, the assessment process used to activate an online crisis response and the steps involved in the initiation and deactivation of a crisis response in New Zealand. This response process is a living document and will be tested and refined on an ongoing basis.

Note the Crisis Response Process will not replace any existing legal requirements, mandate or standard operating procedures in place for any organisation involved.

Purpose of the Crisis Response Process

The Crisis Response Process aims to facilitate the rapid assessment and coordinated response to an online crisis, within the scope outlined below, and the sharing of intelligence and information in a secure and timely manner between all government, NGO's and OSP's involved. This process will connect to the processes developed through the Christchurch Call Shared Crisis Response Protocol, European Union (EU) Crisis Protocol, and the Global Internet Forum for Countering Terrorism (GIFCT) Content Incident Protocol.

The Crisis Response Process details the coordinated response to significantly harmful content that requires an immediate response by multiple parties to mitigate the harm associated with it. This includes content that is or is likely to be objectionable and/or content that should not be visible and viewed by vulnerable members of society. For the purposes of this process vulnerable members of society are defined as those who may experience increased harm, discrimination or intolerance as a result of their race, ethnicity, age, religion, gender and sexual identity both in the physical and online world.

This process has been developed in response to the content associated with the 2019 Christchurch terror attacks. It is envisaged that the primary use of these process will be in relation to terrorist/ violent extremist content online. It is envisaged that this process could also be used in a scenario where significantly harmful content such as video depicting the sexual exploitation of a child is circulated broadly and unprompted on open social media platforms for instance.

Identifying an Online Crisis

An online crisis for the purpose of this process is described as:

'A piece of significantly harmful (highly likely to be 'objectionable') online content that has broad spread both geographically and/or across multiple platforms, and is likely to create significant harm for New Zealanders who are exposed to it'

Any agency participating in the Crisis Response Process can raise concern about a potential online crisis and contact the nominated Crisis Manager to determine whether or not this Crisis Process should be activated.

Government – Government agencies may identify a potential online crisis through their business as usual activity in the online space, through existing relationships or complaints from members of the public.

Online Service Providers - OSP's for the purposes of this document refer to the technology industry, internet service providers, and social networking services. OSP's may notice a spike in activity associated with harmful content for instance and let the Crisis Manager know.

NGOs/ Other's - Other organisations may be made aware of an online crisis from their local community, customer complaints, platform users etc.

The notification of a potential online crisis should be made to the Director of Digital Safety (or their delegate) at DIA as they will act as the Crisis Manager in the first instance (contact points provided on Appendix One). When notifying the Crisis Manager about a potential online crisis, the relevant organisation should relay (wherever possible):

- the nature of the content
- potential/perceived threat(s)
- any information they have available to assist in assessment

Determining if the Crisis Response should be activated

Assessing the Harm of the Online Crisis

Once online content has been flagged to the Crisis Manager, they must assess the situation and determine the how harmful the content is. This process does not replace business as usual delivery and assessment of online harm, this is reserved only for consideration of content that may reach the 'crisis or increased monitoring threshold'.

To make this assessment the following key questions should be considered in conjunction with the judgement of the Crisis Manager. These questions are intended to be a guide to inform the assessment of the need for Crisis process activation:

Key Question	
Harm to the Public	Does the content promote, incite or glorify violence? *Crisis Manager to determine the extent to which the content promotes or glorified terrorist/ violent extremist ideologies*
	Does the content depict matters of crime, cruelty or violence?
	Does the content depict a real-life incident?
	Could vulnerable members of society who are exposed to the content experience physical or psychological harm?

Key Question	
	Is the content appearing or likely to appear on individuals' newsfeeds and homepages? *If yes, this suggests the content is being actively promoted by different platforms or by individuals, including through algorithmic settings. In this case, such indicators suggest higher / increased virality (geographically and by platform), reproducibility & resilience of such material to takedown efforts*
	Do individuals or groups appear the be seeking to deliberately subvert detection and takedown/ removal systems?
	If terrorist or violent extremist content, is it perpetrator/ accomplice produced and/or live streamed?
	Does the content target or involve specific/ minority groups?

Note: the above questions should be re-considered as more information comes to light during the crisis process, it will not often be possible to have answers to all of these questions at the outset to determine if the crisis process is activated.

Other Considerations

There are a number of other factors that may help inform the Crisis Managers decision when assessing the harm of the online content to determine whether a crisis response should be invoked:

Question	Consideration
Is the content likely to be deemed objectionable?	Content that "*describes, depicts, expresses or otherwise deals with matters such as sex, horror, crime, cruelty or violence in such a manner that the availability of the publication is likely to be injurious to the public good*" [1]can be deemed objectionable by the Office of Film and Literature Classification (OFLC). Once content has been classified as objectionable it is prohibited to possess or distribute it.[2] When assessing whether content should be classified as objectionable, the Chief Censor will consider it in line with the definitions in the Films, Videos and Publications Classification Act 1993.
Is the content likely to be appropriate for adults but not for children?	Some content may not be deemed objectionable but may contain high impact cruelty or violence and may not be suitable for all members of the public to view i.e. bystander footage or journalistic coverage of an incident. In these instances, the Chief Censor may classify the content as R18.
If related to a real-life event, does the crisis appear to take place in New Zealand?	If a physical incident/ crisis takes place domestically and the Crisis Manager deems there to be considerable impact to New Zealanders, DIA will drive the Crisis Response Process and reach out to the relevant domestic and international bodies to get support in gathering intelligence and reducing the spread of the content online. The Crisis Manager will update this range of partners with relevant information from the ground level. The Crisis Response Process will feed into the wider DIA Internal Response Process for a Domestic Crisis[3]. DIA will work closely with NZ Police to share intelligence and evidence to support their investigation.

[1] Section 3(1) of the Films, Videos and Publications Act 1993

[2] Objectionable content is prohibited under section 123(1) of the Films, Videos and Publications Act 1993

[3] Depending on the crisis that occurs it may be necessary to liaise with the relevant Minister(s) as well as the Prime Minister

Question	Consideration
If related to a real-life event, and the incident/ crisis took place abroad, does it appear to include, indicate a threat to, or involve New Zealanders?	If the incident/ crisis took place overseas, the Domestic Crisis Response Process may be activated if the Crisis Manager deems there to be considerable impact to New Zealanders. New Zealand will adopt a supporting role and will take direction from the Christchurch Call Shared Crisis Response Protocol, European Union (EU) Response Process to Online Crisis, and the GIFCT Content Incident Protocol should one or more of these protocols be activated. The Crisis Response Team will work alongside the impacted country(s) and platform(s) to gather and share intelligence on the spread of the content including by sharing hashes and URLs with international agencies to contain the spread of the content. We will also work closely with the Ministry for Foreign Affairs and Trade in instances where New Zealand citizens are among the victims.
Did the perpetrator(s) announce their intentions online before the attack?	Did the perpetrator(s) upload any content that appears to have announced their intention to carry out an attack before the incident/crisis? Did the perpetrator(s) promote the attack(s) online i.e. providing links to the where it would be streamed or uploading a manifesto beforehand?
Does the content contain identifiable information about victims or any other person?	Exposure to content that contains identifiable information or images of the victims may reignite a survivor's trauma and/or result in significant psychological effects on a range of vulnerable individuals exposed to it.

