



IN CONFIDENCE

ECLI – vMLC Alert and Incident Management Process

Version 1.4

Date: 28 Aug 2023

RELEASED UNDER THE
OFFICIAL INFORMATION ACT

Table of Contents

1	Overview	3
2	Viewing Incidents assigned to Comtech.....	4
3	Searching for incidents assigned to Comtech	5
4	Types of Incidents	6
5	Acknowledging an Incident.....	7
6	Updating an Incident	7
6.1	Changing the Status of an Incident.....	7
6.2	Logging a Comment on an Incident.....	8
7	Resolving Incidents.....	10
8	Stopping the SLA Clock via <i>Pending SLA</i>	11
9	Transferring an Incident.....	15
10	Closing an Incident	15
11	Bulk Closing Incidents.....	15
12	Alert / Incident Process Flow	19

RELEASED UNDER THE OFFICIAL INFORMATION ACT

1 Overview

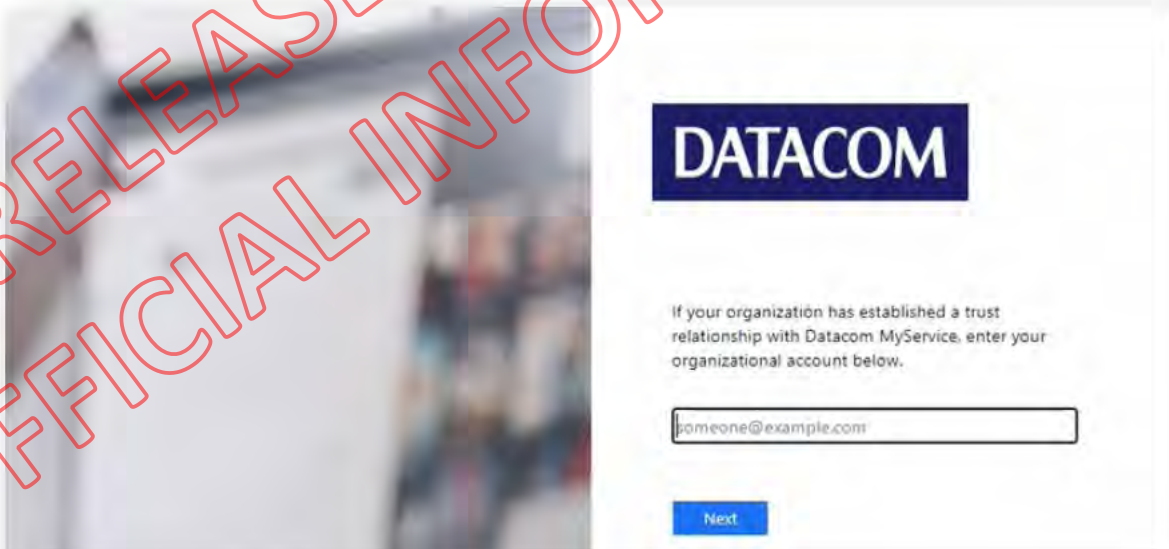
Datacom has recently started to use Cherwell to support MBIE Incident Management systems, replacing a capability previously delivered using CA Service Desk Manager (referred to as R12). The new Cherwell system has been deployed by Datacom to match previous R12 functionality 'like-for-like'.

Note: In contrast with R12, Cherwell refers to a ticket as an *Incident*, which is then further defined as an *Incident* or *Service Request*.

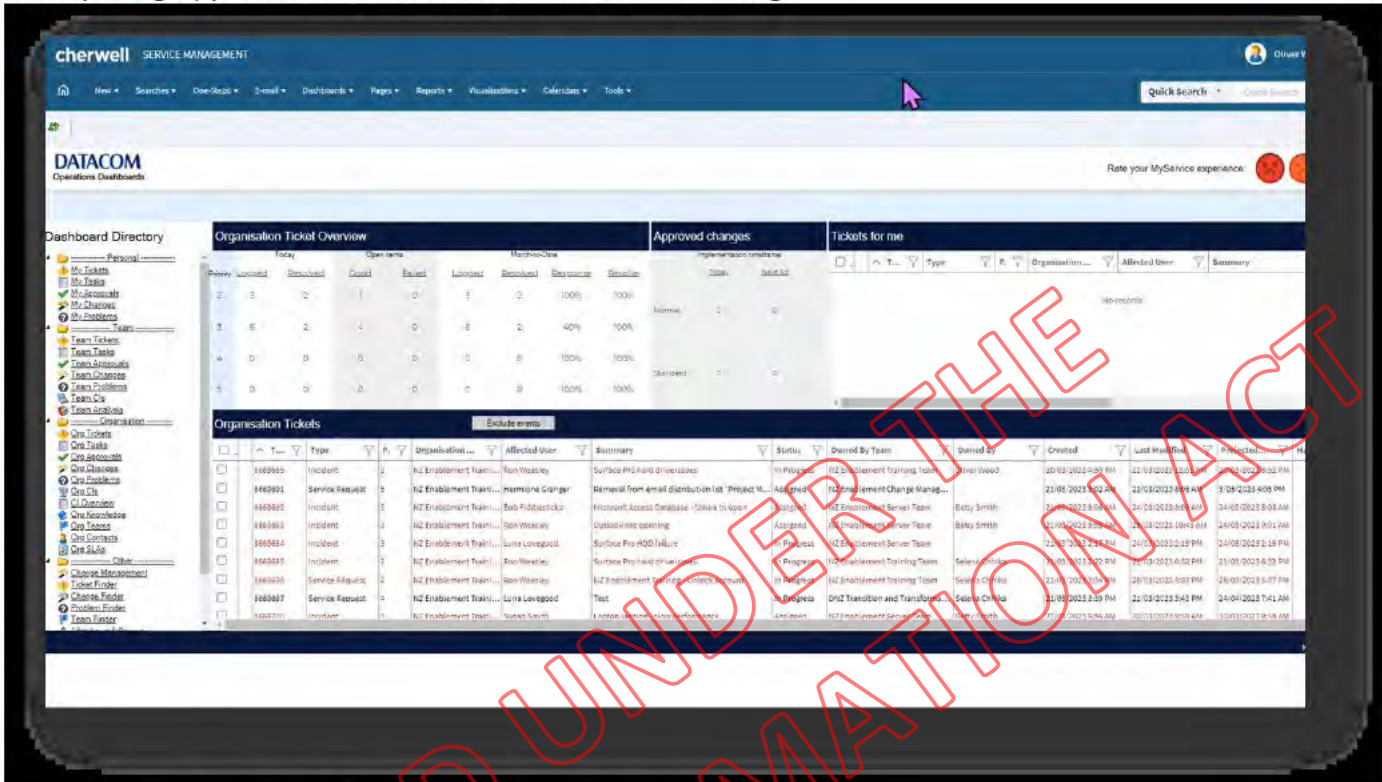
Cherwell records alerts from the vMLC via the monitoring tool (Nagios), raising 'tickets' that may come from an alert or from a phone call raising an Incident with the ECLI Service. If related to the vMLC, Datacom assign these alerts/incidents to Comtech as providers of the vMLC management for MBIE.

The vMLC alerts that have been set up are based on details provided by Comtech along with the priority level for each alert. This is 'one ticket for one alarm'; if a service component is affected that may cause three alerts, the Cherwell system is aware of three alerts and each needs to be acknowledged/resolved and closed otherwise the ticket will remain open and SLAs will be breached, generating emails and more traffic.

To access the Cherwell system, you require your MBIE network login to have access. The application is accessed by using the following URL: OIA 9(2)(c)



After you log in, you will see a dashboard similar to the following:



2 Viewing Incidents assigned to Comtech

To view outstanding alerts/incidents that have been assigned to Comtech, select *Team Tickets* from the Dashboard Directory on the left:





3 Searching for incidents assigned to Comtech

Cherwell provides multiple ways to search for existing records. The three main ways of searching are summarised as follows:

Search Method	When to use	Where to access feature
Quick Search	The best search option to find a ticket if you have the ticket number. Note: this method will show the incidents that were opened <i>but does not show the incidents that were automatically generated.</i> Automatically generated incidents will have an email generated and this can be used to locate the incident of interest.	The top-right of the Cherwell window
Search Manager	A helpful way to look at predefined searches.	Click Searches from the toolbar at the top of the screen, then select Search Manager .
Quick Search Builder	Allows you to create your own searches using comparison clauses. Although this guide focuses on searching for Incidents in Cherwell, you can also use these functions to search for other things such as teams, contact records, Configuration Items, change requests etc.	Click Searches from the toolbar at the top of the screen, then select Quick Search Builder

You can export most search results into a CSV or MS Excel format. To do this, right-click on one of the records and select *Export* from the toolbar.

4 Types of Incidents

Incidents (previously known as Tickets, under R12) can either be automatically generated from an alert/alarm or created through an incident that has been raised with Datacom about a component on the ECLI Service that is not working as expected.

- a) **Automatically generated incidents** are created through Nagios alerting and will be emailed to the Comtech Network Operations Centre (NOC) from ^{OIA 9(2)(c)} [redacted] [@datacom.co.nz](mailto:[redacted]@datacom.co.nz) at Datacom; and
- b) **Incidents** will be raised when a call or email (depending on the severity) is made to Datacom advising that there is some compromise in the ECLI Service relating to the vMLC.

Priority 1 and 2 incidents should be phoned through to the Comtech NOC on **+1 888 830 2548**. The exception being a P2 that is raised through an alarm as this needs investigation from Comtech first.

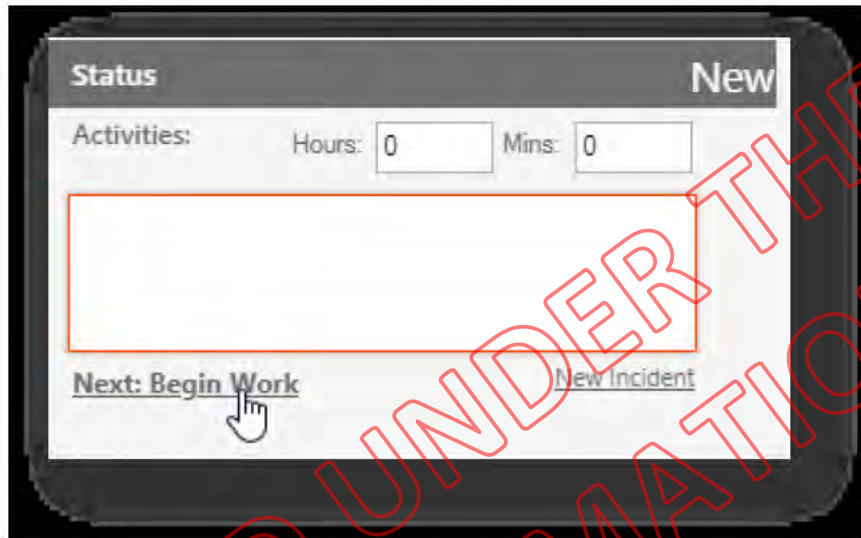
Priority 1 and 2 incidents will have a Datacom Incident Manager assigned due to severity of the Incident and they will run the incident management process. This is generally a conference call with relevant parties involved to work through the issue promptly.

The email address for the Incident Manager is ^{OIA 9(2)(c)} [redacted] [@datacom.co.nz](mailto:[redacted]@datacom.co.nz)
Priority 3 and 4 incidents can be emailed to the Comtech NOC for resolution.

RELEASED UNDER THE OFFICIAL INFORMATION ACT

5 Acknowledging an Incident

Once an incident has been assigned to Comtech (Group MBIE-COMTECH), it must be acknowledged promptly either through updating in Cherwell and updating the Status field to **Begin Work** or by email back to Datacom for them to update by advising that the ticket is being investigated by Comtech (internal process from here as to how Comtech send the details to CTSO¹).



Important Note: If tickets are not acknowledged and updated to 'Begin Work' within a defined period of time, further follow up emails/phone calls from Datacom with SLA breaches will occur, generating more traffic. Acknowledging tickets promptly within Cherwell will avoid this.

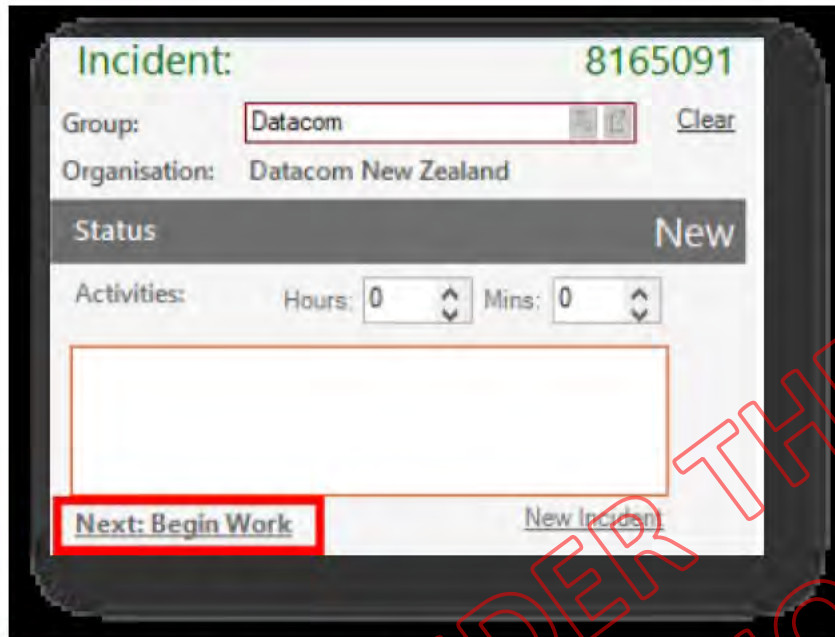
6 Updating an Incident

Incidents should be updated on findings as the investigation progresses. The following sub-headings provide instruction on how to do this in Cherwell.

6.1 Changing the Status of an Incident

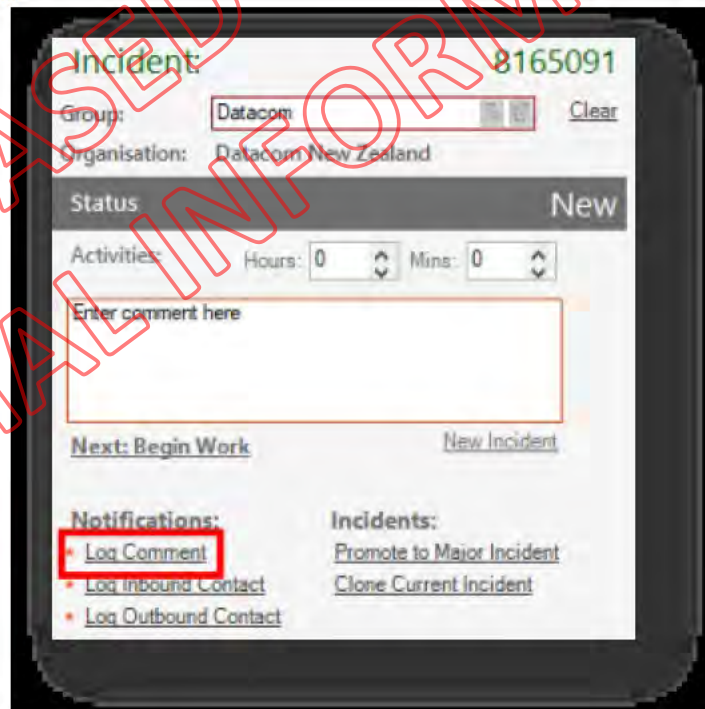
If you need to change the status of an Incident, go to the actions pane of an incident and then click **Next** to update the status of an incident. The Status will then change to the next applicable status:

¹ Refers to the collective name for the support team at Comtech.

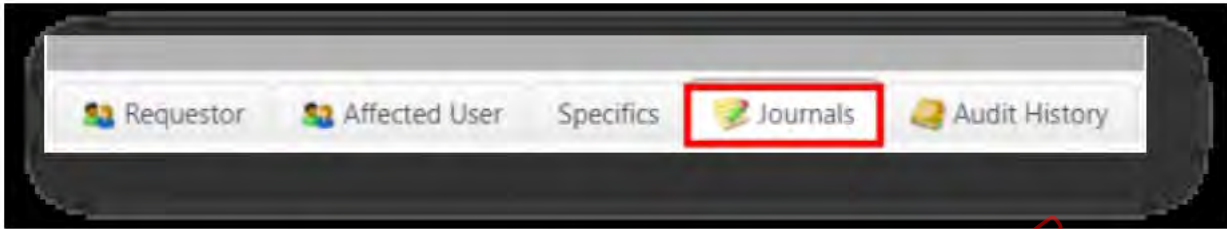


6.2 Logging a Comment on an Incident

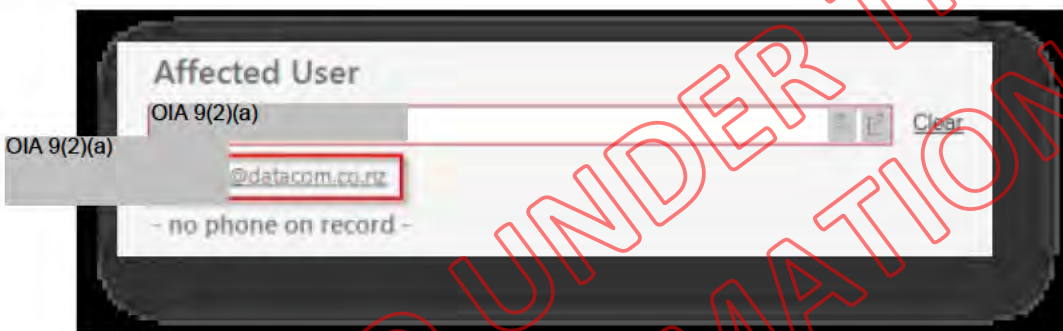
If you need to add a comment to an Incident where the affected user **will not be notified**, go to the activities pane, type your comment into the activities text box and then click *Log Comment* as shown in the screenshot below:



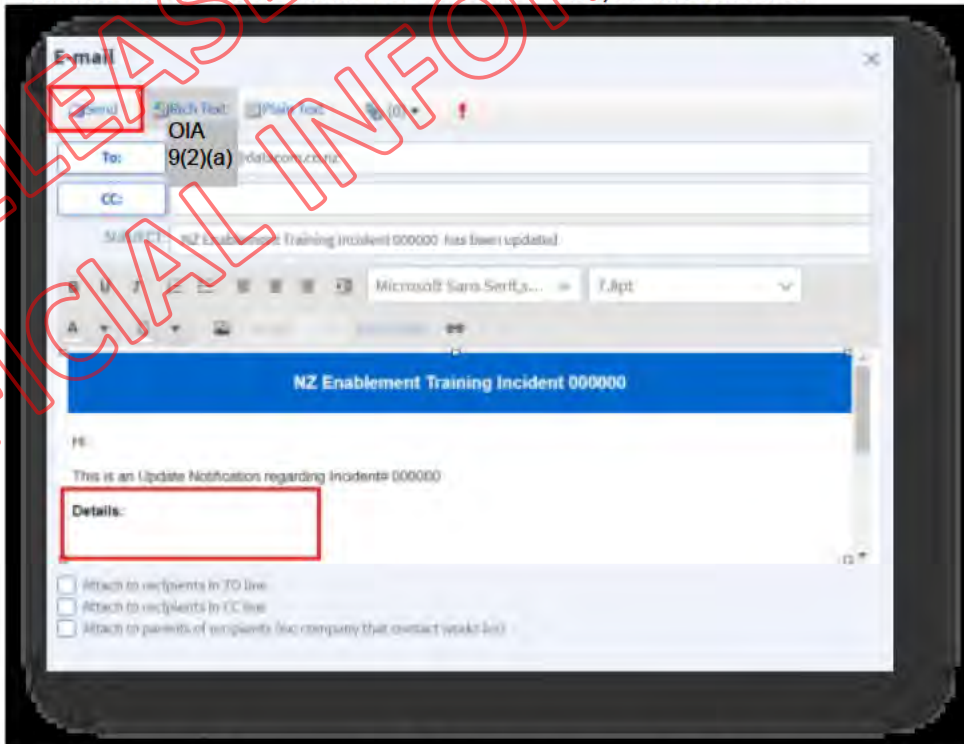
The newly entered comment and all previous comments will appear under the *Journal Notes* tab at the bottom of the incident window as shown in the following screenshot:



If you need to add a comment to an Incident where the affected user will be notified, click the email address link underneath the Affected User, as shown in the below screenshot:



Type your comment underneath 'Details' and then click *Send*, as shown below:



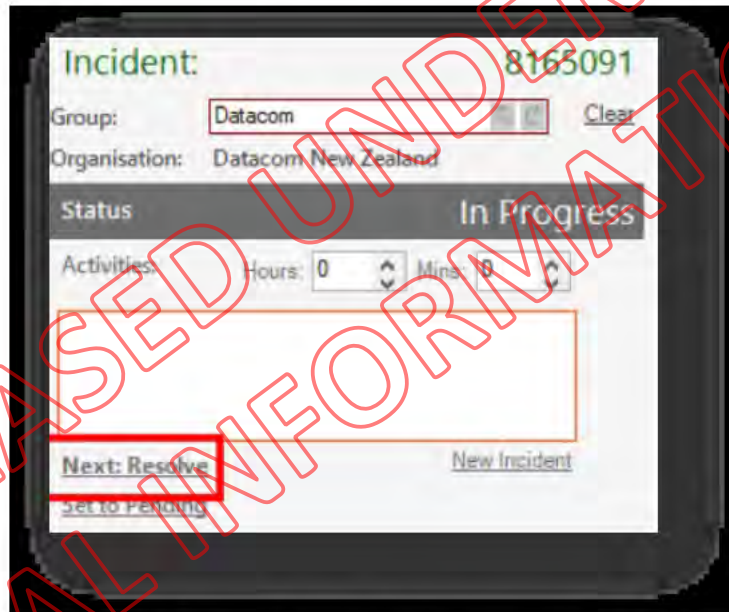
As before, your newly entered comment and all previous comments will appear under the *Journal Notes* tab at the bottom of the incident window.

7 Resolving Incidents

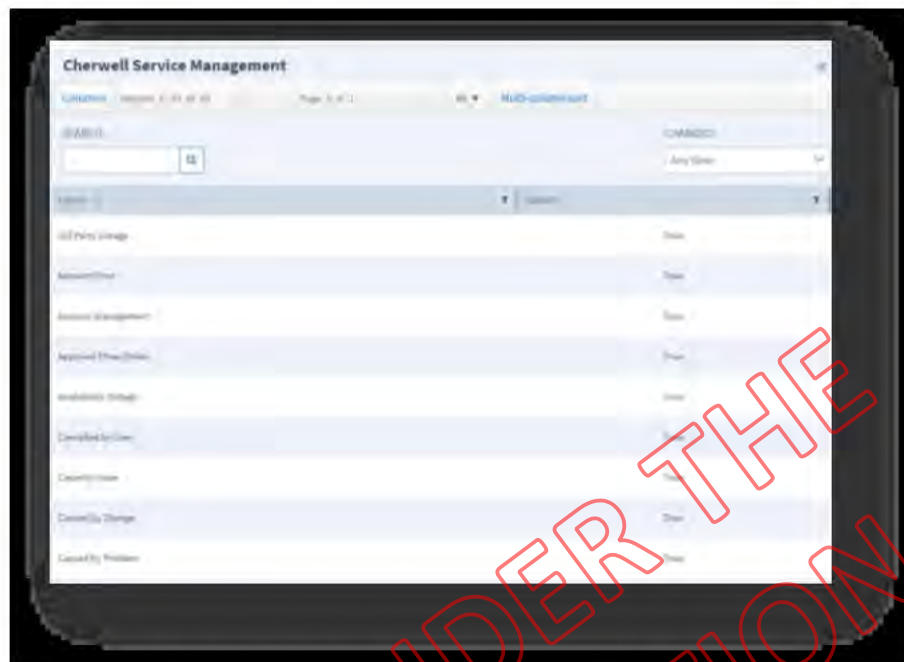
The CTSO will assess the alarm and decide whether:

- The alarm can be cleared on the vMLC and then update the incident in Cherwell to **Resolved**.
- or
- The alarm requires an incident to be raised as there is a broader issue. This would be sent back to Datacom to say that an incident needs to be opened.

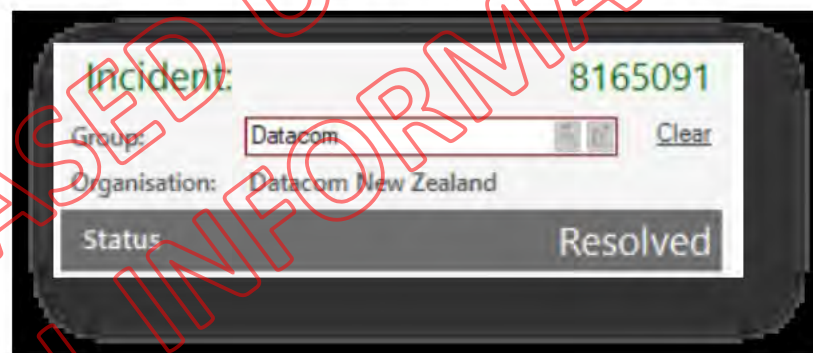
In order to update an incident to **Resolved**, go to the activities pane and click *Next: Resolve* as shown in the below screenshot.



Referring to the screenshot on the following page, use the *Incident Cause Selector* to select a cause code by double clicking on it.



From the *Resolution Details* tab at the bottom of the incident window enter the resolution description and, if applicable, NAF (Not at Fault). After adding the requisite information, click *Save and Resolve*.



Important Note: A ticket needs to be set to Resolved for SLA breach notifications to cease being sent.

8 Stopping the SLA Clock via *Pending SLA*

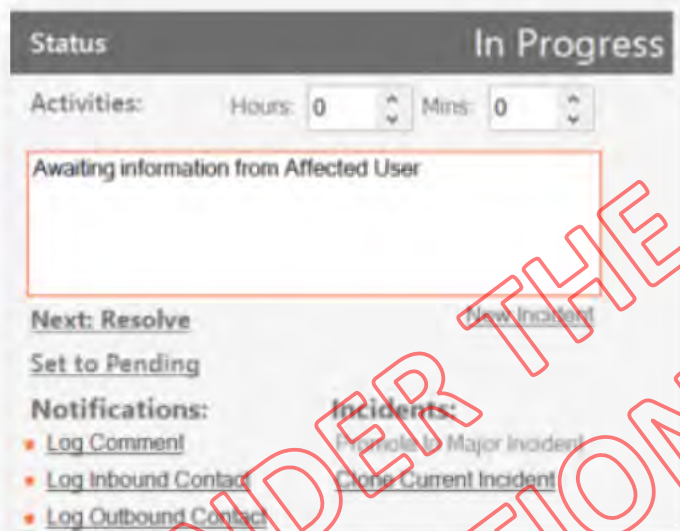
Cherwell does not directly allow users to 'stop the SLA clock' in the same way that R12 did previously; You can, however, can stop the SLA on an incident using the 'Pending SLA' functionality.

Note that the incident will go back to an *In Progress* status automatically once the specified date/time has been reached.

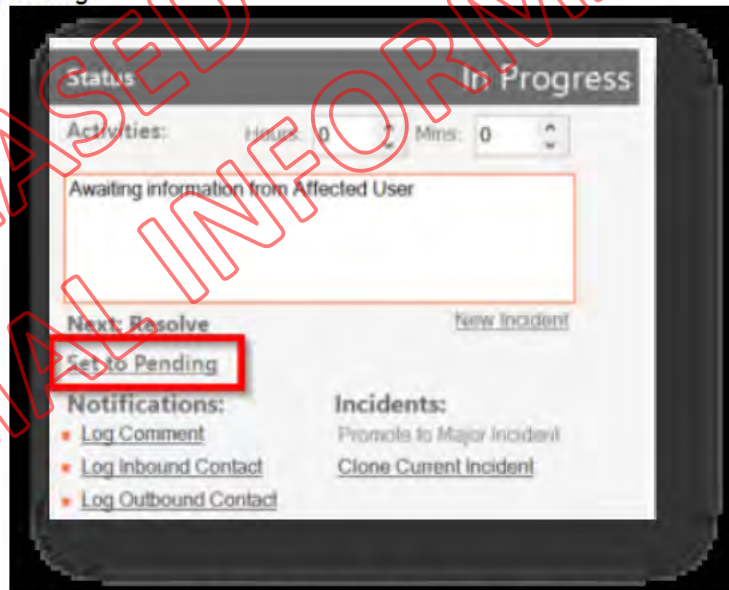
To change the status of an incident to Pending SLA follow the steps below:



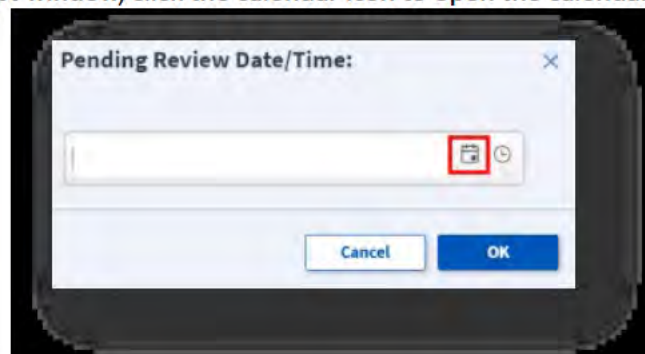
1. From the Action Bar of the incident, add the reason that the incident is being set to Pending into the comments box.



2. Click *Set to Pending*.



3. from the prompt window, click the calendar icon to open the calendar.

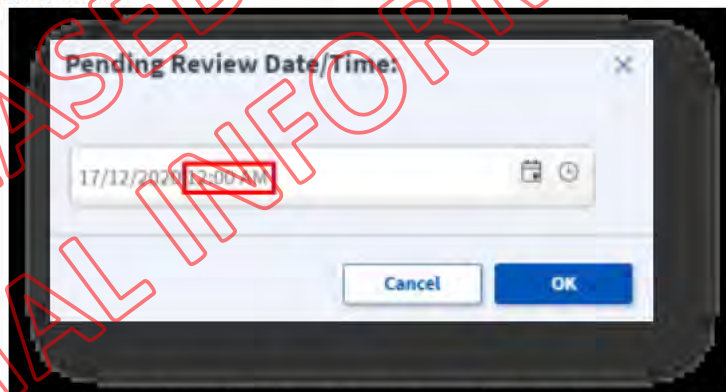




- Select a date for the incident to come off pending SLA. This should be a date 1-2 business days ahead, depending on the customer’s contract.



- If required, change the time by clicking on the time and typing into the box then click Ok. To change the default 'AM' to 'PM' tap the letter 'P' on your keyboard. Likewise tap the letter 'A' to switch back to 'AM'.

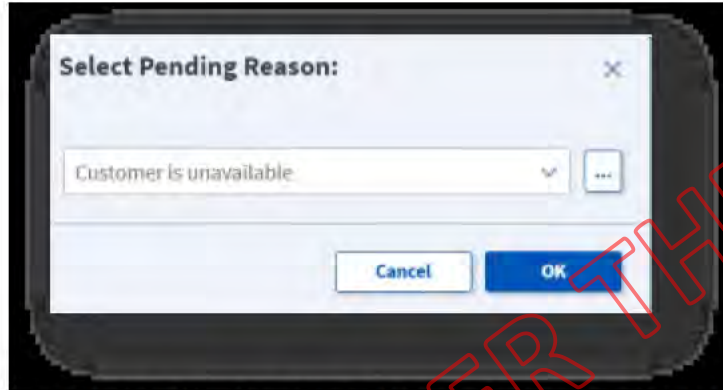


- Select a Pending Reason from the drop-down list and click OK. As this is a global list of options, there will be some that do not apply. The table below gives a list of Pending Reasons for Datacom NZ use:

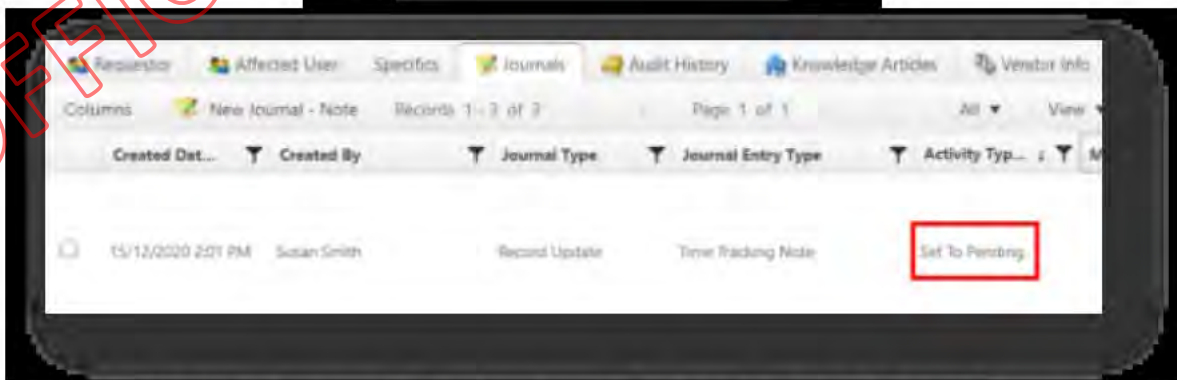
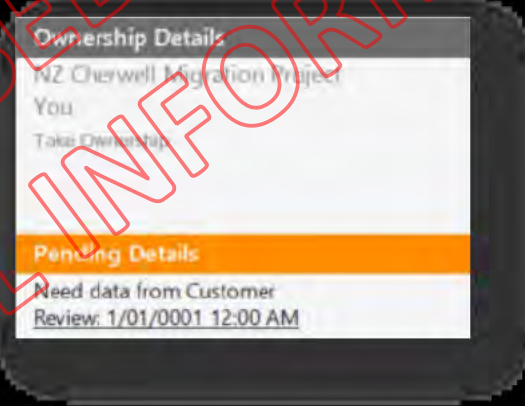
Pending SLA Reason	When to Use:
Customer is Unavailable	This option covers the various situations where you need something from the affected user to progress the incident
Pending Approval	This provides for an incident waiting for approval to progress, such as a hardware request, access request etc. This could include the affected user’s line manager, an SDM, Project Manager etc



Pending Development Fix	This would be used if the incident can only be resolved once release or upgrade has been completed.
-------------------------	---



7. Referring to the screenshots below, the status of the incident will change to Pending and a journal note will be created under the journals tab.



8. Once the date/time specified has been reached, the incident will return to its previous status



9 Transferring an Incident

If the CTSO have found that there is nothing wrong on the vMLC and suspect there may be a network issue back at Datacom, Comtech support emails the Datacom Service Desk via service.desk@mbie.govt.nz to redirect to an appropriate party.

Note

The transfer of an incident by Comtech back to Datacom should only happen for P3/P4 incidents. P1/P2 incidents that are service affecting are managed by the assigned Datacom Incident Manager.

10 Closing an Incident

Once a ticket has been set to **Resolved** status, the ticket will be automatically updated to **Closed** status within 48 hours.

A ticket can also be closed manually.

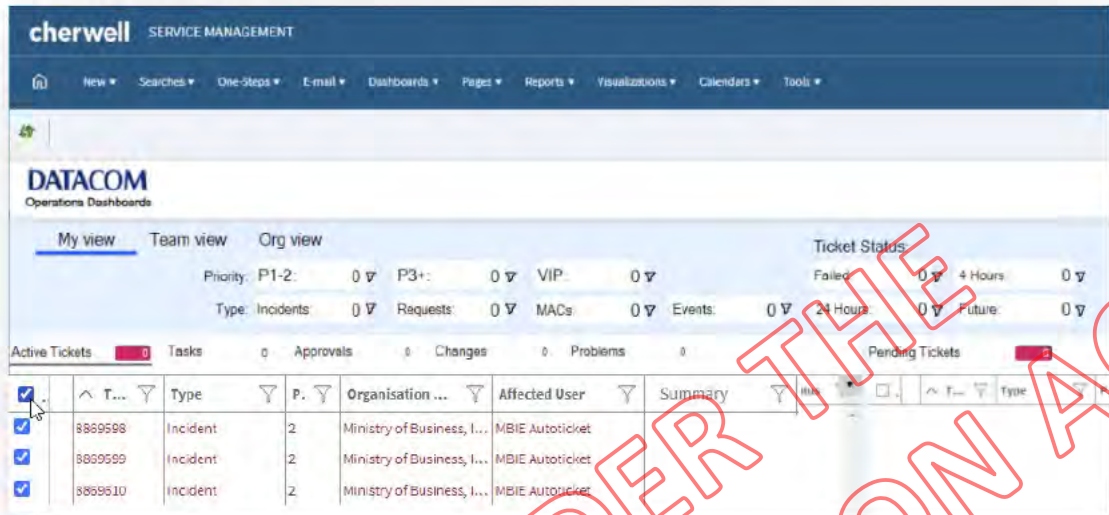
11 Bulk Closing Incidents

If events from the vMLC are not suppressed during maintenance activities, it can result in a large number of incidents being generated within Cherwell.

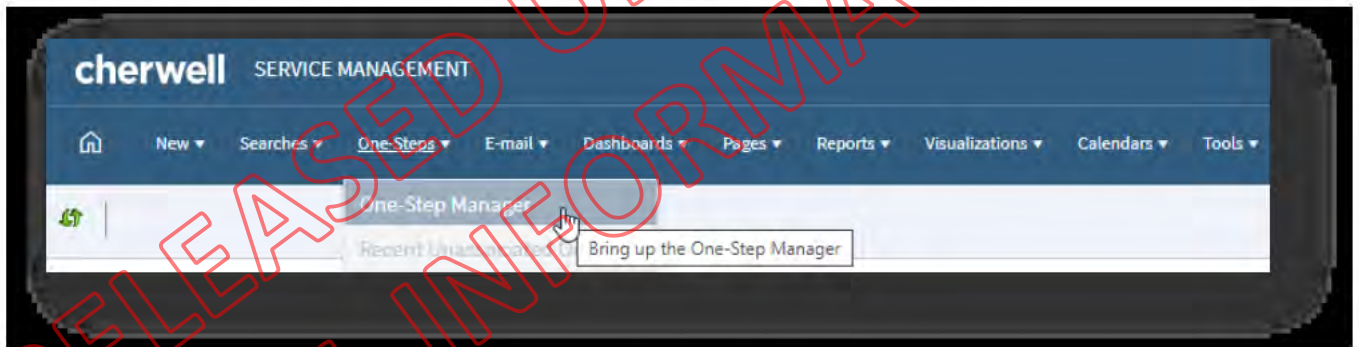
To efficiently deal with these, Cherwell provides a way to 'bulk close' incidents. The way you do this is described in the following pages.



1. As shown in the screenshot below, select the checkbox at the top of the list to select all the incidents you want to close:

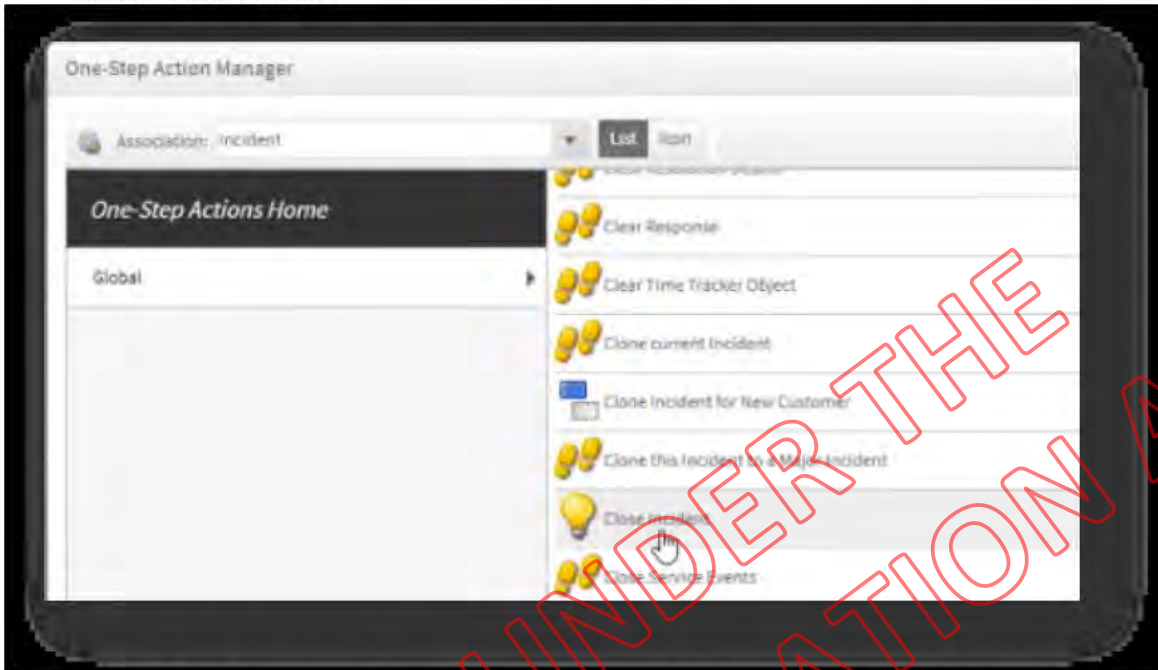


2. From the top menu bar, select *One-Steps*, then select *One-Step Manager*.

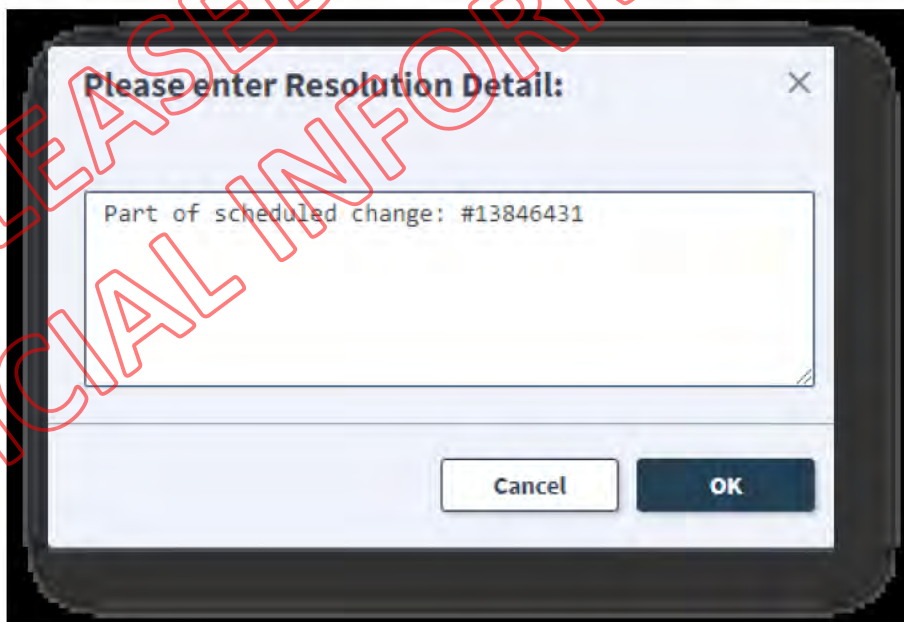




3. You will then be taken into *One-Step Action Manager*, as show below. From the list, double-click on *Close Incident*:

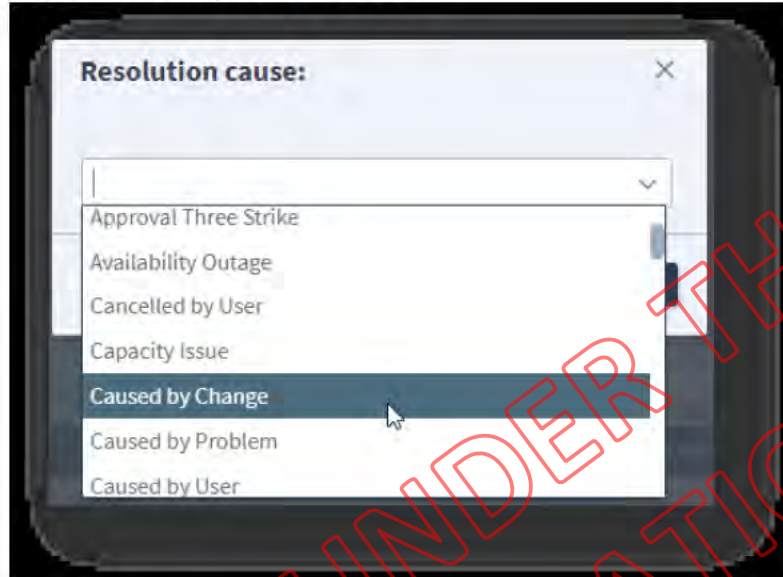


4. You will then be prompted to enter the Resolution Detail, as shown here, followed by the Resolution Cause (shown on the screenshot on the following page):





5. After entering the Resolution Cause, e.g., “Caused by Change”, click on *OK*. All the selected incidents will now have the same resolution details and resolution cause applied to them before having their status updated to *Closed*.



RELEASED UNDER THE
OFFICIAL INFORMATION ACT



IN CONFIDENCE



Probable Caller Location: A rough guide

Version 0.1

Date: 18 November 2016

RELEASED UNDER THE
OFFICIAL INFORMATION ACT



Table of Contents

2. Mobile calling: the basics	3
Mobile networks in New Zealand	3
What you need to make a mobile call	3
How the MNO bills against your subscription	3
Roaming	3
3. Mobile calling: emergency calls	4
What is an emergency call?	4
How is an emergency call initiated?	4
Are calls to numbers such as *555 emergency calls?	4
What is needed to make an emergency call?	4
Emergency roaming	5
Caller ID for emergency roamers	5
4. Probable Caller Location	6
What is it?	6
How do emergency services get PCL?	6
Probable Caller Location (Network).....	6
Probable Caller Location (Handset)	6
Why 'probable' caller location?	7
Why 68 percent?.....	7
When is PCL (Network) available for a call?	9
When is PCL (Handset) available for a call?	9
5. FAQs	10
Could a caller be outside the PCL circle?	10
Can I get PCL for international roamers?	10
Why was no PCL available?.....	10
Why did I get multiple PCLs?	10
What does 'location_method = N' mean?.....	10

2. Mobile calling: the basics

Mobile networks in New Zealand

There are three mobile networks in New Zealand for transmitting mobile voice calls, SMS messages and data. These networks are operated by the Mobile Network Operators (MNOs) Spark, Vodafone, and 2degrees. All cell towers in New Zealand are operated by one of these three companies.

What you need to make a mobile call

To make an ordinary mobile voice call, send an SMS, or send or receive data over one of the New Zealand mobile networks, you need to have a Subscriber Identity Module (SIM) in your mobile device and an active subscription (prepay, plan etc) with the SIM provider. Your subscription identifier is your phone number in an international form known as a Mobile Station International Subscriber Directory Number (MSISDN) e.g. '64271234567'.

You can buy a SIM card from one of the MNOs (Spark, Vodafone, or 2degrees) or from a Mobile Virtual Network Operator (MVNO) who has an arrangement to use the network belonging to one of the MNOs. For example Skinny Mobile is an MVNO that has an arrangement to use Spark's network.

How the MNO bills against your subscription

Every SIM card has a unique identifier called an International Mobile Subscriber Identity (IMSI). The first three digits of the IMSI indicate the SIM's country of origin (Mobile Country Code or MCC) and the next two the company that issued the card (Mobile Network Code or MNC). The MCC for New Zealand is 530. Examples of MNC include 01 for Vodafone, 05 for Spark, 24 for 2degrees and 06 for Skinny Mobile. An IMSI starting with '53024' would therefore have been issued by 2degrees.

When you make a call, your IMSI is sent from your handset to the mobile network, where it is used to look up your MSISDN (phone number) in a subscriber directory. Now the MNO can perform functions such as billing against your subscription and supplying the number to the call recipient as Caller ID.

Roaming

If you have a New Zealand SIM, when you make a call or send an SMS or use mobile data, you will normally use the mobile network of your SIM provider, or if the SIM provider is an MVNO, the MNO whose network they have arrangements to use.

However you can use a second MNO's mobile network where that company has an agreement with your provider. Usually the agreement has been made in order to improve the effective geographical coverage of your provider's network. For example in New Zealand if you are a 2degrees customer but you are outside of the coverage of the 2degrees network, you can roam on the Vodafone network. 2degrees makes its subscriber directory available to Vodafone so it knows who to pass the billing on to.



3. Mobile calling:

emergency calls

What is an emergency call?

To a mobile network, an emergency call is any call flagged as being of Call type = 'Emergency'. The flagging means that rules can be applied e.g. it can be prioritised on the network and be automatically redirected to a particular destination. In New Zealand, this destination is the Spark Initial Call Answering Point (ICAP).

How is an emergency call initiated?

A call is set up as an emergency call if the SIM card or handset has been pre-programmed to recognise the number dialled as an emergency call. In New Zealand all MNOs and their MVNOs have the official emergency number (111) on their SIMs plus other numbers as per the following table:

Number	Comment	Spark SIM	Vodafone SIM	2degrees SIM
111	Official New Zealand emergency number.	✓	✓	✓
112	Universal emergency number from mobiles supported by GSM standard, also emergency number for Europe	✓	✓	✓
911	Emergency number for US	✓	✓	✓
999	Emergency number for UK	x	✓	✓
000	Emergency number for Australia	x	✓	✓
119	Emergency number for parts of Asia	x	x	✓

Handsets are also pre-programmed with emergency numbers but it is not easy to put together a comprehensive list of what numbers are programmed into what handsets as handsets using New Zealand SIMs may have come from anywhere, not just the MNOs/MVNOs themselves.

Are calls to numbers such as *555 emergency calls?

*555 is toll-free like 111 but is for reporting non-emergency matters. It is therefore not programmed into SIMs or handsets and does not initiate an emergency call.

What is needed to make an emergency call?

To make an emergency call in New Zealand, you need to:



1. have a SIM in your mobile device; and
2. be in an area covered by any MNO's network – even if you don't have a subscription with them.

Mobile devices are technically able to make emergency calls even without a SIM but in New Zealand this is not supported. Usually the rationale for a country choosing to do this is that a caller without a SIM cannot be blocked and therefore there is no mitigation available for persistent nuisance calling.

Emergency roaming

All MNOs are required to support emergency calls from any device with any SIM. Where the caller is not an active subscriber of the MNO or an MVNO, this is a special case of roaming known as 'Emergency roaming'.

An emergency roamer is someone who is making an emergency call on a MNO's network:

- where their subscription with the MNO or MVNO has lapsed; or
- that is using a SIM supplied by a NZ or overseas company with no roaming arrangement with the MNO.

In emergency roaming cases, the MNO does not have access to the relevant subscriber directory and therefore cannot determine the caller's MSISDN (phone number). This means that no cross-billing can occur (although the call is free anyway), and a proper Caller ID cannot be provided to emergency services.

Caller ID for emergency roamers

While a 'proper' Caller ID representing the MSISDN (phone number) cannot be provided for emergency roamers, in New Zealand a number of some sort is always provided to emergency services for emergency calls:

1. Spark assigns a unique number that is not the MSISDN but is based on the device's unique identifier, the International Mobile station Equipment Identity (IMEI). The number is formulated as '0911' + '[7 digits of the IMEI]'.
2. 2degrees assigns the number '0221420003' in all cases.
3. Vodafone assigns either '021090000', '021040000' and '021030000' depending on the particular part of the network serving the call.

2degrees and Vodafone additionally assign the above numbers as Caller ID to all emergency callers with international SIMs, even if they can access a subscriber directory and obtain the caller's MSISDN.

OIA 9(2)(b)(ii)



4. Probable Caller Location

What is it?

Probable Caller Location (PCL) is the most likely location of a mobile emergency caller, represented as a circle on a map (described via latitude, longitude, and radius). The emergency caller has a two-thirds likelihood of being somewhere in the circle. PCL is made available to New Zealand emergency service communications and clinical control centres and is intended as supplementary information to support the usual process of question-and-answer establishment and verification of event location.

Probable Caller Location is obtained via two completely separate methods, 'Network' and 'Handset', the former being typically low precision (large radius circle) and available for most emergency calls made from any type of mobile handset, and the latter being typically better precision but only available for calls made from Android handsets. One type of PCL, both types, or neither may be presented for a particular emergency call.

How do emergency services get PCL?

Emergency service provider CAD systems can be set up to request PCL automatically when an emergency call is received. Where CAD systems have not yet been set up to do this, a web interface (web.pcl.govt.nz) is available to request PCL manually.

Manual and automatic PCL requests work the same way. A request contains the emergency caller's mobile number (obtained from Caller ID) and PCL records are returned where there is an exact match between the Caller ID and the MSISDN on a PCL record. All Handset or Network PCL records available in the system are returned. As PCL is only retained for an hour after an emergency call is made, values returned only relate to emergency calls made from the number within the last hour.

Probable Caller Location (Network)

Probable Caller Location (Network) is location information obtained from Google using network information about the emergency call obtained from the relevant MNO.

When an emergency call is initiated, the relevant New Zealand MNO sends the PCL solution a record containing the Caller's MSISDN, the time of the call, and the ID of the cell tower antenna that the call was initiated on. The PCL solution then sends the cell tower ID to the Google Maps Geolocation cloud service, which returns a PCL.

Google can convert a cell tower antenna ID to a PCL because it is already as a matter of course constantly getting information from Android handsets relating to their GPS location and the cell site antennae they can 'see'. The Google Maps Geolocation service uses this information in reverse to infer a probable location given a cell tower antenna ID.

Note that this means that PCL (Network) can be interpreted as 'When people in the past have made calls from this cell tower, 68% have been within this area'. PCL (Network) therefore reflects the population centre of people historically using the cell tower and should not be interpreted as the location or coverage of the cell tower itself which is the information that has been obtained from MNOs in the past. In particular an emergency call made via a cell tower serving a large rural area in which there is one isolated township will have a PCL that reflects the location of the township as this is where most callers will have been located in the past. However the call itself could well have come from someone stopped at the side of a country road a long way from the town.

Probable Caller Location (Handset)

Probable Caller Location (Handset) is location information obtained directly from Android handsets. The Android mobile operating system was developed by Google, so PCL (Handset) is, like PCL (Network), also a Google-based solution.



Modern smartphone handsets have their own inbuilt 'Location services' capability for estimating their location. This is familiar to smartphone owners through their use of mobile mapping and other applications that demonstrate knowledge of the user's location. Location services capability obtains location using one of several technologies depending on what can give the best precision given the environment of the handset at the time, although this logic is all invisible to the user. The most precise location is obtained when the device has a clear line of sight to GPS satellites (more properly referred to by the generic term GNSS), but handset location may also be derived with lower precision from the Wifi access points or cell towers the handset can see.

Probable Caller Location (Handset) is sent from Android handsets to the PCL service via a new Google feature that has been enabled in New Zealand. This feature, usually referred to as Android Emergency Location, triggers the sending of an SMS with location information when an Android user dials an emergency number (111 or 112). The SMS is sent to the PCL service which creates a PCL (Handset) record ready for emergency services to retrieve.

Why 'probable' caller location?

In an ideal world, emergency service providers would be given an exact 'pinpoint' location of the caller that they could have 100% confidence in. However both Handset and Network methods used to derive Probable Caller Location are not exact and so the caller location is instead represented as a finite area, not a pinpoint.

Moreover PCL is not presented as an area in which emergency service providers can have 100% confidence – this could be done but the area would be larger and correspondingly less useful. According to common statistical practice, Google presents location as an area of 68 percent confidence. The upside is that this area will be considerably smaller than one of higher confidence but the downside is that care has to be applied as it can be relied on to reflect the actual location of the caller only about 2/3 of the time.

Why 68 percent?

[Warning – maths!]

In representing the most likely location, Google assumes a *normal* probability distribution. A normal distribution has a characteristic shape as shown in Figure 1 and is defined by its midpoint (mean, μ) and its standard deviation (σ) – the distribution's 'fatness' or 'skinniness'. For any normal distribution 68% of the time the 'real' value is within one standard deviation (σ) of the mean (μ), 95% of the time it is within two standard deviations of the mean and 99.7% of the time it is within three standard deviations from the mean.

In the case of location, we have two dimensions (Figure 2). Separate normal distributions apply to the estimation of latitude and longitude (red and blue in the diagram) although Google assumes that the standard deviation (σ) is the same for each. The Probable Caller Location values provided by Google are latitude, longitude and radius, which correspond to the means μ of each of the red and blue distributions and the standard deviation (σ). The area is therefore that in which the 'real' value is 68% of the time.

Note that Google could have chosen to report the radius as two (or three) standard deviations in which case the caller could be interpreted as being within the new (much larger) circle with 95 (or 99.7) percent confidence. However this is not necessarily 'better' information as a two (three) standard deviation circle covers four (nine) times the area of a one standard deviation circle.

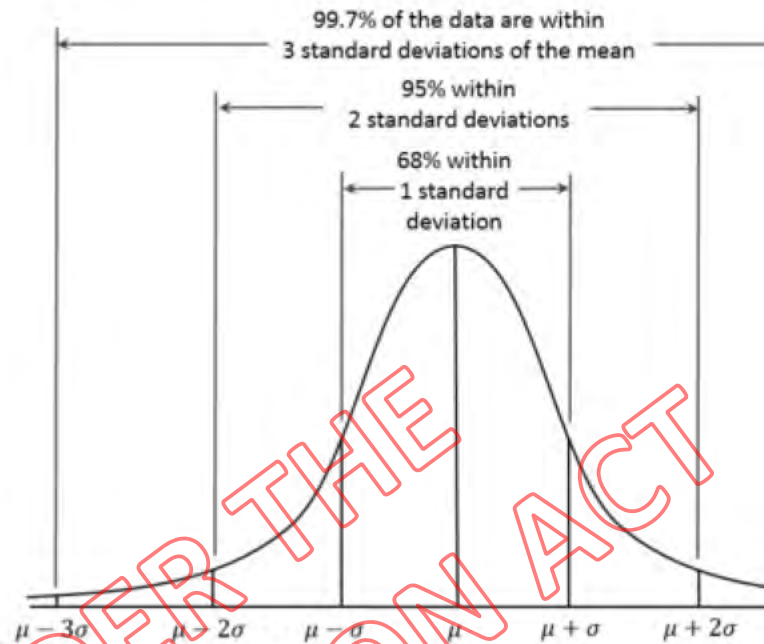


Figure 1 Normal distribution in one dimension (Wikipedia)

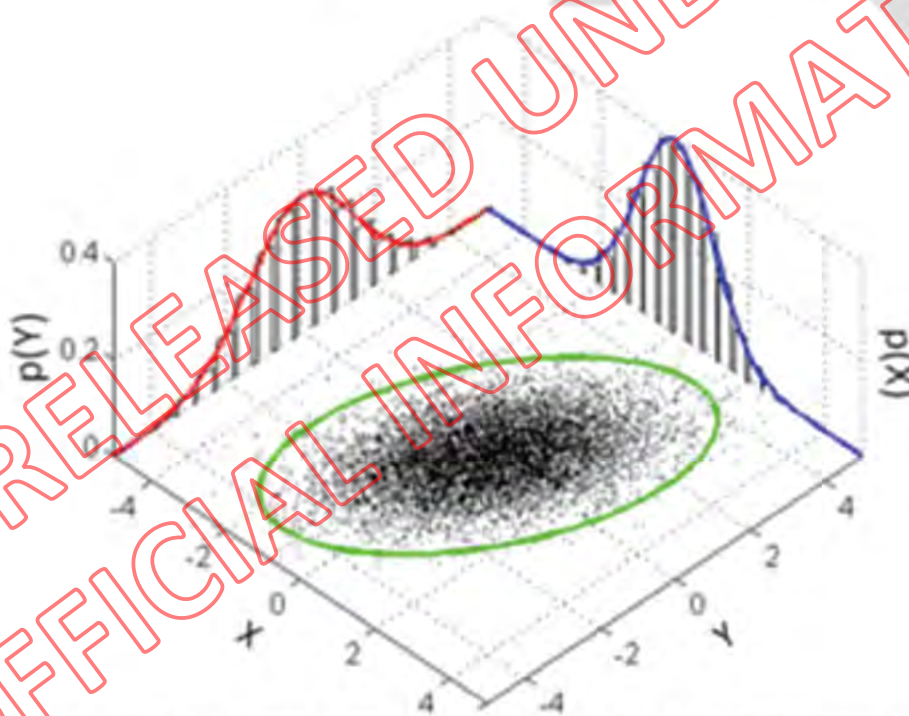


Figure 2 Normal distribution in two dimensions (Wikipedia). If X and Y are instead latitude and longitude, the diagram illustrates how a PCL circle relates to the assumed underlying normal distributions



When is PCL (Network) available

for a call?

