

TRIANGULATION PROCEDURES & SECTION 287 REQUESTS FOR THE STATE COORDINATION UNIT

RADIO OPERATIONS GROUP

Summary

A mobile phone triangulation detects the approximate location of a mobile phone handset currently active and connected to a network within the boundaries of cell site towers.

Legislation

The power to obtain information relating to a triangulation comes from Section 287 Telecommunications Act (Cth) 1997. This section provides an exemption from the privacy provisions of the Act only if the information 'creates a reasonable belief that it is reasonably necessary to prevent or lessen a serious threat to the life or health of a person'.

Telecommunications Act 1997 - Sect 287

Threat to person's life or health

Division 2 does not prohibit a disclosure or use by a person (the first person) of information or a document if:

- (a) the information or document relates to the affairs or personal particulars (including any unlisted telephone number or any address) of another person; and
- (ab) it is unreasonable or impracticable to obtain the other person's consent to the disclosure or use; and
- (b) the first person believes on reasonable grounds that the disclosure or use is reasonably necessary to prevent or lessen a serious threat to the life or health of a person.

This Policy replaces February 2024 Procedure for Triangulation & Section 287 Requests for the State Coordination Unit v1

Document Control Sheet

Document Properties

Title	Procedure for Triangulation & Section 287 Requests for the State Coordination Unit
Subject	Triangulation procedures and actions to be taken by the State Coordination Unit
Command responsible	Communication Services Command
Authorisation	Commissioner of Police
Security Classification	OFFICIAL
Publication date	June 2024
Current version number	2
Review date	June 2025
Document RMS number Linked RMS folder	D/2024/311110 linked to F/2023/54392
Copyright statement	© Crown in right of NSW through NSW Police Force [ENTER YEAR]
Suitable for Public Disclosure	YES

Modification History

Modifica	tion instory		
Versio n#	Version creation date	Author / Position	Summary of changes
1	02/2024	Sen Sgt Mark McCULKIN	Updated to Corporate Policy Document template. Update to include circumstances where person has committed murder or crime of serious violence. Addition of escalation process for declined requests.
2	06/2024	Sen Sgt Mark McCULKIN	Minor updates to basic examples of threats as requested by OGC.

Table of Contents

SUMMARY	2
DOCUMENT CONTROL SHEET	3
PURPOSE	5
Scope	6
Details the actions to be taken by the State Coordination Unit in relation to triangulations	6
Roles & responsibilities	6
PROCEDURE	6
Only the State Coordinator to Authorise	6
ANNEXURE A – PUBLIC INTEREST CONSIDERATION CHECKLIST	13

Purpose

INFORMATION ON SECTION 287 REQUESTS, INCLUDING THE APPLICATION FLOWCHART CAN BE FOUND IN

SOPs - Missing Persons - Using Mobile Phones to Urgently Locate Someone at Risk

2023 SOPS V3.4 - Final published version.pdf (nsw.gov.au)

When to Use a s287 Request in relation to a missing person

A request for a triangulation to locate a missing person should only be made in those instances where there is a reasonable belief that it is reasonably necessary to prevent or lessen a serious threat to the life or health of a person. If a person is reported missing and no other risk factors are identified, then it is unlikely that the request would meet the threshold for a Section 287 request. The following list may provide some guidance on instances that may justify approval of a triangulation to assist in locating a missing person;

- The missing person has made actual or implied threats of self-harm;
- The missing person has a history of self-harm although has not made threats in this instance;
- The missing person has not made threats of self-harm and has no history of self-harm but is known to have serious mental health issues or mental health issues that have escalated in recent times resulting in serious concerns for their safety;
- The missing person is a vulnerable person who suffers from a significantly reduced capacity to care for themselves that may lead to danger (e.g. dementia, children, etc);
- The missing person has gone missing in circumstances that lead you to believe they may be in danger, (e.g. a motorist known to be travelling in an area has not arrived at their destination and is now uncontactable leading you to suspect they may have had an accident).
- A person has committed a murder or a crime of serious violence and their geographical location is unknown, and there are concerns that they may engage in conduct that threatens the life or health of themselves or another person.