Note: The Crisis Response will endeavour to preserve content that is a genuine historical archive or that condemns/raises awareness of an event, in accordance with international human rights law, including freedom of expression.

Risk Consequence Guide

Once the manager has assessed the content in terms of the potential harm, they should consider the severity of the harm that the public may be exposed to. The below table provides non-exclusive guidance on how to consider consequences of content in assessing the situation – not all points have to be met at a given level to constitute, for instance, a severe consequence grading e.g. Targeting or potential targeting of a specific or minority group is not an absolute/deciding requirement for an incident/ potential crisis to be graded/classified as severe. The Crisis Manager will take a decision based on information to hand:

Scale	Harm	Virality	Associated Risk
Severe	Content promotes, incites or glorifies violence Content that glorifies, promotes or incites terrorism/ acts of terrorism/ violent extremism Exposure may cause a high degree of physical or psychological harm The content targets a specific or minority group	Content appears on homepages or newsfeeds Content has a significant volume of shares, likes, comments and views Content may appear on multiple platforms across multiple countries	Content may be classified as objectionable Perpetrator(s) may have announced their intention to carry out the attack(s) or promoted the attack(s) online beforehand Content may include identifiable information or images of the victims
Significant	Content may promote, incite or glorify violence Content may cause some physical or psychological harm Content that glorifies, promotes or incites terrorism/ acts of terrorism/ violent extremism The content may target a specific or minority group	Content appears on homepages or newsfeeds Content has a high number of shares, likes, comments and views Content may appear on more than one platform across multiple countries	There may be propaganda material relating to the crisis appearing online Content may be classified as objectionable or R18 Content may include identifiable information or images of the victims
Moderate	Content that glorifies, promotes or incites terrorism/ acts of terrorism/ violent extremism Content may not be appropriate for children or vulnerable individuals	Content may appear on a limited number of homepages or newsfeeds Content has some shares, likes, comments and views Content may appear on multiple platforms across multiple countries	Content may be classified as R18 or objectionable

Scale	Harm	Virality	Associated Risk
Minor	Content that glorifies, promotes or incites terrorism/ acts of terrorism/ violent extremism Minimum physical or psychological harm	Content has limited number of shares, likes, comments and views Content may appear on multiple platforms across multiple countries	Content may be classified as R18
Minimal	Content that glorifies, promotes or incites terrorism/ acts of terrorism/ violent extremism No measurable physical or psychological harm	Content has very few shares, likes, comments or views Content may appear on multiple platforms across multiple countries Content is not likely to have any increased interaction online due to only being present on a smaller platform with limited reach and use	Content may be classified as R18 or objectionable

Assessing the Virality

Once the Crisis Manager has considered the harm associated with the content, they need to make an assessment about the spread / potential spread of the content. In order to determine the risk of virality of the online content, the Crisis Manager should consider the content in light of the below questions:

Key Question
Has the content appeared on a range of platforms/ across multiple countries?
Has the content received a significant number of shares, likes, comments and views?
Has the content been uploaded online by a perpetrator(s) or apparent accomplices as part of the overall strategy of the attack to increase virality and harm?

Crisis Assessment Matrix

The matrix below can be used as a rough guide to assist in making the decision to activate the crisis response. This is based on risk of virality or spread of the content and the consequence/harm associated with it.

Risk of Virality	Minimal	Minor	Moderate	Significant	Severe
Yes	BAU	Increased Monitoring	Increased Monitoring	Crisis	Crisis
Unsure	BAU	Increased Monitoring	Increased Monitoring	Increased Monitoring	Crisis
No	BAU	BAU	Increased Monitoring	Increased Monitoring	Increased Monitoring
	Risk Consequence Scale				

Response

Once an online crisis has been assessed, the crisis should have the appropriate response assigned to it depending on the severity of the crisis:

Risk Level	Response
Crisis	If the assessment falls between within the crisis section of the matrix then a crisis response should be activated. An example of this is the Christchurch Attack. Before the video was live streamed, the perpetrator shared his intentions and extremist views online. The video features racist slurs as well as the depiction of extreme violence. The video was torrented and shared across multiple platforms in the hours after the attack. It also received significant attention in traditional media and social media with 12 million tweets about the video being posted. Due to the level of violence in the video, the perpetrator's intentions and the high virality of the video, a Crisis Response was activated.
Increased Monitoring	If the assessment falls within the increased monitoring section of the matrix then normal DIA BAU operating procedures should apply along with ongoing monitoring. In this instance the Crisis Manager will send out an update to nominated contacts with any relevant information. Crisis Response participants that have monitoring and/ or complaints systems in place may be able to feed intelligence and trends regarding the online crisis i.e. increased volume of incoming calls to helplines they can share this insight with the Crisis Manager. This information will be used to remain up to date on the status of the online crisis and determine whether a crisis response needs to be implemented. In this instance, the Crisis Manager will send out regular communication with an update on status and an overview of the current landscape. An example of this is the Halle Attack. Although the video was deemed objectionable by OFLC, the content did not receive significant views, shares or likes across social media platforms. In this instance New Zealand chose not to activate a crisis response however they continued to monitor the situation online for a number of days.
BAU	If the assessment falls within the BAU section of the matrix then normal BAU operational procedures and relevant agency / industry and government actions apply. This will apply for most content on the internet that does not meet the criteria for a crisis.

Types of Response to an Online Crisis

When an online crisis is categorised as a crisis, there are a number of tools that may be used to minimise the harm of the online crisis. This section describes some of the tools that may be used and is not intended to cover all possible options – during a Crisis Response other suggestions / options will be considered. The intent is to use the full range of levers available to minimise harm. The responses could include, but are not limited to:

Response	Example of when the response may be used
Adding sites to Family Filters*	Content that is considered R18 and harmful but not objectionable may be added to OSP's family filters. If individuals do not have or choose to opt out of the filter, they will be able to view the content. This response may be appropriate for viral content that should not be viewed by vulnerable New Zealanders
DNS Blocking/Poisoning*	Internet Service Providers can block specific websites in New Zealand for customers using DNS servers. This approach may be used in instances where it is deemed appropriate to block entire websites In the event that any blocking activity is agreed to, DIA will manage, review and validate content to protect staff in ISP's. The data regarding sites to be blocked will be managed and updated by DIA through a managed spreadsheet
Media Campaign to the Public	Content that is spreading online, whether or not deemed objectionable, may benefit from a co-ordinated media campaign to inform the public about the potential harms from the specific content and advice about where to go for help if concerned and staying safe online
Content blocking for School Networks*	Network 4 Learning for instance may block sites to prevent content being viewed by children in schools in New Zealand
Targeted Engagement with Media Outlets	The Crisis Team may engage with media outlets in New Zealand to influence how they report on the content in order to reduce harm to the public
Geo Location Blocking*	Social media platforms may use this option to restrict individual's access to certain online content based on user's geographical location for example this would reduce the risk of vulnerable New Zealander's being exposed to harmful online content emerging from another country
Interstitial's*	The Crisis Team may request the use of Interstitials by social media companies where this is possible, for content that is deemed harmful but not illegal. Social media platforms may reduce individual's exposure to content by limiting the visibility of harmful content. Content containing sensitive or graphic information appears with a warning informing people about the content before they view it. This gives people the option to uncover and view the content at their discretion or not see it at all. This is intended for newsworthy content, historical/freedom of expression content that condemns/raises awareness of an incident/ potential crisis in accordance with international human rights law