The Probable Caller Location solution can present PCL (Network) to an emergency services call taker where all of the following apply.

1. **The mobile voice call was seen by the Network as being an emergency call, i.e. was of Call type = 'Emergency'.** This therefore does not include
 - a. Calls forwarded to the emergency line from other numbers, e.g. non emergency numbers such as Police Stations.
 - b. Calls to the ICAP that were not set up as emergency calls in the network e.g. Spark mobile calls to the Australian emergency number 000 go to the ICAP but are not set up with Call type = "Emergency".
2. **The call was presented to emergency services with a valid Call ID, therefore allowing for the possibility of a match to a PCL records' MSISDN.** This therefore does not include:
 - a. Emergency roamers - whether with international or New Zealand SIM cards; and
 - b. Roamers with international SIMs on the Vodafone and 2Degrees networks.
3. **The call was made within the technical limitations of Network method.** This therefore does not include
 - a. 2G calls made on the Vodafone network, as records for these calls can't for technical reasons be sent until the call is over;
 - b. Vodafone calls made via a femtocell, as Vodafone cannot supply unique IDs for these.
 - c. All emergency roamers as MSISDN cannot be determined for these;
 - d. Calls made on new cell tower antennae that the Google Maps geolocation service doesn't yet have enough data for.

When is PCL (Handset) available for a call?

The Probable Caller Location solution can present PCL (Handset) to an emergency services call taker for a caller to emergency services where all of the following apply.

1. **The mobile voice call was initiated by the calling dialling 111 or 112.** This therefore does not include
 - a. Calls forwarded to the emergency line from other numbers, e.g. non emergency numbers such as Police Stations.
 - b. Calls made to the ICAP that were initiated by dialling other emergency (or non-emergency) numbers e.g. 911 or 999, even if these set up a call of type 'Emergency'.
2. **The call was presented to emergency services with a valid Call ID therefore allowing for the possibility of a match to a PCL records' MSISDN.** As above.
3. **The call was made within the technical limitations of the Handset method.** This therefore does not include
 - a. Emergency calls made from mobile devices other than Android phones e.g. iPhones, Windows phones, non-smartphones.
 - b. Emergency calls made from Android phones
 - i. That have not been enabled with Android Emergency Location; or
 - ii. That have a battery level below a minimum of 5% or
 - iii. That have an international SIM – these are excluded as there is no current solution to prevent these callers being charged for the SMS.



5. FAQs

Could a caller be outside the PCL circle?

Yes. In theory the caller has a 1/3 chance of being outside the circle. However for PCL (Network) in urban areas and all PCL (Handset) they will tend to be outside the circle less frequently than that.

PCL(Network) reports where calls using a given cell tower usually come from, which is not necessarily where the caller actually is. Where a cell covers a large rural area with a small population centre, PCL(Network) will preferentially indicate the population centre where calls would usually have come from in the past.

Can I get PCL for international roamers?

If an emergency call has a Caller ID that is clearly a genuine international number then it is possible that a PCL (Network) will be available. However PCL (Network) cannot be provided in other cases.

PCL (Handset) is not available for international roamers.

Why was no PCL available?

If the mobile caller did not initiate an emergency call (e.g. dialled a non-emergency number and was then forwarded to the emergency line), then no PCL of any kind will be available.

The most common reason for the absence of PCL (Handset) for an emergency mobile call is that the call was not made from an Android phone or the Android phone or had an international SIM.

PCL (Network) is available for most mobile emergency calls – see 'When is PCL (Network) available for a call for the exceptions.

Why did I get multiple PCLs?

The system generates up to two PCL records (one Handset, one Network) per emergency call, and keeps PCL records for an hour after the call was initiated. If the caller made an emergency call more than once within the last hour, more than two PCL records may exist for that number.

What does 'location_method = N' mean?

A PCL may be available but have a 'zero' latitude, longitude, and radius, and be marked as 'location_method = N'.

On a Handset PCL record this means the handset tried to get location but none was available (all available technologies failed).

On a Network PCL record means that the MNO provided a record with information about the Cell ID but no location could be determined from it via Google. Possible reasons are:

- It was a Vodafone call over a femtocell – Vodafone is unable to provide a unique cell identifier in these cases.
- The cell is too new (or has been moved) so the Google Maps Geolocation API does not yet have enough information on it to provide a position;
- The request to Google failed for some other unknown reason.

Is PCL (Network) the same as cell tower information we get from MNOs?

No.

Emergency service providers have in the past made requests to MNOs for the physical address of the cell tower that served an emergency call. They may also have received information on the likely radius of coverage of that tower.

PCL (Network) does not report the position of the cell tower – instead it reports the typical location of callers recently using the cell tower. Figure 3 shows how different the two can be in a rural situation. The PCL (Network) for a particular antenna on a Vodafone cell tower at Ward in the upper South Island is most commonly used by callers in Palliser bay, some 100 km away in the lower North Island.

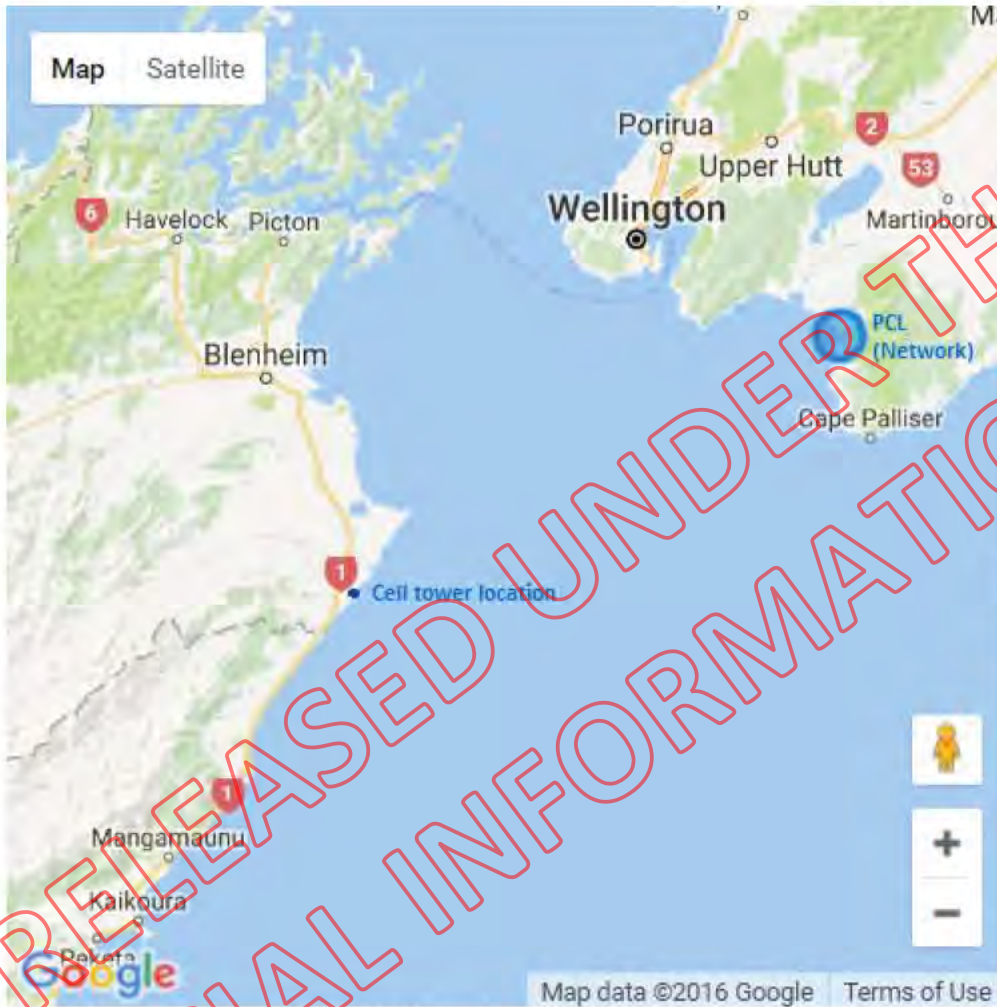


Figure 3 Example showing how PCL (Network) can differ significantly from the location of the caller's cell tower.



IN CONFIDENCE

Probable Caller Location: User Guide

Version 0.3

Date: 10 April 2017

RELEASED UNDER THE
OFFICIAL INFORMATION ACT



Purpose

This document has been written to provide emergency services call takers the basic information on where PCL data comes from, how to access and use it and provides detail on availability and accuracy of the data.

Version history

Date	Version	Author	Description of change
17/03/2017	0.1	Scott Weston	Publish first draft
27/03/2017	0.2	Scott Weston	Added FAQs covering access, use, accuracy and technical support. Updated availability statistics.
10/04/2017	0.3	Scott Weston	Addition of web UI screenshots

Contents

What is Probable Caller Location?	2
Location Source	2
Location Method	2
How do I get PCL information?.....	3
How do I use PCL Information?	4
Could the caller be outside of the PCL circle?	8
Why do I have more than two PCL records?	8
What if no PCL information is available?.....	8
Why do I not always get PCL information?.....	8
I haven't received PCL information in a while what should I do?Error! Bookmark not defined.	

Glossary of terms

Acronym	Term	Description
AEL	Android Emergency Location	Google technology by which handset location is determined, sent by SMS when an emergency call is made on an Android handset.
CAD	Computer Aided Dispatch system	ESP system used by call takers and dispatchers to record details of an event and dispatch response.
	Cell Site or Cell Tower	The antenna that receives and sends data for mobile telephone calls, SMS and data as part of the mobile network.
ESP	Emergency Service Provider	Police, Fire, or Ambulance (St John and Wellington Free).
MNO	Mobile Network Operator	In New Zealand, Spark, 2degrees, and Vodafone.
PCL	Probable Caller Location	A Probable Caller Location is the combination of latitude, longitude and a radius, together provide a circle area where the mobile caller is most likely to be located.



What is Probable Caller Location?

The Probable Caller Location (PCL) service provides New Zealand Police (**Police**), the New Zealand Fire Service (**Fire**) and St John and Wellington Free Ambulance Services (**Ambulance**) call-takers with location data for mobile callers dialling 111. The location data supplied by the PCL service is presented as a circle on a map either within the Computer Assisted Dispatch (**CAD**) system or the backup Web User Interface (**Web UI**). This circle represents the most likely location area of a mobile emergency caller.

The PCL service is not designed to replace the current process of verbal establishment and verification of the emergency event location, but to enhance this process with supplementary information.

Location Source

The system generates up to two records for each mobile emergency call, one from the Network and one from the Handset:

- **Mobile Network (Network PCL)** – derived from the ID of the serving cell site provided in near real-time by Mobile Network Operators (MNOs). The Probable Caller Location (PCL) is provided by Google using statistical analysis to define the probable location of the caller using the cell site. Network PCL is presented to Emergency Service Providers (ESP) call takers for all mobile calls made within New Zealand.
- **Android Handsets (Handset PCL)** – provides the highest precision location data available to the handset at the time of the call. The handset can use GPS, Wi-Fi or cell site information to define its location. The handset also uses Google statistical analysis to define the PCL when using either Wi-Fi or cell site information. Handset PCL is currently only presented to ESP call takers for mobile calls made from Android handsets.

Location Method

The solution uses three methods for determining mobile caller's location:

- **Network Cell Site** – low precision location area - obtained using statistical analysis to define the probable location of the caller that has connected to the cell site. This location method is available to all phones type and all networks.
- **Wi-Fi** – low precision location area - obtained using statistical analysis to define the probable location of the caller that can connect to known Wi-Fi site. This location determination method is only provided by Android handsets in the solution.
- **GPS** – high precision location area - obtained via a phone's GPS receiver that calculates probable location based on time signals transmitted along line of sight by radio from at least four satellites. This location determination method is only provided by Android handsets in the solution.

How do I get PCL information?

Integrated CAD solution

The CAD system automatically makes a request for PCL data once an emergency call is received by the system. A button has been added to your screen that will highlight when PCL data is available, pushing this button will bring up the location information on your map.

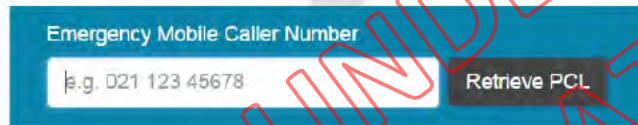
A second request for PCL data will also be made a number of seconds later to provide any additional delayed PCL data with the button highlighting again when new PCL information is available.

Please refer to your agencies training manual on how this information is displayed within the CAD system and what functionality has been added to support it.

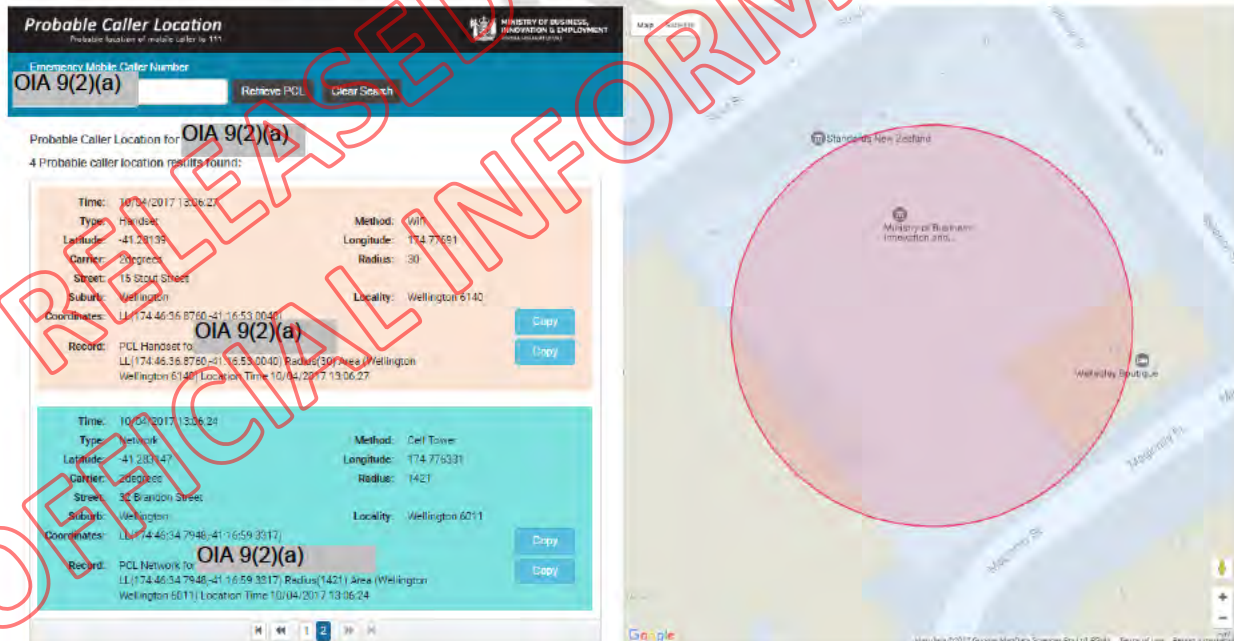
PCL Website

A website ^{OIA 9(2)(c)} is also available to request PCL data manually – this is for use in situations where the CAD system enhancement is unavailable.

Just enter the telephone number of the mobile 111 caller into the search field and press the 'Retrieve PCL' button or hit enter to search for PCL information for that caller.



When PCL information is available it will be displayed on the web interface as below.



Probable Caller Location
Probable location of mobile caller to 111

Emergency Mobile Caller Number
OIA 9(2)(a) Retrieve PCL Clear Search

Probable Caller Location for **OIA 9(2)(a)**
4 Probable caller location results found:

Time: 10/04/2017 13:06:23	Method: Wifi
Type: Hot User	Longitude: 174.77691
Latitude: -41.28195	Radius: 30
Carrier: 2degrees	
Street: 15 Stout Street	Locality: Wellington 6140
Suburb: Wellington	
Coordinates: LL(174.46368760;-41.16530040)	
Record: PCL Handset for OIA 9(2)(a)	Copy
LL(174.46368760;-41.16530040) Radius(30) Area (Wellington Wellington 6140) Location Time 10/04/2017 13:06:23	Copy

Time: 10/04/2017 13:06:24	Method: Cell Tower
Type: Network	Longitude: 174.776331
Latitude: -41.283147	Radius: 1421
Carrier: 2degrees	
Street: 30 Brandon Street	Locality: Wellington 6011
Suburb: Wellington	
Coordinates: LL(174.46347948;-41.16593317)	
Record: PCL Network for OIA 9(2)(a)	Copy
LL(174.46347948;-41.16593317) Radius(1421) Area (Wellington Wellington 6011) Location Time 10/04/2017 13:06:24	Copy



Results will be displayed on a Google map as follows. The most recent record will be drawn as a circle in the middle of the map. This following map shows a Wi-Fi location method:



The following map shows a GPS location method, which has higher precision than Wi-Fi location method:





The page displays the telephone number that was searched and the number of PCL records that have been returned for that telephone number.

OIA 9(2)(a)

Probable Caller Location for [Redacted]

4 Probable caller location results found:

When there is more than one PCL record the top record on the page is the most recent. When there are more than two records that have matched the searched mobile telephone number a paging tab will appear so that older results can also be viewed.



Results will be displayed in text form, as follows.

Time: 10/04/2017 13:06:27

Type: Handset

Latitude: -41.28139

Carrier: 2degrees

Street: 15 Stout Street

Suburb: Wellington

Coordinates: LL(174:46:36.8760,-41:16:53.0040)

Record: PCL Handset for [Redacted]

Method: Wifi

Longitude: 174.77691

Radius: 30

Locality: Wellington 6140

OIA 9(2)(a)

[Copy]

[Copy]

LL(174:46:36.8760,-41:16:53.0040) Radius(30) Area (Wellington Wellington 6140) Location Time 10/04/2017 13:06:27

Tooltips are built into the webpage that provide help text about the data being displayed, just hover your mouse cursor over the label and the help text will be displayed.

Time: Time the callers location was recorded.

The following table defines each data label.

Data Label	Help Text
Time	Time the caller's location was recorded.
Type	Either Network or Handset; Network location is obtained from Google based on the mobile cell tower that the call connects through, Handset location is obtained directly from supported handsets using GPS or other available method.
Method	Method used to obtain the location; either GPS, WiFi, or Cell Tower location.
Carrier	The Mobile Network Operator who has handled the call.
Radius	Location accuracy expressed in meters.
Coordinates	Coordinates in degrees minutes and seconds in a format accepted by Police CAD system.
Record	Location data provided in a format for easy copying.



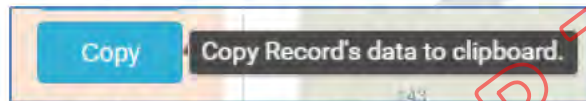
The following data is also presented:

- Latitude
- Longitude
- Street
- Suburb
- Locality

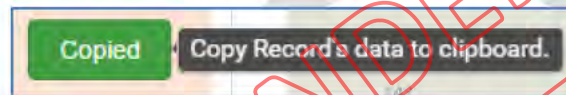
The latitude and longitude define the centre of the circle and the street, suburb and locality provide an address for the centre of the circle.

NOTE - The latitude, longitude and address do not provide a dispatch location.

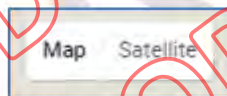
Two copy buttons are provided for quick copying of the key information, when you click the button it



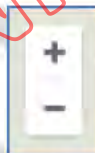
will change colour and confirm that the information has been copied.



Google maps functionality is available for users within the map. User can change the map view to a satellite view by selecting the 'Satellite' button.



Users can also zoom in and out of the map using the plus and minus button or place your mouse cursor over the map and use your mouse scroll wheel, forward zooms in and backwards zooms out.



The following mobile telephone number formats are supported by the PCL website:

Telephone Number Format	Description
0212456768	A valid phone number with leading zero but no leading country code or character.
1021234567	A valid phone number with a leading one and zero, and no country code, for national numbers.
1006421234567	A valid phone number with a leading one double zero and country code, for international numbers.
006123678930	A valid phone number with a leading double zero and country code for calls from overseas SIM cards.
+64212345678	A valid phone number with leading country code.



How do I use PCL Information?

You can use any roads, buildings or landmarks that are within the PCL circle or immediately outside to assist the mobile caller in describing their location.

NOTE - You still need to define and verify the location of the caller.

The PCL information does not provide an address for dispatch or the location of the event.

Could the caller be outside of the PCL circle?

Yes; the caller may be outside the circle as often as for 1 in 3 mobile calls due to the usage of statistical data and analysis.

It is important to note that PCL records with the location method of Cell Tower and Wi-Fi only show the **probable** location of the mobile caller. The probable caller location is determined using Google mapping service that defines the location of a mobile caller based on previously recorded location data of all Google users connected to the same cell tower or surrounding Wi-Fi hotspots and access points.

Why do I have more than two PCL records?

The PCL website returns all PCL records held for a mobile caller's telephone number when a request is made, if a caller has made more than one call to 111 in the last hour the location is returned for all these calls. The most recent location is shown first.

What if no PCL information is available?

When PCL data is unavailable you will need to continue with your normal processes of confirming dispatch location.

What should I do if I haven't received PCL information for a long time?

When consistently, and for over an hour, less than one in three 111 calls do not provide PCL information you should contact your ICT service desk, who provide 24/7 support for this service.

When you are concerned the PCL service is not working as it should, check the PCL website to see whether information is returned for the same telephone number; let your service desk know when you have used the PCL website and what results you received so they can investigate and if required raise an incident ticket on your behalf.



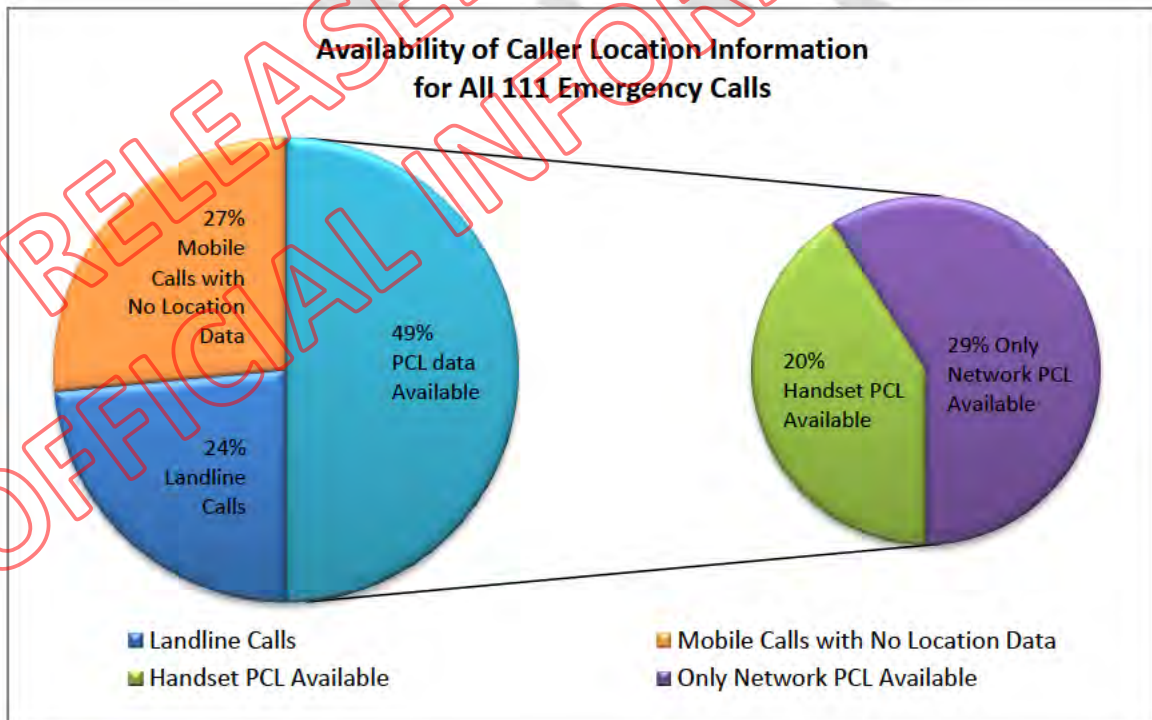
Why do I not always get PCL information?

Following full solution implementation 90% of all mobile 111 emergency calls are projected to have PCL information available.

There are some technical limitations of the mobile network which means that not all mobile emergency calls will have a network PCL, and currently only Android handsets provide handset PCL data. The current location information remains in place for landline calls.

The below table and charts provide an overview of the availability of the different PCL data, correct as of TBD:

Location data	Availability of Location Information for All 111 Emergency Calls
Landline (TESA)	24% (1 in 4) of all emergency calls
Mobile	49% (2 in 4) of all emergency calls
Only Network PCL Available	29% (6 in 20) of all emergency calls
Handset PCL Available	20% (4 in 20) of all emergency calls





IN-CONFIDENCE: RELEASE EXTERNAL

Emergency Caller Location Information (ECLI)

Training Notes – May 2022

Issued by:

Chris Nyman, ECLI Manager Service Integration

Issue date:

13th May 2022

RELEASED UNDER THE
OFFICIAL INFORMATION ACT

Document purpose

This purpose of this document is to provide training notes on some of the key features used within the virtual Location Aggregation Centre (vLAC) application on the ECLI Location Platform. Some functionality has been released relatively recently (Direction of travel), so this may provide a refresher to some staff.

Training components

1. Direction of travel	3
2. Phone number format.....	4
3. Retrieve ECLI button / Background location updates	4
4. Lock Record	6

RELEASED UNDER THE
OFFICIAL INFORMATION ACT

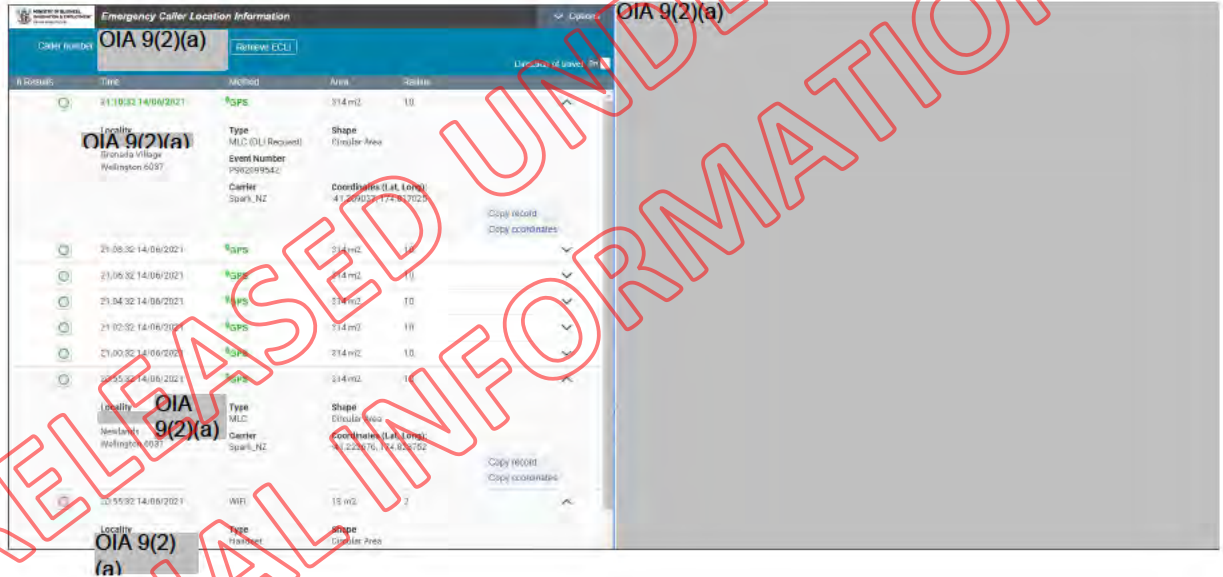
1. Direction of travel

The vLAC Web User Interface (UI) allows you to see the direction a person is travelling if they are on the move and where there are multiple location results in different locations.

The Direction of travel feature can be toggled on or off.

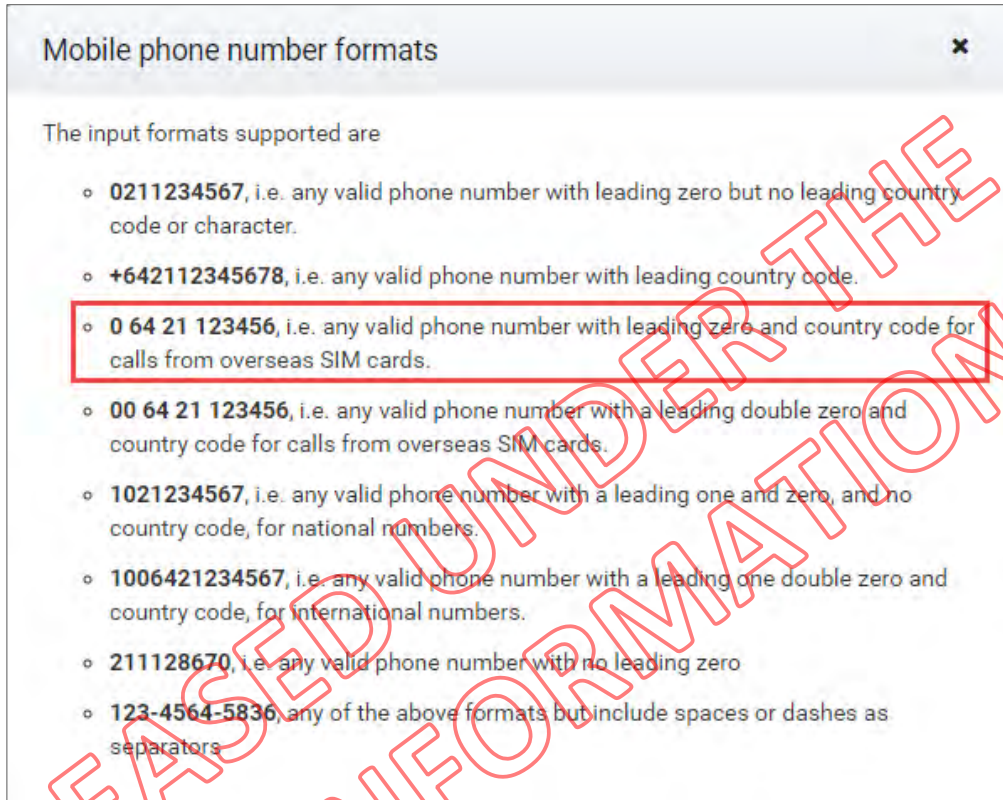


Select multiple locations to show direction of travel. You will see the red arrows to indicate the direction.



2. Phone number format

Phone numbers can be entered into the vLAC Web UI in the format below with the latest format being 0 64 nnnnnnnnnn – i.e., a leading zero followed by a country code and then a local number.



3. Retrieve ECLI button / Background location updates

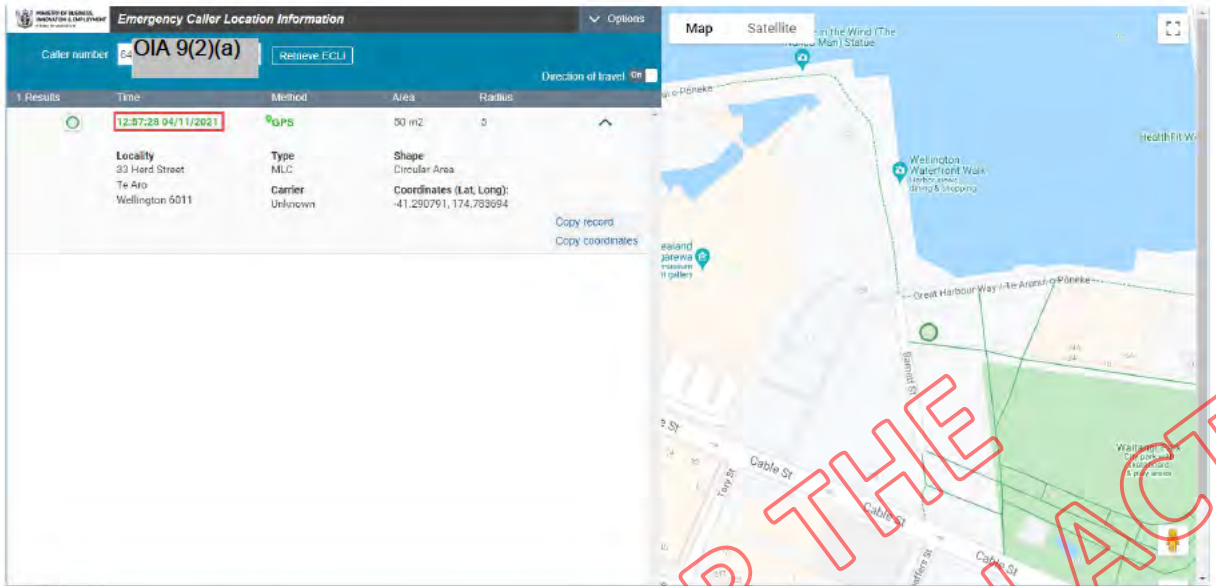
MLC locations (green shapes) no longer continuously update in the background. Instead, when you initially retrieve ECLI, the application will request one further MLC location update.

Note: AML locations (red shapes) still continuously update during an emergency call.

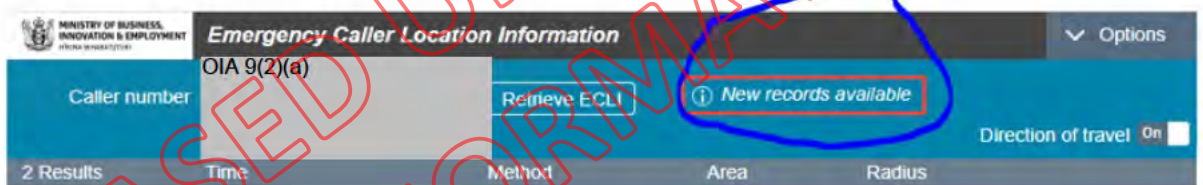
If you are taking an emergency call where the caller is moving and the vLAC Web UI is only showing you MLC locations (green shapes) and you want to make sure you have the latest location details, press **'Retrieve ECLI'** and then as soon as you see the banner **'New records available'** press **'Retrieve ECLI'** again.

Here is an example:

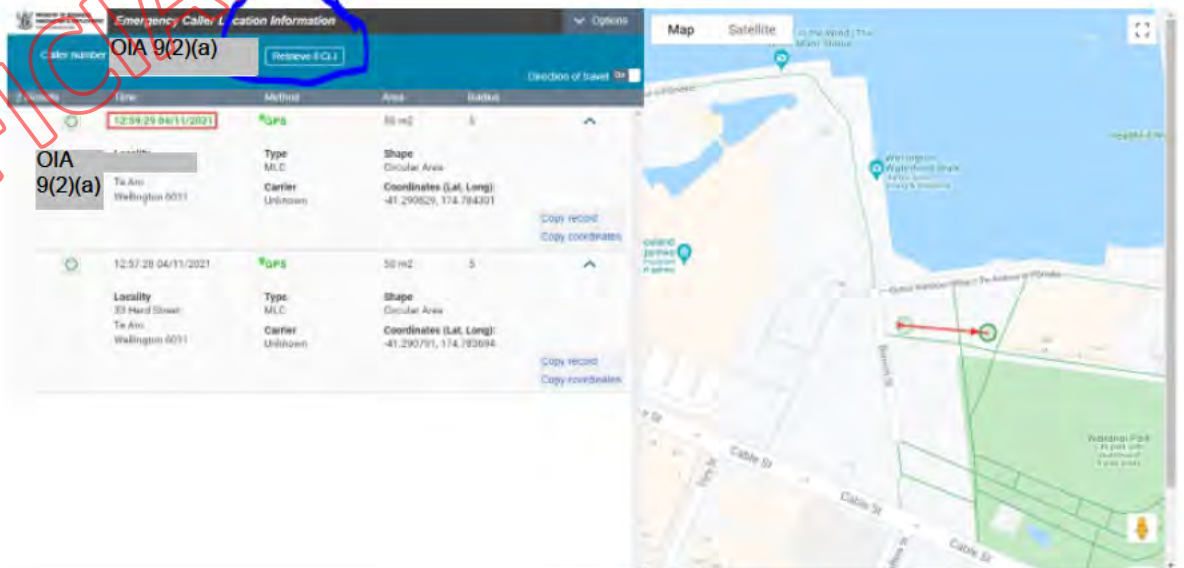
- 1) A user presses **'Retrieve ECLI'**. The vLAC Web UI displays the original location details and requests a single location update from the application.



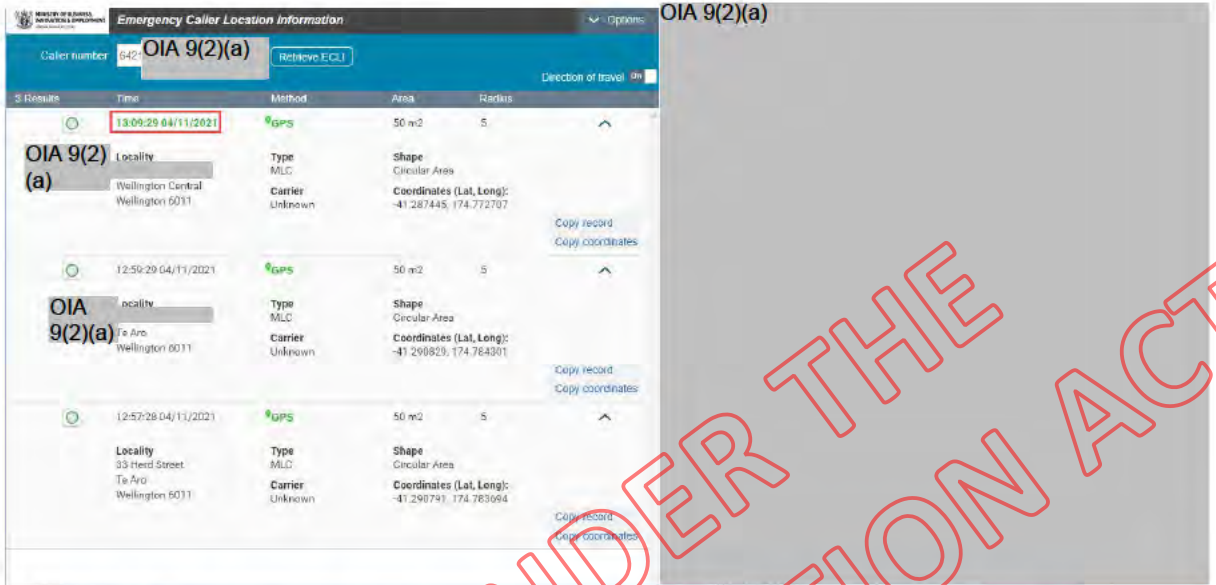
- 2) The vLAC Web UI notifies the user that an updated location is available with the message 'New records available'.



- 3) The user presses 'Retrieve ECLI'. The vLAC Web UI retrieves previous updated location details and requests a new location update. Note that the updated location shown on the screen is close in time to the original location (2 minutes later).



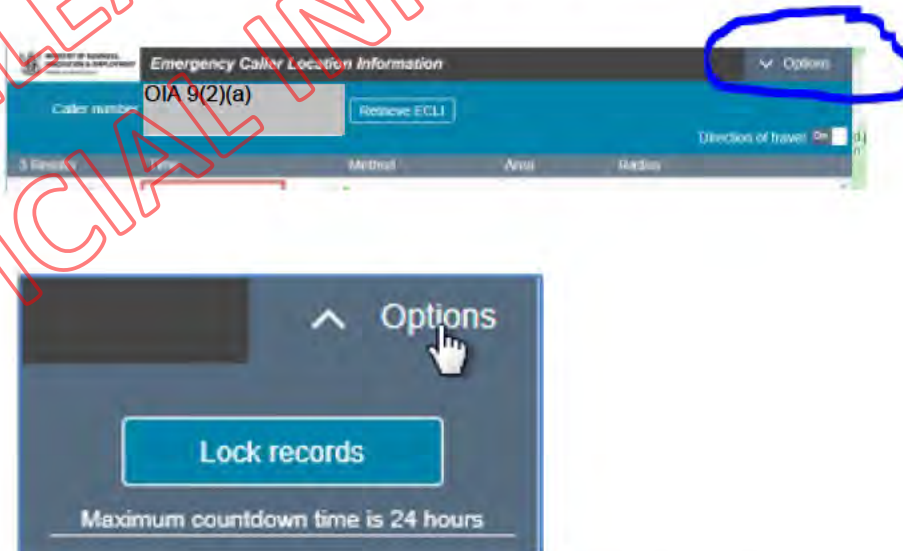
- 4) The user presses 'Retrieve ECLI' again. Now the most up to date location is displayed (10 mins from the original location)



Please note: The maximum number of location records that will be displayed on the vLAC Web UI screen is 20 records.

4. Lock Record

Under 'Options' you can select the button to 'Lock records'



This will lock the records for this mobile phone number for 24 hours, rather than the records being purged in six hours (360 minutes) for privacy reasons. This feature may be useful if the event is on-going.



IN-CONFIDENCE: RELEASE EXTERNAL

Emergency Caller Location Information (ECLI)

Post-Call Instructions Training Notes – May 2022

Issued by:

Marcus Sullivan, ECLI Senior Business Analyst

Issue date:

30/05/2022

Document purpose

This purpose of this document is to provide training notes on the key features of the new **Post-Call Instructions** (PCI) functionality, used within the virtual Location Aggregation Centre (vLAC) **Web UI** application on the ECLI Location Platform.

Training components

1. Post-Call Instructions (PCI) Overview.....	3
2. PCI Option 1: Event Number	5
3. PCI Option 2: Report a Bad Driver.....	6
4. PCI Option 3: Online 105 Reports	7
5. Include Additional Closure Information (Optional).....	8
6. Send Post-Call Instructions SMS Message	9

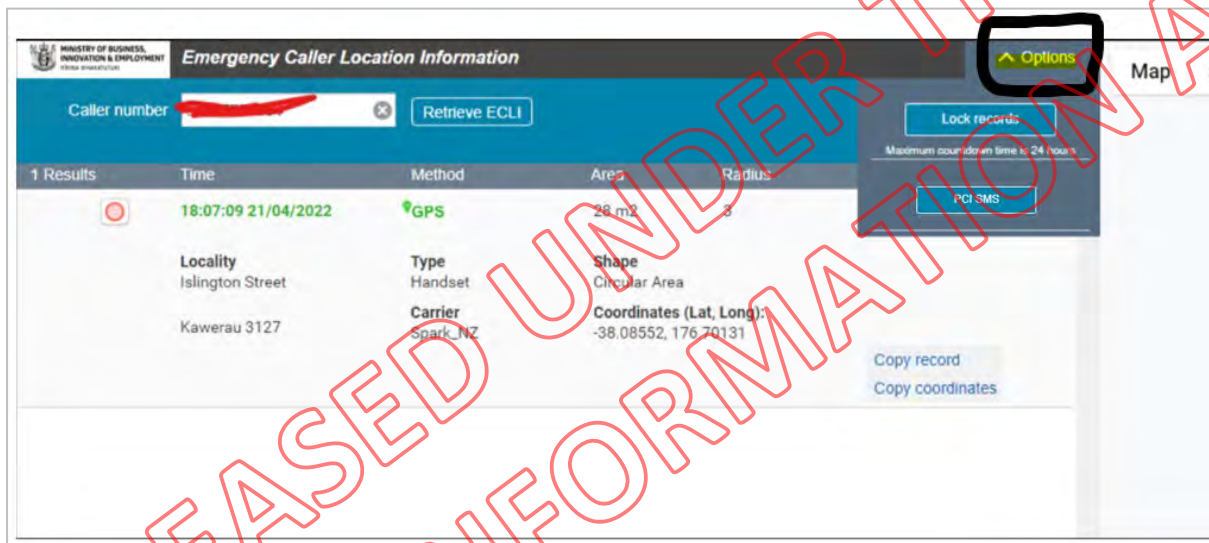
RELEASED UNDER THE
OFFICIAL INFORMATION ACT

1. Post-Call Instructions (PCI) Overview

The PCI feature enables a Police call taker to provide further instructions to an emergency caller through sending a text (SMS) message, after an emergency call has completed. The PCI feature displays selectable options to enable the pre-population of the SMS message.

A NZ Police call taker can open the PCI feature through an option contained on-screen in the vLAC Web UI.

1. The PCI feature is only available if we have retrieved a caller location record through an **ECLI source** i.e., through an **emergency call**.
2. Access to the PCI feature is through the main vLAC Web UI.
3. Select the **Options** field over to the top-right.



4. From the **Options** menu, an option to access the PCI SMS feature is available.



5. Once this PCI SMS button is selected, the PCI feature is opened, and the following information is displayed on-screen as the default state:
 - **Event Number** (PCI option 1, the defaulted selection)
 - **Report a bad driver** (PCI option 2, available for selection)
 - Registration number field is not active (i.e. greyed out)
 - **Online 105 reports** (PCI option 3, available for selection)
 - The NZ Police message text for PCI option 1 (Event Number) is displayed by default i.e. *"From New Zealand Police. DO NOT REPLY TO THIS MESSAGE The event number for your call today is [event number]"*
 - Additional closure information field is not selected by default
 - The mandatory Event Number input field is blank
 - 'Clear all' button is active. This will return the page to its default state i.e., PCI option 1 – 'Event number'
 - 'Copy and send' button is active. On selection, all user input is validated and if successful, the SMS message is sent, and the message text is copied to the Clipboard.
6. Only one PCI feature screen can be opened at a time per emergency call.

Default PCI screen:

The screenshot displays the 'Post-call instructions' screen. On the left, there are three radio button options: 'Event Number' (selected), 'Report a bad driver', and 'Online 105 reports'. Below these is a greyed-out 'Registration Number' field and an 'Additional Closure Information' section with a checked checkbox for 'If the situation changes, call us back on 111'. At the bottom left is an 'Event Number' input field. On the right, a message preview shows: 'From New Zealand Police: DO NOT REPLY TO THIS MESSAGE The event number for your call today is'. At the bottom, there are 'Clear all' and 'Copy and Send' buttons.

2. PCI Option 1: Event Number

1. The 'Event number' PCI option is the **default** selected option each time you open the PCI user interface.
2. You can choose to select one of the other available options but only one PCI option can be selected at the same time.
3. On selection of the 'Provide an event number' option, a specific, non-editable NZ Police message is displayed on-screen. This message template will form the text of the SMS message.
4. The 'Event Number' field is active and is available for manual input (alpha/numeric, no special characters - character limit = **12**).
5. The 'Event Number' field is indicated as **mandatory** for the 'Provide an event number' PCI option.
6. Once the Event Number field contains a reference, the message area will now display the entered event number. "The event number for your call today is [Event Number]"

NB: The event number will be generated from the Police side (through CAD) and then you will manually enter this into the PCI screen. (Currently, the event number format is a letter, followed by nine numbers.)

The screenshot shows a 'Post-call instructions' window with a close button (X) in the top right. On the left, there are three radio button options: 'Event Number' (selected), 'Report a bad driver', and 'Online 105 reports'. Below these is a 'Registration Number' field and an 'Additional Closure Information' section with a checked checkbox for 'If the situation changes, call us back on 111'. At the bottom left is an 'Event Number' input field. On the right, the message content reads: 'From New Zealand Police: DO NOT REPLY TO THIS MESSAGE' followed by 'The event number for your call today is'.

This screenshot is identical to the one above, but the 'Event Number' field now contains the value '12'. Correspondingly, the message content on the right has updated to: 'From New Zealand Police: DO NOT REPLY TO THIS MESSAGE' followed by 'The event number for your call today is 12'.

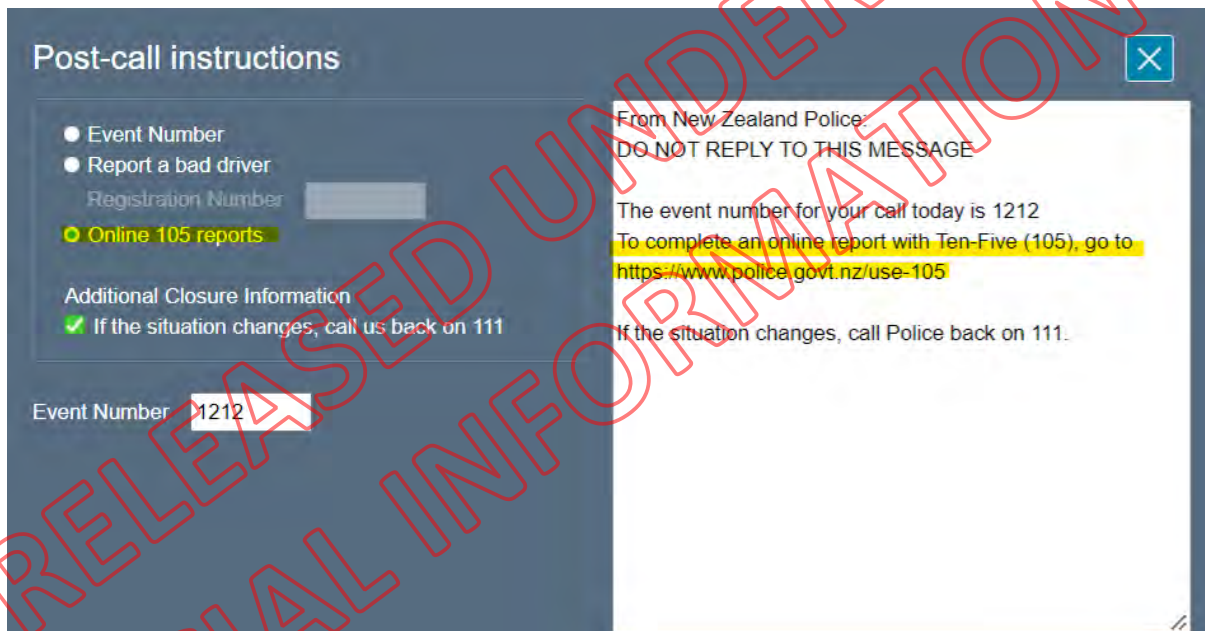
3. PCI Option 2: Report a Bad Driver

1. The 'Report a bad driver' PCI option can be selected in the PCI user interface. Only one PCI option can be selected at the same time.
2. Upon selection of this option, the associated 'Registration number' field is activated and is available for manual input (alpha/numeric, no special characters - character limit = 9).
3. The 'Registration number' field is indicated as **mandatory**.
4. On selection of the 'Report a bad driver' option, a specific, non-editable NZ Police message is displayed on-screen. This message template will form the text of the SMS message.
5. The 'Event Number' field is active and is available for manual input (alpha/numeric, no special characters - character limit = 12).
6. The 'Event Number' field is indicated as **mandatory** for the 'Report a bad driver' option.
7. Once the Event Number field contains a reference, the message area will now display the entered event number. e.g. "The event number for your call is [Event Number]"
8. This message area will contain the recently entered (vehicle) Registration number.
9. This message area will also contain a link to the online Roadwatch report (online form).
<https://forms.police.govt.nz/forms/community-roadwatch-report-unsafe-driving-incident>

The screenshot shows a 'Post-call instructions' window with a close button (X) in the top right corner. On the left, there are three radio button options: 'Event Number', 'Report a bad driver' (which is selected and highlighted in green), and 'Online 105 reports'. Below these, there is a text input field for 'Registration Number' containing 'CAR'. Under 'Additional Closure Information', there is a checked checkbox for 'If the situation changes, call us back on 111'. At the bottom left, there is an 'Event Number' input field containing '1234'. On the right, a preview of an SMS message is shown, starting with 'From New Zealand Police' and 'DO NOT REPLY TO THIS MESSAGE'. The message body contains: 'Thank you for calling to report an unsafe Driving Incident. The event number for your call today is 1234 and the registration number was CAR. If you would like to complete an online Community Roadwatch report, go to https://forms.police.govt.nz/forms/community-roadwatch-report-unsafe-driving-incident. To make a formal complaint visit your nearest Police Station. If the situation changes, call Police back on 111.'

4. PCI Option 3: Online 105 Reports

1. The 'Online 105 reports' PCI option can be selected in the PCI user interface. Only one PCI option can be selected at the same time.
2. On selection of the 'Online 105 reports' option, a specific, non-editable NZ Police message is displayed on-screen. This message template will form the text of the SMS message.
3. The 'Event Number' field is active and is available for manual input (alpha/numeric, no special characters - character limit = **12**).
4. The 'Event Number' field is indicated as **mandatory** for the 'Online 105 reports' option.
5. This message will also contain a link to the online Ten Five (105) report (online form).
<https://www.police.govt.nz/use-105>
6. Once the Event Number field contains a reference, the message area will now display the entered event number in a new paragraph beneath the 105 link. e.g. "The event number for your call is [Event Number]"



5. Include Additional Closure Information (Optional)

1. An 'Additional closure information' field/sub-option can be selected from the PCI screen.
2. This additional closure information field is **always optional**.
3. This additional closure information field can be selected in conjunction with any of the main options (PCI options 1, 2, 3).
4. If this field is selected, the NZ Police message template is automatically populated with additional text "If the situation changes, call Police back on 111" This text is displayed in a new paragraph, below the main text.
5. If this 'Additional closure information' field is subsequently unchecked prior to message submission (selecting 'Copy and Send'), then the additional text is automatically removed from the displayed NZ Police message.

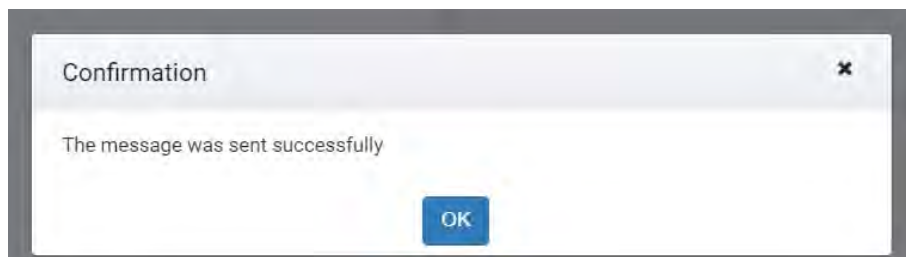
The screenshot displays the 'Post-call instructions' interface. On the left, there are three radio button options: 'Event Number', 'Report a bad driver', and 'Online 105 reports'. Below these is the 'Additional Closure Information' section, which has a checked radio button for 'If the situation changes, call us back on 111'. At the bottom left, the 'Event Number' is set to '1234'. On the right, a preview window shows the resulting message: 'From New Zealand Police: DO NOT REPLY TO THIS MESSAGE. The event number for your call today is 1234. If the situation changes, call Police back on 111.' The text 'If the situation changes, call Police back on 111' is highlighted in yellow in the preview.

6. Send Post-Call Instructions SMS Message

1. Once a PCI option is selected (one of the three available on-screen), and the 'Copy and Send' button is selected, the user input field validation is performed as follows:
 - For PCI option 1, option 2, option 3 - The mandatory Event Number field is validated for entry. If the field is blank a message is displayed on-screen "Please provide an Event Number"
 - For PCI option 2 only - The mandatory Registration number field is validated for entry. If the field is blank a message is displayed on-screen "Please provide a Registration Number"
 - It is possible for both these messages to be displayed at once.

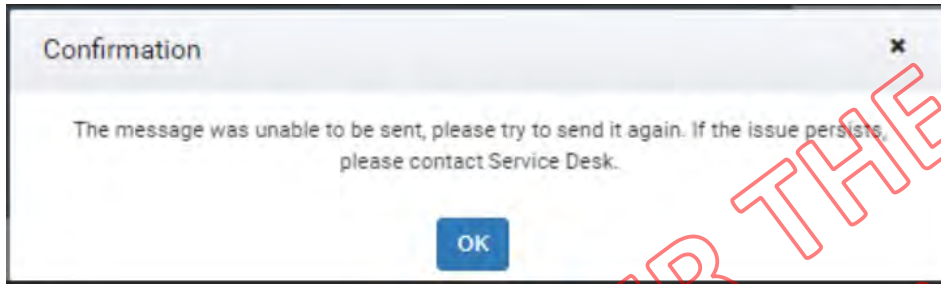
The screenshot shows a 'Post-call instructions' dialog box. On the left, there are three radio button options: 'Event Number' (selected), 'Report a bad driver', and 'Online 105 reports'. Below these is a checkbox for 'Additional Closure Information' with the text 'If the situation changes, call us back on 111'. There are two input fields: 'Event Number' and 'Registration Number', both of which are empty and have red borders indicating validation errors. At the bottom left is a 'Clear all' button and at the bottom right is a 'Copy and Send' button. On the right side of the dialog, there is a preview of an SMS message from New Zealand Police. The message text is: 'From New Zealand Police: DO NOT REPLY TO THIS MESSAGE. Thank you for calling to report an unsafe Driving Incident. The event number for your call today is [redacted] and the registration number was [redacted]. If you would like to complete an online Community Roadwatch report, go to https://forms.police.govt.nz/forms/community-roadwatch-report-unsafe-driving-incident. To make a formal complaint visit your nearest Police Station.' Below the message preview, there are two red error messages: 'Please provide a Registration Number' and 'Please provide an Event number'.

2. Once you have selected the 'Copy and Send' button and field validation is successfully completed, the text message is sent to the emergency caller's cell phone number.
3. A confirmation message is displayed (via an on-screen pop-up) in the PCI user interface to inform you of a successfully sent SMS message. "The message was sent successfully"



4. The SMS message text is then copied to your **Clipboard**.

5. Once the successfully sent confirmation is returned and displayed on-screen, you can close the pop-up message, the PCI screen then closes automatically, and you are returned to your already open Web UI home screen i.e., where you initiated the opening of the PCI feature.
6. In the unlikely occurrence that this SMS message cannot be sent, you will be informed via the following on-screen message, and prompted to retry. "The message was unable to be sent, please try to send it again. If the issue persists, please contact Service Desk."



7. You can close this failure to send message and then click the 'Copy and Send' button again to resend the message.
8. In case of a continued error when trying to send the message, it will be helpful to provide the **Service Desk** with the following information:
 - A screen capture of the PCI screen with your selected message option.
 - A record of the date and time the errors occurred.

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Privacy Policy

Version 5.0 November 2023

RELEASED UNDER THE
OFFICIAL INFORMATION ACT

1. MBIE guiding principles relevant to this policy

1.1 The following MBIE guiding principles are relevant to the Privacy Policy:

- a. ensuring our core values and diverse and inclusive culture, including partnering with Māori, are at the heart of what we do.
- b. protecting organisational reputation
- c. ensuring a healthy, safe and secure environment
- d. being a good employer
- e. complying with legislation, regulations and standards.