Response	Example of when the response may be used
Content Take Down	The Crisis Response team may request the removal of specific content such as videos, posts etc. from platforms. This can help reduce the spread of harmful content online and prevent individuals from being exposed to graphic or sensitive material. DIA will develop the DIA Request to Seek Removal of Online Content templates for content to be taken down (attached as appendix 2). These templates will be used to record why content was removed as part of the response process and can be used by both DIA and the relevant OSP as part of the audit trail for the event
User Profiles*	Social media platforms may pause, block or delete specific users accounts from their websites for non-compliance with their terms of service/ equivalent user requirements. This could be used in instances where individuals or groups are spreading terrorist or violent extremist content online. It is important that online service providers work closely with NZ Police to ensure that if users accounts are paused or deleted that this will not impact the investigation efforts

* These actions may be adopted where appropriate and will be dependent on the technology available for each organisation involved in the response

The Online Crisis Response Process

This section outlines

- The roles and responsibilities that will be stood up during the crisis response process and the crisis deactivation process;
- The crisis process; and
- The deactivation of crisis process.

Roles and Responsibilities

When a Crisis Response is initiated, there will be a number of key roles fulfilled by New Zealand government officials as the core Crisis Team:

Role	Responsibilities
Crisis Manager	This position will be held by the Director of the Digital Safety Team (or their delegate) in the Department of Internal Affairs (DIA). This individual is responsible for activating and deactivating the Crisis Response Process. They will oversee the management and coordination of the response including tasking, driving the virtual war room, decision making and communication with global crisis process representatives (where needed)[4]. The Crisis Manager will be responsible for updating government stakeholders as part of the broader response[5] for both 'Crisis' and 'Increased Monitoring' incidents. The Crisis Manager will be the primary point of contact for global protocols and other crisis responses in New Zealand and will share information / updates with relevant international partners as required. Once the process is deactivated, the Crisis Manager will oversee the completion of a report detailing the actions taken by the agencies involved
Communications Lead	Responsible for writing updates and maintaining key messages relating to the actions being taken as part of the crisis response process. All agencies will be responsible for organising their own comms however the Communications Lead will provide regular updates to the group which representatives can use to inform their own media releases. The Communications Lead will coordinate the release of information relating to the online crisis on both social media and traditional media for the DIA. It will be preferable for other agencies to point to this central information source as much as possible rather than recreate material.
Reporting/ Intelligence Lead	Responsible for receiving and compiling information from multiple sources to provide clear situation reports for each update call. This individual will oversee the coordination of intelligence into the online crisis. They will oversee the maintenance of a central repository where information will be shared with relevant agencies and Ministers, on responses considered and used, agencies involved, and the nature, distribution and spread of the content online. The Reporting/Intel Lead will work closely with the Communications Lead/Crisis Coordinator to ensure relevant actions/next steps are captured and pushed out in a timely manner to relevant domestic and international audiences. The Reporting/ Intelligence Lead will share any data/ intel/ situational updates and reports with relevant international partners.

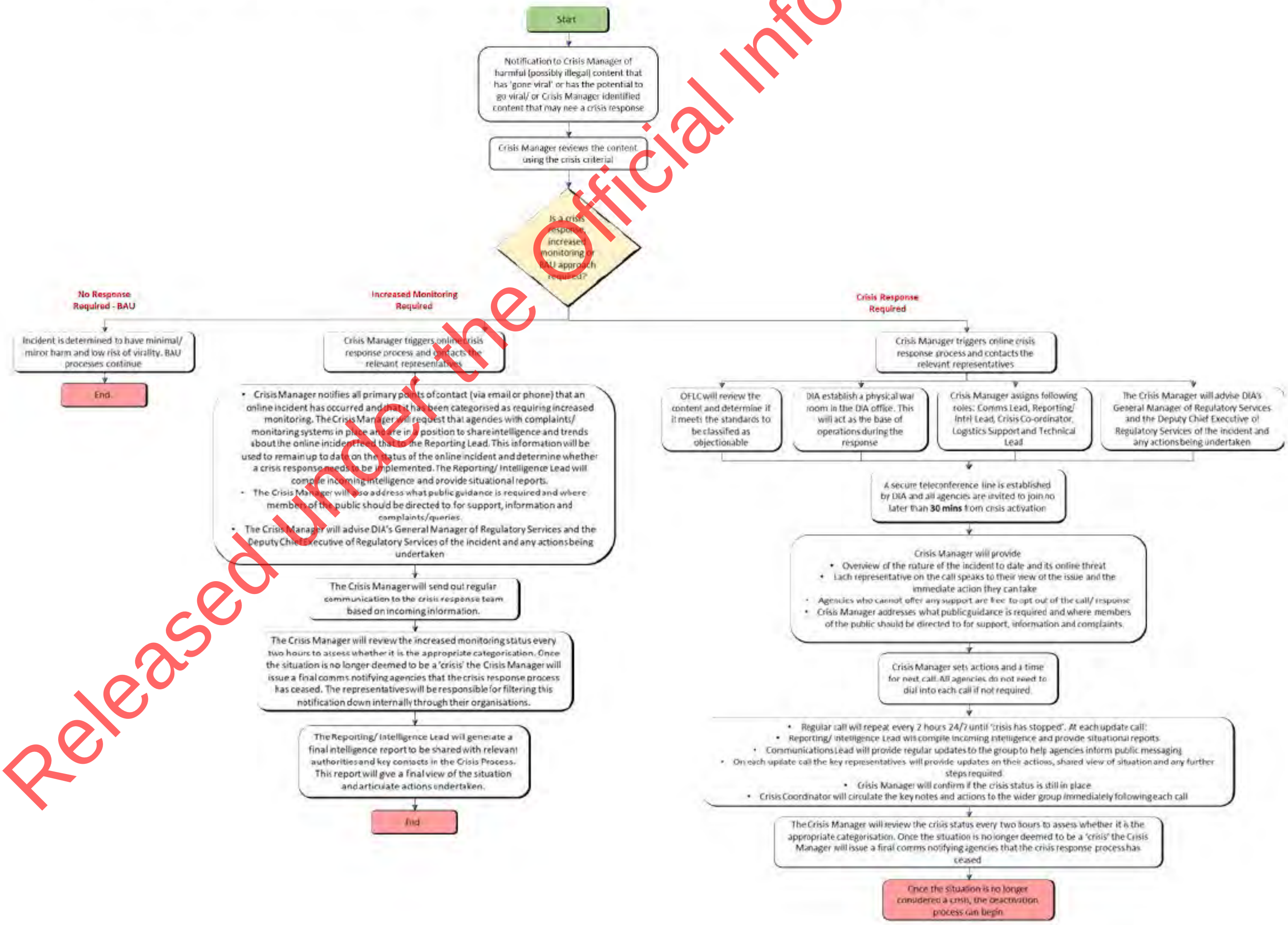
[4] This may include other governments, international law enforcement, OSPs, the GIFCT etc.

[5] Government stakeholders refers to the Minister of Internal Affairs, other Ministers as relevant, Department of Internal Affairs Chief Executive and other executives as necessary.

Role	Responsibilities
Technical Lead	Oversees the fulfilment and feasibility of any technical solutions proposed as part of the response process. They will also ensure that all necessary ICT infrastructure is in place to ensure the efficient operation of the response process once it is activated. This includes the establishment of a secure conference line and file sharing system
Crisis Coordinator	Responsible for the documentation of the actions and decisions taken as part of the crisis response process. They will document all discussions and decisions made in the virtual war room and on conference calls. They will issue invitations to conference calls, prepare and share notes after each update with all relevant parties
Logistics Support	Responsible for coordinating access to the DIA building, refreshments and supporting the Crisis Coordinator throughout the crisis response process

The Crisis Response Process

The steps involved in the Online Crisis Response Process are detailed below, including what is required for the thresholds below 'crisis' where increased monitoring will take place:



Notification to Crisis Manager of harmful (possibly illegal) content that has 'gone viral' or has the potential to go viral/ or Crisis Manager identified content that may nee a crisis response

Crisis Manager reviews the content using the crisis criteria!

Is a crisis response, increased monitoring or BAU approach required?

Incident is determined to have minimal/ minor harm and low risk of virality. BAU processes continue

Crisis Manager triggers online crisis response process and contacts the relevant representatives

- Crisis Manager notifies all primary points of contact (via email or phone) that an online incident has occurred and that it has been categorised as requiring increased monitoring. The Crisis Manager will request that agencies with complaints/ monitoring systems in place and are in a position to share intelligence and trends about the online incident feed that to the Reporting Lead. This information will be used to remain up to date on the status of the online incident and determine whether a crisis response needs to be implemented. The Reporting/ Intelligence Lead will compile incoming intelligence and provide situational reports.
- The Crisis Manager will also address what public guidance is required and where members of the public should be directed to for support, information and complaints/queries.
- The Crisis Manager will advise DIA's General Manager of Regulatory Services and the Deputy Chief Executive of Regulatory Services of the incident and any actions being undertaken

The Crisis Manager will send out regular communication to the crisis response team based on incoming information.

The Crisis Manager will review the increased monitoring status every two hours to assess whether it is the appropriate categorisation. Once the situation is no longer deemed to be a 'crisis' the Crisis Manager will issue a final comms notifying agencies that the crisis response process has ceased. The representatives will be responsible for filtering this notification down internally through their organisations.

The Reporting/ Intelligence Lead will generate a final intelligence report to be shared with relevant authorities and key contacts in the Crisis Process. This report will give a final view of the situation and articulate actions undertaken.

Crisis Manager triggers online crisis response process and contacts the relevant representatives

OFLC will review the content and determine if it meets the standards to be classified as objectionable

DIA establish a physical war room in the DIA office. This will act as the base of operations during the response

Crisis Manager assigns following roles: Comms Lead, Reporting/ Intel Lead, Crisis Co-ordinator, Logistics Support and Technical Lead

The Crisis Manager will advise DIA's General Manager of Regulatory Services and the Deputy Chief Executive of Regulatory Services of the incident and any actions being undertaken

A secure teleconference line is established by DIA and all agencies are invited to join no later than **30 mins** from crisis activation

Crisis Manager will provide

- Overview of the nature of the incident to date and its online threat
- Each representative on the call speaks to their view of the issue and the immediate action they can take
- Agencies who cannot offer any support are free to opt out of the call/ response
- Crisis Manager addresses what public guidance is required and where members of the public should be directed to for support, information and complaints.

Crisis Manager sets actions and a time for next call. All agencies do not need to dial into each call if not required.

- Regular call will repeat every 2 hours 24/7 until 'crisis has stopped'. At each update call:
- Reporting/ Intelligence Lead will compile incoming intelligence and provide situational reports
- Communications Lead will provide regular updates to the group to help agencies inform public messaging
- On each update call the key representatives will provide updates on their actions, shared view of situation and any further steps required
- Crisis Manager will confirm if the crisis status is still in place
- Crisis Coordinator will circulate the key notes and actions to the wider group immediately following each call

The Crisis Manager will review the crisis status every two hours to assess whether it is the appropriate categorisation. Once the situation is no longer deemed to be a 'crisis' the Crisis Manager will issue a final comms notifying agencies that the crisis response process has ceased

Once the situation is no longer considered a crisis, the deactivation process can begin

Engagement with OSPs and global processes during crisis

The focus of the New Zealand crisis response process is about what efforts can be taken by agencies and service providers to minimise harm domestically and protect human rights.

This crisis response process will be activated where the situation is deemed a crisis in New Zealand. In cases where the content has a global concern, responses such as the Christchurch Call Shared Crisis Response Protocol[6] and/or the Global Internet Forum to Counter Terrorism Content Incident Protocol (CIP)[7] and/or EU Crisis Protocol[8] may be activated. Where the Christchurch Call Protocol or other protocols are activated, the Crisis Manager will act as one of the conduits receiving and sharing information, working closely with Department of the Prime Minister and Cabinet (DMPC) , Ministry of Foreign Affairs and Trade (MFAT) and NZ Police representatives. In each instance, the Crisis Manager will be responsible for being the New Zealand contact point for the broader response and feeding intel and information into the global protocols and from the global protocols into the domestic process.

There may also be instances where a global crisis response is not activated, yet the domestic crisis response may be activated (i.e. when an assessment shows the need to mitigate harmful content that is focused on New Zealand).