2. Purpose

2.1 The purpose of the Privacy Policy is to:

- a. describe MBIE's expectations relating to how our people can collect, store, use and share personal information about any person
- b. enable our people to exercise their informed judgement about privacy and manage privacy risks
- c. enable the Chief Privacy Officer to have oversight of MBIE's privacy function and of MBIE's privacy risk.

3. Scope

3.1 This Policy applies to all:

- a. staff, secondees and contractors, employed or engaged on any basis by MBIE (our people), whether they are casual, fixed term or permanent, whether full time or part time and whether they are in New Zealand or in any other country, who have access to any personal information MBIE holds
- b. personal information that MBIE collects, uses, accesses, shares, stores and disposes of.

4. Help

4.1 For any queries related to this policy, please contact the Privacy Team at privacyteam@mbie.govt.nz.

5. Definition of terms

Term	Definition
Notifiable event	A privacy breach that has caused or is likely to cause serious harm which is legally required to be notified to the Office of the Privacy Commissioner.

Title: Privacy Policy

Date of Issue: August 2015

Dep Sec Sponsor: Dep Sec Corporate Services,
Finance and Enablement

Version: 5.0
Policy Classification: Governance

Last Review: November 2023
Next Review: November 2026

Policy Owner: Chief Privacy Officer
Security Classification: Unclassified

Personal information	Any information about an identifiable individual.
Privacy Act request	Request made by individuals under the Privacy Act to: <ul style="list-style-type: none"> • obtain confirmation of whether MBIE holds personal information about them and/or • request access to that personal information and/or • request correction of their personal information.
Privacy event	Events where our people (including third-party service providers) fail to manage personal information in accordance with the law (e.g., Privacy Act) or MBIE's Privacy Policy, processes and standards. It includes: <ul style="list-style-type: none"> • privacy breaches (where personal information is wrongly collected, used, accessed, disclosed, retained, or withheld as set out by the Privacy Act) and • potential privacy breaches ('near misses') (where an action could have resulted in a breach, but the breach does not occur).
Privacy event form	Form our people must complete in MBIE's enterprise event reporting tool whenever MBIE identifies it has failed to manage personal information in accordance with the Privacy Act or MBIE's Privacy Policy, processes, and standards.
Privacy Impact Assessment (PIA)	A Privacy Impact Assessment is a process for assessing how a new or change to an existing process or system will affect people's privacy, both positively and negatively. The process helps to identify risks, controls, and design improvements.
Privacy Threshold Assessment (PTA)	A Privacy Threshold Assessment provides an initial indication of privacy risk.

6. Policy statements

- 6.1 Our people must complete mandatory privacy training during their induction period. MBIE will provide the required mandatory training.
- 6.2 MBIE will collect personal information only when there is a lawful and clear purpose to do so. Where appropriate we will use explicit and informed consent.
- 6.3 MBIE will be open and transparent about how we collect, use, access, share, store and dispose of the personal information in our care, including information that belongs to our people.
- 6.4 Our people will apply the Government Chief Privacy Officer's Data Protection and Use Policy principles where appropriate. This includes, but not limited to, when working with vulnerable communities, children and young persons, and working with Te Tiriti partners where collection and use of personal information may impact Māori.

Title: Privacy Policy
Version: 5.0
Policy Classification: Governance

Date of Issue: August 2015
Last Review: November 2023
Next Review: November 2026

Dep Sec Sponsor: Dep Sec Corporate Services, Finance and Enablement
Policy Owner: Chief Privacy Officer
Security Classification: Unclassified

- 6.5 Our people must follow the MBIE Privacy Impact Assessment Framework. This includes completing Privacy Threshold Assessments for all new projects or initiatives that may impact the way MBIE manages personal information, and Privacy Impact Assessments where recommended.
- 6.6 Our people must report privacy events (breaches and near misses) as soon as practicable via the privacy event form in MBIE's enterprise event reporting tool. If the tool is unavailable, then the privacy event must be reported via email or phone call to MBIE's Privacy Team.
- 6.7 Managers must ensure that any Privacy Act request is responded to in accordance with the Privacy Act.
- 6.8 MBIE will respond to privacy complaints and external compliance investigations within MBIE's service promise and statutory timeframes (where applicable). Statutory timeframes are set by the Office of the Privacy Commissioner and are subject to change.
- 6.9 MBIE will retain personal information only for the period that information is required to fulfil the purpose of the collection and Public Records Act 2005 obligations.

7. Key Accountabilities and Responsibilities

Role	Responsibility
Governance and Oversight	
Secretary for Business, Innovation & Employment and Chief Executive (The Secretary)	<ul style="list-style-type: none"> • Approves major amendments to this Policy • Ensures MBIE meets its obligations under this Policy
Assurance, Risk and Accountability Committee (ARA)	<ul style="list-style-type: none"> • Maintains overall oversight of the status of this policy, including key privacy control and risk areas across MBIE • Endorses new and major amendments to this policy prior to The Secretary approval • As required, the ARA chair will raise concerns about privacy compliance to the Senior Leadership Team (SLT) and to the People, Culture and Capability committee (PCC)
Business Groups: Identify and manage risks in day-to-day operations (1st line)	
Deputy Secretaries (Dep Secs)	<ul style="list-style-type: none"> • Embed this Policy and associated Procedures in their groups • Ensure privacy risks are appropriately assessed and captured in the business group and branch risk registers • Ensure their business groups are compliant with this Policy and have appropriate monitoring and reporting in place, including raising issues and reporting events • Alert the Policy Owner to new areas of functions in their business group that collect and use personal information
General Managers (Tier 3)	<ul style="list-style-type: none"> • Responsible for embedding this Policy into operational activities within their branch • Ensure new and existing employees are made aware of and comply with this Policy

Role	Responsibility
	<ul style="list-style-type: none"> Provide assurance to their Dep Sec that their branch is compliant with this policy and that any matters of non-compliance have been dealt with appropriately
Managers	<ul style="list-style-type: none"> Collect and use personal information, including about kaimahi, legitimately and safely to deliver MBIE's services efficiently and effectively Ensure Privacy Threshold Assessments, and Privacy Impact Assessments where recommended, are completed when creating new or changing existing systems and processes Ensure our people are appropriately trained on how to manage personal information, including raising issues and reporting events Ensure all legal requirements and MBIE-wide policies are complied with when personal information is used and shared within MBIE or other organisations Ensure privacy complaints and compliance investigations are responded to within statutory timeframes
Our People	<ul style="list-style-type: none"> Comply with this policy Complete mandatory Privacy training Manage personal information in accordance with this policy and associated, processes and systems, and practices Respond to individuals' requests for access to, withdrawal of consent, and correction of personal information Identify privacy issues and events and report these
Specialist Functions: Set MBIE-wide expectations, policies and procedures (2nd Line)	
Chief Privacy Officer (Policy Owner)	<ul style="list-style-type: none"> Holds the statutory function of <i>Privacy Officer</i> as defined by the Privacy Act 2020 (s201) The function includes ensuring the Ministry complies with the provisions of the Privacy Act Ensures appropriate and thorough incident management in the event of a significant privacy breach Discretion to lead or commission further investigation of event root cause where there are indicators of potential for harm Ensures the Policy is working effectively Responsible for MBIE's relationships with the Government Chief Privacy Officer and the Privacy Commissioner
Legal Team	<ul style="list-style-type: none"> Provides privacy legal advice, including on information sharing, events, complaints, and on requests for personal information, including grounds for withholding information
Privacy Advisory Group	<ul style="list-style-type: none"> Provides functional leadership for strategic privacy matters Convenes as required for strategic privacy matters

Title: Privacy Policy

Date of Issue: August 2015

Dep Sec Sponsor:

Dep Sec Corporate Services,

Version: 5.0

Last Review: November 2023

Policy Owner:

Finance and Enablement

Policy Classification: Governance

Next Review: November 2026

Security Classification:

Chief Privacy Officer

Unclassified

Role	Responsibility
	<ul style="list-style-type: none"> • Drives the creation of a culture that sets the tone for respect for privacy
Privacy Team	<ul style="list-style-type: none"> • Leads the development, promotion, and embedding of MBIE's privacy capability and culture, including training, education, and awareness • Provides support, advice, guidance, training on privacy considerations, legislative requirements, and best practice across MBIE • Reviews Privacy Threshold and Impact Assessments including providing advice and recommendations around identifying and managing privacy risks • Supports the management of privacy events, complaints and requests with advice and recommendations, and notifying the Office of the Privacy Commissioner of breaches where serious harm has been or could be caused • Provides an organisational view of privacy at MBIE, including trend reporting and insights around reported privacy events, complaints, and completed Privacy Threshold and Impact Assessments, and privacy training completion rates
Business Change Owners	<ul style="list-style-type: none"> • Ensure Privacy Impact Assessment Framework is applied to their projects, including ensuring completion of Privacy Threshold Assessments and resourcing of Privacy Impact Assessments where recommended • Approve and sign off Privacy Threshold Assessments (and Privacy Impact Assessments, if required), apply any practicable Privacy Team recommendations and accept and sign off any privacy risk associated with the projects under their responsibility

8. Procedures

- a. [Requests for accessing and correcting information under the Privacy Act](#)
- b. [Complaints under the Privacy Act 2020](#)
- c. [Privacy Events](#)
- d. [Privacy Impact Assessments](#)

9. Related MBIE policies and documents

- a. [Code of Conduct](#)
- b. [Compliance Policy](#)
- c. [Protective Security Policy](#)
- d. [Records Management Policy](#)
- e. [ICT Acceptable Use Policy](#)
- f. [Risk Management Policy](#)
- g. [Official Information Act Requests Policy](#)

Title:	Privacy Policy	Date of Issue:	August 2015	Dep Sec Sponsor:	Dep Sec Corporate Services, Finance and Enablement
Version:	5.0	Last Review:	November 2023	Policy Owner:	Chief Privacy Officer
Policy Classification:	Governance	Next Review:	November 2026	Security Classification:	Unclassified

- h. [Social Media Policy](#)
- i. [Data merging framework](#)
- j. [Data sharing guidance](#)
- k. [Information Gathering Policy](#)
- l. [Legal Services Policy](#)
- m. [Te Ki Taurangi – Our promise](#)
- n. [Enterprise Data Governance Policy](#)
- o. [Child Protection Policy](#)

10. Relevant legislation, regulations and standards

- a. [Privacy Act 2020](#)
- b. [Privacy Codes of Practice](#)
- c. [Official Information Act 1982](#)
- d. [Public Records Act 2005](#)
- e. Any other legislation with privacy provisions (e.g., Immigration Act 2009)
- f. [Data Protection and Use Policy](#)
- g. [Algorithm Charter](#)

11. Measures of success and compliance management

11.1 The Chief Privacy Officer will assess the effectiveness of this policy based on the following measures of success:

- a. staff are aware of MBIE expectations relating to the collection, storage, use and sharing of personal information as measured by timely and quality completion and submission of Privacy Act requests, Privacy Threshold Assessments, and responses to internal staff surveys
- b. an increase in privacy maturity or maintenance of 'Managed' privacy maturity, as rated by the annual Privacy Maturity Assessment Framework self-assessment and reported to the Government Chief Privacy Officer
- c. an increase in perceptions of MBIE's trustworthiness in managing personal information, as measured by the annual MBIE Privacy Survey, through customer and stakeholder engagement, and measures such as complaints
- d. a reduction in harm caused through privacy events, as measured by a decrease in upheld privacy complaints made to MBIE or the Office of the Privacy Commissioner.

11.2 The Chief Privacy Officer will monitor compliance with this policy as follows:

- a. a completion rate of 95% mandatory privacy training within MBIE's induction period (three months)
- b. completion rate of 100% of Privacy Threshold Assessments for all new initiatives and changes that impact MBIE's management of personal information
- c. completion rate of 100% of Privacy Impact Assessments or documented acceptance of risk from business change owners for all changes where a Privacy Impact Assessment has been recommended

Title:	Privacy Policy	Date of Issue:	August 2015	Dep Sec Sponsor:	Dep Sec Corporate Services, Finance and Enablement
Version:	5.0	Last Review:	November 2023	Policy Owner:	Chief Privacy Officer
Policy Classification:	Governance	Next Review:	November 2026	Security Classification:	Unclassified

- d. event reporting and analysis of all privacy events reported to the Privacy Team to assess the effectiveness of the Policy.
- 11.3 Compliance information regarding the performance of this policy will be provided to the relevant business group and the Enterprise Risk and Compliance branch on a quarterly basis.

12. Non-compliance

- 12.1 Failure to comply with this policy may be considered a breach of the [Code of Conduct](#).
- 12.2 Any action taken as a result of a breach of any of the obligations set out in this policy will be conducted in good faith, a fair process will be followed and the person involved will have a full opportunity to respond to the concerns or allegations.

RELEASED UNDER THE
OFFICIAL INFORMATION ACT

Title: Privacy Policy
Version: 5.0
Policy Classification: Governance

Date of Issue: August 2015
Last Review: November 2023
Next Review: November 2026

Dep Sec Sponsor: Dep Sec Corporate Services,
Finance and Enablement
Policy Owner: Chief Privacy Officer
Security Classification: Unclassified

Impact Analysis template

Introduction

This Impact Analysis template is a key part of MBIE's Privacy Impact Assessment Framework. The Framework provides guidance, examples and tools to support you assess and manage the impacts of a proposed action on individuals' privacy. It is structured to help you build your ideas and implement changes in such a way so as to achieve your objectives while ensuring individuals' personal information is protected. This will help to build and retain the trust of the individuals who provide us with their information, so we can legitimately and safely use personal information in order to *Grow New Zealand for All*.

The Impact Analysis is the second key tool of the Framework:

1. Privacy Threshold Assessment (PTA)
2. **Impact Analysis**
3. PIA Report.

Note: While the Framework won't fix any risks, it will help you identify them early, and to do your best to mitigate or remove them in a considered and proactive way.

Template guidance

When do I need to complete this template?

Use this template when a PTA determines that your initiative has a medium or high degree of privacy risk, to:

- * record how the personal information involved flows within and outside of MBIE; and
- * assess any potential privacy impacts against the 12 Principles of the Privacy Act.

Note: The template is designed to allow you to add and/or edit information as it becomes available or decisions are made.

How long will it take?

This will depend on your initiative and what you are trying to achieve. As a rough guide, initially allow at least 2-4 hours for a medium-risk initiative, and 8-12 hours for a high risk one. This should give sufficient time to examine your initiative from a privacy perspective.

Who needs to be involved?

- * **A PIA guru:** A person trained in how to complete this exercise. They can provide guidance and examples to make your job easier.
- * **Any initiative stakeholders.** This could include: Business subject matter experts, project managers, ICT, Security, Risk and Assurance, Audit, Information and Data, Records Management, Facilities, Procurement, Human Resources, Finance and Legal staff. Additionally, external resources (such as vendors) should also be involved. Organise workshops, meetings and review sessions as required to ensure that risks are appropriately identified and managed.

Further information

For more detailed guidance, see the *Conduct privacy impact assessment* process on the Link.

DATA FLOW TEMPLATE

If you are collecting personal information a Privacy Threshold Assessment (PTA) should have already been completed, as outlined in the *Conduct privacy impact assessment* process. If the PTA indicated a medium or high level of risk to individuals' privacy, complete the Data Flow template on this sheet by following these steps:



- Talk to a PIA guru, who can help you understand how to complete this template and who you can obtain the required information.
- Collect any documentation like data flow diagrams, use cases or architecture diagrams which explain how personal information currently flows, and how it is planned to flow.
- Obtain a list of all known data items that will be collected – including personal and non-personal data.
- Complete the white areas of the template. Guidance notes are provided to the right of each question in orange.
- 'Don't know' is a sufficient answer if details are not yet determined. This template is designed to be revisited as more details arise, or when there are changes or decisions that impact how the content is collected.
- You may want to consult with your architect, business analyst or project manager, or the Information and Data, Compliance, Risk and Intelligence, IT Security, Information Security, Records Management, Audit, Finance or Legal teams to answer some questions.
- Business owner sign off is required.

Once the Data Flow template is complete you will have enough information to complete the Privacy Impact Analysis. The success of the Impact Analysis will be determined by the quality of the details you collect in the Data Flow template.

INITIATIVE DETAILS AND SIGN OFF

Initiative name:	Mobile Caller Location
Brief description of initiative:	The MCL project will address longstanding operational requirements of Emergency Service Providers for probable caller location information from mobile phones. The outcome sought is for the best available caller location to be sent to an emergency service provider when a 111 call is made, without requiring the caller to do anything more than dial 111 on the standard keypad of their mobile phone.
Name and role of person completing template:	Ben Quay, MCL Project Director
Template completion date:	31-Aug-16
Business owner name, role, and sign-off:	Brad Ward

PRINCIPLE 1 - Purpose of Collection of Personal Information

Only collect personal information if you have a justifiable purpose for it

	Category 1	Category 2	Category 3	Category 4	Category 5
What categories of personal information will be collected?	Biometric, physical & behavioural	Biometric, physical & behavioural	Unique identifiers	Other	
List the data items that will be collected in each category	Probable mobile caller location information, includes geolocation coordinates, confidence and accuracy	Network cell tower location information (geolocation coordinates) relating to the cell tower that a mobile caller is connected to	Mobile telephone number (CLI), and mobile device IDs	Call metadata: time stamps of calls, network ids, location source, carrier ids	
Which data items require special care?	All	All	All	All	
Which data items have not been collected previously?	All	All	Mobile device Id. CLI is provided today	All	
Describe the main reason (primary purpose) for collecting the data	Best available caller location to be sent to an emergency service provider when a 111 call is made, in order to assist in address verification of emergency events				
Describe any secondary or future purposes for collecting this data	None				

GUIDANCE NOTES

Add additional columns if you have more data items/categories.

Select the categories of information being collected (as entered on your Privacy Threshold Assessment).

Document all information being collected, not only the data you consider to be personal data. Add additional columns if necessary.

You need to include all information because:

- Some data may not be considered personal until it is combined with other information;
- It may be possible to derive additional information about someone if non-personal information is included;
- You can identify any duplicate information being collected;
- You can identify any information that doesn't need to be collected to meet your objective.

A data item is defined as a piece of information that can be attributed to an individual. You may be collecting many data items within each category. Examples of data fields (by category) are:

- Employee/HR - Salary, grade, employee ID, part time, full time, contract, diversity, financial, benefits, appraisal, disciplinary, leave (parental, sick, holiday, study, sabbatical, other), tax, pension, education details, previous employment details;
- Contact - name (full or part), contact details - home address, home phone, personal mobile, personal email;
- Biographic - date of birth, age, sex, gender, ethnic origin, race, nationality;
- Biometric, physical, behavioural - photo, biometrics (finger, facial, iris), distinguishing facial / body features, location information (surveillance, monitoring or tracking), disabilities, searching individuals' property, persons or premises, CCTV or video/visual recordings, audio and telephony recordings;
- Housing - home address, type of housing (owned, rented, state), identification of occupants, special needs, building design and construction, energy resources and environment;
- Unique identifiers - IRD number, passport number, drivers license number, ACC number, Housing number, Medical number, online identity number, other unique identifiers;
- Children - name, date of birth, sex, gender, age, address, school or educational institution, parents / guardians, physical data;
- Health - mental or physical state (including disabilities), ACC benefits or other government medical benefits, Medical records, health and safety;
- Education - education records past and present, qualifications, special needs, study entitlements, visa status and conditions;
- Immigration - immigration status, refugee status, visa status and conditions, tourism;
- Consumer - credit or loan details, hire purchase, consumer preferences, trading or business details;
- Financial - bank account numbers, credit card numbers, credit / loan details, salary, pension, government benefits;
- Labour and employment - employer and employment records, government benefits, salary, pension, tax, benefits, work visas and conditions, employment law and relations;
- Political - political opinions, affiliations and membership;
- Religious - religions, religious beliefs, or beliefs of a similar nature ;
- Trade Union - trade union membership information;
- Sexual - Information about individuals sexual life;
- Criminal - actual or alleged criminal offences, proceedings or convictions;
- Anonymous - non-identifiable information about individuals that may or may not be traced back to an individual, including aggregated information, statistical, profiling information;
- Other - other information that may be traced back to an identifiable individual, like web session information.

You could check with Information and Data stakeholders to identify if this data is already collected within MBIE and could potentially be re-used, assuming the appropriate privacy principles are complied with (such as Principle 2 which requires you collect personal data directly from the individual concerned, unless an approved exception is in place).

Information that people would generally consider to be more private may require special care, i.e. they need higher levels of security safeguards when being handled because of their sensitive nature. Examples include information about salary, medical records and children. These are types of information more likely to result in harm to an individual, including significant emotional distress, if not appropriately safeguarded. By identifying the data items that may require special care, it will be easier during your assessment to see how a combination of many sensitive data items may mean your process, product, service or systems design may need to consider appropriate additional safeguards. If needed ask your PIA "guru" to help identify data items that may require special care.

Identify the data items that you have not been collected before. Check with the Information and Data team to identify whether there is any future use for data that this initiative could collect.

Include any legislative or regulatory obligations as part of your primary purpose if applicable.

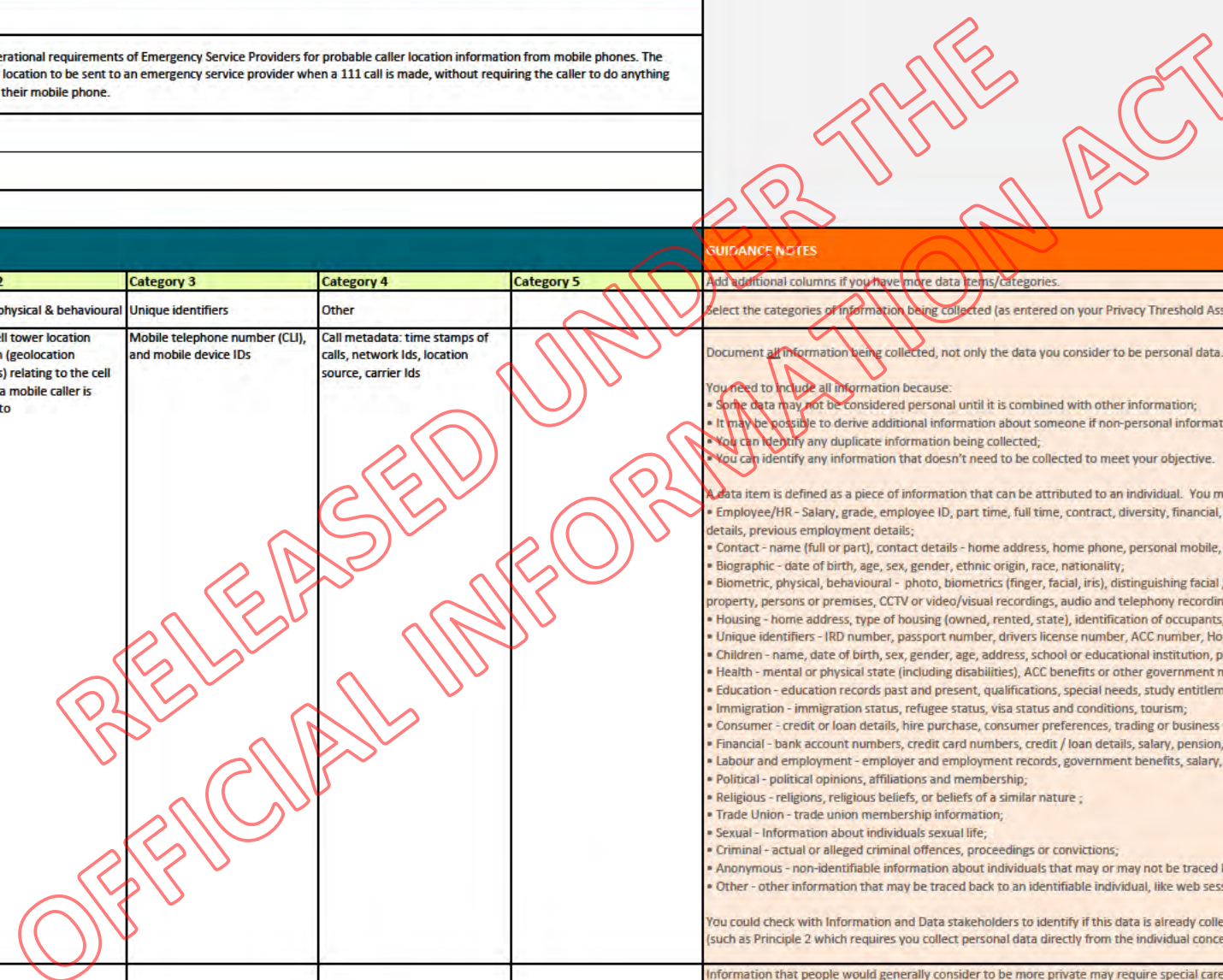
Check with business stakeholders and the Information and Data team to identify if there is any future use for the data you will collect. This requires compliance with other Privacy Principles, such as Principles 2, 3 and 11. Consider how else the information could be used (refer to PTA answers).



Select the appropriate person from the drop down list for each data item.

Note who each data item will be collected from. Examples of other sources are:

- A spreadsheet held internally or externally;
- A public register;
- Another system or application.

If it is a combination of sources, include the various sources you have identified, note which data items come from which source and note it is a combination.



PRINCIPLE 3 - Collection of Information If collecting directly from the individual, tell them about it		
Which data items are mandatory or considered compulsory to collect?	All data elements are required as collectively they establish the probable location area of a caller	List the data fields that are mandatory to collect and describe why. Consider the initiative's primary purpose to determine which data is mandatory. Note any legal reason requiring the collection of certain data items.
How will you tell individuals about the collection of their information?	A new Code of Practice is proposed, subject to agreement and issuance by the Privacy Commissioner, the public will be consulted. Additionally, the project plans to provide information on each emergency service providers website, and will also provide communications to the public, via Ministerial events and other marketing activities.	Include: <ul style="list-style-type: none"> • Whether individuals already know we will be collecting this information about them; • Whether there are any existing MBIE privacy policies, notifications or statements that could be used (and if so, provide links to applicable documentation); • If you are unsure whether any applicable documentation exists; • If you know that no documentation exists and it needs to be drafted. Your PIA "guru" or Legal should be able to help find existing privacy notices, statements or policies that may be relevant.
When will you tell individuals about the collection of their information?	As above. It is not intended that emergency service call takers will advise callers that their location information has been collected as this will add time to an emergency call and may cause delay in dispatching a response. Also, the caller information may not be required, in all cases, to establish location.	Specify whether you will tell individuals before you collect their information, during the process of collection or after the collection. If you are considering not telling them - describe why.
PRINCIPLE 4 - Manner of Collection of Personal Information Be considerate, be fair and don't intrude		
How will this data be collected?	By a mobile caller activating the NZ 111 service by dialling 111 on a mobile device. For Android phones, a hidden SMS text will be sent with the best available probable caller location. For all mobile phones, the cell tower id receiving the 111 call will be sent from the mobile network to a location area service (LAS), the LAS derives the geolocation of the cell tower and its approximate radius using Google Maps Geolocation API.	List the format and manner data will be collected. Examples include: <ul style="list-style-type: none"> • Electronic transfer from an existing database that holds this information; • Paper forms completed by the individual, or on behalf of the individual by another party; • Online forms on MBIE's public websites completed by the individual, or on behalf of the individual by another party; • Spreadsheets held in MBIE; • Publicly available registers; • Video footage; • Sound recordings; • CCTV or moving footage/images; • Biometric files or still photographic images; • From private property or devices. The Information and Data team, and your architect and business analyst should be able to assist with how data is collected.
Attach any diagrams which show how the information will flow		Examples include: <ul style="list-style-type: none"> • System and Infrastructure architecture diagrams - which will illustrate the security mechanisms that will prevent improper access and maintain any separation of information if required. • Process diagrams - which will help you understand the proposed business processes and assess how the business intends to manage the information collected. A process diagram should identify the major components of the business processes and how personal information is collected, used, disclosed and retained through the process. It should also show what the outcome of the processing is; • Data models and data flow diagrams. Internal and external parties should be represented in the maps or diagrams. Future state diagrams should indicate the changes resulting from this initiative - such as any new third parties, data flowing outside of the organisation that didn't previously, or outside of the country. Your business analyst, architect or Information Security teams should be able to assist you.
PRINCIPLE 5 - Storage and Security of Personal Information Once you have information, look after it. Protect it against loss, unauthorised access, use, modification or disclosure and other misuse		
What data fields will be retained and stored and what format will they be stored in?	All data fields described will be retained and stored for no longer than is necessary to establish the location of an emergency caller and facilitate the response to an emergency.	Note where data fields will not be stored. Describe whether storage will be electronic, physical, or both. Examples of: <ul style="list-style-type: none"> • Electronic formats are - text-based documents, spreadsheets, images, photos or diagrams, data tables, sound recordings, still images and moving images; • Physical formats are - paper, image-printed, film-negative, slide, reel or tape, sound-reel or tape and microfilm. Your architect, business analyst or Information and Data team can help with this.
Where will data be stored and who will be responsible for keeping it safe during storage?	The data will be stored in a Location Area Service repository provided as a managed service hosted in the Government cloud (Infrastructure as a Service). MBIE will be the controller of this service.	Describe: <ul style="list-style-type: none"> • Whether any of the data will be encrypted if it is stored electronically; • What safeguards are in place to protect the data if it is stored physically; • The names of internal/external parties responsible for ensuring data is protected when stored; • If data is stored in shared storage facility like a data centre or physical storage facility. • The storage site name, location, region and country; Data must always be stored securely, and in some instances must be encrypted. Seek advice from Records Management and/or Security teams.
What controls will be in place to protect data in transit between internal/external parties?	 Note: At the time of completion of this PIA an initial security risk assessment is underway but not yet completed. Additionally MBIE will seek to accredit the solution, and have also engaged the National Cyber Security Centre (part of GCSB) to provide guidance during solution implementation.	Safeguards are required to protect the data in transit. Security safeguards need to be appropriate and proportionate to the nature of the data being transferred. Information that requires special care will require additional safeguards to ensure appropriate protection from loss, unauthorised access, disclosure, or other misuse. Seek advice from IT and Security about the type of safeguards required. Examples of safeguards are: <ul style="list-style-type: none"> • Encryption of email transfers; • Prohibiting the use of removable devices, like USB sticks; • Securing the IT network that information is transferred across.
Who will have access to the data, who will it be disclosed to and what controls will be in place to protect it?	Emergency service provider call takers will have access to the data for the specific needs of establishing probable caller location. Access logging and audit functionalities will be built.	Document all of the internal and external parties who will have access to the data, and the reason why access is required. Examples include: <ul style="list-style-type: none"> • Individuals who access their data online to carry out a registration process; • Specific staff who access data to perform their role; • Specific internal or external people who access data to provide technical support or administer the service; • Staff at the data centre where data is stored who access data to support the data in storage; • Internal IT or Security staff, or external parties helping to develop, test, or train people on a new system; • Internal audit, investigations and/or compliance staff who audit information. Also describe: <ul style="list-style-type: none"> • How and where the various parties will access data from (e.g.: physical location could be remote, inside or outside of NZ, inside or outside of MBIE); • The type of equipment or device people will access data with (e.g.: MBIE issued IT or telephony equipment, third party equipment via VPN or Citrix session etc.). The IT Security and Security teams can assist with identifying appropriate controls. Describe the security and access controls that will protect the data against unauthorised access. Note: <ul style="list-style-type: none"> • What access and handling protocols will be in place (e.g.: access will be restricted to parties who have legal and business justification to access it and all access attempts will be logged); • Who has access to add, amend, or delete data; • Who has access to assign, change or revoke access privileges; • How remote access will be handled by internal or external parties.
How often will data be accessed by third parties?	Access to the data will be limited to Location Agencies, defined as LAS controller (MBIE), Mobile Network Operators, the Location Area Service provider and public safety organisations (e.g. Police, Fire, Wellington Free and St Johns ambulance).	Describe how frequently data will be accessed by third parties (e.g.: periodically, routinely, or ad-hoc). Confirm with the Security teams what safeguards may be required. These may differ depending on the regularity and the method of access.
What additional safeguards will be in place to protect the data?	To be confirmed following completion of the security assessment.	List any other security safeguards that will be applied as data is collected, used, disclosed, stored, deleted and disposed. Seek advice from your business analyst and IT and Security teams. Examples of other safeguards are: <ul style="list-style-type: none"> • Data Loss Prevention Tools - which minimise the risk that users send private, special or critical information outside MBIE's network by providing controls to determine what data can be transferred; • Email safeguards - like removing "reply all" functionality or removing automatically populated names; • Training users how to email data appropriately (e.g.: by authenticating who the data is being emailed to, checking email addresses for accuracy before sending and not opening unknown email from unidentified senders).
What legal or other commercial safeguards are in place to protect the data?	A new Code of Practice is proposed, subject to agreement and issuance by the Privacy Commissioner. All commercial contracts being established will make reference to the Code and therefore collection, use, disclosure and retention of probable caller location information will be in accordance with the code.	Identify any internal or external agreements which include appropriate privacy and security provisions and cover the collection and use of the personal information in use. <ul style="list-style-type: none"> • Attach any existing schedules, appendices, MoUs, or other contractually binding agreements that may deal with privacy, confidentiality and security. • Describe or attach any new legal contractual documentation or agreements that may be required for new third party relationships, internal or external. Seek assistance from your PIA guru, Information and Data, Security or Legal teams.
PRINCIPLE 6 - Access to Personal Information Individuals can get access to their information		
Can individuals access data about themselves upon request?	Individuals' requests for rights of access to and correction of personal information are likely, however this would be limited due to the proposed retention clause of the new Code that states that information may not be kept for longer than is necessary to establish the location of an emergency caller and facilitate the response to an emergency. Therefore it is unlikely that a request could be fulfilled as the data would likely not exist.	Describe how an individual can access their data if they request it; <ul style="list-style-type: none"> • Attach any operational processes or technical details illustrating how an individual will gain access to their data; • Note if there are already any processes in place. Provide links to any MBIE process that should be used; • Note if third parties may be asked by individuals to provide access to personal data they hold on behalf of MBIE, and if there is a process in place to handle this; • Note if metadata is kept so personal information can be readily identified and located (metadata could be structural or descriptive data which helps identify where or how the data is held); • Note if data will be kept in one or multiple places. Your PIA guru, business analyst or Legal may be able to help with existing processes. Your business analyst, architect or Information and Data team can advise on the relevant technical capabilities available.

PRINCIPLE 7 - Correction of Personal Information Individuals can get their information corrected		
Can an individual request a correction to their data and have the change actioned?	Individuals' requests for rights of access to and correction of personal information are likely, however this would be limited due to the proposed retention clause of the new Code that states that information may not be kept for longer than is necessary to establish the location of an emergency caller and facilitate the response to an emergency. Therefore it is unlikely that a request could be fulfilled as the date would likely not exist.	Include these things: <ul style="list-style-type: none"> Describe how an individual can request correction of their personal information, how the information can be updated and/or how a record of the request will be held against the information for the subject of the request. Attach any operational processes or technical details illustrating how an individual can get their data corrected if they think it's wrong or requires updating; Note if there are already any processes in place. Provide links to any MBIE process that should be used; Note if there is a possibility that third parties may be asked directly by individuals to correct information they hold on behalf of MBIE, and if there is a process in place to handle this; Note if metadata is kept so personal information can be readily identified and located (metadata could be structural or descriptive data which helps identify where or how the data is held); Note if data will be kept in one or multiple places. Your PIA guru or Legal may be able to help with existing process. Your business analyst, architect or Information and Data team can advise on the relevant technical capabilities available.
PRINCIPLE 8 - Accuracy of Personal Information to be Checked before Use Information is checked for accuracy before being used		
Will the accuracy of data collected be verified before it is used?	The location data is the probable location of a caller and not a definitive location, for example an address. In order for an emergency response to be dispatched the location of the event must be confirmed by the caller, the location data is an additional method to assist in verifying the location.	Describe how the information you hold will be accurately linked to the correct person (similar/multiple names, addresses etc. need to be considered). Describe how you will check that data is accurate, complete and up to date before it is used or disclosed. Your business analyst or architect may be able to advise you on this.
PRINCIPLE 9 - Personal Information not to be kept for longer than necessary Securely dispose of information when you no longer need it		
How long will the business retain the data for?	Information may not be kept for longer than is necessary to establish the location of an emergency caller and facilitate the response to an emergency. This period will initially be set at 60mins, in other jurisdiction this period has been reduced to 30mins	Describe how long you need to keep information: <ul style="list-style-type: none"> For business purposes; To meet legislative or public records requirements; For policy reasons; For data storage capacity reasons. The Records Management team should be able to provide guidance.
How will the data retention period be managed and controlled?	Automatically deleted by the LAS when the specified period is reached.	Describe (or attach documents if they are available) how data will be managed to ensure it will only be retained for the planned retention period. Is there a process in place to notify those who are storing personal data internally or externally to MBIE of deletion or destruction requirements when personal information should no longer be retained? Note if there is no operational process to manage and control the data retention period.
How will data disposal or archiving be managed and controlled at the end of the retention period?	There will be no archiving of identifiable data. A log that data was received will be retained but this will not contain personal information.	Describe how the disposal of data will be managed securely at the end of the retention period. Outline if there is an authority/acknowledgement for approving disposal or archiving of data before the end of its agreed lifetime. The Records Management team should be able to provide guidance.
PRINCIPLE 10 - Limits on Use of Personal Information Only use information for the purpose you collect it for, unless one of the exceptions applies		
List any additional uses for the data you are collecting	None additional	If there is a plan to use some or all of the personal information collected for a different purpose to what it was originally collected it for, describe: <ul style="list-style-type: none"> What information will be used; Who will use it and what it will be used for, including how and why information will be used; If you will tell the individuals concerned that you are using the information for a different purpose; Check with the Information and Data team also to see if there is a potential for additional use that could be considered, or if this personal data is already held and could be used by you for the purpose of this initiative.
PRINCIPLE 11 - Limits on Disclosure of Personal Information Only disclose information if you have a valid reason, or one of the permitted exceptions applies		
List any additional disclosure of the data you foresee	None additional	If there is a need to disclose personal information held for a different purpose to what it was collected it for, describe: <ul style="list-style-type: none"> What information you might disclose; Who you might disclose it to and for what purpose; If you think you will need to create or change information sharing arrangements with other internal or external organisations; If you will tell the individuals concerned that you are disclosing to other parties; If there are MoUs in place or other similar agreements to enable the disclosure of information to other parties or if there are no agreements in place. The Legal team should be able to advise you. Check with the Data and Information team also to see if there is a potential for additional disclosure that could be considered, or if this personal data is already held and could be disclosed to you for the purpose of this initiative.
PRINCIPLE 12 - Unique Identifiers Assign unique identifiers only where permitted		
List any unique identifiers being used and describe why it is necessary to use them	A unique identifier may be assigned to the probable caller location information for the purpose of enabling the location agency to audit and monitor the operation of the LAS and the methods by which the information is collected. Noting that identifiable data will not be retained.	If you are using a unique identifier to identify individuals describe: <ul style="list-style-type: none"> How it will be used and where the unique identifier has originated from; How and why the unique identifier will be used to link or match personal information across agencies (if applicable); Any agreements in place to enable the use of a unique identifier if it is provided by another internal/external party. The Legal team should be able to advise you.

RELEASED UNDER THE OFFICIAL INFORMATION ACT

PRINCIPLE 1 - PRIVACY IMPACT ANALYSIS

Once you have completed the Data Flow template, information related to Principle 1 will be automatically copied to this worksheet. Refer to this information to help you to complete an Impact Analysis and identify the risks associated with Principle 1.

- If you have more than five categories on your Data Flow template, add more columns (to the right of column F) so the number of columns on this worksheet matches your Data Flow template. Copy the formula from column F to the new columns so the data from the Data Flow template is copied over.
- Complete the 'Initiative Details and Sign off' section (in white).
- Complete the 'Privacy Analysis and Discussion Points', and 'Risk Identification' sections (in white). Guidance notes are provided to the right in orange.
- Business owner sign off is required.



INITIATIVE DETAILS AND SIGN OFF

Initiative name:	Mobile Caller Location
Brief description of initiative:	The MCL project will address longstanding operational requirements of Emergency Service Providers for probable caller location information from mobile phones. The outcome sought is for the best available caller location to be sent to an emergency service provider when a 111 call is made, without requiring the caller to do anything more than dial 111 on the standard keypad of their mobile phone.
Name and role of person completing template:	
Template completion date:	
Business owner name and sign-off:	

Information recorded on Data Flow Template

	Category 1	Category 2	Category 3	Category 4	Category 5
What categories of personal information will be collected?	Biometric, physical & behavioural	Biometric, physical & behavioural	Unique identifiers	Other	
List the data items that will be collected in each category	Probable mobile caller location information, includes	Network cell tower location information (geolocation)	Mobile telephone number (CLI), and mobile device IDs	Call metadata: time stamps or calls, network ids, location	
Which data items require special care?	All	All	All	All	
Which data items have not been collected previously?	All	All	Mobile device id. CLI is provided today	All	
Describe the main reason (primary purpose) for collecting the data	Best available caller location to be sent to an emergency service provider when a 111 call is made, in order to assist in address verification of emergency events				
Describe any secondary or future purposes for collecting this data	None				

Privacy Analysis and Discussion Points

Principle 1 of the Privacy Act states that personal information should only be collected if there is a justifiable purpose for it. The key requirements of Principle 1 are to:

- Identify all the personal data that will be collected and used by the proposed change or initiative;
- Be convinced that the personal information collected is necessary to meet the purpose of the proposed initiative. The purpose of the initiative or change must be lawful and connected with the business function or activity of the agency.

GUIDANCE NOTES

Use this template to record your thoughts and considerations. This is not a formal report, so notes and bullet points are acceptable. The important part is to ensure all relevant considerations are recorded and considered.

This template is designed to be completed iteratively; it doesn't need to be completed in one go.

Not all of the Privacy Principles will be relevant to your proposal. If you don't have a clear answer for a part of the template or believe a Principle is not relevant, ensure this is noted.

Describe how your initiative complies (or does not comply) with this Principle and summarise any privacy related discussion points. Discussion points may include concerns, issues, uncertainties or questions you want to explore further. Record and evaluate potential options for addressing any discussion points, including identifying any options/solutions that enhance or could enhance privacy practices. Discussion points may identify privacy risks which need to be managed.

Consider the purpose for which you are collecting personal information. If it is designed too narrowly, you may be unable to use information in the way that you and MBIE want to in the future. If defined too broadly, the purposes risk becoming meaningless - MBIE could be collecting information it has no real need for and people could be confused. Consider any secondary purposes you, other parts of MBIE, or other agencies (Government and non-governmental) might have for the information. Does the collection allow for those purposes?

Describe whether you believe each data field is necessary for the proposed initiative and note the fields you consider to be unnecessary because the purpose of the initiative can be achieved without them. For example, if collecting an individual's name, do you require the middle name? Collecting the middle name adds another level of certainty about the individual's identity but if there are other fields being collected to achieve certainty, then it may not be necessary to obtain middle name as well. In this situation you would not collect middle name in order to comply with Principle 1.

Note if any personal data items being collected are particularly sensitive or may require special care and identify these. Data items that may require special care include things like personal information about an individual's health or alleged criminal activities, or information about children in refugee visa applications.

Explain if the personal information already collected will be used for a new, or different, purpose by your initiative. Note whether information already being collected is collected by the business function who owns the initiative, another MBIE function or a party outside of MBIE (Government Agency or otherwise).

Risk Identification

Link to Risk Register	Risk Description <i>Description of the privacy risk (i.e.: the actual/root risk, not the symptom of the risk)</i>	Consequences <i>Key things that may happen if the risk materialises</i>
P1_1		
P1_2		
P1_3		
P1_4		
P1_5		
P1_6		

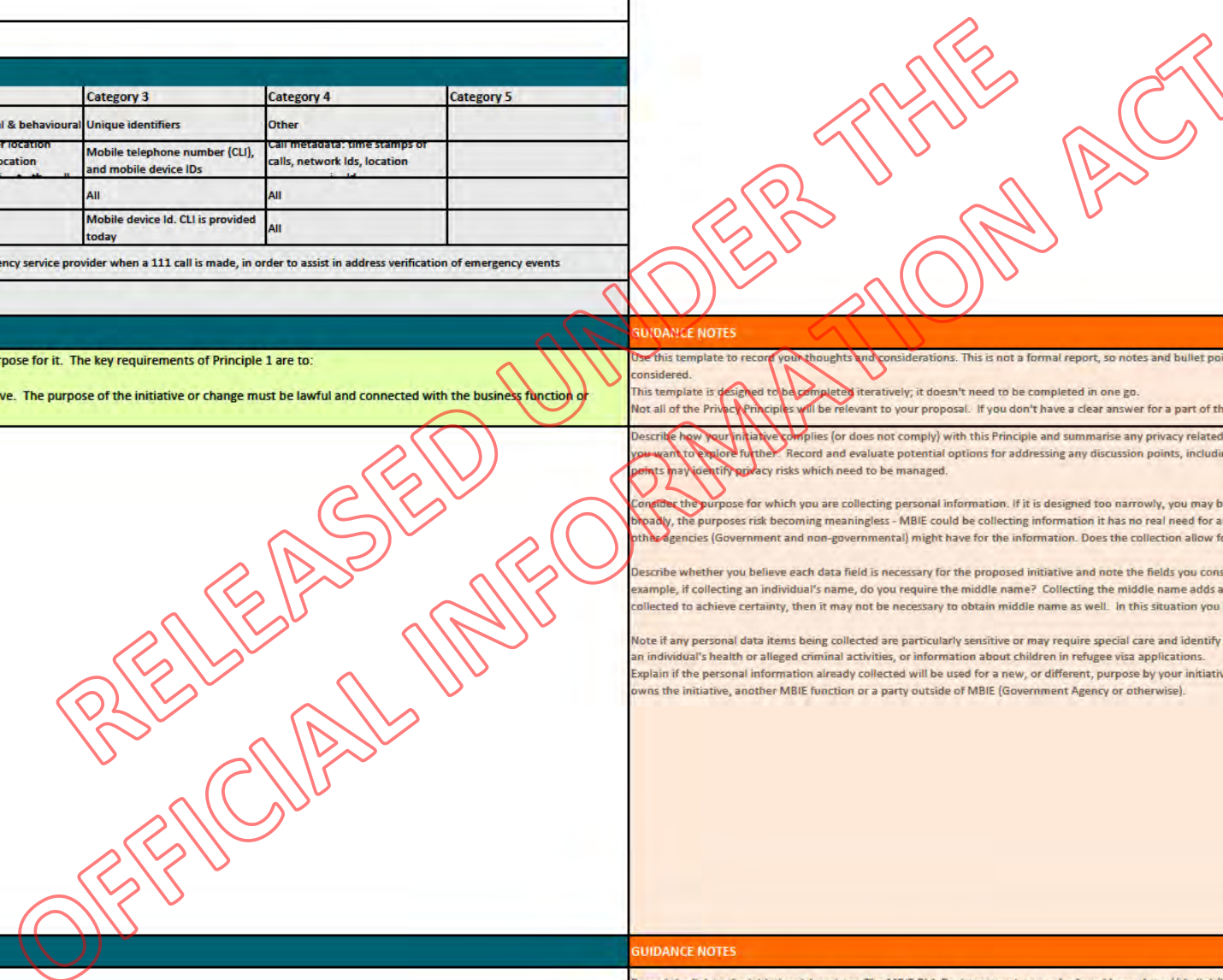
GUIDANCE NOTES

Record the link to the initiative risk register. The MBIE Risk Register template can be found here - <http://thelink/how/Pages/find-the-cpo-project-delivery-templates.aspx>

Record all privacy risks arising from the analysis and discussion points above. Add more rows as required.

Where privacy risks are identified, these must be appropriately managed. Copy these risks into the appropriate risk register (this may be the master initiative risk register, or a specific privacy risk register).

Complete the risk register template by recording: existing controls in place to manage the risk; planned activities, actions, roles, or programmes to treat the risk; and the outcome of the controls and treatments. Ensure responsibilities are identified and regular reviews of the risks, controls, and treatments are undertaken.



PRINCIPLE 2 - PRIVACY IMPACT ANALYSIS

Once you have completed the Data Flow template, information related to Principle 2 will be automatically copied to this worksheet. Refer to this information to help you to complete an Impact Analysis and identify the risks associated with Principle 2.

- If you have more than five categories on your Data Flow template, add more columns (to the right of column F) so the number of columns on this worksheet matches your Data Flow template. Copy the formula from column F to the new columns so the data from the Data Flow template is copied over.
- Complete the 'Initiative Details and Sign off' section (in white).
- Complete the 'Privacy Analysis and Discussion Points', and 'Risk Identification' sections (in white). Guidance notes are provided to the right in orange.
- Business owner sign off is required.



INITIATIVE DETAILS AND SIGN OFF	
Initiative name:	Mobile Caller Location
Brief description of initiative:	The MCL project will address longstanding operational requirements of Emergency Service Providers for probable caller location information from mobile phones. The outcome sought is for the best available caller location to be sent to an emergency service provider when a 111 call is made, without requiring the caller to do anything more than dial 111 on the standard keypad of their mobile phone.
Name and role of person completing template:	
Template completion date:	
Business owner name and sign-off:	

Information recorded on Data Flow Template					
Who are you collecting this information about?	Category 1	Category 2	Category 3	Category 4	Category 5
	Creators				
Will this data be collected directly from individuals, or another source? Note who the other sources are.	The information will be collected indirectly when a caller dials 111 from their mobile phone. Initially on Android phones, a hidden SMS text will be sent to a specific new emergency short-dial number, the SMS text will contain information relating to the callers probable location (note, only if a location can be established). For all phones				

Privacy Analysis and Discussion Points
 Principle 2 of the Privacy Act states that information should be collected directly from the individual whenever possible. We want to be sure that the information provided is accurate and the individual is best placed to provide this. Collecting personal information from an alternate source may be acceptable if there is a justifiable exception.

GUIDANCE NOTES

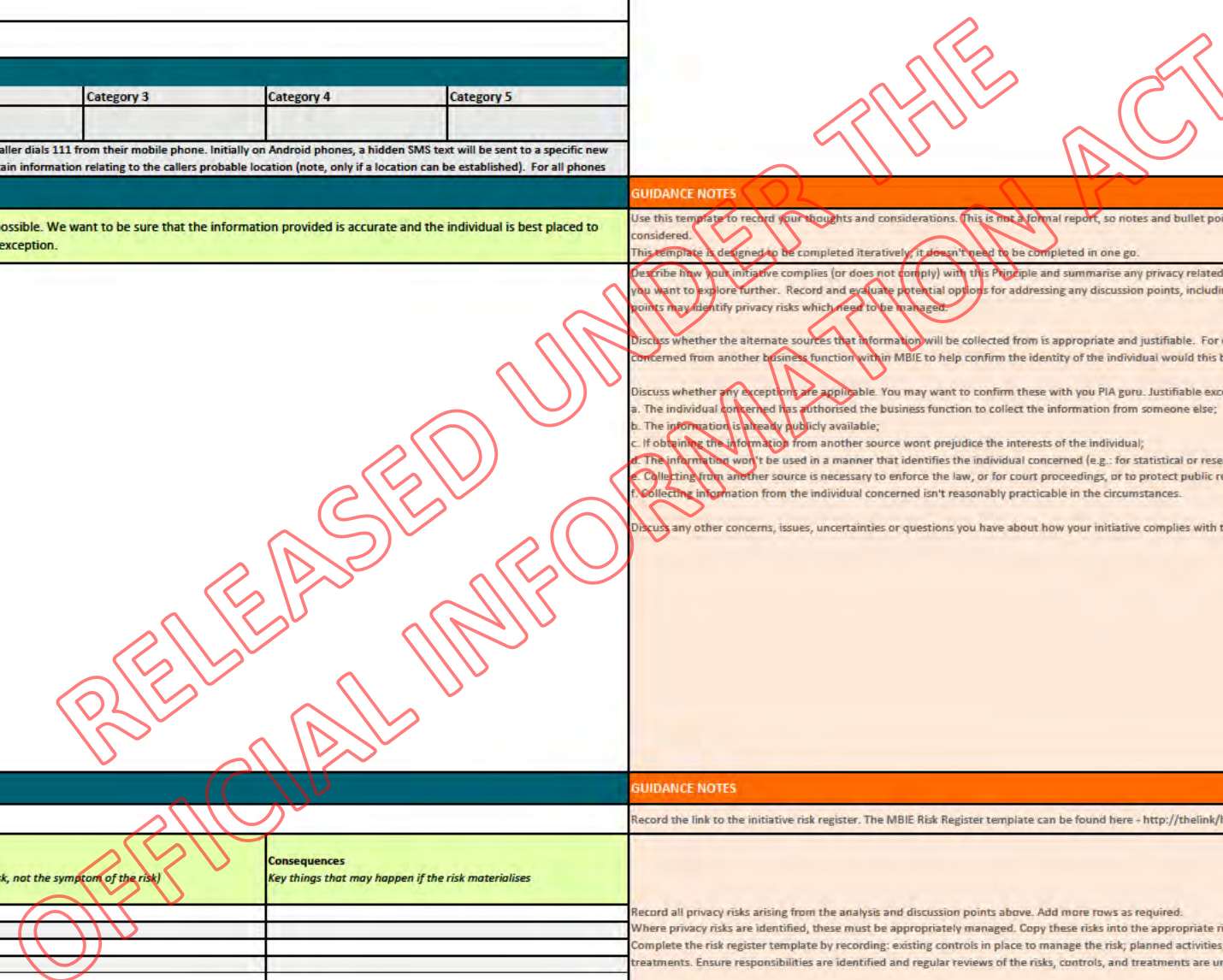
Use this template to record your thoughts and considerations. (This is not a formal report, so notes and bullet points are acceptable. The important part is to ensure all relevant considerations are recorded and considered.)
 This template is designed to be completed iteratively, it doesn't need to be completed in one go.
 Describe how your initiative complies (or does not comply) with this Principle and summarise any privacy related discussion points. Discussion points may include concerns, issues, uncertainties or questions you want to explore further. Record and evaluate potential options for addressing any discussion points, including identifying any options/solutions that enhance or could enhance privacy practices. Discussion points may identify privacy risks which need to be managed.
 Discuss whether the alternate sources that information will be collected from is appropriate and justifiable. For example, if the initiative proposes that you collect personal contact details for the individuals concerned from another business function within MBIE to help confirm the identity of the individual would this be appropriate and justifiable?
 Discuss whether any exceptions are applicable. You may want to confirm these with you PIA guru. Justifiable exceptions are:
 a. The individual concerned has authorised the business function to collect the information from someone else;
 b. The information is already publicly available;
 c. If obtaining the information from another source won't prejudice the interests of the individual;
 d. The information won't be used in a manner that identifies the individual concerned (e.g.: for statistical or research purposes);
 e. Collecting from another source is necessary to enforce the law, or for court proceedings, or to protect public revenue;
 f. Collecting information from the individual concerned isn't reasonably practicable in the circumstances.
 Discuss any other concerns, issues, uncertainties or questions you have about how your initiative complies with this principle.

Risk Identification

GUIDANCE NOTES

Link to Risk Register		
Risk Number	Risk Description <i>Description of the privacy risk (i.e.: the actual/root risk, not the symptom of the risk)</i>	Consequences <i>Key things that may happen if the risk materialises</i>
P2_1		
P2_2		
P2_3		
P2_4		
P2_5		
P2_6		

Record the link to the initiative risk register. The MBIE Risk Register template can be found here - <http://thelink/how/Pages/find-the-cpo-project-delivery-templates.aspx>
 Record all privacy risks arising from the analysis and discussion points above. Add more rows as required.
 Where privacy risks are identified, these must be appropriately managed. Copy these risks into the appropriate risk register (this may be the master initiative risk register, or a specific privacy risk register).
 Complete the risk register template by recording: existing controls in place to manage the risk; planned activities, actions, roles, or programmes to treat the risk; and the outcome of the controls and treatments. Ensure responsibilities are identified and regular reviews of the risks, controls, and treatments are undertaken.



PRINCIPLE 3 - PRIVACY IMPACT ANALYSIS

Once you have completed the Data Flow template, information related to Principle 3 will be automatically copied to this worksheet. Refer to this information to help you to complete an Impact Analysis and identify the risks associated with Principle 3.

- If you have more than five categories on your Data Flow template, add more columns (to the right of column F) so the number of columns on this worksheet matches your Data Flow template. Copy the formula from column F to the new columns so the data from the Data Flow template is copied over.
- Complete the 'Initiative Details and Sign off' section (in white).
- Complete the 'Privacy Analysis and Discussion Points', and 'Risk Identification' sections (in white). Guidance notes are provided to the right in orange.
- Business owner sign off is required.



INITIATIVE DETAILS AND SIGN OFF	
Initiative name:	Mobile Caller Location
Brief description of initiative:	The MCL project will address longstanding operational requirements of Emergency Service Providers for probable caller location information from mobile phones. The outcome sought is for the best available caller location to be sent to an emergency service provider when a 111 call is made, without requiring the caller to do anything more than dial 111 on the standard keypad of their mobile phone.
Name and role of person completing template:	
Template completion date:	
Business owner name and sign-off:	

Information recorded on Data Flow Template	
Which data items are mandatory or considered compulsory to collect?	All data elements are required as collectively they establish the probable location area of a caller
How will you tell individuals about the collection of their information?	A new Code of Practice is proposed, subject to agreement and issuance by the Privacy Commissioner, the public will be consulted. Additionally, the project plans to provide information on each emergency service providers website, and will also provide communications to the public, via Ministerial events and other marketing
When will you tell individuals about the collection of their information?	As above. It is not intended that emergency service call takers will advise callers that their location information has been collected as this will add time to an emergency call and may cause delay in dispatching a response. Also, the caller information may not be required, in all cases, to establish location.

Privacy Analysis and Discussion Points

The key requirements of Principle 3 of the Privacy Act are to ensure individuals know:

- That information is being collected about them and their rights relating to their information;
- Why information is being collected about them, including the consequences if all, or part, of the information is not provided;
- Who else will use the information.

GUIDANCE NOTES

Use this template to record your thoughts and considerations. This is not a formal report, so notes and bullet points are acceptable. The important part is to ensure all relevant considerations are recorded and considered.

This template is designed to be completed iteratively; it doesn't need to be completed in one go.

Not all of the Privacy Principles will be relevant to your proposal. If you don't have a clear answer for a part of the template or believe a Principle is not relevant, ensure this is noted.

Describe how your initiative complies (or does not comply) with this Principle and summarise any privacy related discussion points. Discussion points may include concerns, issues, uncertainties or questions you want to explore further. Record and evaluate potential options for addressing any discussion points, including identifying any options/solutions that enhance or could enhance privacy practices. Discussion points may identify privacy risks which need to be managed.

Have you decided not to tell individuals about all the information you are collecting about them? Note if any will be omitted and explain why the business has chosen not to inform individuals in line with the requirements of this principle.

If you are not notifying individuals, consider whether one of the exceptions in the Principle applies and record your reasoning. It is recommended that you check with your PIA guru or Principal Privacy Adviser to confirm this. Justifiable exceptions include:

- If it would impact the lawful purpose of collecting the information;
- If it could prejudice a criminal investigation;
- If it is not reasonably practicable in the circumstances.

Does an existing privacy statement or notice adequately cover the collection of personal information for your initiative? If not, record what needs to be amended for it to do so. Discuss any other concerns, issues, uncertainties or questions you have about how your initiative complies with this principle.