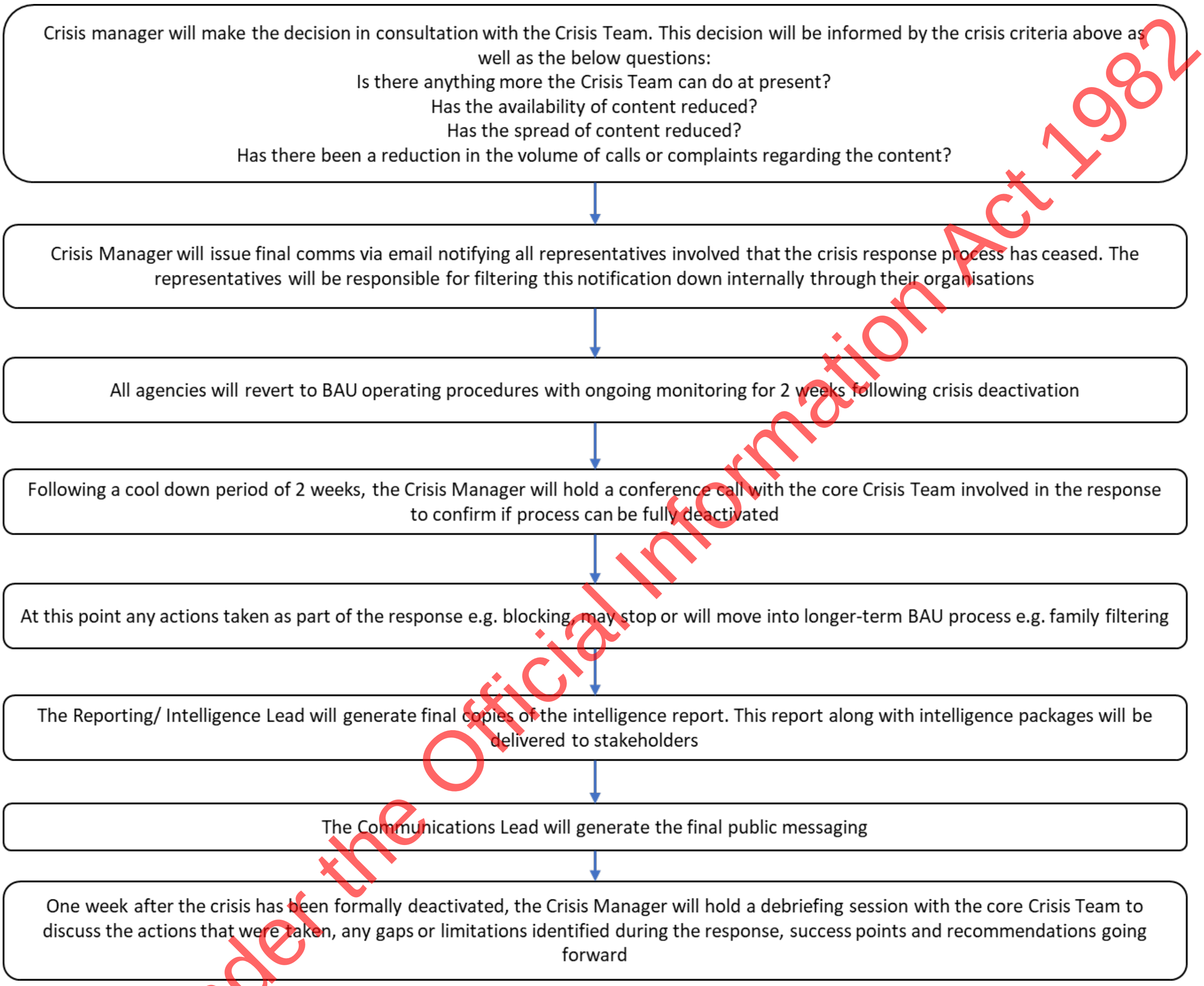
[6] For endorsing governments and OSPs (who support the Christchurch Call to Action to eliminate terrorist and violent extremist content online, herewith referred to as the “Christchurch Call”) to respond rapidly, effectively and in a coordinated manner to the dissemination of TVEC following a terrorist event in a manner consistent with human rights protections, with a view to harm minimisation and disrupting terrorist aims. This protocol is an agreed voluntary mechanism outlining shared crisis response principles and processes for endorsing countries and OSPs to adopt in the event of terrorist and violent extremist attacks with an online component. It is for use in the context of a terrorist or violent extremist attack where a high probability exists for significant online impact given associated content depicting the event. To trigger the threshold for a crisis, the TVEC will most likely be perpetrator or accomplice produced. This is most likely to be activated by the government affected by the real-world terrorist or violent extremist event and can only a Christchurch Call supporting governments and OSPs that have formally endorsed the protocol can officially activate it. Note it does not supersede any domestic or international laws.

[7] The ***GIFCT CIP*** is a process by which GIFCT member companies become aware of, quickly assess, and act on potential content circulating online resulting from a real-world terrorism or violent extremist event. No one individual or organization can activate a content incident. Rather, the protocol is based on the existence of content online relating to the real-world terrorism or violent extremism event—like Christchurch and Halle—and potential distribution of that content, including a live stream of murder or attempted murder produced by the attack’s perpetrator or an accomplice. The GIFCT CIP is a standalone industry process, but was designed to be easily integrated into external crisis response procedures, including the Christchurch Call Shared Crisis Response Protocol developed in response to the commitments of the Christchurch Call to Action to eliminate terrorist and violent extremist content online and the EU’s Crisis Response Protocol. See here for more: https://gifct.org/joint-tech-innovation/

[8] ***The EU Crisis Protocol****: Collective response to viral spread of terrorist and violent extremist content online* may be activated only by an EU Member State or Europol where a crisis is identified within the EU. It aims to facilitate rapid assessment of the online impact of terrorist attacks, secure and timely sharing of critical information between EU Member States law enforcement (LE) and other competent authorities, Union bodies (in particular Europol), OSPs and other relevant stakeholders in accordance with relevant legislation and within the relevant mandates, and to ensure effective coordination and management of the crisis. See more here: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20191007_agenda-security-factsheet-eu-crisis-protocol_en.pdf

Deactivating the Crisis Response

The categorisation of the online crisis will be regularly reviewed. Once it is no longer considered a crisis, the following process will be carried out:



Crisis manager will make the decision in consultation with the Crisis Team. This decision will be informed by the crisis criteria above as well as the below questions:
Is there anything more the Crisis Team can do at present?
Has the availability of content reduced?
Has the spread of content reduced?
Has there been a reduction in the volume of calls or complaints regarding the content?

Crisis Manager will issue final comms via email notifying all representatives involved that the crisis response process has ceased. The representatives will be responsible for filtering this notification down internally through their organisations

All agencies will revert to BAU operating procedures with ongoing monitoring for 2 weeks following crisis deactivation

Following a cool down period of 2 weeks, the Crisis Manager will hold a conference call with the core Crisis Team involved in the response to confirm if process can be fully deactivated

At this point any actions taken as part of the response e.g. blocking, may stop or will move into longer-term BAU process e.g. family filtering

The Reporting/ Intelligence Lead will generate final copies of the intelligence report. This report along with intelligence packages will be delivered to stakeholders

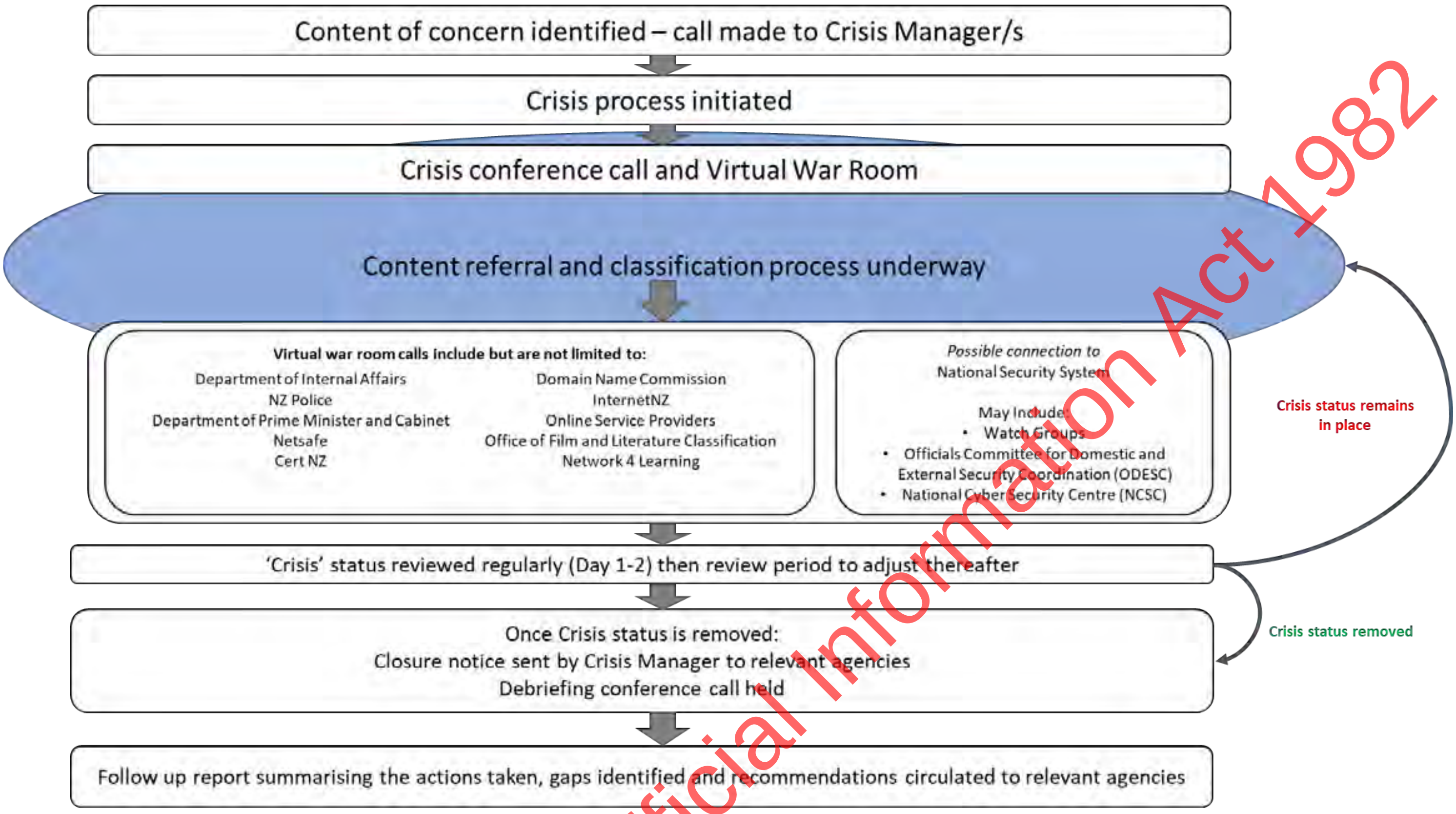
The Communications Lead will generate the final public messaging

One week after the crisis has been formally deactivated, the Crisis Manager will hold a debriefing session with the core Crisis Team to discuss the actions that were taken, any gaps or limitations identified during the response, success points and recommendations going forward

DIA will generate a final report which will detail the background to the crisis, the actions taken and recommendations going forward. This report will be shared, in confidence, with all participants of the response process. A copy of the report and the final version of the intelligence spreadsheet will be saved in the shared location. For more information on this process see the Crisis Response Debriefing Process.

Summary of the Crisis Response Process

The below table illustrates the end-to-end Online Crisis Response Process detailed above:



Content of concern identified – call made to Crisis Manager/s

Crisis process initiated

Crisis conference call and Virtual War Room

Content referral and classification process underway

Virtual war room calls include but are not limited to:

Department of Internal Affairs
NZ Police
Department of Prime Minister and Cabinet
Netsafe
Cert NZ

Domain Name Commission
InternetNZ
Online Service Providers
Office of Film and Literature Classification
Network 4 Learning

Possible connection to
National Security System

May Include:
- Watch Groups
- Officials Committee for Domestic and External Security Coordination (ODESC)
- National Cyber Security Centre (NCSC)

'Crisis' status reviewed regularly (Day 1-2) then review period to adjust thereafter

Crisis status remains in place

Crisis status removed

Once Crisis status is removed:
Closure notice sent by Crisis Manager to relevant agencies
Debriefing conference call held

Follow up report summarising the actions taken, gaps identified and recommendations circulated to relevant agencies

Principles and Expectations of the Crisis Response Process

Principles of Operation

By signing up to the New Zealand Online Crisis Response Process, all participants agree to adhere to the following six principles of operation:

- **Authenticity** - All decisions must reflect the scope of the crisis criteria and fit within the overall aims of the domestic online crisis response process
- **Transparency and Public Confidence** - The New Zealand public are entitled to request government information. Any actions taken during a crisis response must be defendable. We will proactively release messaging to the public to ensure they remain informed of the response process throughout. This will help to keep us accountable, reassure the public and to help prevent harm
- **Speed and Agility** - Situations unfold rapidly in the digital age. During a crisis, the speed of action and our agility to respond to changes in the situation are core to how we operate
- **Intelligence** - The consistent rapid sharing of information and data on a secure platform will be necessary to limit the spread of harm online. This will include sharing URL's, hashes, situational awareness, media and metadata
- **Trust and Accountability**– The Crisis Manager is the key decision maker for the response and is required to take responsibility for any actions taken and decisions made. On the initial crisis conference call if representatives challenge whether a crisis should be called, this can be discussed, reviewed and the crisis status stepped down if required. To ensure accountability there will be appropriate measures put in place and all records will be fully maintained. If at any point during the response the Crisis Team disagree with any decision made by the Crisis Manager and the issue cannot be resolved with Crisis Manager or Crisis Team directly, then an escalation should be made to the DIA General Manager
- **Communication** - During a crisis we will communicate information and updates up to senior stakeholders, across all the agencies involved and outside to the media and public. By having a Communications Lead, DIA will ensure a coordinated and consistent flow of information. There is also onus on other agency partners and OSPs to work collaboratively in the interest of timely harm reduction and to comply with law enforcement requests/ requirements
- **Harm minimisation** - This process is intended to minimise exposure and harm resulting from a terrorist or violent extremist attack, including to society and social cohesion, as well as any victims or intended victims of the attack and to anyone exposed inadvertently to terrorist or violent extremist content
- **Respect for human rights and dignity, and fundamental freedoms** - Any response will be carried out in a rights-respecting manner, including with respect to the rights of any victims or intended victims. New Zealand government agencies must act consistently with the Bill of Rights Act 1990
- **Preserving a free, open, secure and globally connected internet** - No associated tools deployed should undermine functionality and connectivity of the global internet nor compromise its infrastructure

Operational Expectations on Information Sharing

Classifying Content as Objectionable

In the event of an online crisis speed is essential to minimising harm. The Chief Censor will be consulted and where possible, will make an 'interim' decision on classification. Where this is not possible this will be communicated, and guidance developed (such as using the term 'likely objectionable' as used in Christchurch response).

Alerting the Crisis Manager

When an agency is alerted to online content that may require a crisis response, the identifying agency should contact the Crisis Manager via phone (*see appendix 1*).

ICT Information

All conference calls will be scheduled by the Crisis Coordinator. In the event of a crisis response being initiated, they will issue an invite to all representatives which will include the teleconference details. This invite will also include details of the physical war room for representatives who wish to attend the initial launch call, or any follow up calls in person.

All documents related to the Crisis Response Process will be stored in CoLab. A link to the documents can be shared with external stakeholders if required in the event of a crisis incident.