Risk Identification

Link to Risk Register	
Risk Number	Risk Description <i>Description of the privacy risk (i.e.: the actual/root risk, not the symptom of the risk)</i>
	Consequences <i>Key things that may happen if the risk materialises</i>
P3_1	
P3_2	
P3_3	
P3_4	
P3_5	
P3_6	

GUIDANCE NOTES

Record the link to the initiative risk register. The MBIE Risk Register template can be found here - <http://thelink/how/Pages/find-the-cpo-project-delivery-templates.aspx>

Record all privacy risks arising from the analysis and discussion points above. Add more rows as required.

Where privacy risks are identified, these must be appropriately managed. Copy these risks into the appropriate risk register (this may be the master initiative risk register, or a specific privacy risk register).

Complete the risk register template by recording: existing controls in place to manage the risk; planned activities, actions, roles, or programmes to treat the risk; and the outcome of the controls and treatments. Ensure responsibilities are identified and regular reviews of the risks, controls, and treatments are undertaken.



PRINCIPLE 4 - PRIVACY IMPACT ANALYSIS

Once you have completed the Data Flow template, information related to Principle 4 will be automatically copied to this worksheet. Refer to this information to help you to complete an Impact Analysis and identify the risks associated with Principle 4.

- If you have more than five categories on your Data Flow template, add more columns (to the right of column F) so the number of columns on this worksheet matches your Data Flow template. Copy the formula from column F to the new columns so the data from the Data Flow template is copied over.
- Complete the 'Initiative Details and Sign off' section (in white).
- Complete the 'Privacy Analysis and Discussion Points', and 'Risk Identification' sections (in white). Guidance notes are provided to the right in orange.
- Business owner sign off is required.



INITIATIVE DETAILS AND SIGN OFF	
Initiative name:	Mobile Caller Location
Brief description of initiative:	The MCL project will address longstanding operational requirements of Emergency Service Providers for probable caller location information from mobile phones. The outcome sought is for the best available caller location to be sent to an emergency service provider when a 111 call is made, without requiring the caller to do anything more than dial 111 on the standard keypad of their mobile phone.
Name and role of person completing template:	
Template completion date:	
Business owner name and sign-off:	

Information recorded on Data Flow Template	
How will this data be collected?	By a mobile caller activating the NZ 111 service by dialling 111 on a mobile device.
Attach any diagrams which show how the information will flow	

Privacy Analysis and Discussion Points

The key requirement of Principle 4 of the Privacy Act is to ensure personal information is not collected by unlawful means, in an unfair manner, or a manner that intrudes unreasonably upon the personal affairs of the individual concerned.

GUIDANCE NOTES

Use this template to record your thoughts and considerations. This is not a formal report, so notes and bullet points are acceptable. The important part is to ensure all relevant considerations are recorded and considered.

This template is designed to be completed iteratively, it doesn't need to be completed in one go.

Describe how your initiative complies (or does not comply) with this Principle and summarise any privacy related discussion points. Discussion points may include concerns, issues, uncertainties or questions you want to explore further. Record and evaluate potential options for addressing any discussion points, including identifying any options/solutions that enhance or could enhance privacy practices. Discussion points may identify privacy risks which need to be managed.

Will the individual know information is being collected about them? If applicable, describe why any information is being collected in a covert manner rather than in an open and transparent way (visible to the individual concerned). A good rule of thumb here is to consider whether the individual is likely to be concerned or upset about the way their personal information is being collected. Do you have to collect information covertly? Are there any legal requirements that require this?

Discuss any other concerns, issues, uncertainties or questions you have about how your initiative complies with this principle.

Risk Identification

GUIDANCE NOTES

Link to Risk Register

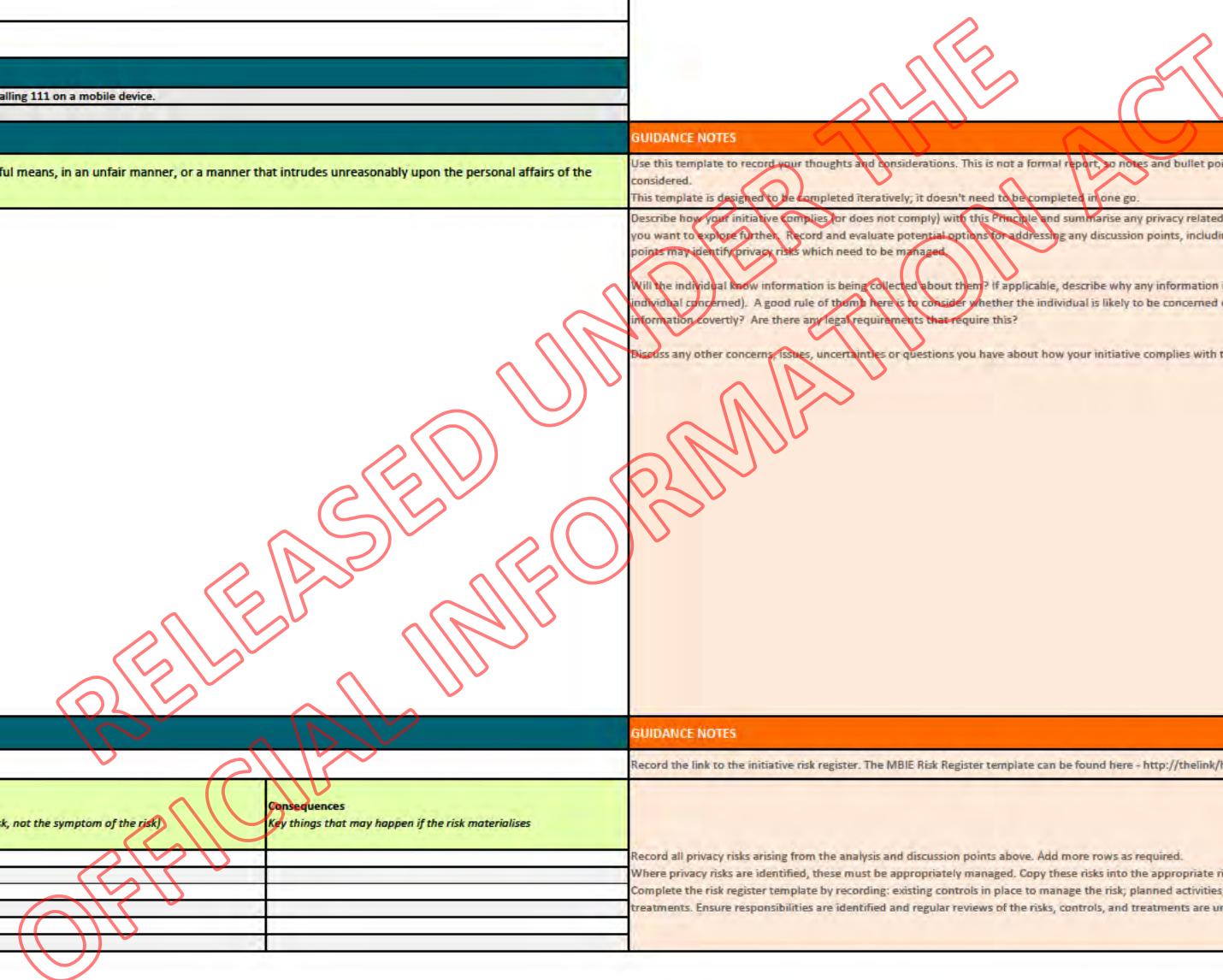
Record the link to the initiative risk register. The MBIE Risk Register template can be found here - <http://thelink/how/Pages/Find-the-cpo-project-delivery-templates.aspx>

Risk Number	Risk Description <i>Description of the privacy risk (i.e.: the actual/root risk, not the symptom of the risk)</i>	Consequences <i>Key things that may happen if the risk materialises</i>
P4_1		
P4_2		
P4_3		
P4_4		
P4_5		
P4_6		

Record all privacy risks arising from the analysis and discussion points above. Add more rows as required.

Where privacy risks are identified, these must be appropriately managed. Copy these risks into the appropriate risk register (this may be the master initiative risk register, or a specific privacy risk register).

Complete the risk register template by recording: existing controls in place to manage the risk; planned activities, actions, roles, or programmes to treat the risk; and the outcome of the controls and treatments. Ensure responsibilities are identified and regular reviews of the risks, controls, and treatments are undertaken.



PRINCIPLE 5 - PRIVACY IMPACT ANALYSIS

Once you have completed the Data Flow template, information related to Principle 5 will be automatically copied to this worksheet. Refer to this information to help you to complete an Impact Analysis and identify the risks associated with Principle 5.

- If you have more than five categories on your Data Flow template, add more columns (to the right of column F) so the number of columns on this worksheet matches your Data Flow template. Copy the formula from column F to the new columns so the data from the Data Flow template is copied over.
- Complete the 'Initiative Details and Sign off' section (in white).
- Complete the 'Privacy Analysis and Discussion Points', and 'Risk Identification' sections (in white). Guidance notes are provided to the right in orange.
- Business owner sign off is required.



INITIATIVE DETAILS AND SIGN OFF	
Initiative name:	Mobile Caller Location
Brief description of initiative:	The MCL project will address longstanding operational requirements of Emergency Service Providers for probable caller location information from mobile phones. The outcome sought is for the best available caller location to be sent to an emergency service provider when a 111 call is made, without requiring the caller to do anything more than dial 111 on the standard keypad of their mobile phone.
Name and role of person completing template:	
Template completion date:	
Business owner name and sign-off:	

Information recorded on Data Flow Template	
What data fields will be retained and stored and what format will they be stored in?	All data fields described will be retained and stored for no longer than is necessary to establish the location of an emergency caller and facilitate the response to an emergency.
Where will data be stored and who will be responsible for keeping it safe during storage?	The data will be stored in a Location Area Service repository provided as a managed service hosted in the Government cloud (Infrastructure as a Service). MBIE will be the controller of this service.
What controls will be in place to protect data in transit between internal/external parties?	Best practice security controls, utilising industry standard encryption techniques will be implemented on the interfaces with the service being hosted in the Government cloud.
Who will have access to the data, who will it be disclosed to and what controls will be in place to protect it?	Emergency service provider call takers will have access to the data for the specific needs of establishing probable caller location. Access logging and audit functionalities will be built.
How often will data be accessed by third parties?	Access to the data will be limited to Location Agencies, defined as LAS controller (MBIE), Mobile Network Operators, the Location Area Service provider and public safety.
What additional safeguards will be in place to protect the data?	To be confirmed following completion of the security assessment.
What legal or other commercial safeguards are in place to protect the data?	A new Code of Practice is proposed, subject to agreement and issuance by the Privacy Commissioner. All commercial contracts being established will make reference to the Code and therefore collection, use, disclosure and retention of probable caller location information will be in accordance with the code.

Privacy Analysis and Discussion Points

The key requirement of Principle 5 is that reasonable steps are taken to protect the personal information collected from loss, unauthorised access, unauthorised use, modification, disclosure and other misuse. This applies when the information is in storage and when it is being moved.

<p>Use this template to record your thoughts and considerations. This is not a formal report, so notes and bullet points are acceptable. The important part is to ensure all relevant considerations are recorded and considered.</p> <p>This template is designed to be completed iteratively; it doesn't need to be completed in one go.</p> <p>Describe how your initiative complies (or does not comply) with this Principle and summarise any privacy related discussion points. Discussion points may include concerns, issues, uncertainties or questions you want to explore further. Record and evaluate potential options for addressing any discussion points, including identifying any options/solutions that enhance or could enhance privacy practices. Discussion points may identify privacy risks which need to be managed.</p> <p>Discuss with your internal stakeholders what safeguards are in place or required, IT, Security, Legal, Procurement, Records Management, Facilities, and HR are all key. IT and Security stakeholders should be able to advise you on the appropriateness of the security components in place and what might be required for changes or new initiatives along with identifying what the standards are that must be adhered to internally or externally.</p> <p>Note any concerns you have about how personal information will be protected. Will existing safeguards be affected? Note where new technologies or processes will improve existing safeguards. Will the methods proposed adequately protect information? Are there additional protective safeguards in place to protect information that requires special care? Discuss whether any physical, technical and operational controls can be applied to protect personal information. Consider safeguards for when the personal information is in storage and when it is being transferred from one place to another (including digital and physical transfer).</p> <p>Are the existing controls in place for staff (such as privacy and security training, policies, incident Management procedures, Acceptable Use Policy, Code of Conduct) governing employee and third party treatment of personal information relevant and adequate? Technology changes quickly, and written "safeguards" such as policies and training may out of date. These must be reviewed if they are to be relied upon. Discuss whether you believe the use of any new devices, channels or methods of collection are adequately protected.</p> <p>Revisit confidentiality, privacy and security clauses in contracts if a change relies on third party contracts already in place (in particular if new locations are required to transfer, access, disclose or store personal information). New third party relationships will require appropriate contract terms to articulate remote access provisions and how privacy and security will be handled.</p> <p>Physical security safeguards should be considered for premises, property, equipment and files. Are these physically secure? Can you obtain details about who has accessed facilities and equipment?</p> <p>Discuss any other concerns, issues, uncertainties or questions you have about how your initiative complies with this principle.</p>	
---	--

GUIDANCE NOTES

<p>Use this template to record your thoughts and considerations. This is not a formal report, so notes and bullet points are acceptable. The important part is to ensure all relevant considerations are recorded and considered.</p> <p>This template is designed to be completed iteratively; it doesn't need to be completed in one go.</p> <p>Describe how your initiative complies (or does not comply) with this Principle and summarise any privacy related discussion points. Discussion points may include concerns, issues, uncertainties or questions you want to explore further. Record and evaluate potential options for addressing any discussion points, including identifying any options/solutions that enhance or could enhance privacy practices. Discussion points may identify privacy risks which need to be managed.</p> <p>Discuss with your internal stakeholders what safeguards are in place or required, IT, Security, Legal, Procurement, Records Management, Facilities, and HR are all key. IT and Security stakeholders should be able to advise you on the appropriateness of the security components in place and what might be required for changes or new initiatives along with identifying what the standards are that must be adhered to internally or externally.</p> <p>Note any concerns you have about how personal information will be protected. Will existing safeguards be affected? Note where new technologies or processes will improve existing safeguards. Will the methods proposed adequately protect information? Are there additional protective safeguards in place to protect information that requires special care? Discuss whether any physical, technical and operational controls can be applied to protect personal information. Consider safeguards for when the personal information is in storage and when it is being transferred from one place to another (including digital and physical transfer).</p> <p>Are the existing controls in place for staff (such as privacy and security training, policies, incident Management procedures, Acceptable Use Policy, Code of Conduct) governing employee and third party treatment of personal information relevant and adequate? Technology changes quickly, and written "safeguards" such as policies and training may out of date. These must be reviewed if they are to be relied upon. Discuss whether you believe the use of any new devices, channels or methods of collection are adequately protected.</p> <p>Revisit confidentiality, privacy and security clauses in contracts if a change relies on third party contracts already in place (in particular if new locations are required to transfer, access, disclose or store personal information). New third party relationships will require appropriate contract terms to articulate remote access provisions and how privacy and security will be handled.</p> <p>Physical security safeguards should be considered for premises, property, equipment and files. Are these physically secure? Can you obtain details about who has accessed facilities and equipment?</p> <p>Discuss any other concerns, issues, uncertainties or questions you have about how your initiative complies with this principle.</p>

Risk Identification

Record the link to the initiative risk register. The MBIE Risk Register template can be found here - <http://thelink/how/Pages/find-the-cpo-project-delivery-templates.aspx>

Link to Risk Register	
Link to Risk Register	
Risk Number	Risk Description <i>Description of the privacy risk (i.e.: the actual/root risk, not the symptom of the risk)</i>
	Consequences <i>Key things that may happen if the risk materialises</i>
PS 1	
PS 2	
PS 3	
PS 4	
PS 5	
PS 6	

GUIDANCE NOTES

<p>Record the link to the initiative risk register. The MBIE Risk Register template can be found here - http://thelink/how/Pages/find-the-cpo-project-delivery-templates.aspx</p> <p>Record all privacy risks arising from the analysis and discussion points above. Add more rows as required.</p> <p>Where privacy risks are identified, these must be appropriately managed. Copy these risks into the appropriate risk register (this may be the master initiative risk register, or a specific privacy risk register).</p> <p>Complete the risk register template by recording: existing controls in place to manage the risk; planned activities, actions, roles, or programmes to treat the risk; and the outcome of the controls and treatments. Ensure responsibilities are identified and regular reviews of the risks, controls, and treatments are undertaken.</p>
--

RELEASED UNDER THE OFFICIAL INFORMATION ACT

PRINCIPLE 6 - PRIVACY IMPACT ANALYSIS

Once you have completed the Data Flow template, information related to Principle 6 will be automatically copied to this worksheet. Refer to this information to help you to complete an Impact Analysis and identify the risks associated with Principle 6.

- If you have more than five categories on your Data Flow template, add more columns (to the right of column F) so the number of columns on this worksheet matches your Data Flow template. Copy the formula from column F to the new columns so the data from the Data Flow template is copied over.
- Complete the 'Initiative Details and Sign off' section (in white).
- Complete the 'Privacy Analysis and Discussion Points', and 'Risk Identification' sections (in white). Guidance notes are provided to the right in orange.
- Business owner sign off is required.



INITIATIVE DETAILS AND SIGN OFF	
Initiative name:	Mobile Caller Location
Brief description of initiative:	The MCL project will address longstanding operational requirements of Emergency Service Providers for probable caller location information from mobile phones. The outcome sought is for the best available caller location to be sent to an emergency service provider when a 111 call is made, without requiring the caller to do anything more than dial 111 on the standard keypad of their mobile phone.
Name and role of person completing template:	
Template completion date:	
Business owner name and sign-off:	

Information recorded on Data Flow Template

Can individuals access data about themselves upon request? Individuals' requests for rights of access to and correction of personal information are likely, however this would be limited due to the proposed retention clause of the

Privacy Analysis and Discussion Points

The key requirement of Principle 6 of the Privacy Act is to ensure that an agency holds personal information in such a way that it can readily be retrieved as the individual concerned is entitled to:

- Obtain confirmation about whether information is being held about them;
- Have access to that information (within 20 working days from date of request).

GUIDANCE NOTES

Use this template to record your thoughts and considerations. This is not a formal report, so notes and bullet points are acceptable. The important part is to ensure all relevant considerations are recorded and considered.

This template is designed to be completed iteratively; it doesn't need to be completed in one go.

Not all of the Privacy Principles will be relevant to your proposal. If you don't have a clear answer for a part of the template or believe a Principle is not relevant, ensure this is noted.

Describe how your initiative complies (or does not comply) with this Principle and summarise any privacy related discussion points. Discussion points may include concerns, issues, uncertainties or questions you want to explore further. Record and evaluate potential options for addressing any discussion points, including identifying any options/solutions that enhance or could enhance privacy practices. Discussion points may identify privacy risks which need to be managed.

Describe what impact the proposed change will have on an individual's ability to access their personal information if they wish to see it. Note if the where existing capability will be improved by the initiative. When an individual requests access to their information, how will this be identified and actioned? Can a decision to grant access or withhold information be made within the 20 working day time limit? Is there a valid reason to extend this time limit or can this information be provided without unnecessary delay? Will requests to third parties with access to the personal information be transferred or processed by the third party? Are there any concerns about finding the information you hold? Will emails involving personal information be appropriately filed to easily identify and retrieve? If information is archived offshore or stored by a cloud provider, can it be retrieved readily and within the timeframe? Will the personal information be up to date and accurate?

Consider the impact of various options for providing access. Are any options more efficient or cost-effective? Identify those options that provide access in the most complete, accurate, and timely way for the individual.

Discuss any other concerns, issues, uncertainties or questions you have about how your initiative complies with this principle.

Risk Identification

Link to Risk Register

GUIDANCE NOTES

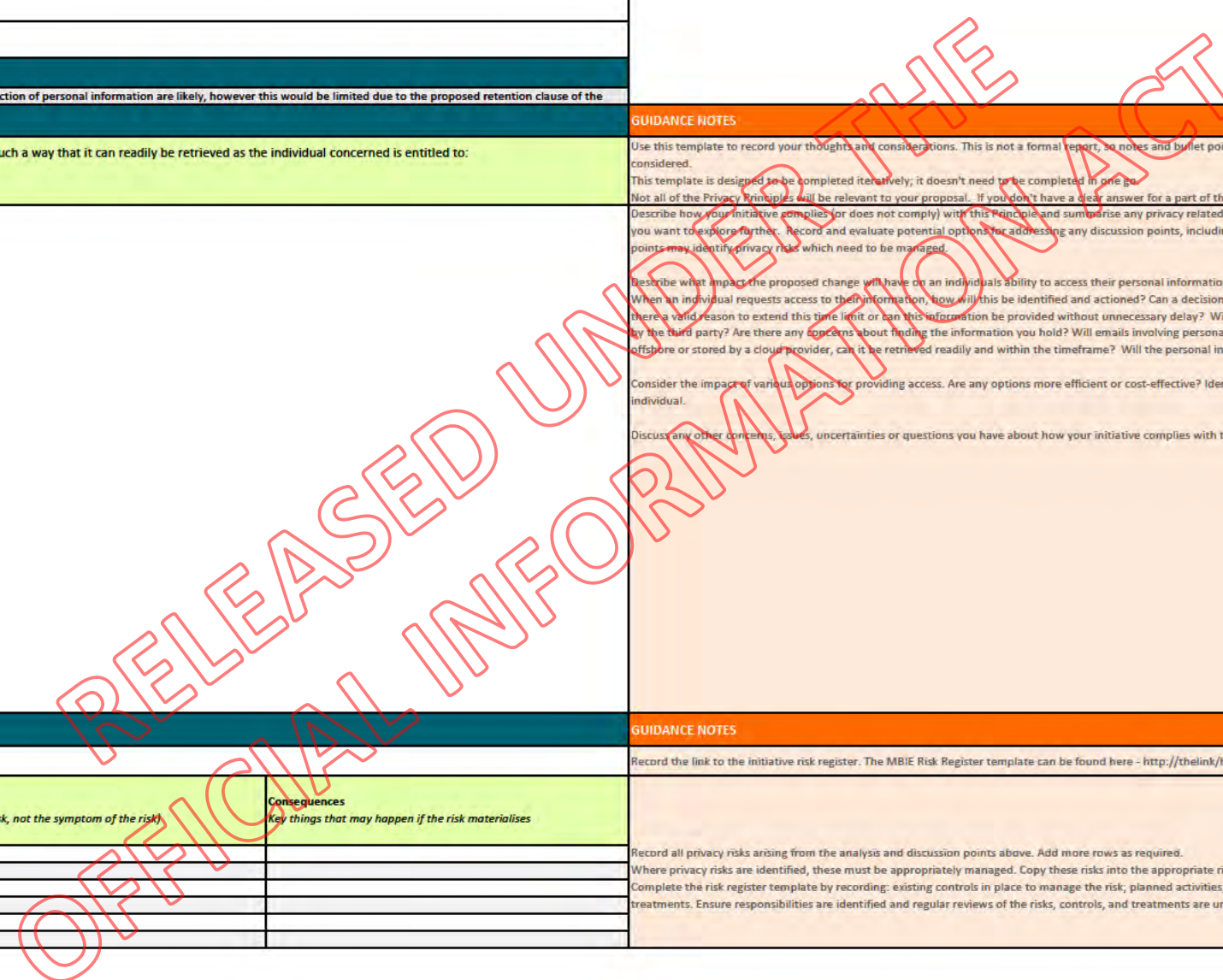
Record the link to the initiative risk register. The MBIE Risk Register template can be found here - <http://thelink/how/Pages/find-the-cpo-project-delivery-templates.aspx>

Risk Number	Risk Description <i>Description of the privacy risk (i.e.: the actual/root risk, not the symptom of the risk)</i>	Consequences <i>Key things that may happen if the risk materialises</i>
P6_1		
P6_2		
P6_3		
P6_4		
P6_5		
P6_6		

Record all privacy risks arising from the analysis and discussion points above. Add more rows as required.

Where privacy risks are identified, these must be appropriately managed. Copy these risks into the appropriate risk register (this may be the master initiative risk register, or a specific privacy risk register).

Complete the risk register template by recording: existing controls in place to manage the risk; planned activities, actions, roles, or programmes to treat the risk; and the outcome of the controls and treatments. Ensure responsibilities are identified and regular reviews of the risks, controls, and treatments are undertaken.



PRINCIPLE 7 - PRIVACY IMPACT ANALYSIS

Once you have completed the Data Flow template, information related to Principle 7 will be automatically copied to this worksheet. Refer to this information to help you to complete an Impact Analysis and identify the risks associated with Principle 7.

- If you have more than five categories on your Data Flow template, add more columns (to the right of column F) so the number of columns on this worksheet matches your Data Flow template. Copy the formula from column F to the new columns so the data from the Data Flow template is copied over.
- Complete the 'Initiative Details and Sign off' section (in white).
- Complete the 'Privacy Analysis and Discussion Points', and 'Risk Identification' sections (in white). Guidance notes are provided to the right in orange.
- Business owner sign off is required.



INITIATIVE DETAILS AND SIGN OFF	
Initiative name:	Mobile Caller Location
Brief description of initiative:	The MCL project will address longstanding operational requirements of Emergency Service Providers for probable caller location information from mobile phones. The outcome sought is for the best available caller location to be sent to an emergency service provider when a 111 call is made, without requiring the caller to do anything more than dial 111 on the standard keypad of their mobile phone.
Name and role of person completing template:	
Template completion date:	
Business owner name and sign-off:	

Information recorded on Data Flow Template	
Can an individual request a correction to their data and have the change actioned?	Individuals' requests for rights of access to and correction of personal information are likely, however this would be limited due to the proposed retention clause of the new Code that states that information may not be kept for longer than is necessary to establish the location of an emergency caller and facilitate the response to an

Privacy Analysis and Discussion Points

The key requirement of Principle 7 of the Privacy Act is to ensure that personal information held by an agency can be corrected because individuals are entitled to request:

- A correction be made to the information stored about them;
- A statement is attached to their information stating that a correction was sought, but not made.

--

GUIDANCE NOTES

Use this template to record your thoughts and considerations. This is not a formal report, so notes and bullet points are acceptable. The important part is to ensure all relevant considerations are recorded and considered.

This template is designed to be completed iteratively; it doesn't need to be completed in one go.

Not all of the Privacy Principles will be relevant to your proposal. If you don't have a clear answer for a part of the template or believe a Principle is not relevant, ensure this is noted.

Describe how your initiative complies (or does not comply) with this Principle and summarise any privacy related discussion points. Discussion points may include concerns, issues, uncertainties or questions you want to explore further. Record and evaluate potential options for addressing any discussion points, including identifying any options/solutions that enhance or could enhance privacy practices. Discussion points may identify privacy risks which need to be managed.

Describe what impact the proposed change will have on an individual's ability to correct their personal information if it is incorrect. Note if the where existing capability will be improved by the initiative. When an individual requests correction of their information, how will this be identified and actioned? Consider who can make corrections and in what circumstances.

Are there any concerns about how information can be located and modified? If information is archived offshore, or stored by a cloud provider, can it be retrieved readily to correct it? Can personal information be verified before you correct it and will a process be in place to do so? Can changes to information be monitored and recorded? If changes will not be made when requested, can you ensure a statement of correction is included with an individual's personal information? Will it always be clear that a statement of correction exists? Can personal information disclosed to other parties be corrected to ensure all records stored are accurate?

Discuss any other concerns, issues, uncertainties or questions you have about how your initiative complies with this principle.

Risk Identification

Link to Risk Register

Risk Number	Risk Description <i>Description of the privacy risk (i.e.: the actual/root risk, not the symptom of the risk)</i>	Consequences <i>Key things that may happen if the risk materialises</i>
P7_1		
P7_2		
P7_3		
P7_4		
P7_5		
P7_6		

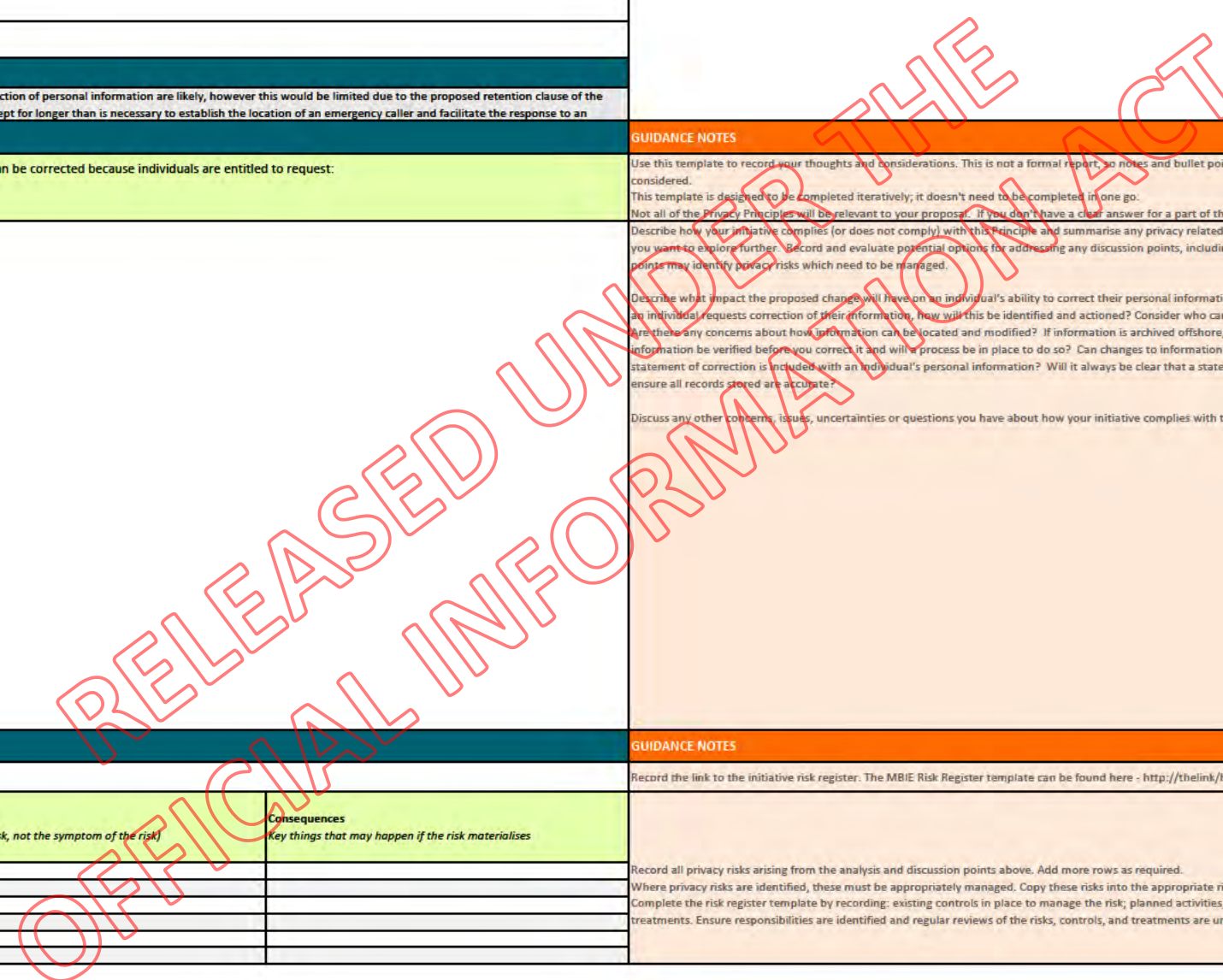
GUIDANCE NOTES

Record the link to the initiative risk register. The MBIE Risk Register template can be found here - <http://thelink/how/Pages/find-the-cpo-project-delivery-templates.aspx>

Record all privacy risks arising from the analysis and discussion points above. Add more rows as required.

Where privacy risks are identified, these must be appropriately managed. Copy these risks into the appropriate risk register (this may be the master initiative risk register, or a specific privacy risk register).

Complete the risk register template by recording: existing controls in place to manage the risk; planned activities, actions, roles, or programmes to treat the risk; and the outcome of the controls and treatments. Ensure responsibilities are identified and regular reviews of the risks, controls, and treatments are undertaken.



PRINCIPLE 8 - PRIVACY IMPACT ANALYSIS

Once you have completed the Data Flow template, information related to Principle 8 will be automatically copied to this worksheet. Refer to this information to help you to complete an Impact Analysis and identify the risks associated with Principle 8.

- If you have more than five categories on your Data Flow template, add more columns (to the right of column F) so the number of columns on this worksheet matches your Data Flow template. Copy the formula from column F to the new columns so the data from the Data Flow template is copied over.
- Complete the 'Initiative Details and Sign off' section (in white).
- Complete the 'Privacy Analysis and Discussion Points', and 'Risk Identification' sections (in white). Guidance notes are provided to the right in orange.
- Business owner sign off is required.



INITIATIVE DETAILS AND SIGN OFF	
Initiative name:	Mobile Caller Location
Brief description of initiative:	The MCL project will address longstanding operational requirements of Emergency Service Providers for probable caller location information from mobile phones. The outcome sought is for the best available caller location to be sent to an emergency service provider when a 111 call is made, without requiring the caller to do anything more than dial 111 on the standard keypad of their mobile phone.
Name and role of person completing template:	
Template completion date:	
Business owner name and sign-off:	

Information recorded on Data Flow Template

Will the accuracy of data collected be verified before it is used? The location data is the probable location of a caller and not a definitive location, for example an address. In order for an emergency response to be dispatched the

Privacy Analysis and Discussion Points

The key requirement of Principle 8 of the Privacy Act is an agency that holds personal information must take reasonable steps to ensure that information is accurate, up to date, complete, relevant and not misleading before using it.

--

GUIDANCE NOTES

Use this template to record your thoughts and considerations. This is not a formal report, so notes and bullet points are acceptable. The important part is to ensure all relevant considerations are recorded and considered.

This template is designed to be completed iteratively; it doesn't need to be completed in one go.

Describe how your initiative complies (or does not comply) with this Principle and summarise any privacy related discussion points. Discussion points may include concerns, issues, uncertainties or questions you want to explore further. Record and evaluate potential options for addressing any discussion points, including identifying any options/solutions that enhance or could enhance privacy practices. Discussion points may identify privacy risks which need to be managed.

Describe the impact your initiative will have on any existing processes that ensure accuracy. These should focus on whether or not the integrity of personal information is impacted, positively or negatively by this initiative or change. Will individuals provide their information directly and will they have the ability to verify their information is accurate before it is used, stored or disclosed? Can they routinely update their information? What would the impact be on the individual if their information was not accurate, or up to date, and is used for this initiative? If databases are held or development is conducted offshore with third parties, are appropriate processes in place to verify accuracy of personal information before implementation? How will information that changes over time (such as marital status, financial, health or address details) be kept up to date? Will your initiative ensure that any personal information disclosed to third parties is also corrected to ensure all records are accurate? If individuals have the same or similar name, how can you be sure personal information is attributed to the correct individual? Note if there is an intention to rely on automated decision-making based on the information provided.

Your IT stakeholders should be able to advise you on what steps are taken to verify data integrity for an existing system and what is proposed for a new initiative. Additionally, your business analysts should recommend processes to ensure accuracy is maintained.

Risk Identification

Link to Risk Register

Risk Number	Risk Description <i>Description of the privacy risk (i.e.: the actual/root risk, not the symptom of the risk)</i>	Consequences <i>Key things that may happen if the risk materialises</i>
P8_1		
P8_2		
P8_3		
P8_4		
P8_5		
P8_6		

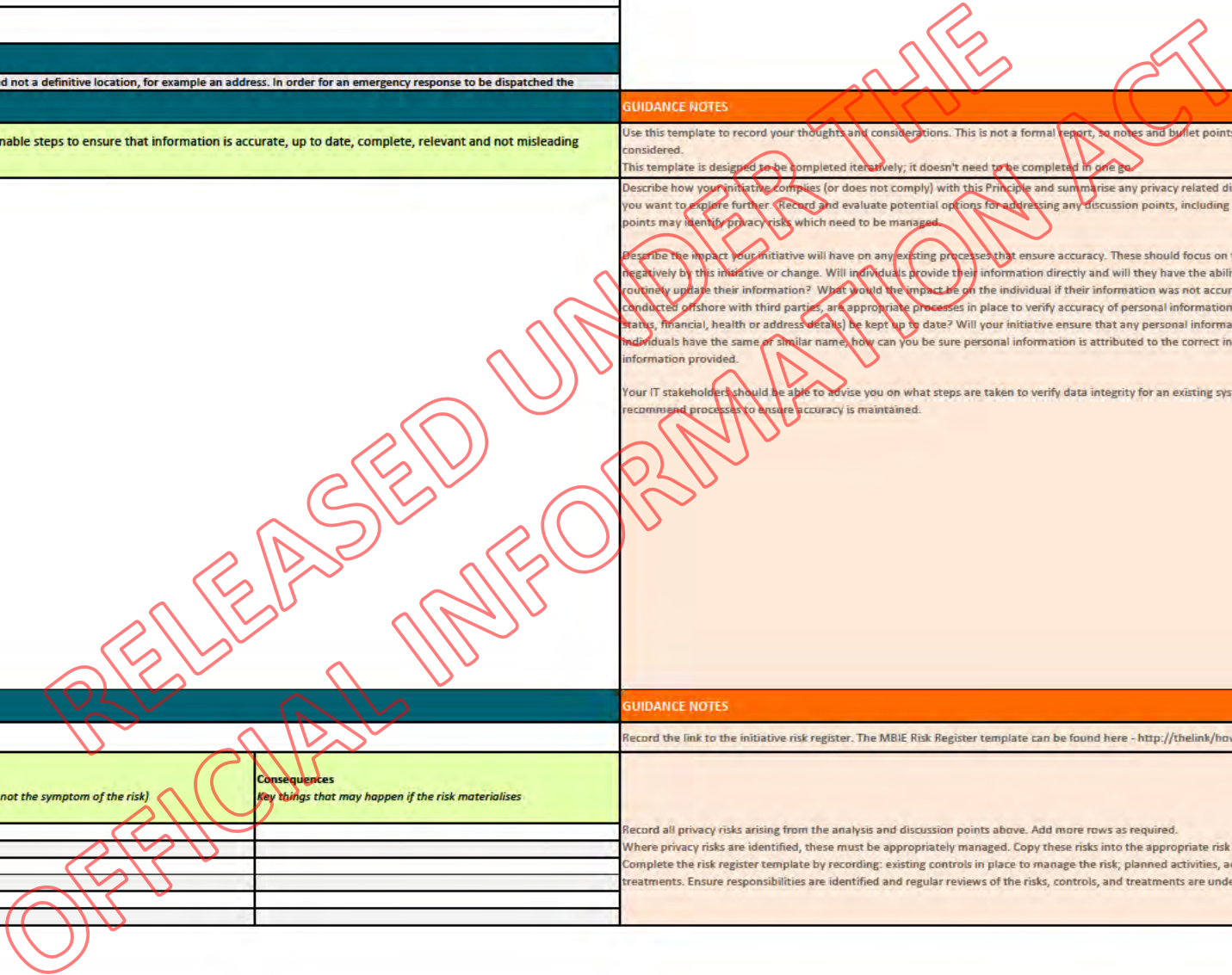
GUIDANCE NOTES

Record the link to the initiative risk register. The MBIE Risk Register template can be found here - <http://thelink/how/Pages/find-the-cpo-project-delivery-templates.aspx>

Record all privacy risks arising from the analysis and discussion points above. Add more rows as required.

Where privacy risks are identified, these must be appropriately managed. Copy these risks into the appropriate risk register (this may be the master initiative risk register, or a specific privacy risk register).

Complete the risk register template by recording: existing controls in place to manage the risk; planned activities, actions, roles, or programmes to treat the risk; and the outcome of the controls and treatments. Ensure responsibilities are identified and regular reviews of the risks, controls, and treatments are undertaken.



PRINCIPLE 10 - PRIVACY IMPACT ANALYSIS

Once you have completed the Data Flow template, information related to Principle 10 will be automatically copied to this worksheet. Refer to this information to help you to complete an Impact Analysis and identify the risks associated with Principle 10.

- If you have more than five categories on your Data Flow template, add more columns (to the right of column F) so the number of columns on this worksheet matches your Data Flow template. Copy the formula from column F to the new columns so the data from the Data Flow template is copied over.
- Complete the 'Initiative Details and Sign off' section (in white).
- Complete the 'Privacy Analysis and Discussion Points', and 'Risk Identification' sections (in white). Guidance notes are provided to the right in orange.
- Business owner sign off is required.



INITIATIVE DETAILS AND SIGN OFF	
Initiative name:	Mobile Caller Location
Brief description of initiative:	The MCL project will address longstanding operational requirements of Emergency Service Providers for probable caller location information from mobile phones. The outcome sought is for the best available caller location to be sent to an emergency service provider when a 111 call is made, without requiring the caller to do anything more than dial 111 on the standard keypad of their mobile phone.
Name and role of person completing template:	
Template completion date:	
Business owner name and sign-off:	

Information recorded on Data Flow Template	
List any additional uses for the data you are collecting	None additional

Privacy Analysis and Discussion Points

The key requirement of Principle 10 of the Privacy Act is that personal information obtained by an agency for one purpose shall not be used for any other purpose, unless it believes on reasonable grounds that the specified exceptions apply.

--

GUIDANCE NOTES

Use this template to record your thoughts and considerations. This is not a formal report, so notes and bullet points are acceptable. The important part is to ensure all relevant considerations are recorded and considered.

This template is designed to be completed iteratively; it doesn't need to be completed in one go.

Describe how your initiative complies (or does not comply) with this Principle and summarise any privacy related discussion points. Discussion points may include concerns, issues, uncertainties or questions you want to explore further. Record and evaluate potential options for addressing any discussion points, including identifying any options/solutions that enhance or could enhance privacy practices. Discussion points may identify privacy risks which need to be managed.

Consider if the original purpose is clearly defined and whether the intended use of the information is consistent with the purpose/s it was collected for (refer to your purposes discussed in Principle 1). If an intended use is not consistent with the purpose for collection, consider whether one of the exceptions in the Principle applies and record your reasoning. It is recommended that you check with your PIA guru or Principal Privacy Adviser to confirm this. Justifiable exceptions include:

- The information source is publicly available and it is not unfair or unreasonable to use the information;
- Authorisation has been obtained from the individual;
- The purpose is directly related to the purpose information was originally collected for;
- To protect public revenue, maintain the law, or for court proceedings;
- To protect public health or safety, or the life or health of the individual concerned or another individual;
- Individuals cannot be identified (i.e. anonymised), or it is used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify an individual.

Do you have authorised or legislative reasons for using the information for a different purpose?

When you are thinking about the use of information and if the intended use is different to the purpose you originally collected it for, consider: should individuals be notified if the intended purpose is different to the original purpose? What is the plan to notify them? Do third party contractual arrangements need to be amended if the intended use of personal information is changed? Is it possible to restrict the use of the personal information so that it can't be used for other purposes? Will staff have appropriate training on what is/isn't acceptable use of personal information?

Consider what opportunities are available for other functions or Groups in MBIE. Consider whether the information could be useful for customer/client services, policy analysis, regulatory enforcement, or other activities conducted by MBIE.

Discuss any other concerns, issues, uncertainties or questions you have about how your initiative complies with this principle.

Risk Identification

Link to Risk Register

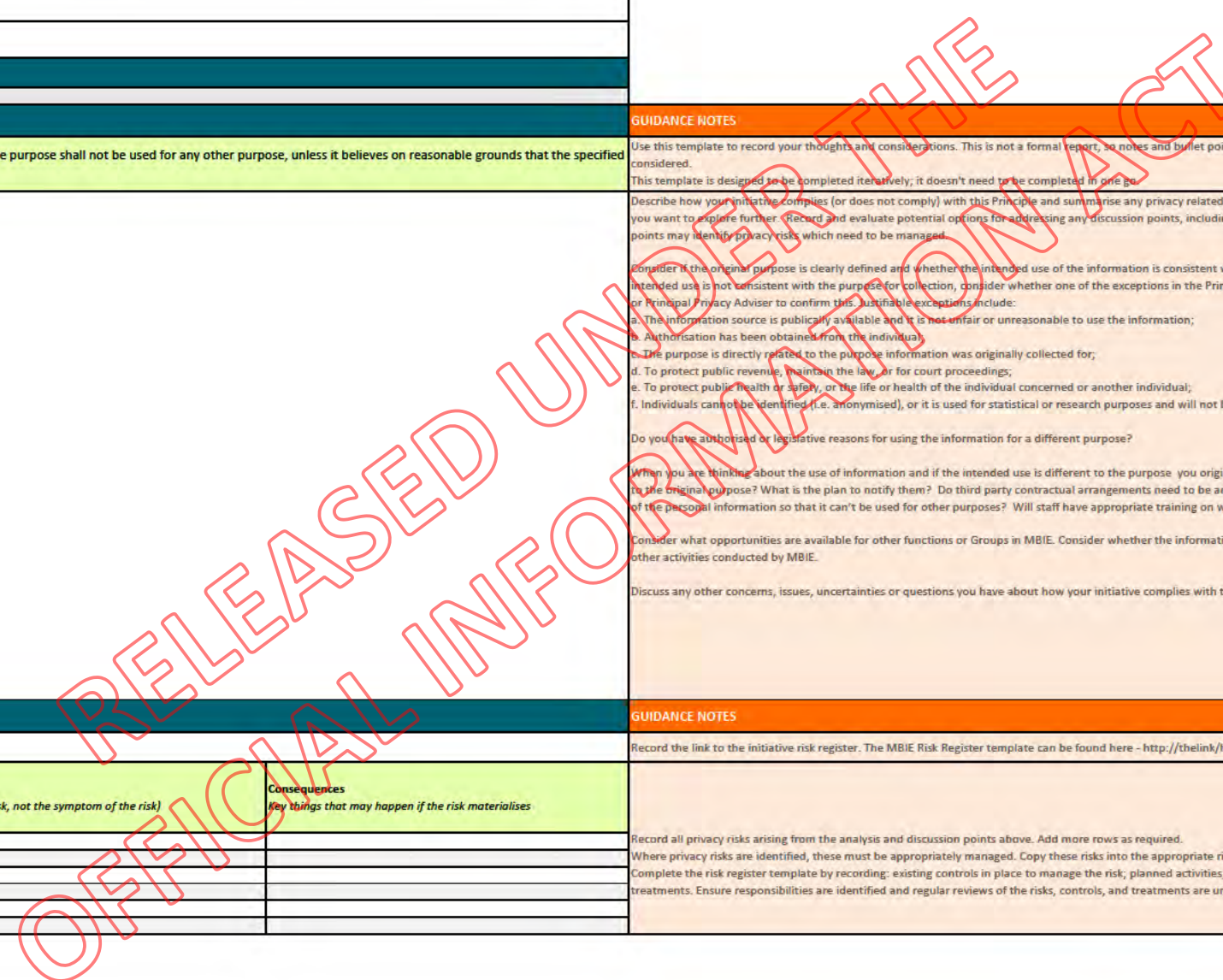
Risk Number	Risk Description <i>Description of the privacy risk (i.e.: the actual/root risk, not the symptom of the risk)</i>	Consequences <i>Key things that may happen if the risk materialises</i>
P10_1		
P10_2		
P10_3		
P10_4		
P10_5		
P10_6		

GUIDANCE NOTES

Record the link to the initiative risk register. The MBIE Risk Register template can be found here - <http://thelink/how/Pages/find-the-cpo-project-delivery-templates.aspx>

Record all privacy risks arising from the analysis and discussion points above. Add more rows as required.

Where privacy risks are identified, these must be appropriately managed. Copy these risks into the appropriate risk register (this may be the master initiative risk register, or a specific privacy risk register). Complete the risk register template by recording: existing controls in place to manage the risk; planned activities, actions, roles, or programmes to treat the risk; and the outcome of the controls and treatments. Ensure responsibilities are identified and regular reviews of the risks, controls, and treatments are undertaken.



PRINCIPLE 11 - PRIVACY IMPACT ANALYSIS

Once you have completed the Data Flow template, information related to Principle 11 will be automatically copied to this worksheet. Refer to this information to help you to complete an Impact Analysis and identify the risks associated with Principle 11.

- If you have more than five categories on your Data Flow template, add more columns (to the right of column F) so the number of columns on this worksheet matches your Data Flow template. Copy the formula from column F to the new columns so the data from the Data Flow template is copied over.
- Complete the 'Initiative Details and Sign off' section (in white).
- Complete the 'Privacy Analysis and Discussion Points', and 'Risk Identification' sections (in white). Guidance notes are provided to the right in orange.
- Business owner sign off is required.



INITIATIVE DETAILS AND SIGN OFF	
Initiative name:	Mobile Caller Location
Brief description of initiative:	The MCL project will address longstanding operational requirements of Emergency Service Providers for probable caller location information from mobile phones. The outcome sought is for the best available caller location to be sent to an emergency service provider when a 111 call is made, without requiring the caller to do anything more than dial 111 on the standard keypad of their mobile phone.
Name and role of person completing template:	
Template completion date:	
Business owner name and sign-off:	

Information recorded on Data Flow Template	
List any additional disclosure of the data you foresee	None additional

Privacy Analysis and Discussion Points

The key requirement of Principle 11 of the Privacy Act is that an agency shall not disclose personal information unless the agency believes, on reasonable grounds, one of the exceptions apply.

--	--

GUIDANCE NOTES

Use this template to record your thoughts and considerations. This is not a formal report, so notes and bullet points are acceptable. The important part is to ensure all relevant considerations are recorded and considered. This template is designed to be completed iteratively; it doesn't need to be completed in one go.

Describe how your initiative complies (or does not comply) with this Principle and summarise any privacy related discussion points. Discussion points may include concerns, issues, uncertainties or questions you want to explore further. Record and evaluate potential options for addressing any discussion points, including identifying any options/solutions that enhance or could enhance privacy practices. Discussion points may identify privacy risks which need to be managed.

Disclosure may involve wider data sharing with other government agencies, private sector agencies, or overseas agencies. This is permitted as long as disclosure complies with the exceptions provided in the principle. Exceptions should be considered on a case by case basis and should not be applied in a wholesale manner to justify extended disclosure to other parties. The exceptions include:

- Disclosure is one of the purposes with which the information was obtained, or is directly related to one of the purposes with which it was collected for;
- Disclosure to the individual the information is about;
- Individuals have authorised you to disclose their information to another organisation;
- Information was from a publicly available source, and it would not be unfair or unreasonable to disclose the information;
- Disclosure is necessary to avoid prejudice to the maintenance of the law by any public sector agency;
- Information will be used in a form which individuals are not identified;
- Information is being used for statistical or research purposes and will not be published in a form where the individuals will be identified in any way.

Consider if the original purpose is clearly defined and whether the intended disclosure of the information is consistent with the purpose/s it was collected for (refer to your purposes discussed in Principle 1). If an intended disclosure is not consistent with the purpose for collection, consider whether one of the exceptions in the Principle applies and record your reasoning. It is recommended that you check with your PIA guru or Principal Privacy Adviser to confirm this.

Your initiative may need additional permissions to disclose information for other purposes. Will individuals be told about the disclosure for a new purpose? Describe how they will be notified. Where individuals are asked for authorisation, describe how the authorisation will be obtained and what the record of the consent will be.

Consider if there are any plans in place to manage potential scope creep in the disclosure of personal information - this is relevant for both changes to existing and for newly proposed initiatives. Have you identified any controls or systems in place that will help manage the use of the information by the third parties once it has been disclosed? Can the third party disclose the information to another party? Are there protocols in place for determining when it is appropriate to disclose the information to another party, either directly or by the third party?

Consider whether the arrangements in place to manage the disclosure are proportionate to the risk the disclosure poses. Does the party receiving the information have sufficient safeguards in place to protect the information when in their care? Are there arrangements in place if the recipient commits a breach? Is the oversight of the disclosure arrangements sufficient to provide MBIE will assurance? Consider the capability of the staff members responsible for disclosing the information. Do you think staff will be appropriately trained on what is/isn't acceptable disclosure of personal information? What protocols will be in place to support the staff members undertaking the disclosure? Will staff members be able to determine when and what should be disclosed? Are delegations clear and in place (where required)? How will you ensure these are followed?

Discuss any other concerns, issues, uncertainties or questions you have about how your initiative complies with this principle.

Risk Identification

Link to Risk Register		
Risk Number	Risk Description <i>Description of the privacy risk (i.e.: the actual/root risk, not the symptom of the risk)</i>	Consequences <i>Key things that may happen if the risk materialises</i>
P11_1		
P11_2		
P11_3		
P11_4		
P11_5		
P11_6		

GUIDANCE NOTES

Record the link to the initiative risk register. The MBIE Risk Register template can be found here - <http://thelink/how/Pages/find-the-cpo-project-delivery-templates.aspx>

Record all privacy risks arising from the analysis and discussion points above. Add more rows as required.

Where privacy risks are identified, these must be appropriately managed. Copy these risks into the appropriate risk register (this may be the master initiative risk register, or a specific privacy risk register).

Complete the risk register template by recording: existing controls in place to manage the risk; planned activities, actions, roles, or programmes to treat the risk; and the outcome of the controls and treatments. Ensure responsibilities are identified and regular reviews of the risks, controls, and treatments are undertaken.



PRINCIPLE 12 - PRIVACY IMPACT ANALYSIS

Once you have completed the Data Flow template, information related to Principle 12 will be automatically copied to this worksheet. Refer to this information to help you to complete an Impact Analysis and identify the risks associated with Principle 12.

- If you have more than five categories on your Data Flow template, add more columns (to the right of column F) so the number of columns on this worksheet matches your Data Flow template. Copy the formula from column F to the new columns so the data from the Data Flow template is copied over.
- Complete the 'Initiative Details and Sign off' section (in white).
- Complete the 'Privacy Analysis and Discussion Points', and 'Risk Identification' sections (in white). Guidance notes are provided to the right in orange.
- Business owner sign off is required.



INITIATIVE DETAILS AND SIGN OFF	
Initiative name:	Mobile Caller Location
Brief description of initiative:	The MCL project will address longstanding operational requirements of Emergency Service Providers for probable caller location information from mobile phones. The outcome sought is for the best available caller location to be sent to an emergency service provider when a 111 call is made, without requiring the caller to do anything more than dial 111 on the standard keypad of their mobile phone.
Name and role of person completing template:	
Template completion date:	
Business owner name and sign-off:	

Information recorded on Data Flow Template	
List any unique identifiers being used and describe why it is necessary to use them	A unique identifier may be assigned to the probable caller location information for the purpose of enabling the location agency to audit and monitor the operation of the LAS and the methods by which the information is collected. Noting that identifiable data will not be retained.

Privacy Analysis and Discussion Points
 The key requirement of Principle 12 of the Privacy Act is that an agency shall not assign a unique identifier to an individual unless the assignment of that identifier is necessary to enable the agency to carry out one or more of its functions efficiently.

(This area is currently blank for user input.)

GUIDANCE NOTES

Use this template to record your thoughts and considerations. This is not a formal report, so notes and bullet points are acceptable. The important part is to ensure all relevant considerations are recorded and considered. This template is designed to be completed iteratively, it doesn't need to be completed in one go.

Describe how your initiative complies (or does not comply) with this Principle and summarise any privacy related discussion points. Discussion points may include concerns, issues, uncertainties or questions you want to explore further. Record and evaluate potential options for addressing any discussion points, including identifying any options/solutions that enhance or could enhance privacy practices. Discussion points may identify privacy risks which need to be managed.

Describe how the use of the unique identifier enables the initiative or activity to be carried out efficiently. Where unique identifiers are used to match data in different databases, describe why this is necessary.

Specific legal authority is required if you collect another unique ID and record it, and it must be necessary for the purpose of your initiative or change. Describe if there is an explicit legal authority to use unique IDs from another organisation (e.g. tax number, medical number or passport number). Record how it is necessary for the purpose of your initiative or activity.

Where an individual is required to provide or disclose their unique identifier, describe why it is required. Describe the consequences of the individual not providing their unique identifier, both for the individual and for the initiative or activity.

Consider whether the outcomes of your initiative can be achieved without assigning a unique identifier. Discuss any other concerns, issues, uncertainties or questions you have about how your initiative complies with this principle.

Risk Identification

Link to Risk Register		
Risk Number	Risk Description <i>Description of the privacy risk (i.e.: the actual/root risk, not the symptom of the risk)</i>	Consequences <i>Key things that may happen if the risk materialises</i>
P11_1		
P11_2		
P11_3		
P11_4		
P11_5		
P11_6		

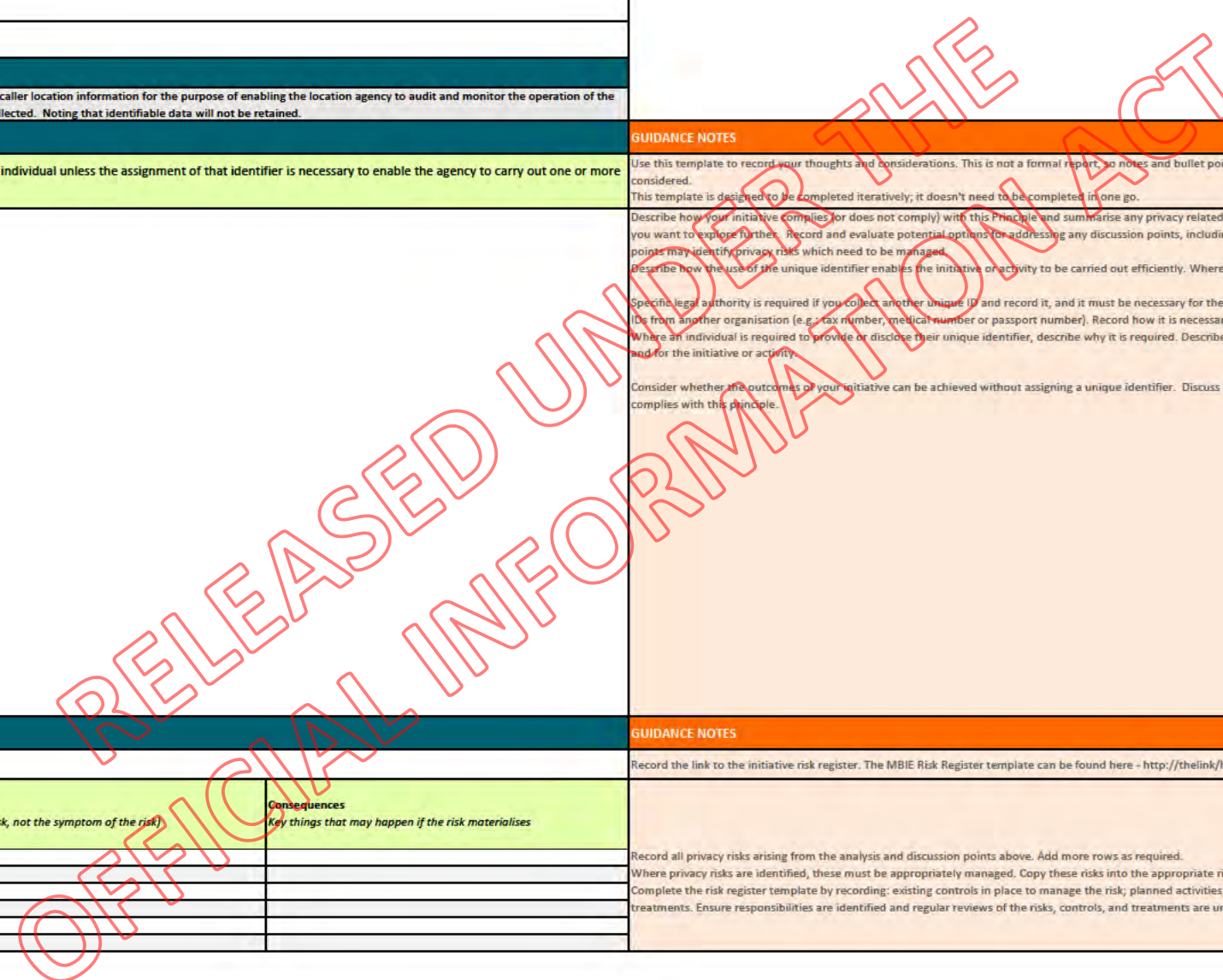
GUIDANCE NOTES

Record the link to the initiative risk register. The MBIE Risk Register template can be found here - <http://thelink/how/Pages/find-the-cpo-project-delivery-templates.aspx>

Record all privacy risks arising from the analysis and discussion points above. Add more rows as required.