Crisis Response Mailbox and Email

A dedicated mailbox that is monitored 24/7 during an online crisis, is managed by DIA. When the Crisis Response Process is initiated, agencies will be asked to submit any data and intelligence relating to the crisis to the mailbox which will be used by the Reporting/ Intelligence Lead to develop situational reports. The crisis response e-mail address is: onlinecrisisres@dia.govt.nz

In the event that the Crisis Team need to contact organisations in order to remove harmful content from their site, the crisis response email address can be used. All members of the Crisis Team have access to the mailbox and can send emails from this mailbox rather than their work email address. This will reduce the risk of staff members exposing their personal information to external organisations and being doxed (having their private information published online).

Communications

A Communications Lead will be appointed for the duration of the crisis response. This individual will work with the points of contact and comms teams from the organisations involved in the crisis response to agree appropriate public messaging and will provide regular updates on each follow-up call. This information can be used to inform each agency's own media releases.

They will work with the points of contact and comms teams from the organisations involved in the crisis response to ensure the public are directed to the necessary helplines and complaint portals. They will also agree on messaging to inform the public on the incident as it unfolds and how they can stay safe online.

They will develop and maintain a document outlining the public messaging each organisation is issuing in order to ensure there is a coordinated and staggered release of information on both social media and traditional media between all organisations. This will ensure that there is a consistent message being filtered out to the wider public and avoid duplication of information being provided to the public.

During a crisis it will be important to communicate information and updates up to senior stakeholders, across all the agencies involved and outside to the media and public. By having a Communications Lead we will ensure there is consistent information flow to the New Zealand Prime Minister or other relevant ministers. If a crisis response requires us to connect with our international partners as in the case of Christchurch, the Communications Lead will work with the crisis response representatives to develop translations for the public messaging.

Expectation of Confidentiality

All agencies and OSPs who volunteer to participate in the Online Crisis Response Process will sign a Confidentiality Agreement (attached as appendix 3). This will cover:

1. **Authority for decision:** In the event of an online crisis and if DNS blocking is utilised, the Department, in consultation with the Chief Censor, will make the decision about what content should be blocked. The Department will accept responsibility for any content that is blocked as part of the crisis response and maintains an appeal process for these decisions to be challenged;
2. **Protection for OSPs**
    a. Protection for the OSP's with regards to the information they share as part of the crisis process which would not normally be shared with the Government or other industries;
    b. Protection for OSP's from viewing objectionable and sharing URLs and hashes for objectionable content for the purposes of the crisis process; and
3. **Confidentiality:** Most information shared during a crisis response is confidential and will not be shared outside of the response, with the exception of information released as part of the crisis response comms.

Additional Considerations

Connection to the International Response Processes

As previously outlined, the Domestic Online Crisis Response Process connects with international response protocols to ensure there is a coordinated response to an online crisis with the shared aim to reduce virality and minimise harm through timely information sharing.

The Global Internet Forum to Counter Terrorism (GIFCT) was established by Facebook, Microsoft, Twitter and YouTube to disrupt terrorist content on their platforms and ensure ongoing knowledge-sharing and technical collaboration. It is now an independent organisation, with its mission to prevent terrorists and violent extremists from exploiting digital platforms. In the event of an online content incident, the GIFCT will appoint a representative to liaise with the platforms and the Domestic Online Crisis Response Team. This does not prevent NZ from requesting information from/liaising with individual platforms as needed and vice versa

In coordination with DPMC/MFAT, information will be shared as required to inform the Christchurch Call Shared Crisis Response, should that Protocol be activated.

The Crisis Manager will be one of the nominated contact points for New Zealand for both the GIFCT and Christchurch Call Protocols. As part of their role, the Crisis Manager will act as a conduit between the Domestic Crisis Response Process and the GIFCT and Christchurch Call Protocols, when the latter are initiated, in close coordination with DMPC and MFAT.

Law Enforcement Guidance

During the crisis response the Crisis Response Team will work closely with the NZ Police to ensure that any steps taken as part of the response do not negatively impact any investigation underway.

The Police representative(s) on the update calls should be able to inform the other stakeholders about what content (where removal is occurring) is required to be sandboxed or preserved and where this is possible. They will also inform the group about any data and intelligence that should be captured where possible. There is an important need to balance public protection and harm minimisation with evidential needs for any criminal case.

Appendix 1: Crisis Response Process Contacts

The below table details a selection of the agencies that may be contacted in the event of an online crisis in New Zealand. Note for each agency there is both a primary, secondary and after-hours point of contact. The complete master list can be found below.

Organisation	Primary Contact	Secondary Contact	Notes
Government			
Department of Internal Affairs (Crisis Manager)*	Jared Mullen, Director, Digital Safety 9(2)(a) [redacted]	John Michael, Deputy Director, Digital Safety 9(2)(a) [redacted]	Phone number can be used 24/7
Alternative Department of Internal Affairs Contacts	Glenn Williams, Manager Digital Violent Extremism Unit 9(2)(a) [redacted] Madeline Sheperd, Principal Advisor Countering Violent Extremism 9(2)(a) [redacted] Nicole Matejic, Principal Advisor 9(2)(a) [redacted] Robert McMillan, Manager Intelligence and Insights 9(2)(a) [redacted] Damian Rapira-Davies, Lead Operations 9(2)(a) [redacted] Tim Houston, Manager Digital Child Exploitation 9(2)(a) [redacted] Carmel Ali, Programme Director Preventing and Countering Violent Extremism 9(2)(a) [redacted]		Please note the Director and Deputy Director of Digital Safety should be contacted in the first instance
CERT NZ	Rob Pope, CERT NZ Director 9(2)(a) [redacted]	Nadia Yousef, Threat and Incident Manager 9(2)(a) [redacted]	

Organisation	Primary Contact	Secondary Contact	Notes
Department of the Prime Minister and Cabinet	Manisha Bhikha 9(2)(a) [redacted]	Paul Ash, Director, National Security Policy Directorate +64 (21) 243 8593 9(2)(a) [redacted] Andy George, Counter-Terrorism Strategic Coordinator 9(2)(a) [redacted]	
New Zealand Customs Service	Simon Peterson, Chief Customs Officer Child Exploitation Operations Team 9(2)(a) [redacted]	Stephen Waugh, Manager Operations – Investigations 9(2)(a) [redacted]	
Ministry of Foreign Affairs and Trade	Sharmila Bernau, Senior Policy Officer, International Security and Disarmament Division 9(2)(a) [redacted]	Gordon Lewin, Policy Officer, International Security and Disarmament Division 9(2)(a) [redacted]	
New Zealand Police	Kelly Knight, High Tech Crimes Team 9(2)(a) [redacted]	Greg Nicholls, Detective Superintendent National Manager: National Security (CT) 9(2)(a) [redacted]	
Classification Office	David Shanks, Chief Censor 9(2)(a) [redacted]	Jolene Armadoros 9(2)(a) [redacted]	
NZDF Intelligence	6(a) [redacted]	6(a) [redacted]	
NZDF National Bomb Data Center	6(a) [redacted]	6(a) [redacted]	
Civil Society/ NGO's			
Domain Name Commission	Brent Carey, Domain Name Commissioner 9(2)(a) [redacted]	Ann Ibrahaim, Manager, Domain Name Commission 9(2)(a) [redacted]	
Internet NZ	Jordan Carter, Group Chief Executive 9(2)(a) [redacted]	Andrew Cushen, Engagement Director 9(2)(a) [redacted]	