Where privacy risks are identified, these must be appropriately managed. Copy these risks into the appropriate risk register (this may be the master initiative risk register, or a specific privacy risk register).

Complete the risk register template by recording: existing controls in place to manage the risk; planned activities, actions, roles, or programmes to treat the risk; and the outcome of the controls and treatments. Ensure responsibilities are identified and regular reviews of the risks, controls, and treatments are undertaken.



DATA FLOW TEMPLATE

If you are collecting personal information a Privacy Threshold Assessment (PTA) should have already been completed, as outlined in the *Conduct privacy impact assessment* process. If the PTA indicated a medium or high level of risk to individuals' privacy, complete the Data Flow template on this sheet by following these steps:



- Talk to a PIA guru, who can help you understand how to complete this template and who you can obtain the required information.
- Collect any documentation like data flow diagrams, use cases or architecture diagrams which explain how personal information currently flows, and how it is planned to flow.
- Obtain a list of all known data items that will be collected – including personal and non-personal data.
- Complete the white areas of the template. Guidance notes are provided to the right of each question in orange.
- 'Don't know' is a sufficient answer if details are not yet determined. This template is designed to be revisited as more details arise, or when there are changes or decisions that impact how the content is collected.
- You may want to consult with your architect, business analyst or project manager, or the Information and Data, Compliance, Risk and Intelligence, IT Security, Information Security, Records Management, Audit, Finance or Legal teams to answer some questions.
- Business owner sign off is required.

Once the Data Flow template is complete you will have enough information to complete the Privacy Impact Analysis. The success of the Impact Analysis will be determined by the quality of the details you collect in the Data Flow template.

INITIATIVE DETAILS AND SIGN OFF

Initiative name:	Emergency Caller Location Information : Phase 2 - iOS and Rebidding
Brief description of initiative:	The MCL project will address longstanding operational requirements of Emergency Service Providers for probable caller location information from mobile phones. The outcome sought is for the best available caller location to be sent to an emergency service provider when a 111 call is made, without requiring the caller to do anything more than dial 111 on the standard keypad of their mobile phone.
Name and role of person completing template:	Ben Quay, MCL Project Director
Template completion date:	31/08/2016 updated 27/02/2017, updated further 21/11/2017
Business owner name, role, and sign-off:	Brad Ward, GM CCC and ECLI business owner

PRINCIPLE 1 - Purpose of Collection of Personal Information

Only collect personal information if you have a justifiable purpose for it

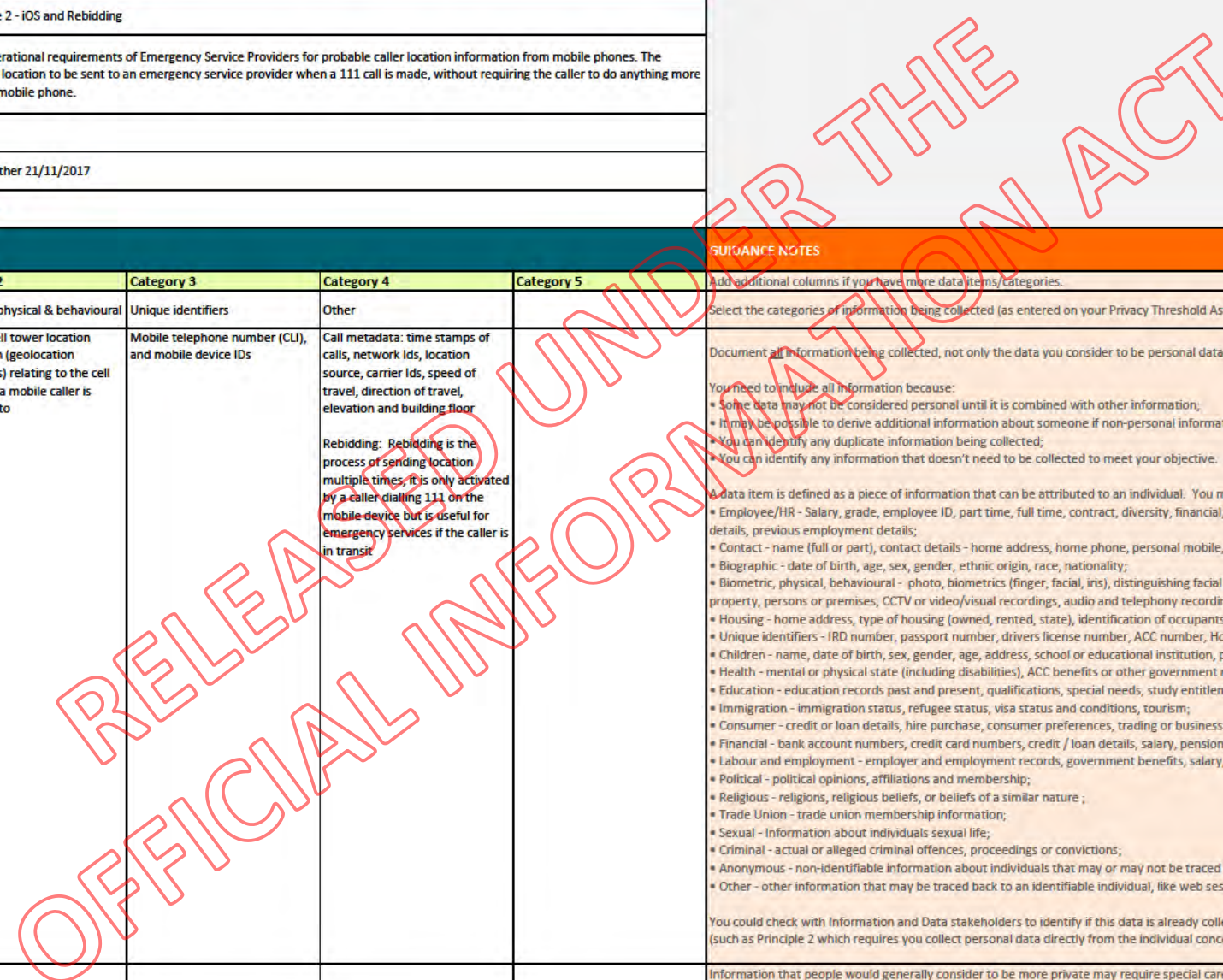
GUIDANCE NOTES


	Category 1	Category 2	Category 3	Category 4	Category 5	
What categories of personal information will be collected?	Biometric, physical & behavioural	Biometric, physical & behavioural	Unique identifiers	Other		Add additional columns if you have more data items/categories. Select the categories of information being collected (as entered on your Privacy Threshold Assessment).
List the data items that will be collected in each category	Emergency caller location information, includes geolocation coordinates, confidence and accuracy	Network cell tower location information (geolocation coordinates) relating to the cell tower that a mobile caller is connected to	Mobile telephone number (CLI), and mobile device IDs	Call metadata: time stamps of calls, network ids, location source, carrier ids, speed of travel, direction of travel, elevation and building floor Rebidding: Rebidding is the process of sending location multiple times, it is only activated by a caller dialling 111 on the mobile device but is useful for emergency services if the caller is in transit		Document all information being collected, not only the data you consider to be personal data. Add additional columns if necessary. You need to include all information because: <ul style="list-style-type: none"> • Some data may not be considered personal until it is combined with other information; • It may be possible to derive additional information about someone if non-personal information is included; • You can identify any duplicate information being collected; • You can identify any information that doesn't need to be collected to meet your objective. A data item is defined as a piece of information that can be attributed to an individual. You may be collecting many data items within each category. Examples of data fields (by category) are: <ul style="list-style-type: none"> • Employee/HR - Salary, grade, employee ID, part time, full time, contract, diversity, financial, benefits, appraisal, disciplinary, leave (parental, sick, holiday, study, sabbatical, other), tax, pension, education details, previous employment details; • Contact - name (full or part), contact details - home address, home phone, personal mobile, personal email; • Biographic - date of birth, age, sex, gender, ethnic origin, race, nationality; • Biometric, physical, behavioural - photo, biometrics (finger, facial, iris), distinguishing facial / body features, location information (surveillance, monitoring or tracking), disabilities, searching individuals' property, persons or premises, CCTV or video/visual recordings, audio and telephony recordings; • Housing - home address, type of housing (owned, rented, state), identification of occupants, special needs, building design and construction, energy resources and environment; • Unique identifiers - IRD number, passport number, drivers license number, ACC number, Housing number, Medical number, online identity number, other unique identifiers; • Children - name, date of birth, sex, gender, age, address, school or educational institution, parents / guardians, physical data; • Health - mental or physical state (including disabilities), ACC benefits or other government medical benefits, Medical records, health and safety; • Education - education records past and present, qualifications, special needs, study entitlements, visa status and conditions; • Immigration - immigration status, refugee status, visa status and conditions, tourism; • Consumer - credit or loan details, hire purchase, consumer preferences, trading or business details; • Financial - bank account numbers, credit card numbers, credit / loan details, salary, pension, government benefits; • Labour and employment - employer and employment records, government benefits, salary, pension, tax, benefits, work visas and conditions, employment law and relations; • Political - political opinions, affiliations and membership; • Religious - religions, religious beliefs, or beliefs of a similar nature ; • Trade Union - trade union membership information; • Sexual - Information about individuals sexual life; • Criminal - actual or alleged criminal offences, proceedings or convictions; • Anonymous - non-identifiable information about individuals that may or may not be traced back to an individual, including aggregated information, statistical, profiling information; • Other - other information that may be traced back to an identifiable individual, like web session information. You could check with Information and Data stakeholders to identify if this data is already collected within MBIE and could potentially be re-used, assuming the appropriate privacy principles are complied with (such as Principle 2 which requires you collect personal data directly from the individual concerned, unless an approved exception is in place.
Which data items require special care?	All	All	All	All		Information that people would generally consider to be more private may require special care, i.e. they need higher levels of security safeguards when being handled because of their sensitive nature. Examples include information about salary, medical records and children. These are types of information more likely to result in harm to an individual, including significant emotional distress, if not appropriately safeguarded. By identifying the data items that may require special care, it will be easier during your assessment to see how a combination of many sensitive data items may mean your process, product, service or systems design may need to consider appropriate additional safeguards. If needed ask your PIA "guru" to help identify data items that may require special care.
Which data items have not been collected previously?	All	All	Mobile device Id. CLI is provided today	All		Identify the data items that you have not been collected before. Check with the Information and Data team to identify whether there is any future use for data that this initiative could collect
Describe the main reason (primary purpose) for collecting the data	Best available caller location to be sent to an emergency service provider when a 111 call is made, in order to assist in address verification of emergency events					Include any legislative or regulatory obligations as part of your primary purpose if applicable.
Describe any secondary or future purposes for collecting this data	None					Check with business stakeholders and the Information and Data team to identify if there is any future use for the data you will collect. This requires compliance with other Privacy Principles, such as Principles 2, 3 and 11. Consider how else the information could be used (refer to PTA answers).

PRINCIPLE 2 - Source of Personal Information

Collect information directly from the individual who it is about, whenever possible

Who are you collecting this information about?	Creators	Creators	Creators	Creators		Select the appropriate person from the drop down list for each data item.
--	----------	----------	----------	----------	--	---



<p>Will this data be collected directly from individuals, or another source? Note who the other sources are.</p>	<p>The information will be collected indirectly when a caller dials 111 from their mobile phone. Initially on Android phones, a hidden SMS text will be sent to a specific new emergency short-dial number, the SMS text will contain information relating to the callers probable location (note, only if a location can be established). For all phones (smart and older) the location of the cell tower receiving the 111 call, along with an approximate coverage radius, will be presented to Emergency Service call takers. There is no ability to turn-off this feature once the service is established.</p> <p>Phase 2 extends the service to provide a handset based solution for iOS 111 callers. The location capabilities and data are the same as that provided by Android's solution, however the key difference is that the mobile network recognises that an emergency call is being made and sends a Network Induced Location Request (NILR) the the phone, this triggers Apple's iOS solution to send location.</p>	<p>Note who each data item will be collected from. Examples of other sources are:</p> <ul style="list-style-type: none"> • A spreadsheet held internally or externally; • A public register; • Another system or application. <p>If it is a combination of sources, include the various sources you have identified, note which data items come from which source and note it is a combination.</p>
<p>PRINCIPLE 3 - Collection of Information If collecting directly from the individual, tell them about it</p>		
<p>Which data items are mandatory or considered compulsory to collect?</p>	<p>All data elements are required as collectively they establish the probable location area of a caller</p>	<p>List the data fields that are mandatory to collect and describe why. Consider the initiative's primary purpose to determine which data is mandatory. Note any legal reason requiring the collection of certain data items.</p>
<p>How will you tell individuals about the collection of their information?</p>	<p>A new Code of Practice TIPC #5 is in force, published by the Privacy Commissioner. See https://privacy.org.nz/the-privacy-act-and-codes/codes-of-practice/telecommunications-information-privacy-code/amendments-and-other-information-on-the-telecommunications-information-privacy-code/</p> <p>ECLI is regulated service and has privacy safeguards in place, as obligated by the TIPC. The TIPC requires location agencies to publish information on their websites about the service, how their data is collected, used, retained and disposed. The TIPC does not require emergency services to advise callers to 111 that their location information is being used.</p>	<p>Include:</p> <ul style="list-style-type: none"> • Whether individuals already know we will be collecting this information about them; • Whether there are any existing MBIE privacy policies, notifications or statements that could be used (and if so, provide links to applicable documentation); • If you are unsure whether any applicable documentation exists; • If you know that no documentation exists and it needs to be drafted. <p>Your PIA "guru" or Legal should be able to help find existing privacy notices, statements or policies that may be relevant.</p>
<p>When will you tell individuals about the collection of their information?</p>	<p>As above. It is not intended that emergency service call takers will advise callers that their location information has been collected as this will add time to an emergency call and may cause delay in dispatching a response. Also, the caller information may not be required, in all cases, to establish location.</p>	<p>Specify whether you will tell individuals before you collect their information, during the process of collection or after the collection. If you are considering not telling them - describe why.</p>
<p>PRINCIPLE 4 - Manner of Collection of Personal Information Be considerate, be fair and don't intrude</p>		
<p>How will this data be collected?</p>	<p>By a mobile caller activating the NZ 111 service by dialling 111 on a mobile device.</p> <p>For Android phones, a hidden SMS text will be sent with the best available probable caller location.</p> <p>For all mobile phones, the cell tower id receiving the 111 call will be sent from the mobile network to a location area service (LAS), the LAS derives the geolocation</p> <p>Phase 2 extends the service to provide a handset based solution for iOS 111 callers. The location capabilities and data are the same as that provided by Android's solution, however the key difference is that the mobile network recognises that an emergency call is being made and sends a Network Induced Location Request (NILR) the the phone, this triggers Apple's iOS solution to send location.</p>	<p>List the format and manner data will be collected. Examples include:</p> <ul style="list-style-type: none"> • Electronic transfer from an existing database that holds this information; • Paper forms completed by the individual, or on behalf of the individual by another party; • Online forms on MBIE's public websites completed by the individual, or on behalf of the individual by another party; • Spreadsheets held in MBIE; • Publicly available registers; • Video footage; • Sound recordings; • CCTV or moving footage/images; • Biometric files or still photographic images; • From private property or devices. <p>The Information and Data team, and your architect and business analyst should be able to assist with how data is collected.</p>
<p>Attach any diagrams which show how the information will flow</p>		<p>Examples include:</p> <ul style="list-style-type: none"> • System and infrastructure architecture diagrams - which will illustrate the security mechanisms that will prevent improper access and maintain any separation of information if required. • Process diagrams - which will help you understand the proposed business processes and assess how the business intends to manage the information collected. A process diagram should identify the major components of the business processes and how personal information is collected, used, disclosed and retained through the process. It should also show what the outcome of the processing is; • Data models and data flow diagrams. <p>Internal and external parties should be represented in the maps or diagrams. Future state diagrams should indicate the changes resulting from this initiative - such as any new third parties, data flowing outside of the organisation that didn't previously, or outside of the country.</p> <p>Your business analyst, architect or Information Security teams should be able to assist you.</p>
<p>PRINCIPLE 5 - Storage and Security of Personal Information Once you have information, look after it. Protect it against loss, unauthorised access, use, modification or disclosure and other misuse</p>		
<p>What data fields will be retained and stored and what format will they be stored in?</p>	<p>All data fields described will be retained and stored for no longer than is necessary to establish the location of an emergency caller and facilitate the response to an emergency. Currently all PII is purged after 60mins for the time it is received in the Location Area Service, no PII is stored in audit</p>	<p>Note where data fields will not be stored. Describe whether storage will be electronic, physical, or both. Examples of:</p> <ul style="list-style-type: none"> • Electronic formats are - text-based documents, spreadsheets, images, photos or diagrams, data tables, sound recordings, still images and moving images; • Physical formats are - paper, image-printed, film-negative, slide, reel or tape, sound-reel or tape and microfilm. <p>Your architect, business analyst or Information and Data team can help with this.</p>
<p>Where will data be stored and who will be responsible for keeping it safe during storage?</p>	<p>OIA 9(2)(c)</p> <p>MBIE is the controller of this service.</p>	<p>Describe:</p> <ul style="list-style-type: none"> • Whether any of the data will be encrypted if it is stored electronically; • What safeguards are in place to protect the data if it is stored physically; • The names of internal/external parties responsible for ensuring data is protected when stored; • If data is stored in shared storage facility like a data centre or physical storage facility. <p>Data must always be stored securely, and in some instances must be encrypted. Seek advice from Records Management and/or Security teams.</p>
<p>What controls will be in place to protect data in transit between internal/external parties?</p>	<p>OIA 9(2)(c)</p> <p>The service is regulated by the Telecommunications Information Privacy Code. The service has been certified and accredited by MBIE and Police using GCIO C&A process.</p>	<p>Safeguards are required to protect the data in transit. Security safeguards need to be appropriate and proportionate to the nature of the data being transferred. Information that requires special care will require additional safeguards to ensure appropriate protection from loss, unauthorised access, disclosure, or other misuse. Seek advice from IT and Security about the type of safeguards required. Examples of safeguards are:</p> <ul style="list-style-type: none"> • Encryption of email transfers; • Prohibiting the use of removable devices, like USB sticks; • Securing the IT network that information is transferred across.
<p>Who will have access to the data, who will it be disclosed to and what controls will be in place to protect it?</p>	<p>Emergency service provider call takers have access to the data for the specific needs of establishing probable caller location. Access logging and audit functionalities are also in place.</p> <p>There is no ability to activate location other than by a caller initiating an emergency call from their mobile device by dialling 111</p>	<p>Document all of the internal and external parties who will have access to the data, and the reason why access is required. Examples include:</p> <ul style="list-style-type: none"> • Individuals who access their data online to carry out a registration process; • Specific staff who access data to perform their role; • Specific internal or external people who access data to provide technical support or administer the service; • Staff at the data centre where data is stored who access data to support the data in storage; • Internal IT or Security staff, or external parties helping to develop, test, or train people on a new system; • Internal audit, investigations and/or compliance staff who audit information. <p>Also describe:</p> <ul style="list-style-type: none"> • How and where the various parties will access data from (e.g.: physical location could be remote, inside or outside of NZ, inside or outside of MBIE); • The type of equipment or device people will access data with (e.g.: MBIE issued IT or telephony equipment, third party equipment via VPN or Citrix session etc.). <p>The IT Security and Security teams can assist with identifying appropriate controls. Describe the security and access controls that will protect the data against unauthorised access. Note:</p> <ul style="list-style-type: none"> • What access and handling protocols will be in place (e.g.: access will be restricted to parties who have legal and business justification to access it and all access attempts will be logged); • Who has access to add, amend, or delete data; • Who has access to assign, change or revoke access privileges; • How remote access will be handled by internal or external parties.
<p>How often will data be accessed by third parties?</p>	<p>Access to the data is limited to Location Agencies, defined as LAS controller (MBIE), Mobile Network Operators, the Location Area Service provider and public safety organisations (e.g. Police, Fire, Wellington Free and St John ambulance).</p>	<p>Describe how frequently data will be accessed by third parties (e.g.: periodically, routinely, or ad-hoc). Confirm with the Security teams what safeguards may be required. These may differ depending on the regularity and the method of access.</p>
<p>What additional safeguards will be in place to protect the data?</p>	<p>See the Mobile Caller Location System Security Certificate & Business Risk Acceptance for details.</p> <p>The system is classified as Sensitive, OIA 9(2)(c)</p>	<p>List any other security safeguards that will be applied as data is collected, used, disclosed, stored, deleted and disposed. Seek advice from your business analyst and IT and Security teams. Examples of other safeguards are:</p> <ul style="list-style-type: none"> • Data Loss Prevention Tools - which minimise the risk that users send private, special or critical information outside MBIE's network by providing controls to determine what data can be transferred; • Email safeguards - like removing "reply all" functionality or removing automatically populated names; • Training users how to email data appropriately (e.g.: by authenticating who the data is being emailed to, checking email addresses for accuracy before sending and not opening unknown email from unidentified senders).
<p>What legal or other commercial safeguards are in place to protect the data?</p>	<p>A new Code of Practice TIPC #5 has been published by the Privacy Commissioner. See https://privacy.org.nz/the-privacy-act-and-codes/codes-of-practice/telecommunications-information-privacy-code/amendments-and-other-information-on-the-telecommunications-information-privacy-code/</p> <p>All commercial contracts established make reference to the Code and therefore collection, use, disclosure and retention of probable caller location information is in accordance with the code.</p>	<ul style="list-style-type: none"> • Identify any internal or external agreements which include appropriate privacy and security provisions and cover the collection and use of the personal information in use. • Attach any existing schedules, appendices, MoUs, or other contractually binding agreements that may deal with privacy, confidentiality and security. • Describe or attach any new legal contractual documentation or agreements that may be required for new third party relationships, internal or external. <p>Seek assistance from your PIA guru, Information and Data, Security or Legal teams.</p>

PRINCIPLE 6 - Access to Personal Information Individuals can get access to their information		
Can individuals access data about themselves upon request?	Individuals' requests for rights of access to and correction of personal information are possible, however this would be limited due to the retention clause of the Code that states that information may not be kept for longer than is necessary to establish the location of an emergency caller and facilitate the response to an emergency. PII is purged after 60mins from being received Therefore it is unlikely that a request could be fulfilled as the data would likely not exist.	<ul style="list-style-type: none"> Describe how an individual can access their data if they request it; Attach any operational processes or technical details illustrating how an individual will gain access to their data; Note if there are already any processes in place. Provide links to any MBIE process that should be used; Note if third parties may be asked by individuals to provide access to personal data they hold on behalf of MBIE, and if there is a process in place to handle this; Note if metadata is kept so personal information can be readily identified and located (metadata could be structural or descriptive data which helps identify where or how the data is held); Note if data will be kept in one or multiple places. <p>Your PIA guru, business analyst or Legal may be able to help with existing processes. Your business analyst, architect or Information and Data team can advise on the relevant technical capabilities available.</p>
PRINCIPLE 7 - Correction of Personal Information Individuals can get their information corrected		
Can an individual request a correction to their data and have the change actioned?	Individuals' requests for rights of access to and correction of personal information are possible, however this would be limited due to the proposed retention clause of the new Code that states that information may not be kept for longer than is necessary to establish the location of an emergency caller and facilitate the response to an emergency. PII is purged after 60mins from being received Therefore it is unlikely that a request could be fulfilled as the data would likely not exist.	<p>Include these things:</p> <ul style="list-style-type: none"> Describe how an individual can request correction of their personal information, how the information can be updated and/or how a record of the request will be held against the information for the subject of the request. Attach any operational processes or technical details illustrating how an individual can get their data corrected if they think it's wrong or requires updating; Note if there are already any processes in place. Provide links to any MBIE process that should be used; Note if there is a possibility that third parties may be asked directly by individuals to correct information they hold on behalf of MBIE, and if there is a process in place to handle this; Note if metadata is kept so personal information can be readily identified and located (metadata could be structural or descriptive data which helps identify where or how the data is held); Note if data will be kept in one or multiple places. <p>Your PIA guru or Legal may be able to help with existing process. Your business analyst, architect or Information and Data team can advise on the relevant technical capabilities available.</p>
PRINCIPLE 8 - Accuracy of Personal Information to be Checked before Use Information is checked for accuracy before being used		
Will the accuracy of data collected be verified before it is used?	The location data is the probable location of a caller and not a definitive location, for example an address. In order for an emergency response to be dispatched the location of the event must be confirmed by the caller, the location data is an additional method to assist in verifying the location.	Describe how the information you hold will be accurately linked to the correct person (similar multiple names, addresses etc. need to be considered). Describe how you will check that data is accurate, complete and up to date before it is used or disclosed. Your business analyst or architect may be able to advise you on this.
PRINCIPLE 9 - Personal Information not to be kept for longer than necessary Securely dispose of information when you no longer need it		
How long will the business retain the data for?	Information may not be kept for longer than is necessary to establish the location of an emergency caller and facilitate the response to an emergency. This period will initially be set at 60mins, in other jurisdiction this period has been reduced to 30mins	<p>Describe how long you need to keep information:</p> <ul style="list-style-type: none"> For business purposes; To meet legislative or public records requirements; For policy reasons; For data storage capacity reasons. <p>The Records Management team should be able to provide guidance.</p>
How will the data retention period be managed and controlled?	Automatically deleted by the LAS when the specified period is reached.	Describe (or attach documents if they are available) how data will be managed to ensure it will only be retained for the planned retention period. Is there a process in place to notify those who are storing personal data internally or externally to MBIE of deletion or destruction requirements when personal information should no longer be retained? Note if there is no operational process to manage and control the data retention period.
How will data disposal or archiving be managed and controlled at the end of the retention period?	There will be no archiving of identifiable data. A log that data was received will be retained but this will not contain personal information	Describe how the disposal of data will be managed securely at the end of the retention period. Outline if there is an authority/acknowledgement for approving disposal or archiving of data before the end of its agreed lifetime. The Records Management team should be able to provide guidance.
PRINCIPLE 10 - Limits on Use of Personal Information Only use information for the purpose you collect it for, unless one of the exceptions applies		
List any additional uses for the data you are collecting	None additional	<p>If there is a plan to use some or all of the personal information collected for a different purpose to what it was originally collected it for, describe:</p> <ul style="list-style-type: none"> What information will be used; Who will use it and what it will be used for, including how and why information will be used; If you will tell the individuals concerned that you are using the information for a different purpose; <p>Check with the Information and Data team also to see if there is a potential for additional use that could be considered, or if this personal data is already held and could be used by you for the purpose of this initiative.</p>
PRINCIPLE 11 - Limits on Disclosure of Personal Information Only disclose information if you have a valid reason, or one of the permitted exceptions applies		
List any additional disclosure of the data you foresee	None additional	<p>If there is a need to disclose personal information held for a different purpose to what it was collected it for, describe:</p> <ul style="list-style-type: none"> What information you might disclose; Who you might disclose it to and for what purpose; If you think you will need to create or change information sharing arrangements with other internal or external organisations; If you will tell the individuals concerned that you are disclosing to other parties; If there are MoUs in place or other similar agreements to enable the disclosure of information to other parties or if there are no agreements in place. The Legal team should be able to advise you. <p>Check with the Data and Information team also to see if there is a potential for additional disclosure that could be considered, or if this personal data is already held and could be disclosed to you for the purpose of this initiative.</p>
PRINCIPLE 12 - Unique Identifiers Assign unique identifiers only where permitted		
List any unique identifiers being used and describe why it is necessary to use them	A unique identifier is assigned to the probable caller location information for the purpose of enabling the location agency to audit and monitor the operation of the LAS and the methods by which the information is collected. Noting that identifiable data will not be retained.	<p>If you are using a unique identifier to identify individuals describe:</p> <ul style="list-style-type: none"> How it will be used and where the unique identifier has originated from; How and why the unique identifier will be used to link or match personal information across agencies (if applicable); Any agreements in place to enable the use of a unique identifier if it is provided by another internal/external party. The Legal team should be able to advise you.

RELEASED UNDER OFFICIAL INFORMATION ACT

8

Impact Analysis template

Introduction

This Impact Analysis template is a key part of MBIE's Privacy Impact Assessment Framework. The Framework provides guidance, examples and tools to support you assess and manage the impacts of a proposed action on individuals' privacy. It is structured to help you build your ideas and implement changes in such a way so as to achieve your objectives while ensuring individuals' personal information is protected. This will help to build and retain the trust of the individuals who provide us with their information, so we can legitimately and safely use personal information in order to *Grow New Zealand for All*.

The Impact Analysis is the second key tool of the Framework:

1. Privacy Threshold Assessment (PTA)
2. **Impact Analysis**
3. PIA Report.

Note: While the Framework won't fix any risks, it will help you identify them early, and to do your best to mitigate or remove them in a considered and proactive way.

Template guidance

When do I need to complete this template?

Use this template when a PTA determines that your initiative has a medium or high degree of privacy risk, to:

- * record how the personal information involved flows within and outside of MBIE; and
- * assess any potential privacy impacts against the 12 Principles of the Privacy Act.

Note: The template is designed to allow you to add and/or edit information as it becomes available or decisions are made.

How long will it take?

This will depend on your initiative and what you are trying to achieve. As a rough guide, initially allow at least 2-4 hours for a medium risk initiative, and 8-12 hours for a high risk one. This should give sufficient time to examine your initiative from a privacy perspective.

Who needs to be involved?

- * **A PIA guru:** A person trained in how to complete this exercise. They can provide guidance and examples to make your job easier.
- * **Any initiative stakeholders.** This could include: Business subject matter experts, project managers, ICT, Security, Risk and Assurance, Audit, Information and Data, Records Management, Facilities, Procurement, Human Resources, Finance and Legal staff. Additionally, external resources (such as vendors) should also be involved. Organise workshops, meetings and review sessions as required to ensure that risks are appropriately identified and managed.

Further information

For more detailed guidance, see the *Conduct privacy impact assessment* process on the Link.

PRINCIPLE 1 - PRIVACY IMPACT ANALYSIS

Once you have completed the Data Flow template, information related to Principle 1 will be automatically copied to this worksheet. Refer to this information to help you to complete an Impact Analysis and identify the risks associated with Principle 1.

- If you have more than five categories on your Data Flow template, add more columns (to the right of column F) so the number of columns on this worksheet matches your Data Flow template. Copy the formula from column F to the new columns so the data from the Data Flow template is copied over.
- Complete the 'Initiative Details and Sign off' section (in white).
- Complete the 'Privacy Analysis and Discussion Points', and 'Risk Identification' sections (in white). Guidance notes are provided to the right in orange.
- Business owner sign off is required.



INITIATIVE DETAILS AND SIGN OFF	
Initiative name:	Emergency Caller Location Information : Phase 2 - iOS and Rebidding
Brief description of initiative:	The MCL project will address longstanding operational requirements of Emergency Service Providers for probable caller location information from mobile phones. The outcome sought is for the best available caller location to be sent to an emergency service provider when a 111 call is made, without requiring the caller to do anything more than dial 111 on the standard keypad of their mobile phone.
Name and role of person completing template:	Ben Quay, MCL Project Director
Template completion date:	31/08/2016 updated 27/02/2017, updated further 21/11/2017
Business owner name and sign-off:	Brad Ward, GM CCC and ECU business owner

Information recorded on Data Flow Template					
	Category 1	Category 2	Category 3	Category 4	Category 5
What categories of personal information will be collected?	Biometric, physical & behavioural	Biometric, physical & behavioural	Unique identifiers	Other	
List the data items that will be collected in each category	Emergency caller location information, includes geolocation coordinates, confidence and accuracy	Network cell tower location information (geolocation coordinates) relating to the cell tower that a mobile caller is connected to	Mobile telephone number (CLI), and mobile device IDs	Call metadata, time stamps of calls, network ids, location source, carrier ids, speed of travel, direction of travel, elevation and building floor	
Which data items require special care?	All	All	All	All	
Which data items have not been collected previously?	All	All	Mobile device id. CLI is provided today	All	
Describe the main reason (primary purpose) for collecting the data	Best available caller location to be sent to an emergency service provider when a 111 call is made, in order to assist in address verification of emergency events				
Describe any secondary or future purposes for collecting this data	None				

Privacy Analysis and Discussion Points

Principle 1 of the Privacy Act states that personal information should only be collected if there is a justifiable purpose for it. The key requirements of Principle 1 are to:

- Identify all the personal data that will be collected and used by the proposed change or initiative;
- Be convinced that the personal information collected is necessary to meet the purpose of the proposed initiative. The purpose of the initiative or change must be lawful and connected with the business function or activity of the agency.

GUIDANCE NOTES

Use this template to record your thoughts and considerations. This is not a formal report, so notes and bullet points are acceptable. The important part is to ensure all relevant considerations are recorded and considered. This template is designed to be completed iteratively; it doesn't need to be completed in one go. Not all of the Privacy Principles will be relevant to your proposal. If you don't have a clear answer for a part of the template or believe a Principle is not relevant, ensure this is noted.

Describe how your initiative complies (or does not comply) with this Principle and summarise any privacy related discussion points. Discussion points may include concerns, issues, uncertainties or questions you want to explore further. Record and evaluate potential options for addressing any discussion points, including identifying any options/solutions that enhance or could enhance privacy practices. Discussion points may identify privacy risks which need to be managed.

Consider the purpose for which you are collecting personal information. If it is designed too narrowly, you may be unable to use information in the way that you and MBIE want in the future. If defined too broadly, the purposes risk becoming meaningless - MBIE could be collecting information it has no real need for and people could be confused. Consider any secondary purposes you, other parts of MBIE, or other agencies (Government and non-governmental) might have for the information. Does the collection allow for those purposes?

Describe whether you believe each data field is necessary for the proposed initiative and note the fields you consider to be unnecessary because the purpose of the initiative can be achieved without them. For example, if collecting an individual's name, do you require the middle name? Collecting the middle name adds another level of certainty about the individual's identity but if there are other fields being collected to achieve certainty, then it may not be necessary to obtain middle name as well. In this situation you would not collect middle name in order to comply with Principle 1.

Note if any personal data items being collected are particularly sensitive or may require special care and identify these. Data items that may require special care include things like personal information about an individual's health or alleged criminal activities, or information about children in refugee visa applications.

Explain if the personal information already collected will be used for a new, or different, purpose by your initiative. Note whether information already being collected is collected by the business function who owns the initiative, another MBIE function or a party outside of MBIE (Government Agency or otherwise).

Risk Identification

Link to Risk Register A full technical risk assessment, including consideration of Privacy risks, has been conducted for the MCL LAS solution. See <http://mako.wd.govt.nz/otcs/llisapi.dll/overview/69964471>

GUIDANCE NOTES

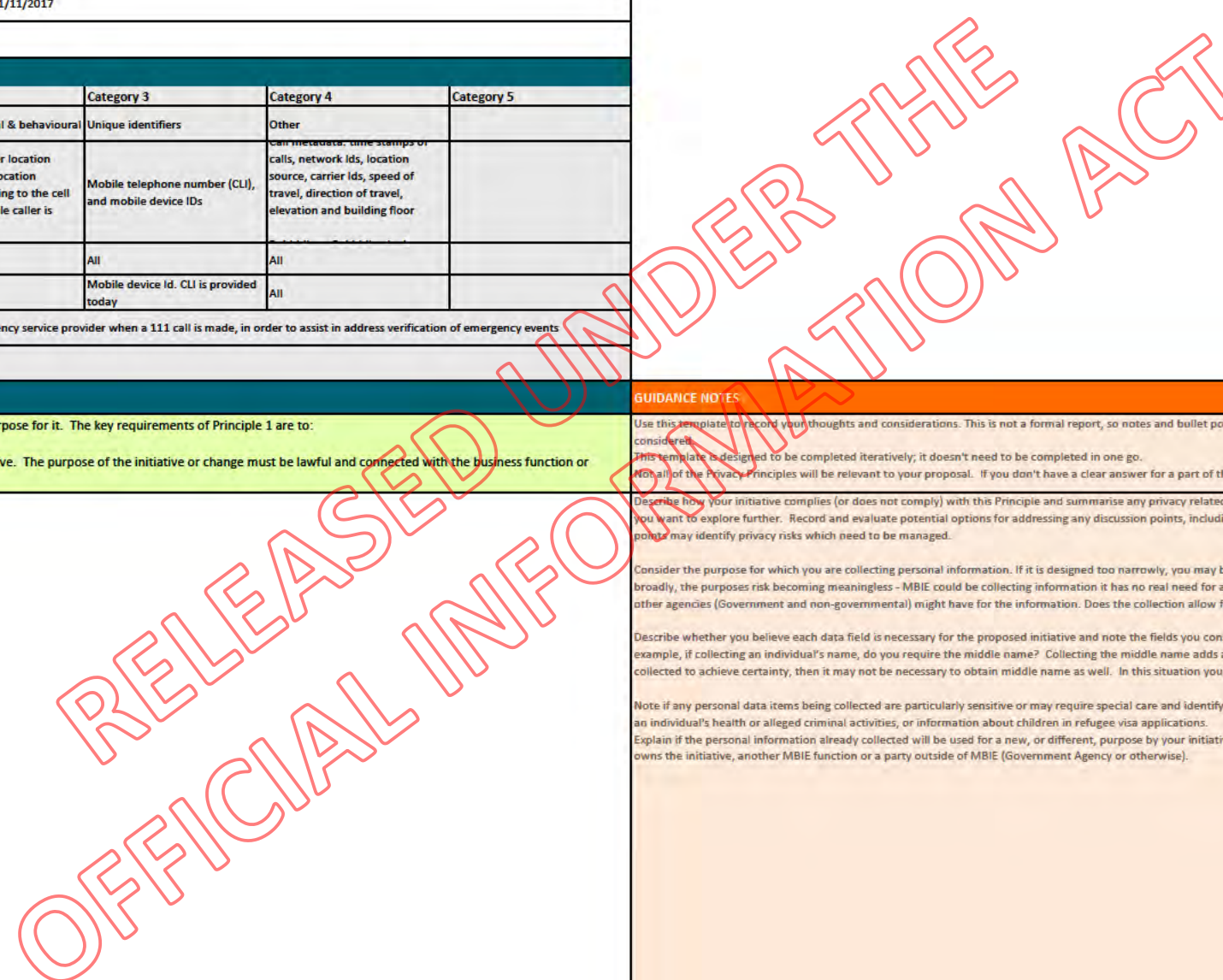
Record the link to the initiative risk register. The MBIE Risk Register template can be found here - <http://thelink/how/Pages/Find-the-cpo-project-delivery-templates.aspx>

Risk Number	Risk Description <i>Description of the privacy risk (i.e.: the actual/root risk, not the symptom of the risk)</i>	Consequences <i>Key things that may happen if the risk materialises</i>
-------------	--	--

P1_1		
P1_2		
P1_3		
P1_4		
P1_5		
P1_6		

Record all privacy risks arising from the analysis and discussion points above. Add more rows as required.

Where privacy risks are identified, these must be appropriately managed. Copy these risks into the appropriate risk register (this may be the master initiative risk register, or a specific privacy risk register). Complete the risk register template by recording: existing controls in place to manage the risk; planned activities, actions, roles, or programmes to treat the risk; and the outcome of the controls and treatments. Ensure responsibilities are identified and regular reviews of the risks, controls, and treatments are undertaken.



PRINCIPLE 2 - PRIVACY IMPACT ANALYSIS

Once you have completed the Data Flow template, information related to Principle 2 will be automatically copied to this worksheet. Refer to this information to help you to complete an Impact Analysis and identify the risks associated with Principle 2.

- If you have more than five categories on your Data Flow template, add more columns (to the right of column F) so the number of columns on this worksheet matches your Data Flow template. Copy the formula from column F to the new columns so the data from the Data Flow template is copied over.
- Complete the 'Initiative Details and Sign off' section (in white).
- Complete the 'Privacy Analysis and Discussion Points', and 'Risk Identification' sections (in white). Guidance notes are provided to the right in orange.
- Business owner sign off is required.



INITIATIVE DETAILS AND SIGN OFF	
Initiative name:	Emergency Caller Location Information : Phase 2 - iOS and Rebidding
Brief description of initiative:	The MCL project will address longstanding operational requirements of Emergency Service Providers for probable caller location information from mobile phones. The outcome sought is for the best available caller location to be sent to an emergency service provider when a 111 call is made, without requiring the caller to do anything more than dial 111 on the standard keypad of their mobile phone.
Name and role of person completing template:	Ben Quay, MCL Project Director
Template completion date:	31/08/2016 updated 27/02/2017, updated further 21/11/2017
Business owner name and sign-off:	Brad Ward, GM CCC and ECU business owner

Information recorded on Data Flow Template					
	Category 1	Category 2	Category 3	Category 4	Category 5
Who are you collecting this information about?	Creators	Creators	Creators	Creators	
Will this data be collected directly from individuals, or another source? Note who the other sources are.	The information will be collected indirectly when a caller dials 111 from their mobile phone. Initially on Android phones, a hidden SMS text will be sent to a specific new emergency short-dial number, the SMS text will contain information relating to the callers probable location (note, only if a location can be established). For all phones (smart and older) the location of the cell tower receiving the 111 call, along with an approximate coverage radius, will be presented to Emergency Service call takers. There is no ability to turn-off this feature once the service is established. Phase 2 extends the service to provide a handset based solution for iOS 111 callers. The location capabilities and data are the same as that provided by Android's solution.				

Privacy Analysis and Discussion Points	
Principle 2 of the Privacy Act states that information should be collected directly from the individual whenever possible. We want to be sure that the information provided is accurate and the individual is best placed to provide this. Collecting personal information from an alternate source may be acceptable if there is a justifiable exception.	

GUIDANCE NOTES
Use this template to record your thoughts and considerations. This is not a formal report, so notes and bullet points are acceptable. The important part is to ensure all relevant considerations are recorded and considered. This template is designed to be completed iteratively, it doesn't need to be completed in one go. Describe how your initiative complies (or does not comply) with this Principle and summarise any privacy related discussion points. Discussion points may include concerns, issues, uncertainties or questions you want to explore further. Record and evaluate potential options for addressing any discussion points, including identifying any options/solutions that enhance or could enhance privacy practices. Discussion points may identify privacy risks which need to be managed. Discuss whether the alternate sources that information will be collected from is appropriate and justifiable. For example, if the initiative proposes that you collect personal contact details for the individuals concerned from another business function within MBIE to help confirm the identity of the individual would this be appropriate and justifiable? Discuss whether any exceptions are applicable. You may want to confirm these with you PIA guru. Justifiable exceptions are: a. The individual concerned has authorised the business function to collect the information from someone else; b. The information is already publicly available; c. Obtaining the information from another source won't prejudice the interests of the individual; d. The information won't be used in a manner that identifies the individual concerned (e.g.: for statistical or research purposes); e. Collecting from another source is necessary to enforce the law, or for court proceedings, or to protect public revenue; f. Collecting information from the individual concerned isn't reasonably practicable in the circumstances. Discuss any other concerns, issues, uncertainties or questions you have about how your initiative complies with this principle.

Risk Identification	
Link to Risk Register	A full technical risk assessment, including consideration of Privacy risks, has been conducted for the MCL LAS solution. See http://mako.iad.govt.nz/otz/iscan.dll?view=69964471
Risk Number	Risk Description <i>Description of the privacy risk (i.e.: the actual/root risk, not the symptom of the risk)</i>
	Consequences <i>Key things that may happen if the risk materialises</i>
P2_1	
P2_2	
P2_3	
P2_4	
P2_5	
P2_6	

GUIDANCE NOTES
Record the link to the initiative risk register. The MBIE Risk Register template can be found here - http://thelink/how/Pages/find-the-cpo-project-delivery-templates.aspx Record all privacy risks arising from the analysis and discussion points above. Add more rows as required. Where privacy risks are identified, these must be appropriately managed. Copy these risks into the appropriate risk register (this may be the master initiative risk register, or a specific privacy risk register). Complete the risk register template by recording: existing controls in place to manage the risk; planned activities, actions, roles, or programmes to treat the risk; and the outcome of the controls and treatments. Ensure responsibilities are identified and regular reviews of the risks, controls, and treatments are undertaken.

RELEASED UNDER THE OFFICIAL INFORMATION ACT

PRINCIPLE 3 - PRIVACY IMPACT ANALYSIS

Once you have completed the Data Flow template, information related to Principle 3 will be automatically copied to this worksheet. Refer to this information to help you to complete an Impact Analysis and identify the risks associated with Principle 3.

- If you have more than five categories on your Data Flow template, add more columns (to the right of column F) so the number of columns on this worksheet matches your Data Flow template. Copy the formula from column F to the new columns so the data from the Data Flow template is copied over.
- Complete the 'Initiative Details and Sign off' section (in white).
- Complete the 'Privacy Analysis and Discussion Points', and 'Risk Identification' sections (in white). Guidance notes are provided to the right in orange.
- Business owner sign off is required.



INITIATIVE DETAILS AND SIGN OFF	
Initiative name:	Emergency Caller Location Information : Phase 2 - iOS and Rebidding
Brief description of initiative:	The MCL project will address longstanding operational requirements of Emergency Service Providers for probable caller location information from mobile phones. The outcome sought is for the best available caller location to be sent to an emergency service provider when a 111 call is made, without requiring the caller to do anything more than dial 111 on the standard keypad of their mobile phone.
Name and role of person completing template:	Ben Quay, MCL Project Director
Template completion date:	31/08/2016 updated 27/02/2017, updated further 21/11/2017
Business owner name and sign-off:	Brad Ward, GM CCC and ECLJ business owner

Information recorded on Data Flow Template	
Which data items are mandatory or considered compulsory to collect?	All data elements are required as collectively they establish the probable location area of a caller
How will you tell individuals about the collection of their information?	A new Code of Practice TIPC #5 is in force, published by the Privacy Commissioner. See https://privacy.org.nz/the-privacy-act-and-codes/codes-of-practice/telecommunications-information-privacy-code/amendments-and-other-information-on-the-telecommunications-information-privacy-code/ ECLJ is regulated service and has privacy safeguards in place, as obligated by the TIPC. The TIPC requires location agencies to publish information on their websites about the service, how their data is collected, used, retained and disposed. The TIPC does not require emergency services to advise callers to 111 that their location information is being used.
When will you tell individuals about the collection of their information?	As above. It is not intended that emergency service call takers will advise callers that their location information has been collected as this will add time to an emergency call and may cause delay in dispatching a response. Also, the caller information may not be required, in all cases, to establish location.

Privacy Analysis and Discussion Points	
The key requirements of Principle 3 of the Privacy Act are to ensure individuals know:	
<ul style="list-style-type: none"> • That information is being collected about them and their rights relating to their information; • Why information is being collected about them, including the consequences if all, or part, of the information is not provided; • Who else will use the information. 	

<p>Use this template to record your thoughts and considerations. This is not a formal report, so notes and bullet points are acceptable. The important part is to ensure all relevant considerations are recorded and considered.</p> <p>This template is designed to be completed iteratively, it doesn't need to be completed in one go.</p> <p>Not all of the Privacy Principles will be relevant to your proposal. If you don't have a clear answer for a part of the template or believe a Principle is not relevant, ensure this is noted.</p> <p>Describe how your initiative complies (or does not comply) with this Principle and summarise any privacy related discussion points. Discussion points may include concerns, issues, uncertainties or questions you want to explore further. Record and evaluate potential options for addressing any discussion points, including identifying any options/solutions that enhance or could enhance privacy practices. Discussion points may identify privacy risks which need to be managed.</p> <p>Have you decided not to tell individuals about all the information you are collecting about them? Note if any will be omitted and explain why the business has chosen not to inform individuals in line with the requirements of this principle.</p> <p>If you are not notifying individuals, consider whether one of the exceptions in the Principle applies and record your reasoning. It is recommended that you check with your PIA guru or Principal Privacy Adviser to confirm this. Justifiable exceptions include:</p> <ol style="list-style-type: none"> if it would impact the lawful purpose of collecting the information; if it could prejudice a criminal investigation; if it is not reasonably practicable in the circumstances. <p>Does an existing privacy statement or notice adequately cover the collection of personal information for your initiative? If not, record what needs to be amended for it to do so. Discuss any other concerns, issues, uncertainties or questions you have about how your initiative complies with this principle.</p>	
--	--

GUIDANCE NOTES

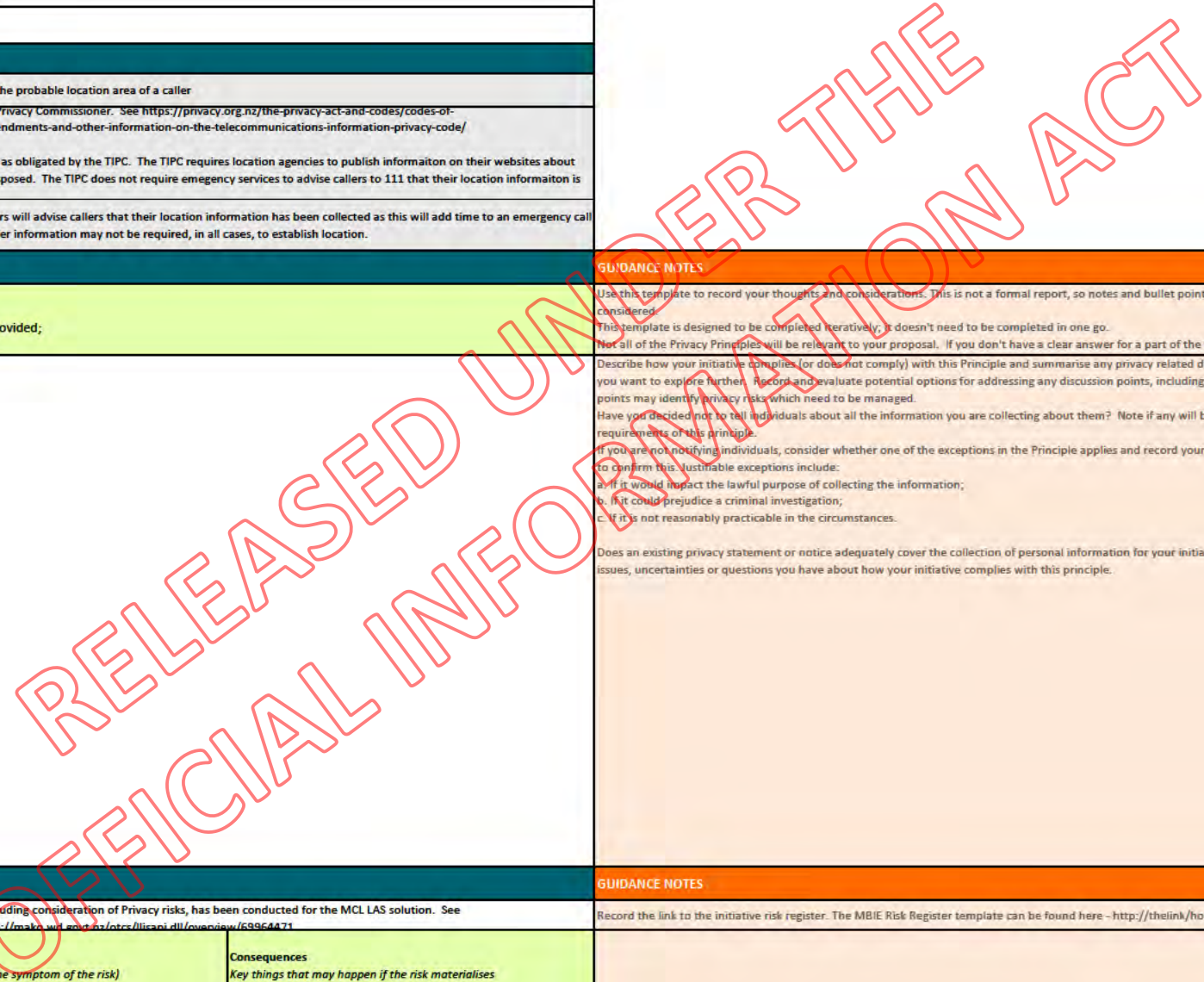
<p>Use this template to record your thoughts and considerations. This is not a formal report, so notes and bullet points are acceptable. The important part is to ensure all relevant considerations are recorded and considered.</p> <p>This template is designed to be completed iteratively, it doesn't need to be completed in one go.</p> <p>Not all of the Privacy Principles will be relevant to your proposal. If you don't have a clear answer for a part of the template or believe a Principle is not relevant, ensure this is noted.</p> <p>Describe how your initiative complies (or does not comply) with this Principle and summarise any privacy related discussion points. Discussion points may include concerns, issues, uncertainties or questions you want to explore further. Record and evaluate potential options for addressing any discussion points, including identifying any options/solutions that enhance or could enhance privacy practices. Discussion points may identify privacy risks which need to be managed.</p> <p>Have you decided not to tell individuals about all the information you are collecting about them? Note if any will be omitted and explain why the business has chosen not to inform individuals in line with the requirements of this principle.</p> <p>If you are not notifying individuals, consider whether one of the exceptions in the Principle applies and record your reasoning. It is recommended that you check with your PIA guru or Principal Privacy Adviser to confirm this. Justifiable exceptions include:</p> <ol style="list-style-type: none"> if it would impact the lawful purpose of collecting the information; if it could prejudice a criminal investigation; if it is not reasonably practicable in the circumstances. <p>Does an existing privacy statement or notice adequately cover the collection of personal information for your initiative? If not, record what needs to be amended for it to do so. Discuss any other concerns, issues, uncertainties or questions you have about how your initiative complies with this principle.</p>
--

Risk Identification

Link to Risk Register	A full technical risk assessment, including consideration of Privacy risks, has been conducted for the MCL LAS solution. See http://mako.wel.govt.nz/otrs/tilicani.dtl/overview/69964471	
Risk Number	Risk Description <i>Description of the privacy risk (i.e.: the actual/root risk, not the symptom of the risk)</i>	Consequences <i>Key things that may happen if the risk materialises</i>
P3_1		
P3_2		
P3_3		
P3_4		
P3_5		
P3_6		

GUIDANCE NOTES

<p>Record the link to the initiative risk register. The MBIE Risk Register template can be found here - http://theink/how/Pages/find-the-cpo-project-delivery-templates.aspx.</p> <p>Record all privacy risks arising from the analysis and discussion points above. Add more rows as required.</p> <p>Where privacy risks are identified, these must be appropriately managed. Copy these risks into the appropriate risk register (this may be the master initiative risk register, or a specific privacy risk register).</p> <p>Complete the risk register template by recording: existing controls in place to manage the risk; planned activities, actions, roles, or programmes to treat the risk; and the outcome of the controls and treatments. Ensure responsibilities are identified and regular reviews of the risks, controls, and treatments are undertaken.</p>



PRINCIPLE 4 - PRIVACY IMPACT ANALYSIS

Once you have completed the Data Flow template, information related to Principle 4 will be automatically copied to this worksheet. Refer to this information to help you to complete an Impact Analysis and identify the risks associated with Principle 4.

- If you have more than five categories on your Data Flow template, add more columns (to the right of column F) so the number of columns on this worksheet matches your Data Flow template. Copy the formula from column F to the new columns so the data from the Data Flow template is copied over.
- Complete the 'Initiative Details and Sign off' section (in white).
- Complete the 'Privacy Analysis and Discussion Points', and 'Risk Identification' sections (in white). Guidance notes are provided to the right in orange.
- Business owner sign off is required.



INITIATIVE DETAILS AND SIGN OFF	
Initiative name:	Emergency Caller Location Information : Phase 2 - iOS and Rebidding
Brief description of initiative:	The MCL project will address longstanding operational requirements of Emergency Service Providers for probable caller location information from mobile phones. The outcome sought is for the best available caller location to be sent to an emergency service provider when a 111 call is made, without requiring the caller to do anything more than dial 111 on the standard keypad of their mobile phone.
Name and role of person completing template:	Ben Quay, MCL Project Director
Template completion date:	31/08/2016 updated 27/02/2017, updated further 21/11/2017
Business owner name and sign-off:	Brad Ward, GM CCC and ECU business owner

Information recorded on Data Flow Template	
How will this data be collected?	By a mobile caller activating the NZ 111 service by dialling 111 on a mobile device.
Attach any diagrams which show how the information will flow	

Privacy Analysis and Discussion Points	
The key requirement of Principle 4 of the Privacy Act is to ensure personal information is not collected by unlawful means, in an unfair manner, or a manner that intrudes unreasonably upon the personal affairs of the individual concerned.	

--	--

GUIDANCE NOTES

Use this template to record your thoughts and considerations. This is not a formal report so notes and bullet points are acceptable. The important part is to ensure all relevant considerations are recorded and considered.

This template is designed to be completed iteratively, it doesn't need to be completed in one go.

Describe how your initiative complies (or does not comply) with this Principle and summarise any privacy related discussion points. Discussion points may include concerns, issues, uncertainties or questions you want to explore further. Record and evaluate potential options for addressing any discussion points, including identifying any options/solutions that enhance or could enhance privacy practices. Discussion points may identify privacy risks which need to be managed.

Will the individual know information is being collected about them? If applicable, describe why any information is being collected in a covert manner rather than in an open and transparent way (visible to the individual concerned). A good rule of thumb here is to consider whether the individual is likely to be concerned or upset about the way their personal information is being collected. Do you have to collect information covertly? Are there any legal requirements that require this?

Discuss any other concerns, issues, uncertainties or questions you have about how your initiative complies with this principle.

Risk Identification

Link to Risk Register	A full technical risk assessment, including consideration of Privacy risks, has been conducted for the MCL LAS solution. See http://mako.wd.govt.nz/otrs/lisani/all/overview/6396447
-----------------------	--

GUIDANCE NOTES

Record the link to the initiative risk register. The MBIE Risk Register template can be found here - <http://theink/how/Pages/find-the-cpo-project-delivery-templates.aspx>

Risk Number	Risk Description <i>Description of the privacy risk (i.e.: the actual/root risk, not the symptom of the risk)</i>	Consequences <i>Key things that may happen if the risk materialises</i>
P4_1		
P4_2		
P4_3		
P4_4		
P4_5		
P4_6		

Record all privacy risks arising from the analysis and discussion points above. Add more rows as required.

Where privacy risks are identified, these must be appropriately managed. Copy these risks into the appropriate risk register (this may be the master initiative risk register, or a specific privacy risk register).

Complete the risk register template by recording: existing controls in place to manage the risk; planned activities, actions, roles, or programmes to treat the risk; and the outcome of the controls and treatments. Ensure responsibilities are identified and regular reviews of the risks, controls, and treatments are undertaken.



PRINCIPLE 5 - PRIVACY IMPACT ANALYSIS

Once you have completed the Data Flow template, information related to Principle 5 will be automatically copied to this worksheet. Refer to this information to help you to complete an Impact Analysis and identify the risks associated with Principle 5.

- If you have more than five categories on your Data Flow template, add more columns (to the right of column F) so the number of columns on this worksheet matches your Data Flow template. Copy the formula from column F to the new columns so the data from the Data Flow template is copied over.
- Complete the 'Initiative Details and Sign off' section (in white).
- Complete the 'Privacy Analysis and Discussion Points', and 'Risk Identification' sections (in white). Guidance notes are provided to the right in orange.
- Business owner sign off is required.



INITIATIVE DETAILS AND SIGN OFF	
Initiative name:	Emergency Caller Location Information : Phase 2 - iOS and Rebidding
Brief description of initiative:	The MCL project will address longstanding operational requirements of Emergency Service Providers for probable caller location information from mobile phones. The outcome sought is for the best available caller location to be sent to an emergency service provider when a 111 call is made, without requiring the caller to do anything more than dial 111 on the standard keypad of their mobile phone.
Name and role of person completing template:	Ben Quay, MCL Project Director
Template completion date:	31/08/2016 updated 27/02/2017, updated further 21/11/2017
Business owner name and sign-off:	Brad Ward, GM CCC and ECU business owner

Information recorded on Data Flow Template	
What data fields will be retained and stored and what format will they be stored in?	All data fields described will be retained and stored for no longer than is necessary to establish the location of an emergency caller and facilitate the response to an emergency. Currently all PII is purged after 60mins for the time it is received in the Location Area Service, no PII is stored in audit.
Where will data be stored and who will be responsible for keeping it safe during storage?	The data will be stored in a Location Area Service repository provided as a managed service hosted in the Government cloud (Infrastructure as a Service). MBIE is the controller of this service.
What controls will be in place to protect data in transit between internal/external parties?	Best practice security controls, utilising industry standard encryption techniques have been implemented on the interfaces with the service being hosted in the Government cloud.
Who will have access to the data, who will it be disclosed to and what controls will be in place to protect it?	Emergency service provider call takers have access to the data for the specific needs of establishing probable caller location. Access logging and audit functionalities are also in place.
How often will data be accessed by third parties?	Access to the data is limited to Location Agencies, defined as LAS controller (MBIE), Mobile Network Operators, the Location Area Service provider and public safety.
What additional safeguards will be in place to protect the data?	See the Mobile Caller Location System Security Certificate & Business Risk Acceptance for details.
What legal or other commercial safeguards are in place to protect the data?	A new Code of Practice TIPC #5 has been published by the Privacy Commissioner. See https://privacy.org.nz/the-privacy-act-and-codes/codes-of-practice/telecommunications-information-privacy-code/amendments-and-other-information-on-the-telecommunications-information-privacy-code/

Privacy Analysis and Discussion Points

The key requirement of Principle 5 is that reasonable steps are taken to protect the personal information collected from loss, unauthorised access, unauthorised use, modification, disclosure and other misuse. This applies when the information is in storage and when it is being moved.

--

GUIDANCE NOTES

Use this template to record your thoughts and considerations. This is not a formal report, so notes and bullet points are acceptable. The important part is to ensure all relevant considerations are recorded and considered. This template is designed to be completed iteratively; it doesn't need to be completed in one go.

Describe how your initiative complies (or does not comply) with this Principle and summarise any privacy related discussion points. Discussion points may include concerns, issues, uncertainties or questions you want to explore further. Record and evaluate potential options for addressing any discussion points, including identifying any options/solutions that enhance or could enhance privacy practices. Discussion points may identify privacy risks which need to be managed.

Discuss with your internal stakeholders what safeguards are in place or required, IT, Security, Legal, Procurement, Records Management, Facilities, and HR are all key. IT and Security stakeholders should be able to advise you on the appropriateness of the security components in place and what might be required for changes or new initiatives along with identifying what the standards are that must be adhered to internally or externally.

Note any concerns you have about how personal information will be protected. Will existing safeguards be affected? Note where new technologies or processes will improve existing safeguards. Will the methods proposed adequately protect information? Are there additional protective safeguards in place to protect information that requires special care? Discuss whether any physical, technical and operational controls can be applied to protect personal information. Consider safeguards for when the personal information is in storage and when it is being transferred from one place to another (including digital and physical transfer).

Are the existing controls in place for staff (such as privacy and security training, policies, Incident Management procedures, Acceptable Use Policy, Code of Conduct) governing employee and third party treatment of personal information relevant and adequate? Technology changes quickly, and written "safeguards" such as policies and training may get out of date. These must be reviewed if they are to be relied upon. Discuss whether you believe the use of any new devices, channels or methods of collection are adequately protected.

Revisit confidentiality, privacy and security clauses in contracts if a change relies on third party contracts already in place (in particular if new locations are required to transfer, access, disclose or store personal information). New third party relationships will require appropriate contract terms to articulate remote access provisions and how privacy and security will be handled.

Physical security safeguards should be considered for premises, property, equipment and files. Are these physically secure? Can you obtain details about who has accessed facilities and equipment?

Discuss any other concerns, issues, uncertainties or questions you have about how your initiative complies with this principle.

Risk Identification

Link to Risk Register: A full technical risk assessment, including consideration of Privacy risks, has been conducted for the MCL LAS solution. See <http://mako.wd.govt.nz/otcs/otcsapi.dll/viewview/69964471>

Risk Number	Risk Description <i>Description of the privacy risk (i.e.: the actual/root risk, not the symptom of the risk)</i>	Consequences <i>Key things that may happen if the risk materialises</i>
PS 1		
PS 2		
PS 3		
PS 4		
PS 5		
PS 6		

GUIDANCE NOTES

Record the link to the initiative risk register. The MBIE Risk Register template can be found here - <http://thelink/how/Pages/find-the-cpo-project-delivery-templates.aspx>

Record all privacy risks arising from the analysis and discussion points above. Add more rows as required. Where privacy risks are identified, these must be appropriately managed. Copy these risks into the appropriate risk register (this may be the master initiative risk register, or a specific privacy risk register). Complete the risk register template by recording: existing controls in place to manage the risk; planned activities, actions, roles, or programmes to treat the risk; and the outcome of the controls and treatments. Ensure responsibilities are identified and regular reviews of the risks, controls, and treatments are undertaken.



PRINCIPLE 6 - PRIVACY IMPACT ANALYSIS

Once you have completed the Data Flow template, information related to Principle 6 will be automatically copied to this worksheet. Refer to this information to help you to complete an Impact Analysis and identify the risks associated with Principle 6.

- If you have more than five categories on your Data Flow template, add more columns (to the right of column F) so the number of columns on this worksheet matches your Data Flow template. Copy the formula from column F to the new columns so the data from the Data Flow template is copied over.
- Complete the 'Initiative Details and Sign off' section (in white).
- Complete the 'Privacy Analysis and Discussion Points', and 'Risk Identification' sections (in white). Guidance notes are provided to the right in orange.
- Business owner sign off is required.



INITIATIVE DETAILS AND SIGN OFF	
Initiative name:	Emergency Caller Location Information : Phase 2 - iOS and Rebidding
Brief description of initiative:	The MCL project will address longstanding operational requirements of Emergency Service Providers for probable caller location information from mobile phones. The outcome sought is for the best available caller location to be sent to an emergency service provider when a 111 call is made, without requiring the caller to do anything more than dial 111 on the standard keypad of their mobile phone.
Name and role of person completing template:	Ben Quay, MCL Project Director
Template completion date:	31/08/2016 updated 27/02/2017, updated further 21/11/2017
Business owner name and sign-off:	Brad Ward, GM CCC and ECU business owner

Information recorded on Data Flow Template

Can individuals access data about themselves upon request? Individuals' requests for rights of access to and correction of personal information are possible, however this would be limited due to the retention clause of the Code that

Privacy Analysis and Discussion Points

The key requirement of Principle 6 of the Privacy Act is to ensure that an agency holds personal information in such a way that it can readily be retrieved as the individual concerned is entitled to:

- Obtain confirmation about whether information is being held about them;
- Have access to that information (within 20 working days from date of request).

GUIDANCE NOTES

Use this template to record your thoughts and considerations. This is not a formal report, so notes and bullet points are acceptable. The important part is to ensure all relevant considerations are recorded and considered.

This template is designed to be completed iteratively; it doesn't need to be completed in one go.

Not all of the Privacy Principles will be relevant to your proposal. If you don't have a clear answer for a part of the template or believe a Principle is not relevant, ensure this is noted.

Describe how your initiative complies (or does not comply) with this Principle and summarise any privacy related discussion points. Discussion points may include concerns, issues, uncertainties or questions you want to explore further. Record and evaluate potential options for addressing any discussion points, including identifying any options/solutions that enhance or could enhance privacy practices. Discussion points may identify privacy risks which need to be managed.

Describe what impact the proposed change will have on an individual's ability to access their personal information if they wish to see it. Note if the where existing capability will be improved by the initiative. When an individual requests access to their information, how will this be identified and actioned? Can a decision to grant access or withhold information be made within the 20 working day time limit? Is there a valid reason to extend this time limit or can this information be provided without unnecessary delay? Will requests to third parties with access to the personal information be transferred or processed by the third party? Are there any concerns about finding the information you hold? Will emails involving personal information be appropriately filed to easily identify and retrieve? If information is archived offshore or stored by a cloud provider, can it be retrieved readily and within the timeframe? Will the personal information be up to date and accurate?

Consider the impact of various options for providing access. Are any options more efficient or cost-effective? Identify those options that provide access in the most complete, accurate, and timely way for the individual.

Discuss any other concerns, issues, uncertainties or questions you have about how your initiative complies with this principle.

Risk Identification

Link to Risk Register A full technical risk assessment, including consideration of Privacy risks, has been conducted for the MCL LAS solution. See <http://mako.wd.govt.nz/otcs/llisani/dll/numbers/69961411>

GUIDANCE NOTES

Record the link to the initiative risk register. The MBIE Risk Register template can be found here - <http://thelink/how/Pages/find-the-cpo-project-delivery-templates.aspx>

Risk Number	Risk Description <i>Description of the privacy risk (i.e.: the actual/root risk, not the symptom of the risk)</i>	Consequences <i>Key things that may happen if the risk materialises</i>
P6_1		
P6_2		
P6_3		
P6_4		
P6_5		
P6_6		

Record all privacy risks arising from the analysis and discussion points above. Add more rows as required.

Where privacy risks are identified, these must be appropriately managed. Copy these risks into the appropriate risk register (this may be the master initiative risk register, or a specific privacy risk register).

Complete the risk register template by recording: existing controls in place to manage the risk; planned activities, actions, roles, or programmes to treat the risk; and the outcome of the controls and treatments. Ensure responsibilities are identified and regular reviews of the risks, controls, and treatments are undertaken.



PRINCIPLE 7 - PRIVACY IMPACT ANALYSIS

Once you have completed the Data Flow template, information related to Principle 7 will be automatically copied to this worksheet. Refer to this information to help you to complete an Impact Analysis and identify the risks associated with Principle 7.

- If you have more than five categories on your Data Flow template, add more columns (to the right of column F) so the number of columns on this worksheet matches your Data Flow template. Copy the formula from column F to the new columns so the data from the Data Flow template is copied over.
- Complete the 'Initiative Details and Sign off' section (in white).
- Complete the 'Privacy Analysis and Discussion Points', and 'Risk Identification' sections (in white). Guidance notes are provided to the right in orange.
- Business owner sign off is required.



INITIATIVE DETAILS AND SIGN OFF	
Initiative name:	Emergency Caller Location Information : Phase 2 - iOS and Rebidding
Brief description of initiative:	The MCL project will address longstanding operational requirements of Emergency Service Providers for probable caller location information from mobile phones. The outcome sought is for the best available caller location to be sent to an emergency service provider when a 111 call is made, without requiring the caller to do anything more than dial 111 on the standard keypad of their mobile phone.
Name and role of person completing template:	Ben Quay, MCL Project Director
Template completion date:	31/08/2016 updated 27/02/2017, updated further 21/11/2017
Business owner name and sign-off:	Brad Ward, GM CCC and ECU business owner

Information recorded on Data Flow Template	
Can an individual request a correction to their data and have the change actioned?	Individuals' requests for rights of access to and correction of personal information are possible, however this would be limited due to the proposed retention clause of the new Code that states that information may not be kept for longer than is necessary to establish the location of an emergency caller and facilitate the response to an

Privacy Analysis and Discussion Points

The key requirement of Principle 7 of the Privacy Act is to ensure that personal information held by an agency can be corrected because individuals are entitled to request:

- A correction be made to the information stored about them;
- A statement is attached to their information stating that a correction was sought, but not made.

GUIDANCE NOTES

Use this template to record your thoughts and considerations. This is not a formal report so notes and bullet points are acceptable. The important part is to ensure all relevant considerations are recorded and considered.

This template is designed to be completed iteratively; it doesn't need to be completed in one go.

Not all of the Privacy Principles will be relevant to your proposal. If you don't have a clear answer for a part of the template or believe a Principle is not relevant, ensure this is noted.

Describe how your initiative complies (or does not comply) with this Principle and summarise any privacy related discussion points. Discussion points may include concerns, issues, uncertainties or questions you want to explore further. Record and evaluate potential options for addressing any discussion points, including identifying any options/solutions that enhance or could enhance privacy practices. Discussion points may identify privacy risks which need to be managed.

Describe what impact the proposed change will have on an individual's ability to correct their personal information if it is incorrect. Note if the where existing capability will be improved by the initiative. When an individual requests correction of their information, how will this be identified and actioned? Consider who can make corrections and in what circumstances.

Are there any concerns about how information can be located and modified? If information is archived offshore, or stored by a cloud provider, can it be retrieved readily to correct it? Can personal information be verified before you correct it and will a process be in place to do so? Can changes to information be monitored and recorded? If changes will not be made when requested, can you ensure a statement of correction is included with an individual's personal information? Will it always be clear that a statement of correction exists? Can personal information disclosed to other parties be corrected to ensure all records stored are accurate?

Discuss any other concerns, issues, uncertainties or questions you have about how your initiative complies with this principle.

Risk Identification

Link to Risk Register A full technical risk assessment, including consideration of Privacy risks, has been conducted for the MCL LAS solution. See <http://mako.wd.govt.nz/otcs/lisan/dll/mvreview/6996447>

GUIDANCE NOTES

Record the link to the initiative risk register. The MBIE Risk Register template can be found here - <http://theink/how/Pages/find-the-cpo-project-delivery-templates.aspx>

Risk Number	Risk Description <i>Description of the privacy risk (i.e.: the actual/root risk, not the symptom of the risk)</i>	Consequences <i>Key things that may happen if the risk materialises</i>
P7_1		
P7_2		
P7_3		
P7_4		
P7_5		
P7_6		

Record all privacy risks arising from the analysis and discussion points above. Add more rows as required.

Where privacy risks are identified, these must be appropriately managed. Copy these risks into the appropriate risk register (this may be the master initiative risk register, or a specific privacy risk register).

Complete the risk register template by recording: existing controls in place to manage the risk; planned activities, actions, roles, or programmes to treat the risk; and the outcome of the controls and treatments. Ensure responsibilities are identified and regular reviews of the risks, controls, and treatments are undertaken.



PRINCIPLE 8 - PRIVACY IMPACT ANALYSIS

Once you have completed the Data Flow template, information related to Principle 8 will be automatically copied to this worksheet. Refer to this information to help you to complete an Impact Analysis and identify the risks associated with Principle 8.

- If you have more than five categories on your Data Flow template, add more columns (to the right of column F) so the number of columns on this worksheet matches your Data Flow template. Copy the formula from column F to the new columns so the data from the Data Flow template is copied over.
- Complete the 'Initiative Details and Sign off' section (in white).
- Complete the 'Privacy Analysis and Discussion Points', and 'Risk Identification' sections (in white). Guidance notes are provided to the right in orange.
- Business owner sign off is required.



INITIATIVE DETAILS AND SIGN OFF	
Initiative name:	Emergency Caller Location Information : Phase 2 - iOS and Rebidding
Brief description of initiative:	The MCL project will address longstanding operational requirements of Emergency Service Providers for probable caller location information from mobile phones. The outcome sought is for the best available caller location to be sent to an emergency service provider when a 111 call is made, without requiring the caller to do anything more than dial 111 on the standard keypad of their mobile phone.
Name and role of person completing template:	Ben Quay, MCL Project Director
Template completion date:	31/08/2016 updated 27/02/2017, updated further 21/11/2017
Business owner name and sign-off:	Brad Ward, GM CCC and ECU business owner

Information recorded on Data Flow Template

Will the accuracy of data collected be verified before it is used? The location data is the probable location of a caller and not a definitive location, for example an address. In order for an emergency response to be dispatched the location

Privacy Analysis and Discussion Points

The key requirement of Principle 8 of the Privacy Act is an agency that holds personal information must take reasonable steps to ensure that information is accurate, up to date, complete, relevant and not misleading before using it.

--	--

GUIDANCE NOTES

Use this template to record your thoughts and considerations. This is not a formal report, so notes and bullet points are acceptable. The important part is to ensure all relevant considerations are recorded and considered.

This template is designed to be completed iteratively; it doesn't need to be completed in one go.

Describe how your initiative complies (or does not comply) with this Principle and summarise any privacy related discussion points. Discussion points may include concerns, issues, uncertainties or questions you want to explore further. Record and evaluate potential options for addressing any discussion points, including identifying any options/solutions that enhance or could enhance privacy practices. Discussion points may identify privacy risks which need to be managed.

Describe the impact your initiative will have on any existing processes that ensure accuracy. These should focus on whether or not the integrity of personal information is impacted, positively or negatively by this initiative or change. Will individuals provide their information directly and will they have the ability to verify their information is accurate before it is used, stored or disclosed? Can they routinely update their information? What would the impact be on the individual if their information was not accurate, or up to date, and is used for this initiative? If databases are held or development is conducted offshore with third parties, are appropriate processes in place to verify accuracy of personal information before implementation? How will information that changes over time (such as marital status, financial, health or address details) be kept up to date? Will your initiative ensure that any personal information disclosed to third parties is also corrected to ensure all records are accurate? If individuals have the same or similar name, how can you be sure personal information is attributed to the correct individual? Note if there is an intention to rely on automated decision-making based on the information provided.

Your IT stakeholders should be able to advise you on what steps are taken to verify data integrity for an existing system and what is proposed for a new initiative. Additionally, your business analysts should recommend processes to ensure accuracy is maintained.

Risk Identification

Link to Risk Register A full technical risk assessment, including consideration of Privacy risks, has been conducted for the MCL LAS solution. See <http://mako.wd.govt.nz/otcs/lisani.dll/mvplaw/69964471>

Risk Number	Risk Description <i>Description of the privacy risk (i.e.: the actual/root risk, not the symptom of the risk)</i>	Consequences <i>Key things that may happen if the risk materialises</i>
P8_1		
P8_2		
P8_3		
P8_4		
P8_5		
P8_6		

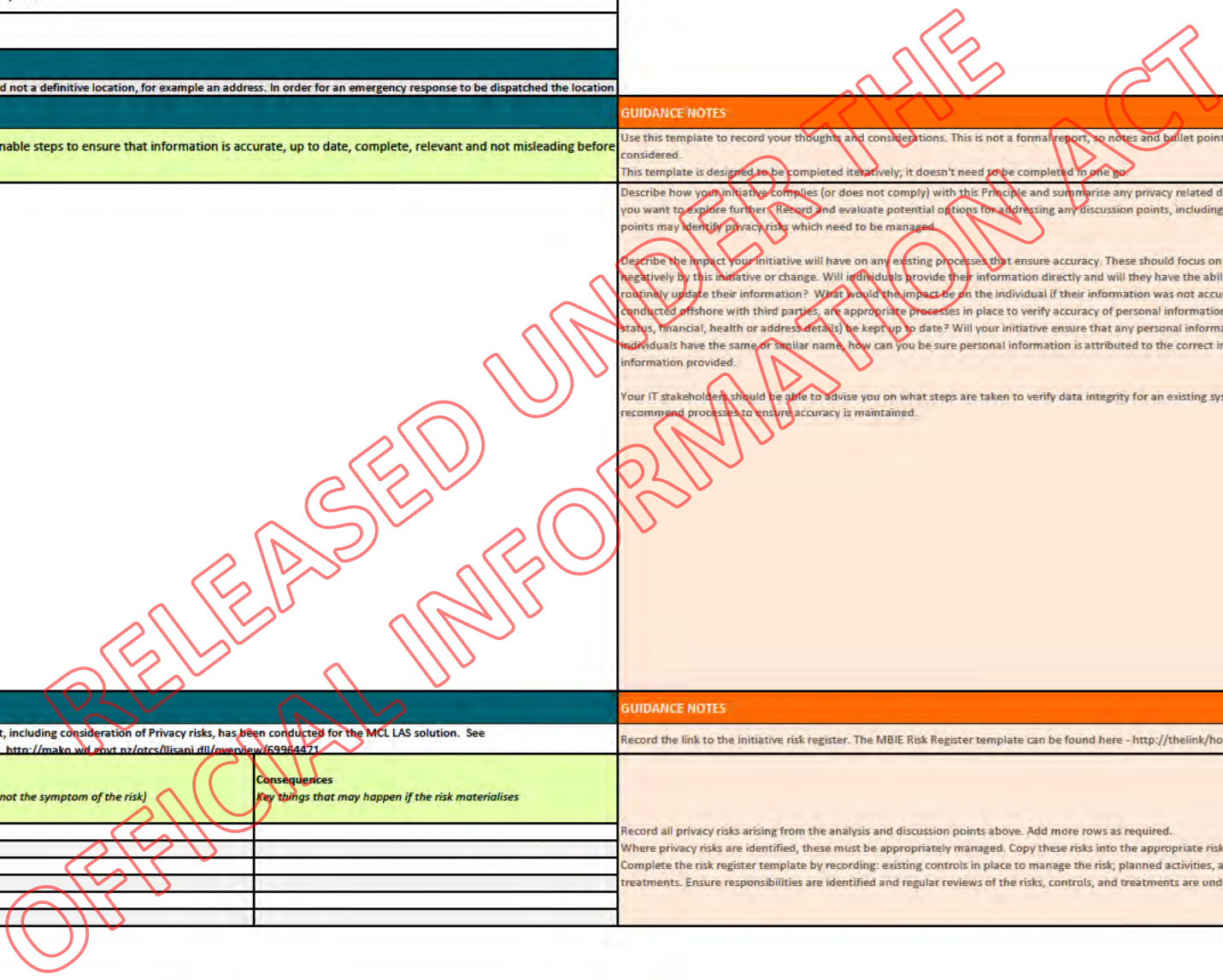
GUIDANCE NOTES

Record the link to the initiative risk register. The MBIE Risk Register template can be found here - <http://theink/how/Pages/find-the-cpo-project-delivery-templates.aspx>

Record all privacy risks arising from the analysis and discussion points above. Add more rows as required.

Where privacy risks are identified, these must be appropriately managed. Copy these risks into the appropriate risk register (this may be the master initiative risk register, or a specific privacy risk register).

Complete the risk register template by recording: existing controls in place to manage the risk; planned activities, actions, roles, or programmes to treat the risk; and the outcome of the controls and treatments. Ensure responsibilities are identified and regular reviews of the risks, controls, and treatments are undertaken.



PRINCIPLE 9 - PRIVACY IMPACT ANALYSIS

Once you have completed the Data Flow template, information related to Principle 9 will be automatically copied to this worksheet. Refer to this information to help you to complete an Impact Analysis and identify the risks associated with Principle 9.

- If you have more than five categories on your Data Flow template, add more columns (to the right of column F) so the number of columns on this worksheet matches your Data Flow template. Copy the formula from column F to the new columns so the data from the Data Flow template is copied over.
- Complete the 'Initiative Details and Sign off' section (in white).
- Complete the 'Privacy Analysis and Discussion Points', and 'Risk Identification' sections (in white). Guidance notes are provided to the right in orange.
- Business owner sign off is required.



INITIATIVE DETAILS AND SIGN OFF	
Initiative name:	Emergency Caller Location Information : Phase 2 - iOS and Rebidding
Brief description of initiative:	The MCL project will address longstanding operational requirements of Emergency Service Providers for probable caller location information from mobile phones. The outcome sought is for the best available caller location to be sent to an emergency service provider when a 111 call is made, without requiring the caller to do anything more than dial 111 on the standard keypad of their mobile phone.
Name and role of person completing template:	Ben Quay, MCL Project Director
Template completion date:	31/08/2016 updated 27/02/2017, updated further 21/11/2017
Business owner name and sign-off:	Brad Ward, GM CCC and ECU business owner

Information recorded on Data Flow Template	
How long will the business retain the data for?	Information may not be kept for longer than is necessary to establish the location of an emergency caller and facilitate the response to an emergency. This period will
How will the data retention period be managed and controlled?	Automatically deleted by the LAS when the specified period is reached.
How will data disposal or archiving be managed and controlled at the end of the retention period?	There will be no archiving of identifiable data. A log that data was received will be retained but this will not contain personal information.

Privacy Analysis and Discussion Points	
The key requirement of Principle 9 is that an agency only keeps personal information for as long as it has a lawful purpose for retaining and using it.	
<p>Describe how your initiative complies (or does not comply) with the Principle and summarise any privacy related discussion points. Discussion points may include concerns, issues, uncertainties or questions you want to explore further. Record and evaluate potential options for addressing any discussion points, including identifying any options/solutions that enhance or could enhance privacy practices. Discussion points may identify privacy risks which need to be managed.</p> <p>When you are thinking about how long you should retain personal information, consider: any relevant legal or public record requirements (e.g.: to comply with tax laws, anticipation of litigation)? Does the business know how long it needs to keep personal information for and the business reasons for keeping it? Will the retention and disposal process be adequate, and does it include steps to check the disposal of records against regulatory requirements before they are destroyed? Does the change or proposed initiative require historical information to be archived? Is it clear what information should be retained and how long it should be retained for? What steps will occur at the end of the agreed retention period to ensure secure destruction or transfer? Is appropriate metadata created and retained? Is the Retention and Disposal Schedule referred to current and do you know when was it last updated? When is it due to be updated? If a change to requirements occurs, can the retention period be amended? How will duplicate copies of personal information be managed to comply with public record, legal or business retention requirements?</p> <p>Talk with the Information and Data team about retention and disposal requirements for records, what existing retention and disposal process are in place, and whether proposals will meet public records requirements.</p> <p>Discuss any other concerns, issues, uncertainties or questions you have about how your initiative complies with this principle.</p>	

GUIDANCE NOTES
Use this template to record your thoughts and considerations. This is not a formal report, so notes and bullet points are acceptable. The important part is to ensure all relevant considerations are recorded and considered. This template is designed to be completed iteratively; it doesn't need to be completed in one go.
Describe how your initiative complies (or does not comply) with the Principle and summarise any privacy related discussion points. Discussion points may include concerns, issues, uncertainties or questions you want to explore further. Record and evaluate potential options for addressing any discussion points, including identifying any options/solutions that enhance or could enhance privacy practices. Discussion points may identify privacy risks which need to be managed.
When you are thinking about how long you should retain personal information, consider: any relevant legal or public record requirements (e.g.: to comply with tax laws, anticipation of litigation)? Does the business know how long it needs to keep personal information for and the business reasons for keeping it? Will the retention and disposal process be adequate, and does it include steps to check the disposal of records against regulatory requirements before they are destroyed? Does the change or proposed initiative require historical information to be archived? Is it clear what information should be retained and how long it should be retained for? What steps will occur at the end of the agreed retention period to ensure secure destruction or transfer? Is appropriate metadata created and retained? Is the Retention and Disposal Schedule referred to current and do you know when was it last updated? When is it due to be updated? If a change to requirements occurs, can the retention period be amended? How will duplicate copies of personal information be managed to comply with public record, legal or business retention requirements?
Talk with the Information and Data team about retention and disposal requirements for records, what existing retention and disposal process are in place, and whether proposals will meet public records requirements.
Discuss any other concerns, issues, uncertainties or questions you have about how your initiative complies with this principle.

Risk Identification																	
Link to Risk Register	A full technical risk assessment, including consideration of Privacy risks, has been conducted for the MCL LAS solution. See http://make.wd.govt.nz/otc/0112011/111/newsview/26364471																
Risk Number	<table border="1"> <thead> <tr> <th>Risk Description</th> <th>Consequences</th> </tr> <tr> <td>Description of the privacy risk (i.e.: the actual/root risk, not the symptom of the risk)</td> <td>Key things that may happen if the risk materialises</td> </tr> </thead> <tbody> <tr> <td>P9_1</td> <td></td> </tr> <tr> <td>P9_2</td> <td></td> </tr> <tr> <td>P9_3</td> <td></td> </tr> <tr> <td>P9_4</td> <td></td> </tr> <tr> <td>P9_5</td> <td></td> </tr> <tr> <td>P9_6</td> <td></td> </tr> </tbody> </table>	Risk Description	Consequences	Description of the privacy risk (i.e.: the actual/root risk, not the symptom of the risk)	Key things that may happen if the risk materialises	P9_1		P9_2		P9_3		P9_4		P9_5		P9_6	
Risk Description	Consequences																
Description of the privacy risk (i.e.: the actual/root risk, not the symptom of the risk)	Key things that may happen if the risk materialises																
P9_1																	
P9_2																	
P9_3																	
P9_4																	
P9_5																	
P9_6																	

GUIDANCE NOTES
Record the link to the initiative risk register. The MBIE Risk Register template can be found here - http://thelink/how/Pages/find-the-cpo-project-delivery-templates.aspx
Record all privacy risks arising from the analysis and discussion points above. Add more rows as required.
Where privacy risks are identified, these must be appropriately managed. Copy these risks into the appropriate risk register (this may be the master initiative risk register, or a specific privacy risk register).
Complete the risk register template by recording: existing controls in place to manage the risk; planned activities, actions, roles, or programmes to treat the risk; and the outcome of the controls and treatments. Ensure responsibilities are identified and regular reviews of the risks, controls, and treatments are undertaken.



PRINCIPLE 10 - PRIVACY IMPACT ANALYSIS

Once you have completed the Data Flow template, information related to Principle 10 will be automatically copied to this worksheet. Refer to this information to help you to complete an Impact Analysis and identify the risks associated with Principle 10.

- If you have more than five categories on your Data Flow template, add more columns (to the right of column F) so the number of columns on this worksheet matches your Data Flow template. Copy the formula from column F to the new columns so the data from the Data Flow template is copied over.
- Complete the 'Initiative Details and Sign off' section (in white).
- Complete the 'Privacy Analysis and Discussion Points', and 'Risk Identification' sections (in white). Guidance notes are provided to the right in orange.
- Business owner sign off is required.



INITIATIVE DETAILS AND SIGN OFF	
Initiative name:	Emergency Caller Location Information : Phase 2 - iOS and Rebidding
Brief description of initiative:	The MCL project will address longstanding operational requirements of Emergency Service Providers for probable caller location information from mobile phones. The outcome sought is for the best available caller location to be sent to an emergency service provider when a 111 call is made, without requiring the caller to do anything more than dial 111 on the standard keypad of their mobile phone.
Name and role of person completing template:	Ben Quay, MCL Project Director
Template completion date:	31/08/2016 updated 27/02/2017, updated further 21/11/2017
Business owner name and sign-off:	Brad Ward, GM CCC and ECU business owner

Information recorded on Data Flow Template

List any additional uses for the data you are collecting: None additional

Privacy Analysis and Discussion Points

The key requirement of Principle 10 of the Privacy Act is that personal information obtained by an agency for one purpose shall not be used for any other purpose, unless it believes on reasonable grounds that the specified exceptions apply.

--	--

GUIDANCE NOTES

Use this template to record your thoughts and considerations. This is not a formal report, so notes and bullet points are acceptable. The important part is to ensure all relevant considerations are recorded and considered.

This template is designed to be completed iteratively; it doesn't need to be completed in one go.

Describe how your initiative complies (or does not comply) with this Principle and summarise any privacy related discussion points. Discussion points may include concerns, issues, uncertainties or questions you want to explore further. Record and evaluate potential options for addressing any discussion points, including identifying any options/solutions that enhance or could enhance privacy practices. Discussion points may identify privacy risks which need to be managed.

Consider if the original purpose is clearly defined and whether the intended use of the information is consistent with the purpose/s it was collected for (refer to your purposes discussed in Principle 1). If an intended use is not consistent with the purpose for collection, consider whether one of the exceptions in the Principle applies and record your reasoning. It is recommended that you check with your PIA guru or Principal Privacy Adviser to confirm this. Justifiable exceptions include:

- The information source is publicly available and it is not unfair or unreasonable to use the information;
- Authorisation has been obtained from the individual;
- The purpose is directly related to the purpose information was originally collected for;
- To protect public revenue, maintain the law, or for court proceedings;
- To protect public health or safety, or the life or health of the individual concerned or another individual;
- Individuals cannot be identified (i.e. anonymised), or it is used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify an individual.

Do you have authorised or legislative reasons for using the information for a different purpose?

When you are thinking about the use of information and if the intended use is different to the purpose you originally collected it for, consider: should individuals be notified if the intended purpose is different to the original purpose? What is the plan to notify them? Do third party contractual arrangements need to be amended if the intended use of personal information is changed? Is it possible to restrict the use of the personal information so that it can't be used for other purposes? Will staff have appropriate training on what is/isn't acceptable use of personal information?

Consider what opportunities are available for other functions or Groups in MBIE. Consider whether the information could be useful for customer/client services, policy analysis, regulatory enforcement, or other activities conducted by MBIE.

Discuss any other concerns, issues, uncertainties or questions you have about how your initiative complies with this principle.

Risk Identification

Link to Risk Register: A full technical risk assessment, including consideration of Privacy risks, has been conducted for the MCL LAS solution. See <http://mako.wd.govt.nz/otcs/lisani.dll/mwnew/69964471>

Risk Number	Risk Description <i>Description of the privacy risk (i.e.: the actual/root risk, not the symptom of the risk)</i>	Consequences <i>Key things that may happen if the risk materialises</i>
P10_1		
P10_2		
P10_3		
P10_4		
P10_5		
P10_6		

GUIDANCE NOTES

Record the link to the initiative risk register. The MBIE Risk Register template can be found here - <http://theink/how/Pages/find-the-cpo-project-delivery-templates.aspx>

Record all privacy risks arising from the analysis and discussion points above. Add more rows as required.

Where privacy risks are identified, these must be appropriately managed. Copy these risks into the appropriate risk register (this may be the master initiative risk register, or a specific privacy risk register).

Complete the risk register template by recording: existing controls in place to manage the risk; planned activities, actions, roles, or programmes to treat the risk; and the outcome of the controls and treatments. Ensure responsibilities are identified and regular reviews of the risks, controls, and treatments are undertaken.



PRINCIPLE 11 - PRIVACY IMPACT ANALYSIS

Once you have completed the Data Flow template, information related to Principle 11 will be automatically copied to this worksheet. Refer to this information to help you to complete an Impact Analysis and identify the risks associated with Principle 11.

- If you have more than five categories on your Data Flow template, add more columns (to the right of column F) so the number of columns on this worksheet matches your Data Flow template. Copy the formula from column F to the new columns so the data from the Data Flow template is copied over.
- Complete the 'Initiative Details and Sign off' section (in white).
- Complete the 'Privacy Analysis and Discussion Points', and 'Risk Identification' sections (in white). Guidance notes are provided to the right in orange.
- Business owner sign off is required.



INITIATIVE DETAILS AND SIGN OFF	
Initiative name:	Emergency Caller Location Information : Phase 2 - iOS and Rebidding
Brief description of initiative:	The MCL project will address longstanding operational requirements of Emergency Service Providers for probable caller location information from mobile phones. The outcome sought is for the best available caller location to be sent to an emergency service provider when a 111 call is made, without requiring the caller to do anything more than dial 111 on the standard keypad of their mobile phone.
Name and role of person completing template:	Ben Quay, MCL Project Director
Template completion date:	31/08/2016 updated 27/02/2017, updated further 21/11/2017
Business owner name and sign-off:	Brad Ward, GM CCC and ECU business owner

Information recorded on Data Flow Template	
List any additional disclosure of the data you foresee	None additional

Privacy Analysis and Discussion Points

The key requirement of Principle 11 of the Privacy Act is that an agency shall not disclose personal information unless the agency believes, on reasonable grounds, one of the exceptions apply.

--	--

GUIDANCE NOTES

Use this template to record your thoughts and considerations. This is not a formal report, so notes and bullet points are acceptable. The important part is to ensure all relevant considerations are recorded and considered.

This template is designed to be completed iteratively; it doesn't need to be completed in one go.

Describe how your initiative complies (or does not comply) with this Principle and summarise any privacy related discussion points. Discussion points may include concerns, issues, uncertainties or questions you want to explore further. Record and evaluate potential options for addressing any discussion points, including identifying any options/solutions that enhance or could enhance privacy practices. Discussion points may identify privacy risks which need to be managed.

Disclosure may involve wider data sharing with other government agencies, private sector agencies, or overseas agencies. This is permitted as long as disclosure complies with the exceptions provided in the principle. Exceptions should be considered on a case by case basis and should not be applied in a wholesale manner to justify extended disclosure to other parties. The exceptions include:

- Disclosure is one of the purposes with which the information was obtained, or is directly related to one of the purposes with which it was collected for;
- Disclosure to the individual the information is about;
- Individuals have authorised you to disclose their information to another organisation;
- Information was from a publicly available source, and it would not be unfair or unreasonable to disclose the information;
- Disclosure is necessary to avoid prejudice to the maintenance of the law by any public sector agency;
- Information will be used in a form which individuals are not identified;
- Information is being used for statistical or research purposes and will not be published in a form where the individuals will be identified in any way.

Consider if the original purpose is clearly defined and whether the intended disclosure of the information is consistent with the purpose/s it was collected for (refer to your purposes discussed in Principle 1). If an intended disclosure is not consistent with the purpose for collection, consider whether one of the exceptions in the Principle applies and record your reasoning. It is recommended that you check with your Privacy Officer or Principal Privacy Adviser to confirm this.

Your initiative may need additional permissions to disclose information for other purposes. Will individuals be told about the disclosure for a new purpose? Describe how they will be notified. Where individuals are asked for authorisation, describe how the authorisation will be obtained and what the record of the consent will be.

Consider if there are any plans in place to manage potential scope creep in the disclosure of personal information - this is relevant for both changes to existing and for newly proposed initiatives. Have you identified any controls or systems in place that will help manage the use of the information by the third parties once it has been disclosed? Can the third party disclose the information to another party? Are there protocols in place for determining when it is appropriate to disclose the information to another party, either directly or by the third party?

Consider whether the arrangements in place to manage the disclosure are proportionate to the risk the disclosure poses. Does the party receiving the information have sufficient safeguards in place to protect the information when in their care? Are there arrangements in place if the recipient commits a breach? Is the oversight of the disclosure arrangements sufficient to provide MBIE will assurance? Consider the capability of the staff members responsible for disclosing the information. Do you think staff will be appropriately trained on what is/ isn't acceptable disclosure of personal information? What protocols will be in place to support the staff members undertaking the disclosure? Will staff members be able to determine when and what should be disclosed? Are delegations clear and in place (where required)? How will you ensure these are followed?

Discuss any other concerns, issues, uncertainties or questions you have about how your initiative complies with this principle.

Risk Identification

Link to Risk Register	A full technical risk assessment, including consideration of Privacy risks, has been conducted for the MCL LAS solution. See http://mako.wd.govt.nz/otcs/lisani/all/mobview/63964471
-----------------------	--

GUIDANCE NOTES

Record the link to the initiative risk register. The MBIE Risk Register template can be found here - <http://theink/how/Pages/find-the-cpo-project-delivery-templates.aspx>

Risk Number	Risk Description <i>Description of the privacy risk (i.e.: the actual/root risk, not the symptom of the risk)</i>	Consequences <i>Key things that may happen if the risk materialises</i>
P11_1		
P11_2		
P11_3		
P11_4		
P11_5		
P11_6		

Record all privacy risks arising from the analysis and discussion points above. Add more rows as required.

Where privacy risks are identified, these must be appropriately managed. Copy these risks into the appropriate risk register (this may be the master initiative risk register, or a specific privacy risk register).

Complete the risk register template by recording: existing controls in place to manage the risk; planned activities, actions, roles, or programmes to treat the risk; and the outcome of the controls and treatments. Ensure responsibilities are identified and regular reviews of the risks, controls, and treatments are undertaken.



PRINCIPLE 12 - PRIVACY IMPACT ANALYSIS

Once you have completed the Data Flow template, information related to Principle 12 will be automatically copied to this worksheet. Refer to this information to help you to complete an Impact Analysis and identify the risks associated with Principle 12.

- If you have more than five categories on your Data Flow template, add more columns (to the right of column F) so the number of columns on this worksheet matches your Data Flow template. Copy the formula from column F to the new columns so the data from the Data Flow template is copied over.
- Complete the 'Initiative Details and Sign off' section (in white).
- Complete the 'Privacy Analysis and Discussion Points', and 'Risk Identification' sections (in white). Guidance notes are provided to the right in orange.
- Business owner sign off is required.



INITIATIVE DETAILS AND SIGN OFF	
Initiative name:	Emergency Caller Location Information : Phase 2 - iOS and Rebidding
Brief description of initiative:	The MCL project will address longstanding operational requirements of Emergency Service Providers for probable caller location information from mobile phones. The outcome sought is for the best available caller location to be sent to an emergency service provider when a 111 call is made, without requiring the caller to do anything more than dial 111 on the standard keypad of their mobile phone.
Name and role of person completing template:	Ben Quay, MCL Project Director
Template completion date:	31/08/2016 updated 27/02/2017, updated further 21/11/2017
Business owner name and sign-off:	Brad Ward, GM CCC and ECU business owner

Information recorded on Data Flow Template	
List any unique identifiers being used and describe why it is necessary to use them	A unique identifier is assigned to the probable caller location information for the purpose of enabling the location agency to audit and monitor the operation of the LAS and the methods by which the information is collected. Noting that identifiable data will not be retained.

Privacy Analysis and Discussion Points	GUIDANCE NOTES
The key requirement of Principle 12 of the Privacy Act is that an agency shall not assign a unique identifier to an individual unless the assignment of that identifier is necessary to enable the agency to carry out one or more of its functions efficiently.	Use this template to record your thoughts and considerations. This is not a formal report so notes and bullet points are acceptable. The important part is to ensure all relevant considerations are recorded and considered. This template is designed to be completed iteratively, it doesn't need to be completed in one go.

Describe how your initiative complies (or does not comply) with this Principle and summarise any privacy related discussion points. Discussion points may include concerns, issues, uncertainties or questions you want to explore further. Record and evaluate potential options for addressing any discussion points, including identifying any options/solutions that enhance or could enhance privacy practices. Discussion points may identify privacy risks which need to be managed. Describe how the use of the unique identifier enables the initiative or activity to be carried out efficiently. Where unique identifiers are used to match data in different databases, describe why this is necessary. Specific legal authority is required if you collect another unique ID and record it, and it must be necessary for the purpose of your initiative or change. Describe if there is an explicit legal authority to use unique IDs from another organisation (e.g. tax number, medical number or passport number). Record how it is necessary for the purpose of your initiative or activity. Where an individual is required to provide or disclose their unique identifier, describe why it is required. Describe the consequences of the individual not providing their unique identifier, both for the individual and for the initiative or activity. Consider whether the outcomes of your initiative can be achieved without assigning a unique identifier. Discuss any other concerns, issues, uncertainties or questions you have about how your initiative complies with this principle.

Risk Identification	GUIDANCE NOTES
----------------------------	-----------------------

Link to Risk Register	A full technical risk assessment, including consideration of Privacy risks, has been conducted for the MCL LAS solution. See http://mako.wd.govt.nz/otcs/lisapi.dll/overview/63964471
-----------------------	--

Risk Number	Risk Description <i>Description of the privacy risk (i.e.: the actual/root risk, not the symptom of the risk)</i>	Consequences <i>Key things that may happen if the risk materialises</i>
P11 1		
P11 2		
P11 3		
P11 4		
P11 5		
P11 6		

Record all privacy risks arising from the analysis and discussion points above. Add more rows as required. Where privacy risks are identified, these must be appropriately managed. Copy these risks into the appropriate risk register (this may be the master initiative risk register, or a specific privacy risk register). Complete the risk register template by recording: existing controls in place to manage the risk; planned activities, actions, roles, or programmes to treat the risk; and the outcome of the controls and treatments. Ensure responsibilities are identified and regular reviews of the risks, controls, and treatments are undertaken.

Record the link to the initiative risk register. The MBIE Risk Register template can be found here - http://thelink/how/Pages/find-the-cpo-project-delivery-templates.aspx
--

RELEASED UNDER THE OFFICIAL INFORMATION ACT



IN CONFIDENCE



ECLI Phase 2 Extension Privacy Impact Assessment Report

Version 1.2

2 December 2020

RELEASED UNDER THE
OFFICIAL INFORMATION ACT

Version control

Version	Author	Description of change	Date
0.1	Keziah Ferrer	Initial Draft.	29 July 2019
0.2	Keziah Ferrer	Updated Draft incorporating feedback from reviewers and review session with the Project team. Incorporated feedback from second round of review.	26 August 2019
0.3	Keziah Ferrer	Incorporated Office of the Privacy Commissioner feedback.	20 September 2019
0.4	Susan Ng & Alan Heward	Updated to align with TIPC Amendment No 7 and removed UC02. Added note on new IPP12. Various changes to reflect implementation of points that were proposals at the time of v0.3.	March-July 2020
0.5	Susan Ng	Updated with feedback from reviewers and sent to OPC for feedback.	5 Aug 2020
0.6	Susan Ng	Updated with feedback from OPC and sent out for team review.	19 Aug 2020
0.7	Susan Ng	Incorporated feedback from team review.	25 Aug 2020
0.8	Susan Ng	Clarification to data flows. Sent to Nikki Farnworth for review.	9 Sep 2020
0.9	Susan Ng	Updated with feedback from Martien Duis, Appendix 2 and minor updates to privacy safeguards.	1 Oct 2020
1.0	Susan Ng	Replaced references to TIPC 2003 to TIPC 2020.	2 Dec 2020
1.1	Marcus Sullivan & Sam Taylor	Updated to reflect changes across ECLI and DLI since 2020. Updated to current MBIE PIA template	1 July 2024
1.2	Sam Taylor	Updated with feedback from project team. Phrasing corrections for accuracy and minor updates to Figure 2 for correctness.	1 August 2024

Consultation

Reviewer	Comments	Date
Susan Ng	Peer review	01/08/19
Alan Heward	Peer review	01/08/19, June-August 2020
Ben Quay	Management review	01/08/19
Peter Fernando	Legal review	01/08/19 (v0.2) and 29 July 2020 (v0.4)
Pam Harris	Management review	21/08/19 and 21 January 2021 (v1.0)
Martien Duis	Legal review	25 September 2020
Nikki Farnworth	Privacy Advisor, MBIE	18 September 2020
Tim Higgs	Peer Review	24 July 2024
Clint Sommers	Peer Review	30 July 2024

Review and sign-off

Name	Role	Date
James Hartley	Business Owner, General Manager, Commerce Consumers and Communications	21 April 2021

RELEASED UNDER THE
OFFICIAL INFORMATION ACT

Contents

Executive Summary..... 5
 Recommendations 6
Initiative Summary 7
 Use Case Assessment..... 8
 Summary of Privacy Impact Assessment 11
PIA Methodology 12
 Scope..... 12
 The Process 12
Information Flows 13
Personal Information 19
Privacy Analysis..... 22
Risk Assessment..... 29
Actions to enhance or minimise impact on privacy..... 34
Conclusion..... 37
Appendix A – Risk Matrices..... 39
Appendix B – PIA Consultation 41

RELEASED UNDER THE
OFFICIAL INFORMATION ACT

Executive Summary

The ECLI service (**the Service**) enables emergency call-takers to receive automatically generated geographical information about the location of a caller when an “emergency call” (as defined under the Telecommunications Information Privacy Code 2003 (**TIPC**)) is connected to a mobile cellular network, from any mobile phone.

In May 2017, MBIE launched the Service, and has since progressively enhanced it by adding new features, functions, and location methods; these and many other enhancements result in a highly available, robust system that is a critical part of the emergency calling service.

The Service is successful in providing life-saving carrier-grade emergency telecommunications services to Emergency Service Providers (**ESPs**). Providing prompt, precise, and accurate location information contributes to time savings for ESPs and improves their delivery and operational performance to save lives and property.

Following requests from NZ Police and NZ Search and Rescue for the ECLI service to be extended, to provide location information for emergency response situations beyond 111 calls, the ECLI team developed a set of use cases, highlighting instances where an outcome could have been improved or changed if extended ECLI capability was available ([ECLI Phase 2 Capability Extension Use Cases v1.0](#)). The use cases were shared with the Office of the Privacy Commissioner (OPC), who gave their support for the extended use of the service in ‘active’ situations (where a device is now). Following a public consultation, the Privacy Commissioner authorised the extension of the service “to enable emergency services to more quickly locate people at risk of harm but who have not made a call to 111”.

On 7 May 2020 Amendment No7 of the TIPC came into effect, providing the regulatory framework for the extended use, known as Device Location Information (DLI).

A Privacy Impact Assessment (PIA) - ECLI Phase 2 Extension was developed to identify the associated risks and processes to manage them. This was socialised with key external stakeholders as part of the wider consultation process and approved by the ECLI Business Owner in April 2021. This PIA has been updated (in 2024) to reflect the current status and technology updates since 2021.

In June 2023, MBIE and NZ Police sought the support of Ministers to prepare a Cabinet paper, in consultation with other relevant agencies seeking approval to extend the scope of the ECLI service. This Cabinet paper was subsequently approved by Ministers and the implementation of DLI is scheduled for 2024.

With this implementation, ESPs will be able to leverage DLI in the following situation:

- **Extend emergency response coverage** – Extend service coverage to emergency response situations beyond 111 calls and provide location information to ESPs and Search and Rescue (SAR) operations. The [TIPC 2020 Schedule 4](#) enables and regulates the privacy aspects of this Service extension. Schedule 4 includes a new definition “Emergency Location Information” (**ELI**) in relation to information received, collected, used, processed, held, and disclosed in accordance with the TIPC 2020 Schedule 4.

A foreseeable consequence of enabling the service extension to emergency response situations beyond 111 calls, is that the underlying technology (which technically enables device location information to be retrieved on request) has the potential to be leveraged by Public Safety

Organisations (**PSOs**) who may obtain warrants authorising the collection, disclosure, and use of device location information (**DLI**) for a purpose not authorised by Schedule 4 of the TIPC 2020.

In these circumstances DLI will not be collected and disclosed under TIPC 2020 Schedule 4, but rather under the authority of the warrant issued. Unwarranted access to DLI for a purpose not authorised by Schedule 4 is not permitted. While the collection of any additional information by MBIE carries with it the consequence that this information may be accessed under the authority of a warrant, given the sensitivity of the information that may now be accessed through extension of the Service, this document discusses the following, additional, use case for the purposes of transparency.

- **Allow for warranted access to active location information as a consequence of the Service extension** (i.e. where a device is now) – Provide active location information for public safety and law enforcement organisations to support their primary objectives in circumstances authorised by law (under a warrant). Where an agency seeks active location information for any purpose not specifically provided for in TIPC 2020 Schedule 4, any provision of such information would be subject to authorisation under the appropriate Act (e.g. Intelligence and Security Act or Search and Surveillance Act).

Recommendations

Considering this PIA, the following activities (in addition to existing Privacy protections) are recommended to ensure that the Service remains compliant with Privacy Act 2020 and TIPC 2020, therefore ensuring the privacy of the personal information collected. These recommendations are in order of priority and contribute to the reduction of the risk ratings:

1. **PS06 – ECLI Privacy Framework and PS08 Consult Privacy Commissioner** – Finalise and implement the [Privacy Framework](#) for the Service extension to enable a standardised approach to lawful disclosure and use of location information by authorised parties. This will include reporting, assurance and governance structures to support transparency and ensure continued legal compliance. The Privacy Framework has been designed in collaboration with the ESPs and the Office of the Privacy Commissioner (**OPC**) was consulted regarding the overall framework. The Service will continue working with the ESPs and OPC to implement the privacy framework.
2. **SC12 – Monitoring and alerting** – Implement and test the effectiveness of the enhanced monitoring and alerting for the ECLI Phase 2 Extension (e.g., being able to investigate sudden spikes within the Service).
3. **PS09 – Proactive release** – Ensure relevant ECLI Phase 2 Extension information and documents are proactively released.
4. **PS10 – Extended background checks for named individuals** – Ensure all users who have access to the Service undergo appropriate background checks relevant to their roles.
5. **SC32 – Privacy statement & Policy on website** – Review and update Privacy statement and Policies on MBIE and ESP websites to ensure that the TIPC 2020 and Service extension are covered by their policies.
6. **SC33 – SOPs for Privacy** – Ensure all relevant business standard operating procedures (**SOPs**) are created or updated to reflect the use case that will be implemented in Phase 2 ECLI Extension and use case that will be implemented because of this i.e. warranted access. Ensure any new or updated SOPs provided by the Service are communicated to all ESPs and PSOs.

The following recommendations are not directly related to a specific risk but have been recommended as additional compliance mechanisms:

7. **Reporting and Analytics** – Guidance on data and analytic principles from the OPC¹ for reporting purposes should be considered to support safe and effective data analytics.
8. **Regular Privacy Impact Assessments** – Revisit this PIA each time a major enhancement or functionality change is proposed to ensure that any new risks are captured and addressed.

Initiative Summary

This PIA has been conducted to consider all privacy risks associated with the use cases that MBIE has identified for implementation at present. Therefore, it is not limited to TIPC Schedule 4, but also includes a privacy impact assessment to identify risks associated with allowing warranted access to active location information and mitigation strategies in relation to the same.

The proposed use of the Service extension to provide extended emergency response coverage is legal and is regulated by the TIPC. Further, the Service being called upon in relation to warrants authorising DLI collection and disclosure to PSOs is governed by the applicable law enforcement Acts providing warranted access. The two use cases of the Service extension will enhance New Zealand's emergency services, search and rescue operations, public safety and law enforcement initiatives.

From a social licence and benefit perspective, the risk to life or health and safety of an individual has a greater social benefit than the potential infringement on an individual person's privacy. Use of the Service for this purpose is demonstrably necessary and remains proportionate to minimising the potential privacy intrusions.

Privacy safeguards and security controls will be in place to ensure the risk and potential harm of unlawful or unauthorised use or disclosure are managed within the Service.

Detailed analysis of the privacy implications of the collection, use and disclosure of DLI, having regard to the two use cases above, is covered in the [Privacy analysis](#) section of this report.

¹ Principles for safe and effective use of data and analytics - <https://privacy.org.nz/news-and-publications/guidance-resources/principles-for-the-safe-and-effective-use-of-data-and-analytics-guidance/>

Use Case Assessment

The following table defines an assessment of the scenarios that will be supported by the Service extension and how they are provided for in the TIPC 2020 Schedule 4 or the applicable law enforcement Acts providing warranted access.

	Scenario	Service Response	Covered by
	The emergency caller who calls 111 is the person-in-need who stays on the call until their location is verified. (This is the existing ECLI service)	ECLI is activated automatically and ESP attending the call is able to use ECLI to verify the caller's location.	TIPC 2020 Schedule 4
Extend Emergency Response coverage (DLI)			
	Provide ESPs responding to emergency response situations with location information of a mobile device that wasn't used to make an emergency 111 call . Example: A person threatening self-harm goes missing after calling their parent. The parent calls 111. Police receive the 111 call and need to locate the person threatening self-harm quickly after the person doesn't respond to calls from Police.	ECLI is automatically activated for the parent, but this is not the location required for the emergency response. Police would assess the "serious threat" conditions (based on their defined serious threat model) and activate location detection for the device of the person-in-need. Since the person-in-need is not the emergency caller, Police would request the Service to provide device location information (DLI) as defined in the TIPC, for the mobile device of the person-in-need.	TIPC 2020 Schedule 4 TIPC 2020 Schedule 4
	Enable improved patient/event outcomes by allowing all ESPs to continue querying location information after an emergency 111 call has been disconnected (e.g. caller falls unconscious and disconnects call accidentally, device stops operating, caller travelling through cell black spots with limited/no coverage, etc.) Examples: 1. FENZ transfers several calls to Police but if there is call loading at Police, FENZ are unable to transfer the 111 call in progress. Police are unable to continue receiving the location after the 111 call is disconnected. 2. Search and rescue missions where the emergency caller is the person-in-need but moves location after making the 111 call. The search and rescue mission requires a location update after the 111 call is terminated.	ECLI is activated and updated while the 111 call is in progress. When the 111 call is disconnected, ECLI updates are automatically terminated. The ESP will have to request Police to approve and submit a request to receive location updates as DLI provided by the Service.	TIPC 2020 Schedule 4 TIPC 2020 Schedule 4

	Scenario	Service Response	Covered by
	<p>The scenarios below describe situations where an ESP requires the location for a specific device for emergency response but there is no associated emergency call or caller:</p> <ul style="list-style-type: none"> • An ESP has concern for the safety of a missing person (regardless of whether the person wishes to be found) • An ESP learns about a potential life threatening event in progress (not necessarily from a call) • An ESP receives a distress call transferred from another provider (e.g. Mental Health organisation, Plunket Line, Health Line, etc.) or from a non-111 line managed by an ESP e.g. NZ Police’s 105 (ten five) service for non-emergency calls, *555 for road accidents/incidents, ESP general phone numbers, etc. <p>Examples:</p> <ol style="list-style-type: none"> 1. Police receive call about a missing tramp who is not responding to calls to check on their safety. 2. A caller has just witnessed somebody being taken and driven away against their will. 3. A person has made a threat on a social media live feed in relation to killing a Member of Parliament. The person making the threat is known to Police, but it is unknown if they have the ability to follow through on it. 4. Whakarongorau Formerly Homecare Medical receives a suicide attempt call where the caller provides vague information about their location. Whakarongorau alerts an ESP who calls the person directly but there is no response. The ESP requires an accurate location for the emergency response unit and to avoid spending extra time combing the area in an attempt to locate the person. 5. Police pursuing an offender with a firearm that was used against Police. The offender is on the move. Police need to locate the offender quickly before any member of the public or Police could potentially be put in danger. 6. Police are contacted by a caller who has received a call from an abusive partner who is on a violent rampage and is threatening to go to the caller’s house to inflict harm. Police not only require the caller’s location but also need to locate the partner quickly. 	<p>The ESP would assess the “serious threat” conditions and request NZ Police to review/approve the request for DLI. OIA 6(c)</p>	<p>TIPC 2020 Schedule 4</p>

	Scenario	Service Response	Covered by
OIA 6(c)			

RELEASED UNDER THE
OFFICIAL INFORMATION ACT

Summary of Privacy Impact Assessment

A privacy risk workshop with key project stakeholders including the ECLI Programme Director, ECLI Risk and Security Advisor and ECLI Senior Business Analyst identified privacy risks and rated the risks using the MBIE Risk Management Framework. The workshop participants also reviewed and identified the appropriate privacy safeguards and security controls in place to manage these risks.

The risks related to the ECLI Phase 2 extension were then reassessed against TIPC 2020 Schedule 4 and the twelve (12) information privacy principles of the Privacy Act and rated based on the consequence and the likelihood of the risk occurring.

The risks were given a *current risk rating* considering the current privacy safeguards and security controls in place to manage that risk, as well as *target risk rating* that considers any additional privacy safeguards or security controls that will be in place for the ECLI Phase 2 Extension.

A total of fifteen (15) privacy risks (Table 5 - PIA Risk Matrix) were identified; Two (2) were rated as Medium, nine (9) were rated as Low, four (4) were rated as Very Low and no risks were rated as High or Very High for the current risk ratings. This is because there are existing privacy safeguards and security controls in place for the Service and the effectiveness of these controls were assessed in the previous Security Accreditation for Phase 1 of the Service. As most of the identified risks are already managed by the Service a cross reference of the correlated risks is shown in Table 6 – Privacy cross reference to existing ECLI Risk Matrix.