Organisation	Primary Contact	Secondary Contact	Notes
Netsafe	Martin Cocker, Chief Executive Officer 9(2)(a)	Sarah White, Contact Centre Manager 9(2)(a)	
Telecommunications Forum	TBC, Chief Executive Office	Clare Dobson, TCF Programme Manager 9(2)(a)	
Industry			
2degrees	Mathew Bolland, Chief of Corporate Affairs 9(2)(a)	Sara Lipanovic, Regulatory Policy Manager 9(2)(a)	
Chorus	Julian Kersey, Manager Regulatory and Policy Affairs 9(2)(a)	Sally Ma, Regulatory and Policy Affairs Manager 9(2)(a)	
Enable Fibre Broadband	Salinda Lekamge, Information and Cyber Security Manager 9(2)(a)	Elissa Bradley, Legal Counsel 9(2)(a)	
Facebook	Mia Garlick, Director of Policy Australia, New Zealand & Pacific 9(2)(a)	Nick McDonnell, Head of Policy New Zealand +61 436 860 826 9(2)(a)	
Global Internet Forum to Counter Terrorism	Contact through Crisis Manager		
Google	Ross Young, Senior Manager, Public Policy and Government Affairs at Google 9(2)(a)	Google's Australia New Zealand Government Affairs and Public Policy Team gappanz@google.com	Note these mailboxes are not monitored 24/7.
Network for Learning	Larrie Moore, Chief Executive Officer +64 27 561 0180 9(2)(a)	Gavin Costello, Chief Information and Security Officer 9(2)(a)	
Spark NZ	John Wesley-Smith, Regulatory and Industry Affairs, Spark New Zealand 9(2)(a)	Leela Gantman Corporate Relations Director, Spark New Zealand 9(2)(a)	
TikTok	TikTok incident management team (24/7) govreport@tiktok.com		

Organisation	Primary Contact	Secondary Contact	Notes
Twitter	Kara Hinesley, Head of Public Policy, Government, and Philanthropy, Australia & NZ 9(2)(a)	Kathleen Reen, Senior Director of Public Policy, Government, and Philanthropy, APAC +65 9131 2404 9(2)(a)	
Ultrafast Broadband	Duty Manager 0800 833 364 dutymanager@ultrafast.co.nz	Jon Edney, Security Specialist 9(2)(a) Hiramai Rogers, General Council 9(2)(a)	
Vocus Group	Stephen Kurzeja 9(2)(a)	Emily Acland 9(2)(a)	
Vodafone	TBC	Josh Reedy, Security Operations Manager 9(2)(a) Tom Thursby, Lead Legal Counsel, and Head of Public Policy 9(2)(a)	

Appendix 2: DIA Request to Seek Removal of Online Content and Preservation Request

Request to Seek Removal of Online Content

Te Tari Taiwhenua
Internal Affairs

Request Details			
Request Number		Date / Time (UTC)	
Agency making request	*i.e. Department of Internal Affairs*		
Email Address	*i.e. Jane.Doe@dia.govt.nz*	Phone Number	

Provider Details	
Relevant Service Provider Details	*i.e. Spark*

Overview of Online Content to be Removed	
Outline of Circumstances	*Circumstances to include the considerations and decisions undertaken by the smaller agency group to allow transparency.*
FVPC Act Definition – Objectionable Material[9]	*i.e. Likely to be determined objectionable' , OFLC are reviewing content and an interim decision is/ has been made etc..*
Relevant URL	
Date/Time (UTC) Of the Material Shared/Posted	
Screenshot	

[9] Refers to the Films, Videos and Publications Act 1993

Assistance Sought	*i.e. Following review of the material [Provider Name] request assistance to take this material down and reduce the physical and psychological New Zealanders may be exposed to*
Forensic	*i.e. Any attribution and traffic data pertaining to the material is sought to be preserved prior to take down*

Preservation Request

Target Account Identifier	*i.e. For preservation of information relevant to [Insert name] account.*
Target Account URL	
Target Account Data to be Preserved and Date Range	*i.e. include all information to be preserved and from what date ranges*
User Notification	*Confirm whether the User should be notified of request or not*
Confirmation of preservation reference number and expiry	Please send to my email above confirmation of the preservation reference number and date of expiry of the preservation order

Appendix 3: Confidentiality Agreement

1. **Information Sharing**: Once an Online Crisis has been declared by the Crisis Manager in accordance with the Response Process, the following applies to the sharing of information between Participants.

    a. **Objectionable material**: The Participants acknowledge that there may be information giving rise to the Online Crisis that is objectionable as defined in the Films, Videos and Publications Classification Act 1993, the holding and sharing of which in certain circumstances may be an offence under that Act.

    b. **Purposes for holding or sharing the potentially Objectionable material:** The Participants agree that they will share any content and information, including potentially objectionable material, solely related to the Crisis Response Process and only with other Participants as required.

    c. **For the avoidance of doubt** the Participants expressly acknowledge that no information or content relating to the Online Crisis will be shared with or forwarded to other parties for the purposes of supply or distribution (as those terms are defined in Films, Videos and Publications Classification Act 1993) to members of the public.

    d. **Instruction of the Crisis Manager:** Information will only be shared by Participants in accordance with express instructions from the Crisis Manager or his/her/its agent.

    e. **In requesting or sharing information**, the Participants will comply with all applicable New Zealand laws, including the Privacy Act 1993.

2. **DNS Blocking**: In the event of an Online Crisis:

    a. the Crisis Manager will make the decision about if DNS blocking is required, and what content should be blocked;

    b. the Crisis Manager or his/her/its agent will maintain a central repository of the domain content to be blocked and, will share this with Participants;

    c. the Crisis Manager will be the contact point for any complaints about any content that is blocked as part of the crisis response and will accept responsibility for the blocking of such content;

    d. if Participants receive complaints about content being removed or blocked in accordance with the Crisis Manager's instruction, these complaints can be directed to the Crisis Manager by Participants. The Department of Internal Affairs will have no responsibility for any content that has been blocked or removed other than in accordance with the Crisis Manager's instructions.

3. **Participants:** In the event a Participant becomes aware of new content that may be related to the Online Crisis they will:

    a. proactively notify the Crisis Manager of the existence of such information in a timely manner; and

    b. seek the instructions of the Crisis Manager in relation to the blocking of access to, or the taking down of the content.

4. **Good Faith and Confidentiality:** The Participants all acknowledge that:

    a. they are entering into this Response Process in good faith for the purposes of preventing harm from the distribution and availability of content which has been or may be assessed as injurious to the public good and this has been entered into having balanced the potential for harm from the public dissemination and availability of such content against the right to free speech.

b. those non-government Participants may be asked to share information with government Participants that they would not normally share in the ordinary course of business, and that information is to be treated as confidential and not to be used for any purposes other than those expressly identified in this Appendix.

5. **Official Information Act:** Participants acknowledges that the Department of Internal Affairs and other government participants are subject to the provisions of the Official Information Act 1982 and may be required to disclose information pursuant to that Act. Participants should mark any information "Commercial: In Confidence" if it wishes to protect specific commercial information. No information obtained through the Response Process will be disclosed without first notifying affected Participants and consulting with them in relation to any information that relates to them prior to the release or withholding of the information. The Department does not guarantee, however, that such marked information will be protected from disclosure.