See [Privacy Impact Assessment](#) section for the detailed privacy findings.

Subsequently, twelve (12) privacy safeguards and twenty-four (24) security controls have been recommended to treat risk and enhance privacy. The workshop participants considered that with full application of effective security controls and the proposed implementation of the privacy safeguards the target residual risk ratings are lowered, with one (1) rated as Medium risk, ten (10) rated as Low risk, with the remaining four (4) reassessed as Very Low.

PIA Methodology

Scope

The scope of the PIA is for the Service extension, including the following activities:

- Analysis and descriptions of the data flows as they relate to the collection, aggregation, storage, receipt, transmission and destruction of personal information contained in and transacted by the Service.
- Analysis of the Information Privacy Principles (IPP), as they relate to the information and data flows in the Service and particularly in the context of TIPC 2020 Schedule 4; and
- Identification, description, and assessment of risks to privacy including identifying privacy safeguards and security controls.

Out of Scope

Excluded from the scope of the PIA are:

- The privacy analysis, assessment or review of systems that inform or receive data from the Service (e.g. mobile network operators (MNOs) systems, ESP systems);
- Aspects of information security not relevant to Information Privacy Principle 5, i.e. integrity or availability considerations; and

Sampling, testing or auditing of any security controls implemented by MBIE, Service Providers and ESPs.

The Process

The privacy risks have been reviewed and assessed in collaboration with the key stakeholders.

This PIA was initiated in mid-to-late 2019, with a finalised version confirmed with the Office of the Privacy Commissioner at the time. Subsequently updates have been made to reflect Amendment No 7 to the TIPC (which was issued as TIPC 2020 in December 2020), which specifically affects the Service. After this, in late June 2020, the new Privacy Act 2020 was passed, coming into effect from 1 December 2020. The current version of this PIA considers all of the previous and updates and changes to the Service technology since 2020 in preparation of the implementation of the DLI service into production.

Information Flows

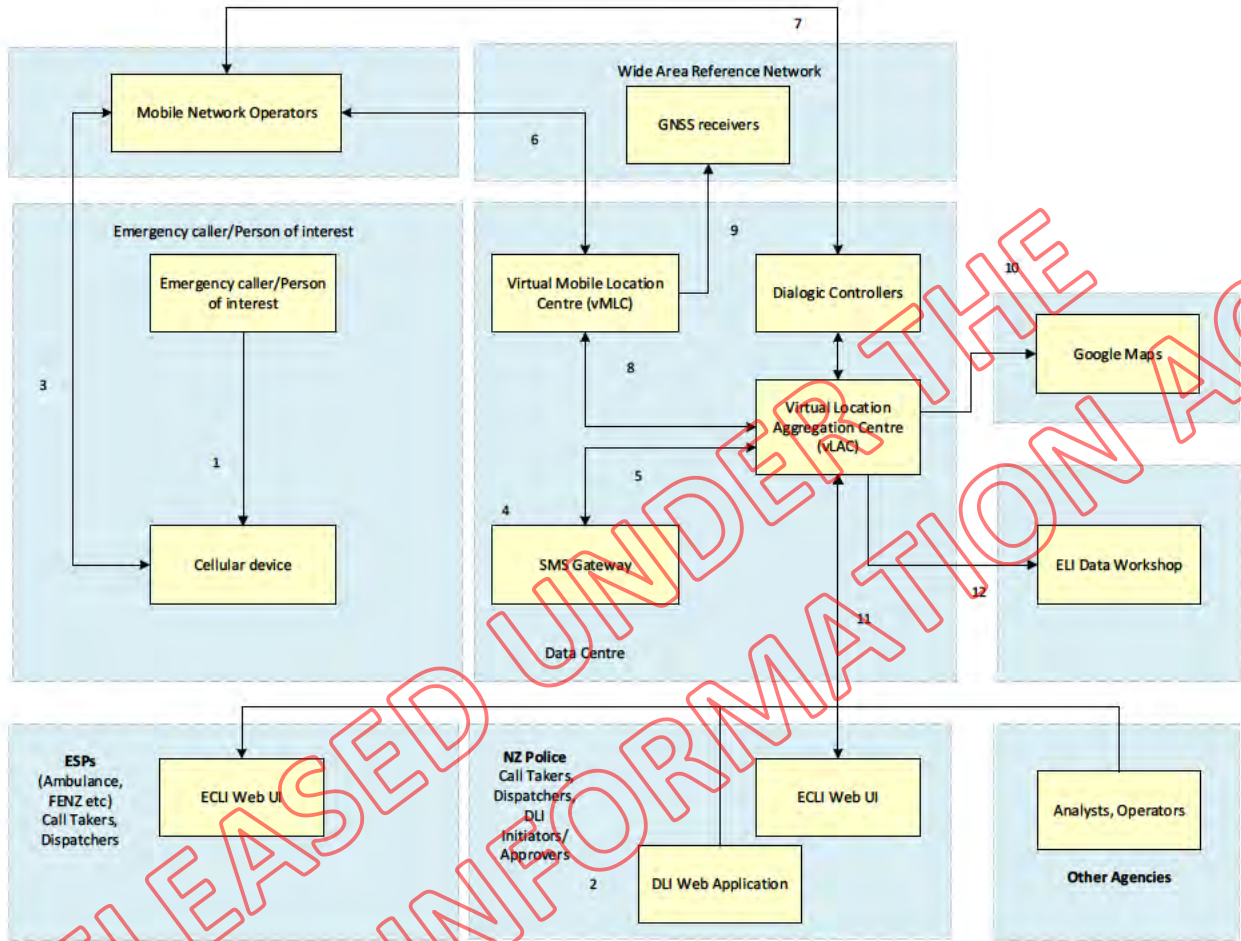


Figure 1: Information Flows – summarised view

Information flow	ECLI	DLI
1. The emergency caller or person of interest has a cellular device that is used to collect location information via the mobile network. The cellular device is used to make an emergency call (in the case of ECLI) and/or used by the Service to query location information (in the case of DLI).	Yes	No
2. A request for DLI is made through the DLI web application. [Redacted]	No	Yes
3. For an emergency call, the MNOs receive and transmit location information from a cellular device.	Yes	Yes
4. When an emergency caller calls 111, the SMS Gateway receives AML SMS messages from AML-enabled cellular devices. Android AML rebidding (implemented in December 2019) provides AML updates every 2 minutes.	Yes	No

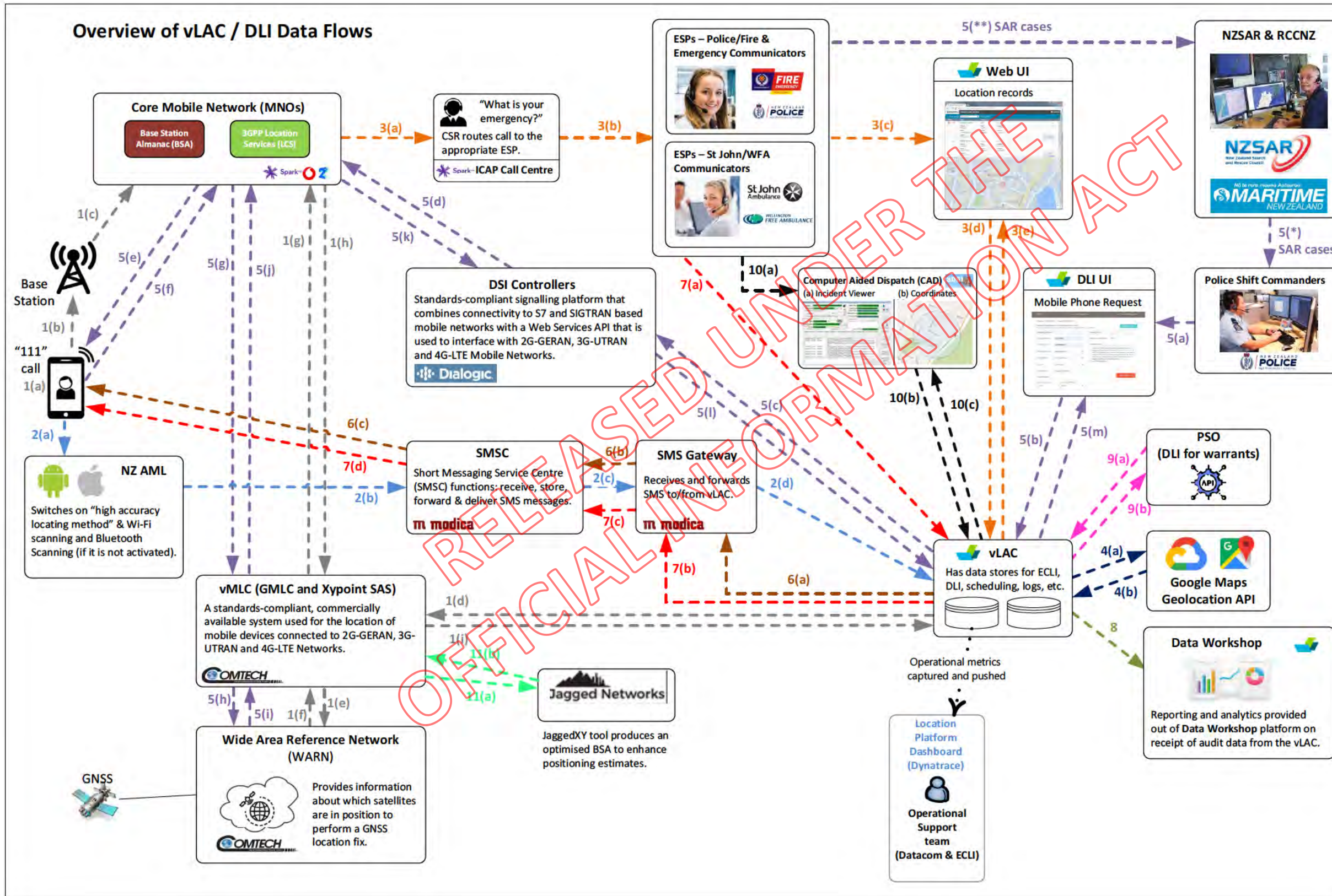
Information flow	ECLI	DLI
<p>5. The SMS Gateway communicates with the vLAC through a vLAC service interface (OIA 9(2)(c)). For 111 calls, this flow receives the message originating from the AML SMS message. This flow also delivers outbound text SMS messages to cellular devices as follows:</p> <ol style="list-style-type: none"> ESP communications to callers, i.e. Post-Dispatch Information (PDI) sent by St John and WFA, Post-Call Instruction (PCI) sent by NZ Police SMS notification of DLI detection (TIPC 2020 Schedule 4 section 4). 	Yes	Yes
<p>6. The virtual Mobile Location Centre (vMLC) integrates directly with MNO mobile networks to deliver richer location information for all cellular devices.</p>	Yes	Yes
<p>7. The Dialogic Controller integrates directly with MNO mobile networks to deliver location information for active cellular devices in the case of DLI.</p>	No	Yes
<p>8. The vMLC is also used to request updated location records from the respective MNOs for ongoing mobile based emergency calls. The following components are used in this flow:</p> <ul style="list-style-type: none"> 3GPP Location Services (LCS) – MNOs core 3G UTRAN and 4G E-UTRAN mobile networking components with 3GPP standards compliant location services enabled interfaces. Used by the vMLC to calculate the location of a mobile based emergency call (for ECLI) or a cellular device (for DLI). MNO Signalling Endpoint – Networking component used to manage signalling traffic between the MNOs and the vMLC. MNO Base Station Almanac (BSA) Configuration file that defines the cell site characteristics for the MNO. <p>The resulting location information is then forwarded from the vMLC to the vLAC, including updated location records for ongoing mobile based emergency calls and/or the duration of DLI collection requests.</p>	Yes	Yes
<p>9. The vMLC interacts with GNSS receivers in the Wide Area Reference Network (WARN) to provide information about satellites that are in position to perform a GNSS location fix.</p>	Yes	Yes
<p>10. The Service invokes Google Maps.</p>	Yes	Yes
<p>11. NZSAR, ESPs, PSOs and other agencies use the Service to obtain the mobile caller's ECLI or cellular device's DLI.</p>	Yes	Yes
<p>12. Operational data is anonymised and pushed to the Data Workshop platform to provide dashboard reports that visualise business performance metrics.</p> <p>Report/audit location data from the Service and Type Allocation Code reference data, genuine call data and benefit reporting data are provided to the Data Workshop platform. Any personal information is anonymised via obfuscation and/or hashing during the data ingestion process. Disclosure log reporting (TIPC 2020 Schedule 4 clauses 7(3) and 8(3)) will use anonymised data. OIA 6(c)</p>	Yes	Yes

Information flow	ECLI	DLI
OIA 6(c)		

Figure 2 below presents an enriched view of the abstracted information flows and interactions shown in Figure 1 above. Figure 2 aligns directly with other design documentation for the Service.

RELEASED UNDER THE
OFFICIAL INFORMATION ACT

Figure 2: Information Flows – detailed view



Information flow	ECLI	DLI
<p>Flow 1 Determine GPS location fix (grey flow in Figure 2):</p> <ul style="list-style-type: none"> [1(a) – 1(c)] When an emergency caller uses a telecommunications device to make an emergency 111 call, the location information is transmitted to the MNO Base Station and the MNO Core Mobile Network. [1(d) – 1(i)] The 111 call triggers the vLAC to request the vMLC to make direct requests to the WARN and MNO Core Mobile Networks to provide richer GPS location information back to the vLAC. The vLAC requests fresh locations every 10 minutes for the duration of the call. See Figure 1 #6 and also Flow 3 below. 	Yes	No
<p>Flow 2 AML location message: (light blue flow)</p> <p>[2(a) – 2(d)] An emergency 111 call from an Android or Apple iOS smartphone will trigger an AML message with high accuracy location information to be sent via the Short Messaging Service Centre (SMSC) and SMS gateway to the vLAC. See also Figure 1 #4.</p>	Yes	No
<p>Flow 3 ESP 111 call handling (orange flow)</p> <p>[3(a) – 3(b)] At the same time as Flows 1 and 2 above, an emergency call is received by the Initial Call Answering Platform (ICAP) Call Centre. Staff at the ICAP Call Centre route genuine emergency calls to the appropriate ESP.</p> <p>[3(c) – 3(e)] An ESP call taker who attends to the emergency call uses the ECLI web user interface (UI) to query the ECLI of the phone that made the 111 call. Typically, Flows 1 and/or 2 would have completed and their resulting location(s) are presented to the call taker. The ESP call taker can also refresh the query to retrieve fresh location updates during the call.</p> <p>If the ESP call taker determines that DLI collection is required for a person of interest who is not the 111 caller, Flow 5 is then triggered.</p>	Yes	No
<p>Flow 4 Location mapping (dark blue flow)</p> <p>[4(a) – 4(b)] The vLAC makes calls to the Google Maps Geolocation API to render mapping visualisation data.</p>	Yes	Yes
<p>OIA 6(c)</p>	No	Yes
<p>Flow 6 DLI SMS notification (brown flow)</p> <p>[6(a) – 6(c)] This flow sends an SMS to the cellular device to notify DLI collection.</p>	No	Yes

Information flow	ECLI	DLI
<p>Flow 7 Post-Dispatch Information (PDI) and Post-Call Instruction (PCI) (red flow)</p> <p>[7(a) – 7(d)] St John and WFA use this flow to send additional Post-Dispatch Information (PDI) and Post-Call Instruction (PCI) to the person of interest e.g. to notify patient care instructions while waiting for the ambulance to arrive.</p>	Yes	Yes
<p>Flow 8 Reporting & monitoring (green flow)</p> <p>[8] Operational data is presented as dashboard reports to monitor service performance. Audit information is anonymised and ingested into the Data Workshop platform.. Disclosure log reporting for DLI (TIPC Schedule 4 sections 7(3) and 8(3)) will be produced using anonymised data stored in the Data Workshop platform.</p>	Yes	Yes*
<p>Flow 9 DLI API requests from PSOs (pink flow)</p> <p>[9(a) – 9(b)] PSOs may submit warranted requests for DLI collection. A future technical development may enable warranted DLI requests via an API. With this API option, the vLAC follows Flow 5 to collect the requested DLI that is stored in the vLAC until it is retrieved by the PSO. In case of warrant based DLI requests, the vLAC has multiple data stores, each data store is specific to only one PSO to allow that PSO to request and access DLI generated for them. This safeguards data privacy such that the data requested by one PSO is not inadvertently accessible to other PSOs. DLI is expunged from the vLAC when it is delivered to or retrieved by the PSO. DLI related location information, for PSOs, will not be ingested into the reporting and analytics platform.</p>	No	Yes
<p>Flow 10 CAD Integration with Ambulance (black flow)</p> <p>[10(a) – 10(b)] This flow sends ECLI to the St John and WFA CAD system. When the St John or WFA receives a 111 call, the CAD system requests the ECLI available for that phone number and populates the ECLI details into the CAD. Typically, flows 1 and/or 2 would have completed and their resulting location(s) would be integrated into the CAD.</p>		
<p>Flow 11 JaggedXY BSA Optimisation (bright green flow)</p> <p>[11(a) – 11(b)] Location detail records are sent from the vMLC to the JaggedXY tool. JaggedXY creates an optimised Base Station Almanac (BSA) and pushes this back into the vMLC. This optimised BSA is then loaded and used by the vMLC when doing its positioning estimates.</p>		

Personal Information

The following table categorises the PI that is collected, retained, used and disclosed in the ELIS, the various system environments and its format within these. This exists as a reference for all systems and components which form part of the ELIS and technical artefacts.

Table 1 – PI collected by the ELIS reproduced from [ELIS Personal Information Standard](#)

The current ELIS comprises the following:

- Location Platform (and associated software components)
- Data Workshop (and associated software components)
- virtual Mobile Location Centre (vMLC) (and associated software components)
- JaggedXY
- Dialogic DSI controllers (and associated software components)

Personal Information Categories	Systems Environment	Format
<p>1. Biometric, physical, and behavioural information</p> <p>Location Information (geospatially rendered or as data files). Location Information itself is classified as PI and it <u>does not</u> have to be combined with other unique identifier(s) e.g. a mobile device number to meet this classification.</p> <p>Location information means personal information indicating the approximate geographical position of a device, which may include the latitude, longitude, altitude and direction of travel of that device.</p> <p><i>NB: The ELIS does not collect, use, or store biometric data.</i></p>	<p>Production Platform, including back-ups – accessible only to authorised ELIS, MBIE, Comtech (for location services) and Datacom personnel (for operational support).</p> <p>Production Platform only, accessible only to authorised users of the ELIS including Emergency Service Providers (ESPs) and the Relevant Government Agency.</p>	Raw data
	<p>Development/Test Platforms – accessible only to authorised ELIS, MBIE, Comtech and Datacom personnel for development, testing and operational support of the ELIS</p>	Raw <u>test</u> data, including consensual use of personal mobile devices, or dedicated test devices.

Personal Information Categories	Systems Environment	Format
<p>2. Contact information / Unique Identifiers</p> <p><i>Mobile device number (MSISDN)</i> – used to contact the device.</p> <p><i>International Mobile Subscriber Identity (IMSI)</i> – used by the mobile network operator to identify the subscriber. The first 3 digits represent the mobile country code (MCC), which is followed by the mobile network code (MNC), either 2 or 3 digits. The remaining characters contain unique information (which ELIS obfuscates).</p> <p><i>International Mobile Equipment Identity (IMEI)</i> – used by the mobile device manufacturer to identify the model and its origin. It is a 14 – 16 character code, the first 8 characters identifying the 'Type Allocation Code' (TAC) which defines the model and origin of the phone, the remaining characters contain unique information (which ELIS obfuscates).</p>	<p>Reporting and Analytics – accessible only to authorised ELIS personnel and MBIE Systems Administration (who require access to manage enterprise level applications) for systems reporting and analytics.</p> <p><u>Anonymised</u> (unique identifiers) and aggregated reporting and analytical outputs are made available to ESPs, Mobile Network Operators (MNOs) and the ELI team.</p>	<p>OIA 9(2)(c)</p>
<p>3. User Information</p> <p>User access for ESPs, the Relevant Government Agency, and third-party support vendors</p>	<p>Production Platform, including back-ups – accessible only to authorised ELIS, MBIE Systems Administration (who require access to manage enterprise level applications), and Datacom personnel for operational support.</p>	<p>Raw data</p>

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Personal Information Categories	Systems Environment	Format
<p>And</p> <p>'Initiator' and 'Approver' user roles to identify NZ Police individuals who can raise and who can approve a DLI request.</p>	<p>Production Platform only, authorised users of the Service including ESPs and the Relevant Government Agency.</p>	
	<p>Development/Test Platforms – accessible only to authorised ELIS, MBIE and Datacom personnel for development, testing and operational support of the Service.</p>	<p>Raw <u>test</u> data</p>
	<p>Reporting and Analytics – accessible only to authorised ELIS personnel and MBIE Systems Administration (who require access to manage enterprise level applications) for systems reporting and analytics.</p> <p>Reporting and analytical outputs are made available where user ID is authenticated and/or 'Approver' names are used to inform ESPs and the EII team.</p>	<p>Raw data</p>

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Privacy Analysis

The privacy analysis follows the information 'life cycle' of personal information, through its collection, use, retention, processing, disclosure and destruction.

Table 1 - Privacy Analysis

Principle	Requirement	Assessment	Privacy Risks and whether it is an existing or new risk
Principle 1 – Purpose of Collection	<p>Principle 1 of the Privacy Act states that personal information should only be collected for a lawful purpose connected with a function or activity of the agency, and the collection of the information is necessary for that purpose. The key requirements of Principle 1 are to:</p> <ul style="list-style-type: none"> Identify all the personal data that will be collected and used by the proposed change or initiative; Be convinced that the personal information collected is necessary to meet the purpose of the proposed initiative. The purpose of the initiative or change must be lawful and connected with the business function or activity of the agency. If the lawful purpose for collecting personal information does not require the collection of an individual's identifying information, the agency may not acquire the individual's identifying information. 	<p>In the TIPC Amendment No 5 Schedule 4 – ECLI (mobile), the collection of ECLI information is authorised for the following purposes:</p> <ul style="list-style-type: none"> the permitted primary purpose is to enable an emergency service provider to facilitate a response to an emergency call. the permitted secondary purpose is to maintain records of the ECLI used to establish the location of an emergency caller and to help monitor and audit the operation of the Service system. <p>Both of above categories are necessary and proportionate in the disclosure of PI.</p> <p>Information currently collected is automatic and requires no user interaction beyond the original initiation of a 111 call.</p> <p>For ECLI Phase 2 Extension, UC01 for extended emergency response will provide active location (where a device is now) and location information of cellular devices in the absence of an emergency call from the individual as authorised by the prevailing TIPC 2020 Schedule 4. ECI will be provided to extend the emergency response coverage beyond 111 calls and support search and rescue operations.</p> <p>OIA 6(c)</p> <p>UC01 and UC03 are necessary and proportionate in the disclosure of PI.</p> <p>Information currently collected is automatic and requires no user interaction beyond the original initiation of a 111 call.</p> <p>In preparation for ECLI Phase 2 Extension, the project is developing the ECLI Privacy Framework that will enable a standardised approach to lawful disclosure and use of location information by authorised parties. See PS06.</p> <p>There are existing Privacy Policies in place for MNOs, MBIE, ESPs and Public Safety Organisations specifying their purpose of collection of personal information.</p>	<p>All existing risks identified for ECLI, with additional context or risk drivers</p> <p>R01 – Personal information is used for another purpose not related to the original purpose of collection.</p> <p>R02 – Personal information is collected outside of the authorised and legal purpose (new risk context and driver from ECLI Phase 2 capabilities).</p> <p>R03 – Individuals are not given advance notice of the new Phase 2 ECLI capabilities (new risk context introduced by ECLI Phase 2 capabilities).</p> <p>Existing ECLI risk LAP-60, 61</p>

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Principle	Requirement	Assessment	Privacy Risks and whether it is an existing or new risk
<p>Principle 2 – Source of personal information</p>	<p>The Privacy Act requires that all information be collected from the individual unless the agency believes on reasonable grounds an exception applies.</p> <p>TIPC 2020 Schedule 4 provides an express authority for the Service to collect ELI from the relevant telecommunication device or the relevant network operator, in accordance with Schedule 4.</p> <p>As an example of an exception that applies generally (but not under Schedule 4), paragraph 2(d) of Privacy Act 1993, Principle 2 states:</p> <p><i>(d) non-compliance is necessary:</i></p> <ul style="list-style-type: none"> <i>i. to avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences; or</i> <i>ii. for the enforcement of a law imposing a pecuniary penalty; or</i> <i>iii. for the protection of the public revenue; or</i> <i>iv. for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation);</i> 	<p>OIA 6(c)</p> <p>For example, where the person-in-need is with the caller who makes the 111 call and triggers ELI for the caller's phone, use of the caller's ELI is permitted under TIPC 2020 Schedule 4.</p> <p>The Service provides three sources of location information, depending on the type of telecommunications device:</p> <ul style="list-style-type: none"> • Handset-based location provides high-precision GPS and Wi-Fi derived location from smartphones running the Google's Android operating system and Apple's iOS based on the AML standard ETSI TR 103 393. • 3GPP Location Services provides location derived from multiple techniques using the 'Control' plane of the mobile networks to calculate the location of telecommunications device. <p>Collection of information for the ECLI Phase 2 Extension is not automatic, however will still be collected without interaction by the individual concerned.</p>	<p>Existing ECLI risk LAP-62</p>

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Principle	Requirement	Assessment	Privacy Risks and whether it is an existing or new risk
<p>Principle 3 – Collection of Information</p>	<p>The key requirements of Principle 3 of the Privacy Act are to ensure individuals know:</p> <ul style="list-style-type: none"> • That information is being collected about them and their rights relating to that information; • Why information is being collected about them, including the consequences if all, or part, of the information is not provided; • Who else will receive the information. <p>Individuals should be advised about the collection of their personal information before the information is collected, or as soon as practicable after collection.</p> <p>This principle offers some exceptions if choosing not to advise individuals about the information being collected.</p> <p>This application of this principle is modified in TIPC 2020 Schedule 4 as follows:</p> <ul style="list-style-type: none"> • Clause 4 (4) exempts the location agency from notifying the individual of collection of ECLI • Clause 4 requires DLI collection notification to the individual unless clause 4 (2) applies • Clause 5 specifies the general duty of transparency for location agencies. 	<p>As for the Service as currently provided (and in accordance with the TIPC), it is not intended under Phase 2 that emergency service call takers will advise callers that their location information has been collected as this will add time to an emergency call and may cause delay in dispatching a response. Clause 4(4) exempts MBIE from notifying an individual of the collection of ECLI.</p> <p>All data elements collected are required as collectively they establish the probable location area of a caller and/or person of interest.</p> <p>There are existing Privacy Policies in place for MNOs, MBIE, ESPs and Public Safety Organisations specifying their purpose of collection of personal information. The ECLI specific Privacy statements are published on MBIE and ESP websites.</p> <p>ESPs collect, store, use and disclose information on the probable location of the caller and/or person of interest to help emergency response in accordance with the TIPC. It is intended that this will continue under the Phase 2 Extension.</p> <p>For ECLI Phase 2 Extension, this will be extended to support the following categories:</p> <ul style="list-style-type: none"> • Emergency Response – The use of active location (where a device is now) and location information of cellular devices in the absence of an emergency call from the individual concerned in accordance with the prevailing TIPC 2020 Schedule 4. ELI will also be provided to search and rescue operations to extend the emergency response coverage beyond 111 calls. • The TIPC 2020 Schedule 4 requires DLI collection requests to trigger SMS notification to the device on the onset of DLI activation. The Service will automatically send the SMS notification. However, authorised users are able to disable the SMS notification if they have reason to believe that the notification would likely prejudice the physical or mental health of the individual concerned or another individual. This decision must be reviewed within 7 days. Initially, only NZ Police users will be authorised to submit DLI collection requests and/or disable the SMS notification. The NZ Police Shift Commanders and/or Supervisors will be responsible for: <ol style="list-style-type: none"> a) Approving DLI collection requests before they are submitted b) Deciding whether the SMS notification should be disabled c) Reviewing within 7 days to ensure if the rationale to withhold the SMS notification is still correct. 	<p>R02 – Personal information is collected outside of the authorised and legal purpose (new risk context and driver from ECLI Phase 2 capabilities).</p> <p>R03 – Individuals are not given advance notice of the new Phase 2 ECLI capabilities (new risk context introduced by ECLI Phase 2 capabilities).</p> <p>Existing ECLI risk LAP-60, 62</p>
<p>Principle 4 – Manner of Collection</p>	<p>The key requirement of Principle 4 of the Privacy Act is to ensure personal information is not collected by unlawful means, in an unfair manner, by a means that, in the circumstances of the case (particularly in circumstances where personal information is being collected from children or young persons), or a manner that intrudes unreasonably upon the personal affairs of the individual concerned.</p>	<p>Personal information is not collected by unlawful means, in an unfair manner, or a manner that intrudes unreasonably. This will also apply to the collection of personal information from a minor.</p> <p>Data will be collected when a mobile caller activates the NZ 111 service by dialling 111 on a mobile device, or might be collected</p> <ul style="list-style-type: none"> • if a serious threat to life or health is assessed when an individual has called another public safety organisations number e.g. a call about a child’s safety is made to Oranga Tamariki, or, • A mobile caller has called a non-emergency number (e.g. Plunket Line, HealthLine, National Poisons line) and the call is triaged requiring upgrade to an emergency call. <p>Where the location information does not come from the person of interest’s device, location information of that person of interest will be collected under TIPC 2020 Schedule 4.</p> <p>NB: Location information may be collected from a minor, for example, a child or young person activates the NZ 111 service by dialling 111 from their own mobile device.</p> <p>For ECLI Phase 2 Extension, this will be extended to support the following categories:</p> <ul style="list-style-type: none"> • Emergency Response – The use of active location (where a device is now) and the location information of cellular devices in the absence of an emergency call from the individual concerned in accordance with the prevailing TIPC 2020 Schedule 4. ELI will also be provided to search and rescue operations to extend the emergency response coverage beyond 111 calls. <p>There are no privacy risks identified with this Principle for the in-scope Use Cases. However, there may be public concern regarding the use of active location information and location information from other location capable devices (IoT) for possible future use cases. There are privacy safeguards and security controls in place to ensure the risk and potential harm of unlawful or unauthorised disclosure are managed within the Service.</p>	<p>Existing ECLI risk LAP-63, EC-126</p> <p>New ECLI risk EC-117</p>

Principle	Requirement	Assessment	Privacy Risks and whether it is an existing or new risk
Principle 5 – Storage and Security of personal information	The key requirement of Principle 5 is that reasonable steps are taken to protect the personal information collected from loss, unauthorised access, unauthorised use, modification, disclosure and other misuse. This applies when the information is in storage and when it is being moved.	<p>Several security controls have been implemented as part of the Service to ensure the Service is protected against information loss, unauthorised access, unauthorised use, modification, disclosure, and other misuse. The most pertinent control being the obfuscation and anonymization of PI for non-operational purposes (e.g. reporting). Additional security controls are being implemented as part of the Phase 2 Extension.</p> <ul style="list-style-type: none"> The Service undergoes regular security penetration testing performed by an independent third-party. All data fields containing Personal Information will be retained and stored for no longer than is necessary for the purposes for which the Personal Information was collected, e.g. in an emergency to establish the location of an emergency caller and facilitate the response to an emergency. Access to the data is based on user roles. Audit logging is in place at the application, OS and network layers. Extensive reporting is performed with all solution partners. Security Assurance obligations are agreed and in place with key solution partners. Risk Management is a continual process. <p>Further information on applicable security and privacy controls are identified in <i>Table 2 - Detailed Privacy Findings</i> on page 29.</p> <p>The Service aligns with a number of industry good practice security frameworks including;</p> <ul style="list-style-type: none"> OWASP top-10 Australian Signals Directorate (ASD) Top-35 US FCC Communications Security, Reliability & Interoperability Council (CSRIC) guidance GSMA security guidance EENA Security guidance 	<p>Existing ECLI risk LAP-60, 64, 68, 69</p> <p>R04 – An individual is able to be identified from a number of aggregated or anonymised data sets, or through the unique identifier in the reporting and analytics server (existing risk identified for ECLI).</p> <p>R05 – Errors in assigning roles and access privileges within the Service may allow unauthorised individuals to access personal information (existing risk identified for ECLI Phase 2 capabilities).</p> <p>R06 – Datacom, ESPs and other agencies are unable to adequately detect, manage or respond to security or privacy incidents. This could result in breach of the Privacy Act 1993 (existing risk identified for ECLI).</p> <p>R07 – Personal information stored with the Service is not securely deleted (existing risk identified for ECLI, although it was not identified in the previous PIA).</p> <p>R08 – A Service user (e.g. ESPs and other agencies) deliberately discloses personal information to an unauthorised party (existing risk identified for ECLI).</p> <p>R09 – A Service user (e.g. ESPs and other agencies) accidentally discloses personal information to an unauthorised party (existing risk identified for ECLI, although it has not been identified in the previous PIA).</p> <p>R10 – Outsourced Service Provider administrators (e.g. Datacom, Comtech) may deliberately or accidentally disclose personal information to an unauthorised party (existing risk identified for ECLI, although it has not been identified in the previous PIA).</p> <p>R11 – Security controls within the Service are insufficient, allowing information to be compromised (existing risk identified for ECLI).</p> <p>R15 – Foreign government exercises legal powers to obtain information hosted in cloud (existing risk identified for ECLI, although it has not been identified in the previous PIA).</p>
Principle 6 – Access to personal information	<p>The key requirement of Principle 6 of the Privacy Act is to ensure that an agency holds personal information in such a way that it can readily be retrieved as the individual concerned is entitled to:</p> <ul style="list-style-type: none"> Obtain confirmation about whether information is being held about them; Have access to that information (within 20 working days from the date of request). 	<p>Individuals' requests for access to and the correction of personal information are likely, however this would be limited due to the retention clause of the TIPC that states that information may not be kept for longer than is necessary to establish the location of an emergency caller and facilitate the response to an emergency. Therefore it is unlikely that MBIE could fulfil the request as the data would likely not exist.</p> <p>Where the location information has become a record of another agency that used the location information, access or correction of information is still possible by request to the relevant agency (ESPs, law enforcement agencies and public safety organisations) subject to their processes or transferring the request under Section 39 of the Privacy Act.</p>	<p>Existing ECLI risk LAP-65</p> <p>R12 – Business processes and/or system design do not enable MBIE to respond to Privacy Act Requests such as rights to access or correct personal information stored within the Service (existing risk identified for ECLI).</p>
Principle 7 – Correction of personal information	<p>The key requirement of Principle 7 of the Privacy Act is to ensure that personal information held by an agency can be corrected as individuals are entitled to request:</p> <ul style="list-style-type: none"> A correction be made to the information stored about them; A statement is attached to their information stating that a correction was sought, but not made. 	<p>Individuals' requests for access to and the correction of personal information are likely, however this would be limited due to the retention clause of the TIPC that states that information may not be kept for longer than is necessary to establish the location of an emergency caller and facilitate the response to an emergency. Therefore it is unlikely that MBIE could fulfil the request as the data would likely not exist.</p> <p>Where the location information has become a record of another agency that used the location information, access or correction of information is still possible by request to the relevant agency (ESPs, law enforcement agencies and public safety organisations) subject to their processes or transferring the request under Section 39 of the Privacy Act.</p>	<p>Existing ECLI risk LAP-65</p> <p>R12 – Business processes and/or system design do not enable MBIE to respond to Privacy Act Requests such as rights to access or correct personal information stored within the Service (existing risk identified for ECLI).</p>

Principle	Requirement	Assessment	Privacy Risks and whether it is an existing or new risk
<p>Principle 8 – Accuracy of personal information</p>	<p>The key requirement of Principle 8 of the Privacy Act is an agency that holds personal information must take reasonable steps to ensure that information is accurate, up-to-date, complete, relevant and not misleading before using it.</p> <p>This application of this principle is modified in TIPC 2020 where clause 3 (4) requires an ESP to take all reasonable steps to ensure that the device relates to the individual where location is necessary for the purpose of responding to the serious threat.</p>	<p>The Service will review the SOPs developed by ESPs to verify that those SOPs include procedures that require the ESP to take reasonable steps to ensure that the mobile device number submitted for an authorised DLI request relates to the individual concerned.</p> <p>The Service has a core operating assumption that a location of a mobile device is a sufficient proxy for the location of the individual.</p> <p>The Service is still reliant on information received from the different MNOs. The level of location accuracy depends on a number of factors such as the type of cellular device and the location source available.</p> <p>The location data is the probable location of a caller/person of interest and not a definitive location, for example an address. In order for an emergency response to be dispatched the location of the event must be confirmed by the caller, the location data is an additional method to assist in verifying the location.</p> <p>For ECLI Phase 2 Extension, the use of active information will potentially improve the accuracy of information stored within the Service. This will assist ESPs and public safety organisations to facilitate immediate and accurate response as it relies on active location (where a device is now).</p> <p>In all instances the ECLI System collects information with no knowledge about the mobile device user, thus there is no bias in the collected information.</p> <p>Statistically speaking 50% of the NZ population will make a genuine, or non-genuine, 111 call in any given year. As the Service collects information automatically, both genuine and non-genuine location records are retained for the permitted primary purpose. Processing of the <i>ICAP Genuine call report</i> permits removal of the ECLI records related to 'non-genuine' calls that have already been anonymised and obfuscated within the reporting systems.</p>	<p>R13 – There is a risk that information will be incorrectly recorded within the Service (existing risk identified for ECLI, although it has not been identified in the previous PIA).</p>
<p>Principle 9 – Retention of personal information for longer than necessary</p>	<p>The key requirement of Principle 9 is that an agency only keeps personal information for as long as it has a lawful purpose for retaining and using it.</p> <p>This principle is upheld in TIPC 2020 Schedule 4 clause 6. This clause also requires that any information retained by MBIE for monitoring or auditing the operation of the Service, is in a form that is not capable of identifying individuals.</p>	<p>Information is not kept for longer than is necessary for the purposes for which the Personal Information was collected, e.g. to establish the location of an emergency caller and facilitate the response to an emergency.</p> <p>A Purge task is configured to automatically run every five minutes and purge all PI from the Service after a defined period. The Purge task currently runs every 5 minutes to purge data older than six (6) hours. This feature supported extended search missions prior to the establishment of TIPC 2020 Schedule 4. The Service extension will run a new purge task every 5 minutes to purge data older than seventy-two (72) hours.</p> <p>ESPs, PSOs, and law enforcement agencies will have their own retention requirements under their legal obligations.</p> <p><u>Data Retention details</u></p> <ul style="list-style-type: none"> • Device location records – Automatically purged by the Service after the specified period for each use is reached. • Audit data retention – All data kept for audit and reporting purposes shall be retained for a period of 7 years. • Security/event log retention – Retained for a minimum of one year. Retained online for a minimum of 60 days. <p>There will be no archiving of identifiable data. Reporting/Audit data will be retained but this will not contain personal information except for location information, (where location information means personal information indicating the approximate geographical position of a device, which may include the latitude, longitude, altitude and direction of travel of that device).</p> <p>When operational data is extracted for monitoring and auditing purposes, the procedures require anonymisation via obfuscation and/or hashing prior to ingestion into the Data Workshop platform. The appendices in the Privacy Safeguards list the data elements retained and also identify the data elements where obfuscation and/or hashing are applied.</p>	<p>Existing ECLI risk LAP-62, 66</p> <p>R14 – Personal information is retained by the Service for longer than necessary (existing risk identified for ECLI).</p>

Principle	Requirement	Assessment	Privacy Risks and whether it is an existing or new risk
Principle 10 – Limits on use of personal information	<p>The key requirement of Principle 10 of the Privacy Act is that personal information obtained by an agency for one purpose shall not be used for any other purpose, unless it believes on reasonable grounds that the specified exceptions apply.</p> <p>In TIPC 2020 Schedule 4 clause 3 limits the use of ELI collected under Schedule 4 to the permitted primary purpose and the permitted secondary purpose. The permitted primary purpose permits:</p> <ul style="list-style-type: none"> the use of ECLI to respond to an emergency call the use of DLI to prevent or lessen serious threat to the life or health of the individual concerned of another individual 	<p>The following ECLI Phase 2 Capability Extension Use Cases have been identified:</p> <ul style="list-style-type: none"> Extend emergency response coverage – Extend service coverage to emergency response situations beyond 111 calls and to provide ELI to Search and Rescue (SAR) operations. ELI will be used for the permitted primary purpose or permitted secondary purpose. <p>OIA 6(c)</p> <p>Reason codes will be applied to both use cases to identify the purpose for the collection of information. These reason codes have been agreed between MBIE and ESPs and will be agreed between MBIE and PSO's in due course.</p> <p>The following controls and privacy safeguards are in place to ensure personal information is only used for a justifiable purpose:</p> <ul style="list-style-type: none"> PS01 – Policies and procedures for collection, retention, use and disclosure of ECLI PS03 – Controlling access to production data PS04 – Monitoring the usage of ECLI and ensuring compliance with the limitation on its retention PS05 – Provision of relevant training to employees SC11 – Audit logging SC12 – Monitoring and alerting SC47 – Staff code of Conduct 	<p>R01 – Personal information is used for another purpose not related to the original purpose of collection (existing risk identified for ECLI).</p> <p>Existing ECLI risk LAP-60</p>
Principle 11 – Limits on disclosure of personal information	<p>The key requirement of Principle 11 of the Privacy Act is that an agency shall not disclose personal information unless the agency believes, on reasonable grounds, one of the exceptions apply.</p> <p>The application of this principle is modified by TIPC 2020 Schedule 4:</p> <p>3. Collection, use, disclosure and accuracy of ELI</p> <ol style="list-style-type: none"> A location agency may collect, use or disclose ELI if it believes on reasonable grounds that: <ol style="list-style-type: none"> the collection, use or disclosure is necessary for a permitted primary purpose or permitted secondary purpose; and In the case of a disclosure – the disclosure is to another location agency. 	<p>Outsourced Service Provider administrators (e.g. Datacom) have access to the underlying infrastructure and may have access to the complete information stored within the Service. However, contractual agreements and SLAs with Service Providers along with Audit Logging, Monitoring and Alerting are in place to manage risk regarding unauthorised disclosure.</p> <p>The Service has implemented safeguards to ensure that requests for location information have the necessary authorisation. For example, before the Service+ accepts a request to initiate DLI collection, the user who approves the DLI request is prompted to confirm the request as follows:</p> <p><i>By approving this location request as 'user ID' I confirm that:</i></p> <ol style="list-style-type: none"> <i>this location request is being made in accordance with the applicable standard operating procedures;</i> <i>all reasonable steps have been taken to ensure that the cellular device relates to the individual whose location is necessary to determine for a permitted purpose;</i> <i>making a location request is appropriate in these circumstances because it enables an emergency service provider to facilitate a response to an emergency call or prevent or lessen a serious threat to the life or health of an individual; and</i> <i>I have been authorised to approve this request.</i> <p>Under the Data Use and Sharing Agreement (DUSA) between MBIE and Participating ESPs (NZ Police, FENZ, WFA and ST John), either party may conduct audits to verify compliance of either of those party's obligations under the DUSA.</p>	<p>Existing ECLI risk LAP-60, 67, 68, 69</p> <p>R04 – An individual is able to be identified from a number of aggregated or anonymised data sets, or through the unique identifier in the reporting and analytics server (existing risk identified for ECLI).</p> <p>R07 – Personal information stored with the ECLI Service is not securely deleted (existing risk identified for ECLI, although it has not been identified in the previous PIA).</p> <p>R08 – A Service user (e.g. ESPs and other agencies) deliberately discloses personal information to an unauthorised party (existing risk identified for ECLI).</p> <p>R09 – A Service user (e.g. ESPs and other agencies) accidentally discloses personal information to an unauthorised party (existing risk identified for ECLI, although it has not been identified in the previous PIA).</p> <p>R10 – Outsourced Service Provider administrators (e.g. Datacom, Comtech) may deliberately or accidentally disclose personal information to an unauthorised party (existing risk identified for ECLI, although it has not been identified in the previous PIA).</p> <p>R11 – Security controls within the Service are insufficient, allowing information to be compromised (existing risk identified for ECLI).</p>

Principle	Requirement	Assessment	Privacy Risks and whether it is an existing or new risk
Principle 12 – Disclosure of personal information outside NZ	The requirement of Principle 12 is to ensure that disclosures of information to overseas entities are only made where there are equivalent privacy safeguards in place in the overseas jurisdiction, or where the individual concerned has expressly authorised such disclosure.	<p>The Service is contained within New Zealand and does not process or store offshore any information for the primary purposes that it was collected. Neither does the Service disclose this information to overseas entities. OIA 9(2)(c) [REDACTED]. However, this does not count as disclosure and fits with acceptable hosting for NZ government.</p> <p>In consideration of secondary purposes, that is reporting, and analysis directly related to the operation of the ECLI Service, anonymised and obfuscated information may be stored offshore (Australia). Although this is still within the direct management and control of the Service.²</p> <p>In this context Principle 12 does not apply since the intent of Principle 12 relates to disclosure to overseas entities where that overseas entity uses the information for its own purposes (and not simply processing or storing the information for a New Zealand entity).</p> <p>Irrespective of Principle 12, MBIE is accountable for Privacy related to the Service, and has exercised prudence with all organisations involved in the delivery of the Service including wholly NZ based organisations, to ensure alignment with the Privacy Act and TIPC Amendment No 5 & 7.</p>	Existing ECLI risk LA-04 relating to Assurance, LA-17 & LA-21 related to ECLI support organisations.
Principle 13 – Unique identifiers	<p>The key requirement of Principle 13 of the Privacy Act is that an agency shall not assign a unique identifier to an individual unless the assignment of that identifier is necessary to enable the agency to carry out one or more of its functions efficiently.</p> <p>An agency must take steps to minimise the risk of misuse of a unique identifier e.g. by showing truncated account numbers in receipts or correspondence.</p>	<p>ELI collected by the Service does not create or assign new unique identifiers for the devices (or any relevant individuals) concerned.</p> <p>However, the Service operational data identifies the caller's mobile phone number and/or device identifiers such as the IMSI and IMEI. Every 5 minutes, the operational data store purge's location data older than the agreed operational data retention period. Currently that agreed operational data retention period is six (6) hours and will be extended to seventy-two (72) hours for DLI (service extension) location data.</p> <p>Audit/Reporting data is retained before each purge and the audit data is ingested into the reporting and analytics server after the data has been anonymised (i.e. any PI is obfuscated and/or hashed).</p> <p>Location Information (geospatially rendered or as data files). Location Information itself is classified as PI and it does not have to be combined with other unique identifier(s) e.g. a mobile device number to meet this classification.</p> <p>Location information means personal information indicating the approximate geographical position of a device, which may include the latitude, longitude, altitude and direction of travel of that device. Current Privacy Safeguards and Security Controls are in place to ensure compliance with this principle and to mitigate Risk04:</p> <ul style="list-style-type: none"> • PS02 – Breach of requirements policies and procedures • PS04 – Monitoring the usage of ECLI and ensuring compliance with the limitation on its retention <p>Additional Privacy Safeguards and Security Controls are in place to control access to Personal Information within the ELIS. These are also relevant in this location information context and are as follows:</p> <ul style="list-style-type: none"> • PS03 – Controlling access to production data • PS05 – Provision of relevant training to employees • SC02 – Access control • SC18 – Staff vetting • SC47 – Staff code of conduct 	Existing ECLI risk LAP-69 R04 – An individual is able to be identified from a number of aggregated or anonymised data sets, or through the unique identifier in the reporting and analytics server (existing risk identified for ECLI).

² Storing information offshore with a third party hosting provider is not of itself, a disclosure: <https://privacy.org.nz/blog/privacy-2-0/>

Risk Assessment

Table 2 - Detailed Privacy Findings

Risk ID	Risk Description	Existing/New risk	Reference to ECLI Risk Assessment or Previous PIA ³	Risk Causes	Current Controls	Current Risk Ratings			Additional Privacy Controls ⁴	Target Risk Ratings		
						Likelihood	Impact	Risk Rating		Likelihood	Impact	Risk Rating
R01.	Personal information is used for another purpose not related to the original purpose of collection. Potential breach of: Principle 1, 6 and 10, and TIPC	Existing risk identified for ECLI.	LAP-60	<ul style="list-style-type: none"> Additional use cases for Phase 2 Extension (e.g. including active locations) could be abused by ESPs and other agencies without a justifiable purpose. ESPs and other agencies may want to use ECLI to fulfil another business process that is outside of the defined purpose in TIPC. ESP and other agencies use of the Service solution or ECLI data expands in scope. Personal information is used by MBIE to support another business process. If authorisation for MBIE staff to access personal information is too widely approved, and not maintained, then personal information may be used or disclosed inappropriately. 	<i>Privacy Safeguards</i> PS01 – Policies and procedures for collection, retention, use and disclosure of ECLI PS02 – Breach of requirements policies and procedures PS03 – Controlling access to production data PS04 – Monitoring the usage of ECLI and ensuring compliance with the limitation on its retention PS05 – Provision of relevant training to employees <i>Security Controls</i> SC11 – Audit logging SC12 – Monitoring and alerting SC31 – Privacy Code of Practice from Office of Privacy Commissioner SC32 – Privacy statement & Policy on website SC47 – Staff code of Conduct	Rare	Moderate	Low	<i>Privacy Safeguards</i> PS06 – ECLI Privacy Framework PS07 – Data Sharing and Use Agreement PS11 – Disclosure Log <i>Security Controls</i> SC33 – SOPs for Privacy	Rare	Minor	Low
R02.	Personal information is collected outside of the authorised and legal purpose. Potential breach of: Principle 1, 3, and TIPC	Existing risk identified for ECLI.	LAP-61	<ul style="list-style-type: none"> MNOs, MBIE, ESPs and other agencies may want to collect additional personal information without a justifiable purpose. ECLI Phase 2 use cases may require additional personal information. 	<i>Privacy Safeguards</i> PS01 – Policies and procedures for collection, retention, use and disclosure of ECLI. <i>Security Controls</i> SC31 – Privacy Code of Practice from Office of Privacy Commissioner SC32 – Privacy statement & Policy on website SC47 – Staff code of Conduct	Rare	Moderate	Low	<i>Privacy Safeguards</i> PS06 – ECLI Privacy Framework PS07 – Data Sharing and Use Agreement PS11 – Disclosure Log <i>Security Controls</i> SC33 – SOPs for Privacy	Rare	Minor	Low

RELEASED UNDER THE OFFICIAL INFORMATION ACT

³ MCL – PIA <https://mako.wd.govt.nz/otcs/lisapi.dll/link/64400129>

⁴ Not all security controls are listed here as the security risk assessment document is updated on a regular basis, and is the master source of controls.

Risk ID	Risk Description	Existing/New risk	Reference to ECLI Risk Assessment or Previous PIA ³	Risk Causes	Current Controls	Current Risk Ratings			Additional Privacy Controls ⁴	Target Risk Ratings		
						Likelihood	Impact	Risk Rating		Likelihood	Impact	Risk Rating
R03.	Individuals are not given advance notice of the new Phase 2 ECLI capabilities. This could lead to individuals not being aware of what information is collected, the nature of its use, and eventually may feel a loss of control over their information. Potential breach of: Principle 1 and 3 and TIPC	Existing risk identified for ECLI	LA-12, EC-117	<ul style="list-style-type: none"> Privacy Policies of MNOs, Public Safety Organisations and MBIE may have not been updated. Additional use cases for Phase 2 Extension (e.g. Including active locations). Service capability is extended to receive location information from any location capable device via the mobile network (e.g. IoT devices). 	<i>Privacy Safeguards</i> PS01 – Policies and procedures for collection, retention, use and disclosure of ECLI	Possible	Minor	Low	<i>Privacy Safeguards</i> PS06 – ECLI Privacy Framework PS08 – Consult Privacy Commissioner and Mobile Networks operators (MNOs) PS09 – Proactive release <i>Security Controls</i> SC32 - Privacy statement & Policy on website SC31 OPC TIPC consultation	Possible	Minor	Low
R04.	An individual is able to be identified from a number of aggregated or anonymised data sets, or through the unique identifier in the reporting and analytics server. Potential breach of: Principle 5, 11, and 12	Existing risk identified for ECLI.	LAP-69	<ul style="list-style-type: none"> Technical failure during the hashing and obfuscation process. 	<i>Privacy Safeguards</i> PS02 – Breach of requirements policies and procedures PS04 – Monitoring the usage of ECLI and ensuring compliance with the limitation on its retention <i>Security Controls</i> SC34 – End to end functional testing SC00 – Comply with non-functional requirements	Rare	Moderate	Low	N/A	Rare	Moderate	Low
R05.	Errors in assigning roles and access privileges within the Service may allow unauthorised individuals to access personal information. Potential breach of: Principle 5 Note: Each specific role will have a named individual against the role to enforce accountability.	Existing risk identified for ECLI.	LA-32	<ul style="list-style-type: none"> Inadequate training of administrator staff. Insufficient process documentation exists. The access permissions required for the roles is not configured correctly. 	<i>Privacy Safeguards</i> PS05 – Provision of relevant training to employees PS03 – Controlling access to production data <i>Security Controls</i> SC02 – Access Control - Authorisation roles or policy SC18 – Staff Vetting SC47 – Staff code of Conduct	Unlikely	Minor	Low	<i>Privacy Safeguards</i> PS10 - Extended background checks for named individuals PS11 – Disclosure Log	Unlikely	Minor	Low

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Risk ID	Risk Description	Existing/New risk	Reference to ECLI Risk Assessment or Previous PIA ³	Risk Causes	Current Controls	Current Risk Ratings			Additional Privacy Controls ⁴	Target Risk Ratings		
						Likelihood	Impact	Risk Rating		Likelihood	Impact	Risk Rating
R06.	Datacom, ESPs and other agencies are unable to adequately detect, manage or respond to security or privacy incidents. This could result in breach of the Privacy Act 1993. Potential breach of: Principles 5 Note: Moderate impact as the worst case scenario such as a significant privacy or security incident.	Existing risk identified for ECLI.	LA-28	<ul style="list-style-type: none"> Roles and responsibilities defined in the Support and Operational Model may not be followed. New ESPs involved for Phase 2 may not be familiar of the incident management process for ECLI. Different definitions of what constitutes a "security/privacy incident". 	<i>Privacy Safeguards</i> PS02 – Breach of requirements policies and procedures PS05 – Provision of relevant training to employees <i>Security Controls</i> SC11 – Audit logging SC12 – Monitoring and alerting SC22 – Notification of incidents and breaches	Unlikely	Minor	Low	<i>Security Controls</i> SC12 - Monitoring and alerting - there will be enhanced alerting for Phase 2 ECLI Extension (e.g. being able to investigate sudden spikes within ECLI).	Unlikely	Minor	Low
R07.	Personal information stored with the Service Provider is not securely deleted when the contract with the Service Provider ends, resulting in the potential unauthorised disclosure of information. Potential breach of: Principle 5 and 11, and TIPC	Existing risk identified for ECLI. Although it had not been identified in the previous PIA.	LA-05	<ul style="list-style-type: none"> The secure removal of data on Service Provider equipment is unverified. Service Provider (Datacom) may not have adequate secure deletion processes in place to ensure information is securely deleted. 	<i>Privacy Safeguards</i> PS01 – Policies and procedures for collection, retention, use and disclosure of ECLI PS04 – Monitoring the usage of ECLI and ensuring compliance with the limitation on its retention <i>Security Controls</i> SC19 – Purging of Probable Call Location (PCL) records SC42 – Contractual Agreement & SLA's with Vendor / Service Provider SC43 – Certified & Accredited data centre	Rare	Minor	Very Low	N/A	Rare	Minor	Very Low
R08.	A Service user (e.g. ESPs and other agencies) deliberately discloses personal information to an unauthorised party. Potential breach of: Principle 5 and 11, and TIPC	Existing risk identified for ECLI.	LA-34, LAP-67	<ul style="list-style-type: none"> The Service user may be curious about a particular incident or person. Insufficient training of ECLI Service user regarding the use of the service. Insufficient awareness of ECLI Service user regarding acceptable information handling practices. 	<i>Privacy Safeguards</i> PS02 – Breach of requirements policies and procedures PS03 – Controlling access to production data PS04 – Monitoring the usage of ECLI and ensuring compliance with the limitation on its retention <i>Security Controls</i> SC11 – Audit logging SC12 – Monitoring and alerting SC47 – Staff code of Conduct	Rare	Moderate	Low	PS06 – ECLI Privacy Framework	Rare	Moderate	Low
R09.	A Service user (e.g. ESPs and other agencies) accidentally discloses personal information to an unauthorised party. Potential breach of: Principles 5 and 11, and TIPC	Existing risk identified for ECLI. Although it has not been identified in the previous PIA.	LAP-67	<ul style="list-style-type: none"> The Service user may share personal information with someone who claims to have the authority to access the information (e.g. false representation). The Service user may discuss personal information and is overheard by an unauthorised party. Human error. A technical fault in the Service leads to a ECLI Service user being able to see PI that they have no purpose to see (e.g. presented with incorrect Service location record for dropped or Initial Call Answering Platform (ICAP) filtered call) 	<i>Privacy Safeguards</i> PS02 – Breach of requirements policies and procedures PS03 – Controlling access to production data PS04 – Monitoring the usage of ECLI and ensuring compliance with the limitation on its retention <i>Security Controls</i> SC11 – Audit logging SC12 – Monitoring and alerting SC47 – Staff code of Conduct	Rare	Moderate	Low	PS06 – ECLI Privacy Framework	Rare	Moderate	Low

Risk ID	Risk Description	Existing/New risk	Reference to ECLI Risk Assessment or Previous PIA ³	Risk Causes	Current Controls	Current Risk Ratings			Additional Privacy Controls ⁴	Target Risk Ratings		
						Likelihood	Impact	Risk Rating		Likelihood	Impact	Risk Rating
R10.	Outsourced Service Provider administrators (e.g. Datacom, Comtech) may deliberately or accidentally disclose personal information to an unauthorised party. Potential breach of: Principle 5 and 11, and TIPC	Existing risk identified for ECLI. Although it has not been identified in the previous PIA.	LA-17	<ul style="list-style-type: none"> Disgruntled employees. Curious staff. Inadequate controls built into service contracts. Inadequate assurance of security performance and controls execution within the Service Provider and their third parties. Inadequate training and education of policy for third party Service Providers. 	<i>Privacy Safeguards</i> PS02 – Breach of requirements policies and procedures PS03 – Controlling access to production data PS04 – Monitoring the usage of ECLI and ensuring compliance with the limitation on its retention <i>Security Controls</i> SC11 – Audit logging SC12 – Monitoring and alerting SC18 – Staff Vetting SC31 – Privacy Code of Practice from Office of Privacy Commissioner SC42 – Contractual Agreement & SLA's with Vendor / Service Provider	Unlikely	Moderate	Medium	N/A	Unlikely	Moderate	Medium
R11.	Security controls within the Service are insufficient and allow a malicious individual to compromise information, leading to unauthorised disclosure. Potential breach of: Principles 5 and 11, and TIPC	Existing risk identified for ECLI.	LAP-64	<ul style="list-style-type: none"> The Service may be provided in a multi-tenanted environment. Disgruntled Service Provider staff. Curious Service Provider staff. Targeted attack from a motivated third party to access Service information. High profile incident attracts interest from third parties seeking access to specific information. 	<i>Security Controls</i> SC13 – Secure SDLC SC23 – Solution Certification & Accreditation SC26 – Operating system patching SC27 – Application patching SC28 – Restrictive administrative privileges SC29 – Application Whitelisting SC35 – Security Penetration testing Refer to Part A and Part B documents (Security Controls) sections.	Rare	Moderate	Low	<i>Security Controls</i> SC35 – Security Penetration testing SC51 – Automated security testing PS11 – Disclosure Log	Rare	Moderate	Low
R12.	Business processes and/or system design do not enable MBIE to respond to Privacy Act Requests such as rights to access or correct personal information stored within the ECLI Service. Potential breach of: Principle 6 and 7	Existing risk identified for ECLI.	LAP-65	<ul style="list-style-type: none"> Service operational data is automatically purged after a defined period of time and as such the information may simply not be there, therefore MBIE cannot respond to these requests. DLI location records older than the defined period of time (seventy-two (72) hours) are automatically purged every 5 minutes. 	<i>Privacy Safeguards</i> PS01 – Policies and procedures for collection, retention, use and disclosure of ECLI PS02 – Breach of requirements policies and procedures PS05 – Provision of relevant training to employees	Rare	Insignificant	Very Low	<i>Security Controls</i> SC33 – SOPs for Privacy	Rare	Insignificant	Very Low
R13.	There is a risk that information will be incorrectly recorded within the Service. Potential breach of: Principle 8 and TIPC	Existing risk identified for ECLI. Although it has not been identified in the previous PIA.	LA-56, 58, LAP-68	<ul style="list-style-type: none"> The level of location accuracy depends on a number of factors such as the type of mobile phone/IoT device and the location source available. Reliant on information from the different MNOs. 	<i>Privacy Safeguards</i> PS04 – Monitoring the usage of ECLI and ensuring compliance with the limitation on its retention <i>Security Controls</i> SC34 – End to end functional testing SC00 – Comply with non-functional requirements	Rare	Insignificant	Very Low	N/A	Rare	Insignificant	Very Low

Risk ID	Risk Description	Existing/New risk	Reference to ECLI Risk Assessment or Previous PIA ³	Risk Causes	Current Controls	Current Risk Ratings			Additional Privacy Controls ⁴	Target Risk Ratings		
						Likelihood	Impact	Risk Rating		Likelihood	Impact	Risk Rating
R14.	Personal information is retained by the Service for longer than necessary. Potential breach of: Principle 9 and TIPC	Existing risk identified for ECLI.	LA-55, LAP-66	<ul style="list-style-type: none"> Known limitation with Modica service where excessive logging of traffic causes multiple copies of an AML TXT message to be retained. Technical failure wherein the ECLI Purge Task stops working. <p>Note: The TIPC does not specify a specific retention period. It only states that information is not kept for longer than is required for a permitted primary purpose (i.e. to establish the location of an emergency caller and facilitate the response to an emergency) or a permitted secondary purpose.</p>	<p><i>Privacy Safeguards</i></p> <p>PS04 – Monitoring the usage of ECLI and ensuring compliance with the limitation on its retention</p> <p><i>Security Controls</i></p> <p>SC19 – Purging of Probable Call Location (PCL) records (within ECLI)</p> <p>SC24 – Operational Assurance Plan</p> <p>SC34 – End to end functional testing</p>	Almost Certain	Minor	Medium	<p>SC19 Purge of Geolocation information (within Modica)</p> <p>SC51 Security event monitoring</p> <p>SC63 – Assurance Reporting</p> <p>Specific remediation plan with Modica to align with TIPC#7 Modica Logging</p>	Possible	Minor	Low
R15.	A foreign government agency of a country where the cloud services are hosted exercises legal powers on information stored within the ECLI Reporting infrastructure. This results in: <ul style="list-style-type: none"> The foreign government Agency gaining access to ECLI information (anonymised PI); and/or MBIE being unable to gain access to ECLI information stored within the cloud service. Potential breach of: Principle 5 and TIPC	Existing risk identified for ECLI. Although it has not been identified in the previous PIA.	N/A	<ul style="list-style-type: none"> ECLI Reporting is hosted in Sydney and Melbourne. Microsoft is a US owned company. Nature of cloud services. 	<p><i>Security Controls</i></p> <p>SC08 – Encryption of data at rest</p> <p>SC22 – Notification of incidents and breaches</p> <p>SC42 – Contractual Agreement & SLA's with Vendor / Service Provider</p> <p>SC43 – Certified & Accredited data centre</p>	Rare	Minor	Very Low	<p><i>Security Controls</i></p> <p>SC52 – Specify hosting locations</p>	Rare	Minor	Very Low

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Actions to enhance or minimise impact on privacy

Following are the Privacy Safeguards and Security Controls identified to enhance the privacy of personal information stored and processed within the Service and manage the identified privacy risks.

Privacy Safeguards

Table 3 – Privacy Safeguards

Reference	Privacy Safeguards	Description
PS01	Policies and procedures for collection, retention, use and disclosure of ELI	<p>MBIE personnel are not involved in the day-to-day handling of ELI for ESPs and DLI for warranted access. As such, MBIE’s written policies and procedures with respect to ELI/DLI relate to:</p> <ul style="list-style-type: none"> the design of the Service, MBIE’s role (as the relevant government agency) in the administration and monitoring of the Service, and the governance arrangements for the Service as a whole. <p>The Terms of Reference for the governance board define MBIE’s privacy responsibilities in the governance of the Service.</p> <p>The Support and Operational Model (SOM) outlines the processes for support and operation of the Service.</p> <p>The MBIE System Security Certificate provides a summary of risk and assurance activities undertaken to ensure system security. This includes all phases from policy, design, implementation, testing and day to day operational practices.</p>
PS02	Breach of requirements policies and procedures	<p>Complaints or queries from the public about possible privacy breaches are directed to the relevant ESP or Network Operator. Information available on the MBIE website provides links to these agencies. Records retained by the ESPs are in accordance with the period defined in their data retention policies.</p> <p>The existing MBIE privacy complaints process will apply for any queries directed to MBIE. Escalation will be to the Director and Product Owner of the Service for investigation and resolution.</p> <p>The Emergency Location Information System (ELIS) Privacy Breach Notification Policy (effective 12 September 2022) provides guidance on how the relevant government agency for the ELIS (RGA) manages any breach affecting personal information.</p> <p>OIA 9(2)(c)</p>
PS03	Controlling access to production data	<p>Access to production data is restricted to a minimal number of specified roles and named individuals.</p> <p>Multi-factor authentication is required for production access. Noting the vLAC Web UI and DLI Web application front-end web applications do not have multi-factor authentication.</p> <p>MBIE reviews continued business need of all staff access each quarter.</p> <p>ESP staff authorisation is fully managed by each ESP, not MBIE.</p> <p>MBIE does not have any visibility of the ESP authorisation process.</p>
PS04	Monitoring the usage of ECLI and ensuring compliance with the limitation on its retention	<p>ELI in the vLAC is stored for a maximum of only 72 hours and then purged. DLI for warranted access is purged on delivery to the PSO. The purge function has been tested and demonstrated to be effective. It is monitored to ensure continuous operation. Any failure of this function will trigger a Dynatrace alert.</p> <p>Use of and access to the vLAC environments and database is monitored and reviewed for unusual activity.</p> <p>The volumes of ELI/DLI requests by ESPs/PSOs, with longer term trending information, are reported monthly to the Service’s Director and Product Owner. Additional monthly reporting is then undertaken with ESPs and PSOs.</p> <p>Ad hoc activity reports can be generated, with various criteria to list these requests on the vLAC. MBIE will investigate unusual activity or request volumes.</p> <p>Audit reports that allow the Service to monitor ELI transactions and to check that the purge function is working do not include any personal information (PI) which could be used to identify a caller, their SIM card or their device. The ELI audit record is anonymised by the removal of the phone number (MSISDN), the equipment identification number (IMEI) & the Subscriber Identifier (IMSI).</p> <p>Each ESP/PSO will receive monthly summaries of their DLI requests to allow the ESP/PSO to reconcile and audit these against their systems.</p> <p>The Service may establish random audits of ELI and/or DLI accessed and will work with ESPs/PSOs to conduct such audits.</p>
PS05	Provision of relevant training to employees	<p>ESPs and PSOs have trained their staff on the collection, retention, use and disclosure of ELI and/or DLI.</p> <p>All staff involved in the administration of the vLAC, and/or have access to production data and/or anonymised reporting data are subject to the New Zealand Government Code of Conduct for the State Services <i>Standards of Integrity and Conduct</i> [https://ssc.govt.nz/resources/code/].</p> <p>Compulsory privacy training and an overview of operational policies relating to individual privacy has been provided to all staff of the Service as part of the induction process"</p>
PS06	ECLI Privacy Framework	<p>Develop the ECLI Privacy Framework to enable a standardised approach to lawful disclosure and use of location information by authorised parties, in a way that recognises and supports both existing privacy protections, evolving expectations around non-disclosure of personal information, the societal value of location information, and the increasing potential for realising that societal value through advances in technology.</p>
PS07	Data Sharing and Use Agreement	<p>Data Sharing and Use agreement in relation to the Service between MBIE, Fire and Emergency New Zealand, New Zealand Police, St John and WFA.</p>

Reference	Privacy Safeguards	Description
PS08	Consult Privacy Commissioner	Use opportunity to raise and progress both overall framework with Privacy Commissioner, and specific immediate need for SAR use case changes and implementation.
PS09	Proactive release	Proactive release of information promotes good government, openness and transparency and fosters public trust and confidence in agencies. The TIPC 2020 Schedule 4 includes a requirement for MBIE to provide quarterly disclosure reporting to OPC. MBIE anticipates also providing an annual transparency report. MBIE will also initially (post-go live date of DLI), provide OPC with copies of the monthly summary reports (sent to ESPs), for location agency monitoring to align with TIPC 2020 Schedule 4 clause 7(2)(c)
PS10	Extended background checks for named individuals	There will be extended background checks for named individuals who will have access to information stored within the Service.
PS11	Disclosure Log	DLI disclosures will be logged and reported to the Privacy Commissioner each quarter. These reports will not contain PI, even in anonymised form. The Service website will publish annual transparency reports of DLI disclosures (without PI) to align with industry good practice.
PS12	Assurance of Compliance	Each ESP and PSO provided written compliance assurance at MBIE's request. Due diligence on this assurance included review of the ESP/PSO's privacy safeguards, evidential demonstration of good process, and confirmation that the ESP/PSO system has certification and accreditation approval. MBIE reviewed and approved each ESP/PSO's Standard Operating Procedures regarding ELI/DLI collection, usage and retention. For ESPs, MBIE reviewed the criteria and procedures for a) assessing serious threat, b) approving and escalating DLI requests to NZ Police, and c) NZ Police procedures for approving requests to collect DLI. For PSOs, the review focused on procedures relating to warranted access to DLI. Assurance compliance due diligence will apply if any other agency is authorised under TIPC 2020 Schedule 4 clause 2. Under the Data Use and Sharing Agreement (DUSA) between MBIE and Participating ESPs (NZ Police, FENZ, WFA and ST John), either party may conduct audits to verify compliance of either of those party's obligations under the DUSA.

Security Controls

Table 4 – Security Controls

Reference	Security Controls	Description
SC00	Comply with non-functional requirements	Comply with non-functional requirements specified in the Service requirements.
SC02	Access Control – Authorisation roles or policy	Authorisation based on security groups' roles or policy definition. This applies to Service administration users.
SC08	Encryption of data at rest	Data is encrypted at rest at the SAN layer.
SC11	Audit logging	Application audit logs are stored in a dedicated database table. OS and network logs are captured by MBIE's existing SIEM (Splunk).
SC12	Monitoring and alerting	Nagios for operational monitoring as per the Service Operational Monitoring Design. Dynatrace is used for the Location Platform operational monitoring and alerting. Red Hat's Advanced Cluster Security (ACS) application will be used across ECLI's OpenShift clusters for the purposes of SIEM and integrated into the ELI tenancy within the overall MBIE SIEM (Splunk). The use of the ACS application captures container and container platform events and insights. The Service is integrated into MBIE security reporting.
SC13	Secure SDLC	Secure coding principles to address OWASP Top 10 vulnerabilities Code check-in/check-out Regular security vulnerability testing of code during development Code peer review Secure source code repository using role-based ACLs Security verification testing prior to penetration test
SC18	Staff Vetting	ECLI Staff and/or Service Provider to obtain positive Police check of potential support staff before they are given logical or physical access to the Service.
SC19	Purging of ELI records	A Purge Task is configured to automatically run every five minutes to purge all Personal Information (PI) from the ECLI Service system that is 6 hours old. The time is calculated from the start of the 111 call. This is configured to purge service extension DLI location data that is 72 hours old. <u>Monitoring of the Purge Task</u> <ul style="list-style-type: none"> The service is monitored by the ECLI operational support team The service is configured to automatically restart on failure If the service does not run after a restart, a P3 incident is raised.

Reference	Security Controls	Description
		PSO DLI data is purged on delivery to PSO's and also purged after specific time limits as a default fail safe.
SC22	Notification of incidents and breaches	Service Provider will report all information security incidents and breaches to the affected agencies. The Emergency Location Information System (ELIS) Privacy Breach Notification Policy provides guidance on how the relevant government agency for the ELIS (RGA) manages any breach affecting personal information.
SC23	Solution Certification & Accreditation	The overall Service will be subject to the MBIE C&A Process.
SC26	Operating system patching	Patch operating system vulnerabilities.
SC27	Application patching	Patch software vulnerabilities.
SC28	Restrictive administrative privileges	The privileges of administrative/ privileged users are limited to only those required for their duties. Separation of user accounts and privileged accounts.
SC29	Application whitelisting	Prevention of unauthorised software executing on ECLI Service servers.
SC31	Privacy Code of Practice from Office of Privacy Commissioner	A TIPC 2020 has been published by the Privacy Commissioner. See https://www.privacy.org.nz/assets/Codes-of-Practice-2020/Telecommunications-Information-Privacy-Code-2020-website-version.pdf
SC32	Privacy statement & Policy on website	ESPs and PSOs will satisfy this control requirement by updating their own websites with statements as required.
SC33	SOPs for Privacy	Relevant business SOPs are created or updated to reflect Privacy considerations and guidance for staff. Ensure the use cases defined for Phase 2 ECLI Extension are covered in the updated SOPs.
SC34	End to end functional testing	System integration testing based on test cases, and test exit report.
SC35	Security Penetration testing	Security verification testing performed by project. Security penetration testing by external auditor. Perform regular security penetration testing of the Service annually or when significant changes are made to the service.
SC42	Contractual Agreement & SLA's with Vendor/ Service Provider	Contracts with Datacom for the delivery and support of the Service. Datacom holds an agreement with Google for Google Maps API plan.
SC43	Certified & Accredited data centre	The DSCG IaaS is certified for government use and all certification artefacts will be reviewed.
SC47	Staff code of conduct	State Sector Code of Conduct applies to all government sector staff. Individual private sector policies would apply for WFA, St John Datacom, and NZSAR volunteers who are not State Sector staff.
SC51	Automated security testing	Automated security testing is planned to be implemented as part of the DevSecOps process.
SC52	Specify hosting locations	Specify that data is stored only in Australia or countries with equivalent privacy laws as New Zealand for services hosted in overseas cloud (e.g. Microsoft services).

Refer to the *ECLI Part A and Part B documents (Security Controls)* sections for a complete list of the security controls. The table above only includes the security controls that have been recommended to mitigate the privacy risks identified in this PIA report.

Conclusion

This PIA identifies privacy risks arising from the ECLI Phase 2 Extension and outlines the relevant privacy safeguards and security controls for managing these risks. A privacy analysis was completed to ensure the lifecycle of personal information through its collection, use, retention, processing, disclosure and destruction is compliant with the Privacy Act 1993, Privacy Act 2020 and schedule 4 of the Telecommunications Information Privacy Code.

The use case prioritised for ECLI Phase 2 Extension, and the consequential use case,⁵ will enhance New Zealand's emergency services, search and rescue operations, and public safety and law enforcement activities.

MBIE have considered the risks and benefits associated with the introduction of the new use cases for ECLI Phase 2 Extension and are satisfied that the benefits of the use cases outweigh the associated privacy risks. The principles of proportionality and necessity have been applied throughout the design.

Privacy safeguards and security controls will be in place to ensure the risk and potential harm of unlawful or unauthorised disclosure are managed within the Service. Existing governance structures will be used to provide assurance of privacy and security protections.

In preparation for ECLI Phase 2 Extension, the project developed a strategy for enabling lawful disclosure and use of location information from the Service. That strategy document highlighted the following activities that will be completed:

- **Develop ECLI Privacy Framework** – Develop a high-level framework to enable a standardised approach for all parties related to lawful disclosure and the use of location information across all (or most) current and future potential use cases, in a way that recognises and supports both existing privacy protections, evolving expectations around non-disclosure of personal information, the societal value of location information, and the increasing potential for realising that societal value through advances in technology.
- **Implement initial extended ECLI and SAR use** – Based on that framework, enable a standardised approach to lawful disclosure and use of location information in initial extended ECLI use case scenarios (per recent advice) and for the search and rescue (SAR) use case, as these use cases are advanced and technology-ready.
- **Consult Privacy Commissioner and MNOs** – Use this opportunity to raise and progress both overall framework with the Privacy Commissioner, and the specific immediate need for ECLI Phase 2 Extension changes and implementation. Consult with MNOs on intended framework. [Note: Completed, and encompassed within TIPC Amendment No 7]
- **Detail framework** – Using any feedback from OPC, prepare framework in consultation with specific use case stakeholders as appropriate that will enable and regulate a standardised approach to lawful disclosure and use of location information across all categories of current uses, as well as providing a framework for potential future uses and evolving privacy expectations.
- **Work with Privacy Commissioner to enable framework to be implemented** – Consult regarding the whole framework, considering in particular what MNOs need to have to be comfortable that they will be complying with their privacy obligations. [Note: Completed, and encompassed within TIPC Amendment No 7]

⁵ Refer to UC01 and UC03 in [ECLI Phase 2 Capability Extension Use Cases V1.0](#)

In-Confidence

MBIE's Certification and Accreditation process will be completed prior to the ECLI Phase 2 Extension go-live in order for MBIE and users of the Service to gain assurance that the Service has been configured securely and that privacy safeguards and security controls are in place and effective.

RELEASED UNDER THE
OFFICIAL INFORMATION ACT

Appendix A – Risk Matrices

Table 5 - PIA Risk Matrix illustrates the rating of each identified privacy risk with the identified privacy safeguards and security controls in place.

Table 5 - PIA Risk Matrix

Impact	Likelihood				
	Rare	Unlikely	Possible	Likely	Almost Certain
Extreme	15	19	22	24	25
Major	10	14	18	21	23
Moderate	6 R01, R02, R04, R08, R09, R11,	9 R10	13	17	20
Minor	3 R07, R15	5 R05, R06	8 R03	12	16 R14
Insignificant	1 R12, R13	2	4	7	11

Subsequently,

Table 6 – Privacy cross reference to existing ECLI Risk Matrix

ECLI Risk Matrix (Privacy focus)

Impact	Extreme	15	19	22	24	25
	Major	10	14	18	21	23
	Moderate	6 LA-34, 56, 58, LAP-60, 61, 64, 67, 69, EC-117	9 LA-17	13	17	20
	Minor	3 LA-05, LAP- 62	5 LA-28, 32, LAP-63, 68	8 LA-12	12	16 LAP-66
	Insignificant	1 LAP-65	2	4	7	11
		Rare	Unlikely	Possible	Likely	Almost Certain
		Likelihood				

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Appendix B – PIA Consultation

Name	Role	Internal/External	Consulted/Informed
Alan Heward	Security and Risk Advisor	Internal	Consulted
Martien Duis	Solicitor	Internal	Consulted
Pam Harris	ECLI Manager Service Enhancements	Internal	Consulted
Susan Ng	ECLI Senior Business Analyst	Internal	Consulted
Peter Fernando	Senior Associate, Duncan Cotterill	External	Consulted
Tania Turfrey	Manager Legal Services	Internal	Informed
Shelley MacDonald	Senior Solicitor	Internal	Informed
Eve Kennedy	Policy Advisor, Office of the Privacy Commissioner	External	Consulted
Ian Martin	NZ Police CMC (TCF NZSAR Working Party)	External	Consulted
Win Van Der Velde	NZSAR (TCF NZSAR Working Party)	External	Consulted
Hon Kris Faafoi	Minister for Broadcasting, Communications and Digital Media	External	Informed
Hon Stuart Nash	Minister of Police	External	Informed

RELEASED UNDER THE OFFICIAL INFORMATION ACT



Data Use and Sharing Agreement

in relation to the Emergency Location Information
Service

—
Ministry of Business, Innovation and Employment (MBIE)

Fire and Emergency New Zealand (FENZ)

New Zealand Police (NZP)

The Priory in New Zealand of the Most Venerable Order of the Hospital of St John of
Jerusalem (St John)

—
The Wellington Free Ambulance Service (Incorporated) (WFA)

Data Use and Sharing Agreement

in relation to the Emergency Location Information Service

Details	4
1. Defined terms and interpretation	6
1.1 Defined terms	6
1.2 Interpretation	7
2. Commencement and term	7
2.1 Commencement and Initial Term	7
2.2 Extension	7
3. Use of ELI Service	7
3.1 Emergency Calls	7
3.2 Use of ELI Service in accordance with the Code	8
3.3 Other statutorily authorised use	Error! Bookmark not defined.
4. Capturing and sharing ECR Data	8
4.1 ECR Data capture	8
4.2 Sharing of ECR Data	8
4.3 Processing and using ECR Data	8
5. Use of ECR Data	8
5.1 Monitoring, auditing, analytics, KPIs, enhancements, and optimisation	8
5.2 Form of reports	8
5.3 Sharing reports with Participating ESPs	8
5.4 Sharing reports	8
5.5 Publishing reports and data sets	9
6. Information and audit	9
6.1 Privacy	9
6.2 Publicity	9
6.3 Mutual audit	9
7. Changes to this Agreement	9
7.1 Process of changes to this Agreement	9
7.2 Consequences of changes	9
7.3 Suspension	9
8. Accession, voluntary exit, and termination	9
8.1 Accession by further ESPs	9
8.2 Voluntary exit by Participating ESP	10
8.3 Termination by convenience	10
8.4 Survival	10
9. Liability	10
9.1 Exclusion	10
9.2 Limitation	10
10. Warranties	10
10.1 Mutual warranties	10
10.2 Other warranties excluded	11
11. Dispute resolution	11
11.1 Dispute resolution process	11
11.2 Dispute notice	11
11.3 Negotiation and escalation	11

11.4	Arbitration	11
11.5	Appeals on points of law	11
11.6	Decision	11
11.7	Continued performance	11
11.8	Urgent relief	11
12.	General	12
12.1	Further assurance	12
12.2	Amendments	12
12.3	Notices	12
12.4	Entire agreement	12
12.5	Governing law	12
12.6	Assignment	12
12.7	Counterparts	12
	Execution	13
	Schedule 1 – Key details	14
	Schedule 2 – Data collection, protection, and sharing specification	15
	Schedule 3 – Privacy	22
	Schedule 4 – Letter of Accession Template	23

RELEASED UNDER THE
OFFICIAL INFORMATION ACT

Details

Date

Parties

Name **Ministry of Business, Innovation and Employment**
Short form name **MBIE**
Notice details Address: 15 Stout Street, PO Box 5488, Wellington
Email: pam.harris@mbie.govt.nz
Attention: ECLI Manager Service Enhancements

Name **Fire and Emergency New Zealand**
Short form name **FENZ**
Notice details Address: Level 12, 80 the Terrace, PO Box 2133, Wellington
Email: Paul.Turner@fireandemergency.nz
Attention: National Manager Response Capability

Name **New Zealand Police**
Short form name **NZP**
Notice details Address: 180 Molesworth Street, Wellington PO Box 3017
Email: michael.higgie@police.govt.nz
Attention: : Emergency Communications Centres National Operations Manager

Name **The Priory in New Zealand of the Most Venerable Order of the Hospital of St John of Jerusalem**
Short form name **St John**
Notice details Address: 2 Harrison Road, Ellerslie, Auckland, 1051
Email: OIA 9(2)(a) @stjohn.org.nz
Attention: Ambulance Communications Manager – Continuous Improvement

Name **The Wellington Free Ambulance Service (Incorporated)**
Short form name **WFA**
Notice details Address: 19 Davis Street, Pipitea, Wellington 6011
Email: OIA 9(2)(a) @wfa.org.nz
Attention: Executive Director

Background

- A In May 2017, MBIE established a service enabling emergency call takers to receive certain location information relating to emergencies and emergency calls (the **ELI Service**). The ELI Service receives and processes emergency location information (**ELI**) and makes ELI available to emergency service providers.
- B FENZ, NZP, WFA and St John (together the **Participating ESPs**) provide emergency services in New Zealand, including taking emergency calls.
- C Since establishment of the ELI Service, the Participating ESPs have been using the ELI Service to deliver better outcomes for New Zealanders.
- D MBIE is extending the scope of the ELI Service and requires usage information about the ELI Service to:
- (i) monitor and audit the use of the ELI Service in accordance with the Telecommunications Information Privacy Code 2020;
 - (ii) demonstrate and monitor performance against the relevant key performance indicators for the ELI Service, including by demonstrating the benefits for users, stakeholders, and the public; and
 - (iii) support enhancements to, and optimisation of, the ELI Service.
- E The parties are entering this agreement to record the terms on which the Participating ESPs will use the ELI Service, collect data in relation to that use and disclose that data to MBIE.
- F While MBIE and the Participating ESPs are the original parties under this agreement, the parties intend that other emergency service providers may join this agreement with MBIE's consent.

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Agreed terms

1. Defined terms and interpretation

1.1 Defined terms

In this Agreement:

Agreement means this agreement, including its Schedules and together with any variations agreed between the parties in accordance with clause 12.2.

Business Day means any day other than a Saturday, a Sunday or a public holiday (as defined in the Holidays Act 2003) in Wellington, New Zealand.

Code means *Schedule 4: Emergency location information of the Telecommunications Information Privacy Code 2020*.

Commencement Date means the commencement date identified in the Key Details Schedule.

Contact Centre means a contact centre for emergency calls operated by one or more Participating ESPs.

ELI Service means the emergency location information service provided by the Relevant Government Agency (currently MBIE) to Participating ESPs.

Emergency Call means:

- (a) an emergency telecommunication originating in New Zealand; and
- (b) any other telecommunication placed by a person using a device and requiring an emergency response.

ESP means any public safety organisation that provides emergency services, including FENZ, NZP, St John and WFA.

Emergency Call Related Data (or “**ECR Data**”) means any Data associated with an Emergency Call that a Participating ESP collects, stores, or shares under or for the purposes of this Agreement.

ESP Representative means the person identified as such in the Key Details Schedule.

Damages means liabilities, expenses, losses, damages and costs.

Data means data or information in any format however generated, stored, processed, retrieved, or produced.

Government Agency means any state or government and any governmental, local governmental, semi-governmental, judicial, statutory or regulatory entity, authority, body or agency or any person charged with the administration of any law.

Initial Term means the initial term identified in the Key Details Schedule.

Key Details Schedule means Schedule 1 (Key details).

KPIs means the then-current key performance indicators specified in Key Details Schedule.

Location Agency has the meaning given to that term in the Code.

MBIE Representative means the person identified as such in the Key Details Schedule.

Participating ESP means:

- (a) at the Commencement Date, FENZ, NZP, WFA and St John; and
- (b) each ESP that joins this Agreement by accession under clause 8.1.

Personal Information means all information subject to Privacy Laws.

Privacy Laws means the Privacy Act 2020, the Unsolicited Electronic Messages Act 2007, the Health Information Privacy Code 2020, the Telecommunications Information Privacy Code 2020 (including each of its amendments) and any other legislation, principles, industry codes and policies relating to the handling of Personal Information.

Related Entity means, in respect of MBIE, any of the following:

- (a) any Crown Entity (as that phrase is defined in the Crown Entities Act 2004) that the MBIE monitors or is required to provide services and resources to under applicable legislation as notified to the ESP Representative by MBIE from time to time;
- (b) any ESP; and
- (c) any Government Agency.

Relevant Government Agency has the meaning given to that term in the Code.

Schedule means a schedule to this Agreement.

Term means the term of this Agreement as set out in clause 2.

1.2 Interpretation

In this Agreement, unless the context requires otherwise:

- (a) derivations of any defined word or term shall have a corresponding meaning;
- (b) the headings to clauses are inserted for convenience only and shall be ignored in interpreting this Agreement;
- (c) the word including and other similar words do not imply any limitation;
- (d) a reference to a party includes its personal representatives, successors and permitted assigns;
- (e) a person includes any individual, company, corporation, firm, partnership, trust, unincorporated body of persons or government agency;
- (f) the plural includes the singular and vice versa;
- (g) a reference to a statute includes all regulations and other subordinate legislation made under that statute. A reference to any legislation (including subordinate legislation) includes that legislation as amended or replaced from time to time; and
- (h) an obligation not to do something includes an obligation not to allow or cause that thing to be done.

2. Commencement and term

2.1 Commencement and Initial Term

This Agreement starts on the Commencement Date and ends on expiry of the Initial Term, unless sooner terminated in accordance with its terms or extended in accordance with clause 2.2 (the **Term**).

2.2 Extension

- (a) This Agreement expires at the end of the Initial Term unless the MBIE Representative and the ESP Representative agree in writing on or before the end of the Initial Term for the term to be extended for the extension period specified in the Key Details Schedule (or such other extension period agreed in writing).
- (b) The terms of this Agreement apply during any extension as they applied during the Initial Term unless the MBIE Representative and the ESP Representative otherwise agree in writing.
- (c) If this Agreement is extended, then upon expiry of the then-current extension period, this Agreement will expire unless the MBIE Representative and the ESP Representative agree in writing on or before the end of that extension period for the term to be extended for another extension period agreed in writing.

3. Use of ELI Service

3.1 Emergency Calls

To provide maximum benefit and deliver the efficiencies agreed through the business case, each Participating ESP agrees to:

- (a) use the ELI Service when handling all Emergency Calls received by any of its Contact Centres;

- (b) integrate use of the ELI Service, and capturing ECR Data for the purposes of this Agreement, into its processes for handling Emergency Calls; and
- (c) follow all standard operating procedures advised by MBIE from time to time regarding use of the ELI Service in relation to Emergency Calls.

3.2 Use of ELI Service in accordance with the Code

The parties acknowledge that the Code, authorises use of the ELI Service to enable a Participating ESP to, in accordance with the Code:

- (a) facilitate a response to an Emergency Call; and/or
- (b) prevent or lessen a serious threat to the life or health of an individual.

4. Capturing and sharing ECR Data

4.1 ECR Data capture

Each Participating ESP will maintain a record of ECR Data in the manner and form described in Schedule 2 (Data collection, protection, and sharing specification).

4.2 Sharing of ECR Data

Each Participating ESP will disclose ECR Data to MBIE in accordance with Schedule 2 (Data collection, protection, and sharing specification). Notwithstanding any other arrangements between any one or more Participating ESPs, each Participating ESP hereby authorises each other Participating ESP to disclose ECR Data in accordance with this Agreement.

4.3 Processing and using ECR Data

If any ECR Data is provided by a Participating ESP to MBIE in an anonymised way, MBIE will not process and use that ECR Data in a way, including matching the anonymised ECR Data with other data points, which results in the identification of any individual to whom that ECR Data relates.

5. Use of ECR Data

5.1 Monitoring, auditing, analytics, KPIs, enhancements, and optimisation

MBIE may use the ECR Data shared under this Agreement for the purposes of:

- (a) monitoring and auditing the use of the ELI Service in accordance with the Code;
- (b) demonstrating and monitoring performance against the KPIs; and
- (c) supporting enhancements to, and optimisation of, the ELI Service, including undertaking analytics and identifying business intelligence in relation to the ELI Service.

5.2 Form of reports

MBIE may use the ECR Data to prepare reports regarding the use and benefits of the ELI Service, including with respect to the KPIs and in accordance with the Code, provided that such reports do not include any individual's name, residential address, or phone number, nor disclose any other personal information contained within or derived from the ECR Data.

5.3 Sharing reports with Participating ESPs

MBIE will share any report created in accordance with clause 5.2 with the applicable Participating ESP.

5.4 Sharing reports

MBIE may share any report created in accordance with clause 5.2:

- (a) with any Location Agency, Government Agency, or minister of the Crown or parliamentary officer or body;
- (b) supplier of services and/or deliverables for the ELI Service or mobile operating system or device manufacturer (OIA 9(2)(b)(ii)), provided such disclosure is subject to undertakings of confidentiality;
- (c) to the extent disclosure is required by law (including under the Official Information Act 1982);

- (d) with prospective or current customers who use, or are considering using, any location service product provided by MBIE; or
- (e) in press releases or other marketing or informational material about the ELI Service.

5.5 Publishing reports and data sets

MBIE may publish any report created in accordance with clause 5.2, or any anonymised set of ECR Data, on a website or portal under the control of, or operated by, a Government Agency.

6. Information and audit

6.1 Privacy

In performing this Agreement, each party will at all times comply with the obligations set out in Schedule 3 (Privacy).

6.2 Publicity

Except as permitted by this Agreement, no party may make any media release or other public announcement relating to the existence of this Agreement or its terms, or the ELI Service, except with the other parties' prior written agreement. The Participating ESPs acknowledge that, in its capacity as the Relevant Government Agency under the Code, MBIE may make media releases or other public announcements regarding the ELI Service.

6.3 Mutual audit

- (a) MBIE and each Participating ESP will co-operate with and assist each other in relation to any audit that either of them proposes to undertake to verify compliance with either of those party's obligations under this Agreement.
- (b) Any audit will be undertaken remotely, without direct access to the other party's systems or premises, on not less than 20 Business Days' notice, and no more frequently than once in each 12 month period (unless a party has reasonable grounds to consider that there has been non-compliance with any material obligation under this Agreement, in which case the 12 months' frequency restriction does not apply).
- (c) The party undertaking the audit will provide the other party with a full, unredacted, copy of any audit report (and all other documents generated as part of the audit) within 10 Business Days after completion of the audit.

7. Changes to this Agreement

7.1 Process of changes to this Agreement

The MBIE Representative may, by written notice and in consultation with the ESP Representative, change this Agreement at any time.

7.2 Consequences of changes

Where MBIE has made a change to this Agreement in accordance with clause 7.1, if a Participating ESP reasonably considers that the change is materially detrimental to that Participating ESP, it may voluntarily exit this Agreement in accordance with clause 8.2.

7.3 Suspension

The MBIE Representative may, upon notice to the relevant Participating ESP, suspend a Participating ESPs' access to and use of the ELI Service, in part or in full:

- (a) for non-trivial security, confidentiality, operational, or technical reasons or concerns; or
- (b) if a Participating ESP commits, or allows to be committed, a non-trivial breach of this Agreement.

8. Accession, voluntary exit, and termination

8.1 Accession by further ESPs

An ESP who has been authorised as an *emergency service provider* under the Code may request to join this Agreement as a Participating ESP provided such ESP:

- (a) executes a letter of accession in the form set out in Schedule 4 (Letter of Accession Template); and
- (b) delivers a copy of the signed letter of accession to MBIE.

MBIE will countersign the signed letter of accession and return a copy to the ESP to confirm MBIE's authorisation for that ESP to be a Participating ESP.

8.2 Voluntary exit by Participating ESP

A Participating ESP may at any time elect to discontinue its participation in this Agreement by giving the MBIE Representative not less than 90 days' written notice. Upon expiry of that notice:

- (a) MBIE may retain any ECR Data already shared; and
- (b) the Participating ESP who gave notice is removed as a party to this Agreement with immediate effect, but remains subject to clause 8.4 (as if this Agreement had been terminated in relation to that Participating ESP).

8.3 Termination by convenience

MBIE may terminate this Agreement by giving the ESP Representative not less than 90 days' written notice.

8.4 Survival

Upon termination or expiry of this Agreement (or exit by Participating ESP under clause 8.2):

- (a) MBIE may retain any ECR Data already shared under this Agreement; and
- (b) this clause 8.4 and clauses 9, 10, 11, and 12 together with other provisions that are by their nature intended to survive, will remain in full force and effect.

9. Liability

9.1 Exclusion

Regardless of the head of loss, whether arising under contract, tort (including negligence), breach of statutory duty, or any other theory of liability, no party to this Agreement (the **First Party**) has any liability to another party except in respect of the First Party's breach of this Agreement.

9.2 Limitation

If a party is liable for breach of this Agreement (the **Breaching Party**), then to the maximum extent permitted by law (except for wilful neglect, fraud or gross negligence), the following limitations and exclusions apply:

- (a) the Breaching Party is not liable for any loss suffered by any person as a result of information provided or not provided in the ELI Service, including for death or personal injury, any indirect, consequential, or special Damages, any loss of revenue, loss of profit, loss of business, anticipated savings, loss of goodwill, business opportunity, increased operating costs, or loss of reputation, or any third party loss; and
- (b) for any liability that is not excluded by clause 9.1 above, the Breaching Party's aggregate liability under this Agreement during the Term is limited to \$100,000.

10. Warranties

10.1 Mutual warranties

Each party warrants and represents to the other parties that:

- (a) the execution and delivery of this Agreement has been properly authorised by all necessary corporate action; and
- (b) it has full corporate power and lawful authority and the legal power to execute and deliver this Agreement and to perform, or cause to be performed, their obligations under this Agreement.

10.2 Other warranties excluded

The ELI Service is provided on an “as is” basis. To the maximum extent permitted by law, MBIE disclaims all other warranties, whether express, implied, or statutory, including any implied warranties of merchantability and fitness for a particular purpose, title, non-infringement and any warranties arising from course of dealing or course of performance. Each Participating ESP acknowledges and agrees that MBIE does not have any responsibility, and is not liable, for the accuracy, fitness for purpose, or content of the ELI Service.

11. Dispute resolution

11.1 Dispute resolution process

Subject to clause 11.8, a party may not commence any arbitration or other proceeding relating to a dispute between the parties unless the party has complied with clauses 11.2 to 11.3.

11.2 Dispute notice

If there is a dispute between any of the parties in relation to this Agreement, any of the parties involved in the dispute (each an **Involved Party**) may give the MBIE Representative and the ESP Representative notice of the nature and details of the dispute.

11.3 Negotiation and escalation

- (a) Within five Business Days of receipt of the notice of dispute, the MBIE Representative and the ESP Representative will meet and attempt to resolve the dispute.
- (b) If the dispute is not resolved within five Business Days of that meeting, any Involved Party may by written notice to the other Involved Parties (with such notice copied to the MBIE Representative and the ESP Representative) escalate it to senior managers of the Involved Parties who shall meet to endeavour to resolve the dispute.

11.4 Arbitration

If the dispute is not resolved within 20 Business Days of receipt of the notice of dispute under clause 11.2, any Involved Party may by notice to all other Involved Parties refer the dispute to arbitration (with such notice copied to the MBIE Representative and the ESP Representative). The arbitration will be conducted in Wellington by a single arbitrator under the Arbitration Act 1996. If the Involved Parties do not agree on an arbitrator within five Business Days of receipt of the notice referring the dispute to arbitration, the arbitrator shall be appointed by the President of the New Zealand Law Society (or his/her nominee) at the request of any of the Involved Parties.

11.5 Appeals on points of law

The parties waive any right to seek a determination by the court of a preliminary point of law (pursuant to section 4, Second Schedule to the Arbitration Act 1996) and to appeal on a question of law (pursuant to section 5, Second Schedule to the Arbitration Act 1996).

11.6 Decision

The arbitrator will determine the dispute and deliver to each Involved Party a written decision. The decision must specify brief reasons for the decision. The decision will be final and binding on the Involved Parties.

11.7 Continued performance

Regardless of any dispute, each party shall continue to perform this Agreement to the extent practicable, but without prejudice to their respective rights and remedies.

11.8 Urgent relief

Nothing in this clause 11 will preclude a party from seeking urgent interlocutory relief before a court.

12. General

12.1 Further assurance

Each party will do all acts and things necessary to implement and to carry out its obligations under this Agreement.

12.2 Amendments

Except as otherwise provided in this Agreement, this Agreement may only be amended, supplemented or novated in writing executed by all parties.

12.3 Notices

- (a) Any notice given pursuant to this Agreement will be deemed to be validly given if personally delivered, posted, or sent by electronic means, to the address or email address of the party set out in the "Parties" section of this Agreement or to such other address or email address as the party to be notified may designate by written notice given to all the other parties.
- (b) Any notice given pursuant to this Agreement will be deemed to be validly given:
 - (i) in the case of personal delivery, when received;
 - (ii) in the case of posting, on the second day following the date of posting;
 - (iii) in the case of electronic transmission by email, at the time of transmission, provided that an email is not deemed received unless (if receipt is disputed) the party giving notice produces a printed copy of the email which evidences that the email was sent to the email address of the party given notice.

12.4 Entire agreement

This Agreement constitutes the entire agreement, understanding and arrangement (express and implied) between the parties relating to the subject matter of this Agreement and supersedes and cancels any previous agreement, understanding and arrangement relating thereto whether written or oral.

12.5 Governing law

This Agreement is governed by the laws of New Zealand and the parties submit to the non-exclusive jurisdiction of the courts of New Zealand.

12.6 Assignment

- (a) No Participating ESP may assign, transfer, novate, or subcontract this Agreement, or any of its rights or obligations under this Agreement, without first obtaining MBIE's written consent.
- (b) MBIE may assign, transfer or novate any or all of its rights and obligations under this Agreement to any Related Entity by giving notice in writing to the ESP Representative.

12.7 Counterparts

This Agreement may be executed in any number of counterparts (including facsimile or scanned PDF counterpart), each of which shall be deemed an original, but all of which together shall constitute the same instrument. No counterpart shall be effective until each party has executed at least one counterpart.

Execution

EXECUTED as an agreement

For and on behalf of

Ministry of Business, Innovation and Employment by:



Signature of authorised signatory

James Hartley—General Manager Digital, Communications & Transformation

Name of authorised signatory

For and on behalf of

The Wellington Free Ambulance Service (Incorporated) by:



Signature of authorised signatory

Kate Jennings – Executive Director – Clinical Communications and Patient Coordination.

Name of authorised signatory

For and on behalf of

Fire and Emergency New Zealand by:



Signature of authorised signatory

Kerry Gregory, DCE Service Delivery

Name of authorised signatory

For and on behalf of

New Zealand Police by:



Signature of authorised signatory

Michael Higgle

Name of authorised signatory

For and on behalf of

The Priory in New Zealand of the Most Venerable Order of the Hospital of St John of Jerusalem by:



Signature of authorised signatory

Cameron Brill, DCE Corporate Operations

Name of authorised signatory

Schedule 1 – Key details

Contract details

Item	Detail
Commencement Date	1 March 2022
Initial Term	Three years from the Commencement Date
Extension Period	Two years
MBIE Representative	Role / title: ELI Manager Service Enhancements Email: pam.harris@mbie.govt.nz Phone: OIA 9(2)(a)
ESP Representative	Role / title: Emergency Communications Centres National Operations Manager Email: michael.higgie@police.govt.nz Phone: OIA 9(2)(a)

Key Performance Indicators

The current KPIs are:

- **Strategic Outcome 1: Improved preservation of life and property**
 - KPI 1: Reduction in No Speech Emergency Calls
 - KPI 2: Reduced structural fire damage costs through faster response
 - KPI 3: Reduced location verification time for P1 emergencies

- **Strategic Outcome 2: Operational efficiency improvements for emergency services**
 - KPI 4: Reduced average time to verify mobile caller's location
 - KPI 5: Improved location accuracy through reduced area of uncertainty

Schedule 2 – Data collection, protection, and sharing specification

1. ECR Data collection and storage

1.1 Data fields to be collected and stored

Each Participating ESP will collect and store the following fields of ECR Data for all Emergency Calls (including Emergency Calls referred by another ESP):

(a) **NZP**

#	Field name	Field description	Specification / required data	Notes
1.	Event Number	Call ID	Required	Unique call identifier assigned by the NZ Police CAD system. The Call ID is not, by itself, personal information about the individual concerned.
2.	Entry Start Date Time	Date and time when call taker starts entering details of the call	Required	
3.	Acceptance Date Time	Date and time when the call taker has sufficient details, including the location and a quick understanding of what is occurring, to accept the call	Required	Closest measure of address verification time
4.	Caller Phone Number	Contact number for call back	Required	This is not necessarily the caller's phone number. Not anonymised in accordance with paragraph 3.2 below
5.	Dispatch Duration	Time in seconds after the call acceptance to dispatch the first unit	Required	
6.	Acceptance Type Code*	The description of the nature of the event when the call is accepted	Optional	Contains No Speech Emergency Call. Blanks for all other call types. NZ Police will advise MBIE of updates to this field.
7.	Closure Type Code*	The final description of the event	Optional	Contains No Speech Emergency Call. Blanks for all other call types. NZ Police will advise MBIE of updates to this field.
8.	Highest Priority		Required	MBIE intends to use this field as reference data. NZ Police will advise MBIE of updates to this field.
9.	Result	The result code when the call is closed	Required	MBIE intends to use this field as reference data. NZ Police will advise MBIE of updates to this field.
10.	NZTM Northing	Address latitude of the incident in New Zealand Transverse Mercator 2000 Projection	Required	
11.	NZTM Easting	Address longitude of the incident in New Zealand Transverse Mercator 2000 Projection	Required	

#	Field name	Field description	Specification / required data	Notes
12.	ECLI Record	True/False	Required	Denotes whether ECLI was recorded for the event
13.	ECLI Text	ECLI message recorded in the call remarks/comment	Optional	The ECLI message. Contains the phone number which is not anonymised in accordance with paragraph 3.2 below

(b) **St John**

#	Field name	Field description	Specification / required data	Notes
1.	PCL	ECLI Available flag (0 or 1 values)	Required	Denotes whether ECLI is available for the call
2.	Date Time	Date and timestamp of the incident	Required timestamp formatted as 'DD/MM/YYYY hh:mm:ss'	This is the response_date column in CAD and is the date and time of the incident being generated in CAD. See paragraph 1.2 (Timestamps) below.
3.	ID	CAD Incident ID	Required	Unique call identifier assigned by the ESP CAD system
4.	Priority Description	Final priority associated with the incident	Required	MBIE intends to use this field as reference data. St John will advise MBIE of updates to this field.
5.	Address Latitude	Address latitude of the incident	Required, expressed in decimal degrees up to 7 decimal places	Latitude recorded in the CAD for the location address of the emergency
6.	Address Longitude	Address longitude of the incident	Required, expressed in decimal degrees up to 7 decimal places	Latitude recorded in the CAD for the location address of the emergency
7.	Time Phone Pickup	Time the call taker picked up the ringing phone	Optional	NULLs timestamps in the data are possible
8.	Time Address Entered	Time the address was entered	Optional	NULLs timestamps in the data are possible
9.	Time ProQA Opened	ProQA is opened only after address and phone number have been verified	Optional	Closest equivalent to address verification time, NULLs timestamps in the data are possible
10.	phoneNumber	Caller's phone number	Required, anonymised in accordance with paragraph 3.2 below	From Response_ANIALI table. This matches the WFA 'Phone Encryption' field.
11.	PCL Comment	ECLI message recorded in the call remarks/comment	Required for calls where ELI Service was available/used. Phone number anonymised in accordance with paragraph 3.2 below.	The ECLI message contains the ECLI source, phone number, timestamp, latitude, longitude, area (optional), location description (optional), radius (optional), shape (optional).

(c) WFA

#	Field name	Field description	Specification / required data	Notes
1.	TS_Call_Start	Call start date and time	Required timestamp formatted as 'DD/MM/YYYY hh:mm:ss'	See paragraph 1.2 (Timestamps) below.
2.	Call_ID	Call ID	Required	Unique call identifier assigned by the ESP CAD system
3.	Category_Type	Final priority associated with the incident	Required	MBIE intends to use this field as reference data. WFA will advise MBIE of updates to this field.
4.	Phone encryption	Caller's phone number	Required, anonymised in accordance with paragraph 3.2 below.	Caller's phone number (not to be confused with the call back contact number if that is different from the caller's phone number)
5.	Address_latitude_event	Address latitude of the emergency event	Required, expressed in decimal degrees up to 7 decimal places.	Latitude recorded in the CAD for the location address of the emergency
6.	Address_latitude_caller	Address latitude of the emergency caller	Required, expressed in decimal degrees up to 7 decimal places.	Latitude recorded in the CAD for the location address of the caller, derived from the ECLI record used for the call
7.	Address_longitude_event	Address longitude of the emergency event	Required, expressed in decimal degrees up to 7 decimal places.	Longitude recorded in the CAD for the location address of the emergency
8.	Address_longitude_caller	Address longitude of the emergency caller	Required, expressed in decimal degrees up to 7 decimal places.	Longitude recorded in the CAD for the location address of the caller, derived from the ECLI record used for the call
9.	Verified_Address_Timestamp	Time the address of the emergency was verified address	Required – see notes. Timestamp formatted as 'DD/MM/YYYY hh:mm:ss'.	This is the date and time ProQA was opened NULLs timestamps in the data are possible
10.	ECLI_Available	TRUE/FALSE flag	Required	Denotes whether ECLI was available for the call
11.	Radius (m)	Radius of the ECLI record used for the call	Optional	

(d) **FENZ**

Extract File Header

A header for each extract will be added to the top of the file. It will contain three rows formatted as such:

- Report generated timestamp: [yyyy-mm-dd hh:mm:ss:sss]
- Report date range: [yyyy-mm-dd hh:mm:ss] to [yyyy-mm-dd hh:mm:ss]
- Report row count: [nnnn]

Extract File Body

General Business Rules

1. For Events with ECLI comments, all events are extracted;
2. For Events with no ECLI comments, only response event types from NZ mobile phone numbers are extracted.

#	Column	Format	Business Rule	Description
1.	FENZEventNum	String	N/A	This is the FENZ Event Number assigned to an Event in ICAD
2.	FirstCallerNum	String	Hashed using the MBIE business rules for Hashing mobile numbers. If null, there was no registered first caller. The obfuscation is applied to numbers. For non-number entries, the obfuscation is not applied but the value is still hashed.	Phone number of the person who is flagged as the first caller in ICAD
3.	CallSource	String	N/A	This is the source of the call (what system or process generated the event)
4.	EventType	String	EventType is formatted to more friendly names for response events.	This is the Event type of the event used in the incident. FENZ will advise MBIE of updates to this field.
5.	EventStartTimeUTC	DateTime	Formatted to UTC time	This is the UTC time of the start of the event. The Start of the event is the point where the "create new event" action is triggered in ICAD, even before the event has been saved. The saved time becomes the CallTakerConfirmedTime
6.	CallTakerConfirmedTimeUTC	DateTime	Formatted to UTC time	This is the UTC time where the person creating the event saves the event for the first time. CallTakerConfirmedTime indicates when the call taker has finished their part of the job to the point where the dispatcher can respond units. If the CallTakerConfirmedTime is the same as the EventStartTime this means the event was automatically generated with a location and no initial call taking was done.

#	Column	Format	Business Rule	Description
7.	Latitude	Number	Converted from NZTM and rounded to 6 decimal places	Latitude in decimal format for the event
8.	Longitude	Number	Converted from NZTM and rounded to 6 decimal places	Longitude in decimal format for the event
9.	TA	String	N/A	This is the Territorial Authority (TA) for the event as noted in ICAD at the time of the event
10.	ECLIComment	String	<p>The comment is retrieved where the comment has 'ECLI ' or 'PCL ' and then the comments are only valid for the extract if they have the following:</p> <ul style="list-style-type: none"> • A phone number • LL() • Location time • the keywords (Handset, Mcl, Network) <p>Comment text before ECLI/PCL is removed</p> <p>Comment text after the location time and Shape() sections is removed</p> <p>The phone number is Hashed as per MBIE business rules for Hashing.</p> <p>Duplicate rows are removed for events that have the same call details including the ECLI comment at the same ECLI timestamp</p> <p>A null or blank ECLI comment indicates the event did not use ECLI.</p>	This is the ECLI String from the ECLI website pasted into ICAD general remarks field. Double quotes are place around the ECLI Comment so that commas within the ECLI String do not impact the file format. (File format is CSV.)
11.	RespondedToEvent	Number	1 if Event has been responded to, 0 otherwise	Defines if the event was responded to i.e. if a unit was dispatched.

1.2 Timestamps

- To support data consistency and to avoid daylight savings confusion, each Participating ESP will use all reasonable endeavours to use a UTC (Coordinated Universal Time) timestamp for its ECR Data.
- If any Participating ESP is unable to use a UTC timestamp for any ECR Data, that Participating ESP will advise MBIE whether the timestamps used in that ECR Data are in NZST or NZST/NZDT, to assist MBIE derive the correct time for call matching purposes.

1.3 Priority Category or Event Type

Each Participating ESP will advise MBIE in writing if the Participating ESP changes its coding system for any of the following fields (as identified in the table in paragraph 1.1 above), to assist MBIE to adjust its upload processes and reports:

(a) **NZP**

Acceptance Type Code
Closure Type Code
Highest Priority
Result

(b) **STJ**

Priority Description

(c) **WFA**

Category_Type

(d) **FENZ**

EventType

2. Password arrangements

2.1 Password length requirement

Each password must be 16 characters in length (or longer) and aligned to NZISM requirements for password length (as NZISM is updated from time to time).

2.2 Password for encryption of ECR Data files

Each Participating ESP will advise MBIE, via a separate email or SMS text, of each password used by the Participating ESP when encrypting any ECR Data files shared with MBIE. The password used by the Participating ESP does not need to be unique to each ECR Data file.

3. Anonymization, obfuscation and hashing of ECR Data

3.1 Anonymization by removing individuals' names

Each Participating ESP will remove from its ECR Data any individual's name. No Participating ESP will remove any information in the fields specified in paragraph 1.1 above (as some of those fields, such as address, are required by MBIE to confirm the accuracy of the ECR Data).

3.2 Mobile phone number obfuscation and hashing

Except to the extent agreed in writing with MBIE, each Participating ESP will obfuscate and hash each phone number in the ECR Data as follows:

- (a) using a pepper string managed in accordance with paragraph 3.3 below. A "pepper string" is a random string of characters applied to the mobile phone number before that number is hashed; and
- (b) hashed using an algorithm advised by MBIE from time to time.

3.3 Pepper string arrangements

OIA 9(2)(c)

4. Sharing ECR Data with MBIE

4.1 Provision of baseline data

Except to the extent agreed in writing with MBIE, within 20 Business Days after each Participating ESP becomes a party to this agreement, that Participating ESP will share with MBIE the following baseline values to assist MBIE with its key performance indicators (KPI) reporting:

Average address verification times

- (a) average address verification times prior to the Participating ESP commencing use of the ELI Service, for the period between May 2016 and June 2018; and
- (b) average address verification times since the Participating ESP commenced using of the ELI Service, for the period between May 2016 and June 2018.

4.2 Format

OIA 9(2)(c)

4.4 Frequency of sharing

- (a) Within 20 Business Days after each Participating ESP becomes a party to this agreement, the frequency and timing by which each Participating ESP will commence sharing regular ECR Data feeds with MBIE will be agreed between MBIE and each Participating ESP.
- (b) If agreement between MBIE and a Participating ESP is not reached by expiry of the time period in (a) above, that Participating ESP will share the ECR Data with MBIE, on a consistent regular daily or weekly basis, and at a consistent regular time of day, each as determined by the Participating ESP and notified to MBIE.

Schedule 3 – Privacy

1. Privacy requirements

1.1 MBIE's role under Privacy Laws

Under the Code, MBIE is the Relevant Government Agency responsible for the Emergency Location Information System (ELIS) system which receives and processes emergency location information (ELI) and makes ELI available to emergency service providers (including the Participating ESPs). MBIE will at all times comply with all Privacy Laws in relation to Personal Information obtained under this Agreement. MBIE will:

- (a) procure that access to such Personal Information is given only to its personnel who reasonably require access for a lawful purpose;
- (b) notify the relevant Participating ESPs if MBIE becomes aware of an actual or potential breach of the Privacy Laws by itself or any of its personnel or receives a privacy complaint relating to information provided by or in respect of a Participating ESP;
- (c) provide the relevant Participating ESP with any information or assistance reasonably requested by the Participating ESP for the purposes of investigating an actual or potential breach of Privacy Laws or a privacy complaint;
- (d) co-operate with the relevant Participating ESP to rectify or minimise any breach of Privacy Laws or any privacy complaint; and
- (e) co-operate, and provide the relevant Participating ESP with assistance in co-operating, with any investigations or recommendations made by a privacy regulator in connection with the handling of such Personal Information.

1.2 Participating ESP obligations

Having regard to MBIE's role identified in paragraph 1.1 above, each Participating ESP will at all times comply with all Privacy Laws in relation to Personal Information. Without limiting the foregoing, each Participating ESP must:

- (a) ensure that access to the Personal Information is given only to its personnel who reasonably require access for a lawful purpose;
- (b) immediately notify MBIE if that Participating ESP becomes aware of an actual or potential breach of the Privacy Laws by itself or any of its personnel or receives a privacy complaint;
- (c) promptly provide MBIE with any information or assistance reasonably requested by MBIE for the purposes of investigating an actual or potential breach of Privacy Laws or a privacy complaint;
- (d) comply with all directions given by MBIE to rectify or minimise any breach of Privacy Laws or any privacy complaint; and
- (e) co-operate, and provide MBIE with assistance in co-operating, with any investigations or recommendations made by a privacy regulator in connection with the handling of Personal Information.

Schedule 4 – Letter of Accession Template

Letter of Accession

Date [insert date]

Acceding Party [insert acceding party's full legal name] (Acceding Party)

Background

- A. The Ministry of Business, Innovation and Employment (MBIE), [Fire and Emergency New Zealand (FENZ), New Zealand Police (NZP), the Priory in New Zealand of the Most Venerable Order of the Hospital of St John of Jerusalem (St John) and The Wellington Free Ambulance Service (Incorporated) (WFA)] are parties to a *Data Use and Sharing Agreement in relation to the Emergency Location Information Service (Agreement)* dated [insert date]. [FENZ, NZP, St John and WFA] are Participating ESPs under the Agreement.
- B. Clause 8.1 of the Agreement contemplates that, subject to MBIE's authorisation, other ESPs may join the Agreement by executing a letter of accession in this form.
- C. The Acceding Party signs this letter of accession for the purpose of becoming a Participating ESP under, and being bound by, the Agreement.

Terms of accession

- 1. The Acceding Party confirms that it has been supplied with a copy of the Agreement.
- 2. The Acceding Party covenants with the parties to the Agreement (whether original or by accession) to observe, perform and be bound by all the terms of the Agreement to the intent and effect that the Acceding Party is deemed to be a party to the Agreement, as a Participating ESP (in addition to any other Participating ESPs).
- 3. The Acceding Party's notice details for the purposes of the Agreement are:

Address: [insert]

Facsimile: [insert]

Email: [insert]

Attention: [insert]

- 4. Subject to MBIE's authorisation, as evidenced by MBIE's countersignature of this letter, the Acceding Party will be a Participating ESP under the Agreement from the date of this letter.

Execution

For and on behalf of [insert Acceding Party's full legal name] by:

Signature of authorised signatory

Name of authorised signatory

By countersigning this letter, MBIE authorises the Acceding Party to become a Participating ESP for the purposes of the Agreement

For and on behalf of the
Ministry of Business, Innovation and Employment
by:

Signature of authorised signatory

Name of authorised signatory