Who Can Request?

A request for a triangulation or other S287 request should only come from a Duty Officer or Supervisor. Exceptions to this rule may occur when officers working in remote areas do not have ready access to a Duty Officer or Supervisor. This is to ensure that ongoing triangulations are included in the Supervisor's changeover in the event that a triangulation continues over to the next shift.

Note: While not prescribed under the Act, a basic investigation should take place prior to commencing a triangulation. This should include, but not be limited to, speaking to the person reporting, confirming details of the threat, sighting text messages/emails, attending the missing person's address, calling the missing person's mobile and/or land line, etc.

Refer to Basic Investigation Questionnaire Sheet before considering a S287 request.

Scope

Details the actions to be taken by the State Coordination Unit in relation to triangulations.

Roles & responsibilities

Assistant commissioner – Communication Services Command	Document Sponsor
Commander – Radio Operations Group	Document Owner
Inspector/Manager	Ensure adherence to policy
Requesting Officer	Provide required and relevant information at time of request to ensure adherence to Policy

Procedure

Only the State Coordinator to Authorise

The only officer permitted to authorise a triangulation is the State Coordinator at the State Coordinator Unit. A Sergeant or Constable at Sydney Radio Operations Centre (SROC) may take a telephone request for a triangulation but must present those details to the SCU for assessment. This authority extends to substantive Sergeants when relieving in the position of State Coordinator

(including covering meal breaks and other short absences from the workplace).

Procedure for State Coordinators

All requests must be made by telephone to the SCU. Under no circumstances should requests be made over the air or via a CAD job. The details of the request will be recorded in the Indigo system, S287 Request Form or SCU Log Book. These details should include the Duty Officer's or Supervisor's name, contact number, the mobile phone number to be triangulated, the missing person's name and brief circumstances.

Ensure that the Command requesting the triangulation has created a CAD job. Depending on the type of incident, this CAD should include the description the circumstances surrounding the threat by or to the missing person, clothing worn, any vehicle(s) being driven etc. A Police COPS Event number should be included in the CAD message when the Event is created. The SCU must complete an electronic

S287 request form in the CAD job (regardless of whether the request is approved or declined).

A triangulation will end when the requesting officer contacts the SCU and requests that the triangulation be terminated. This contact can be made by telephone or via CAD. If at any time the SCU is not satisfied that the conditions of S287 are being met for a current triangulation then the SCU should contact the requesting officer and seek clarification. If the SCU is not satisfied that the triangulation meets the conditions of S287 then the SCU is authorised to terminate the triangulation after consulting with the requesting officer. A triangulation can also be cancelled by the SCU if satisfied that the triangulation is no longer adding value to the investigation into the location of the missing person. Examples where a triangulation is not considered to be of further value, include (list is not exhaustive);

- The triangulation area has not moved for an extended period and the area has been extensively patrolled by Police
- The handset has been turned off for an extended period
- The triangulation area is so large as to be considered unsearchable
- The handset signal is so erratic that a suspected location for the missing person cannot be identified

It should be noted that investigating Commands can apply for 'Live CAD' through the Telephone Interception Unit which provides the opportunity for Commands to monitor the triangulation themselves. Procedures for applying for 'Live CAD' is contained in the 'Missing Persons, Unidentified Bodies and Human Remains SOPs' available on the intranet. It should also be noted that the resources of the SCU are limited, and lengthy monitoring of a triangulation is not possible.

Declined Requests

If a request is declined by the State Coordinator, a comprehensive reason for "decline" is recorded in the SCU Logbook or in the Indigo system, and in CAD using the SCU S287 deployment form. The SCU must verbally remind the Duty Officer at the time of a declined request of this escalation process if they disagree with the decision by the SCU.

Should the Duty Officer disagree with the decision made by the SCU they should liaise with their Commander to seek a review and contact the ROG Commander on EN 54474 during business hours, or via the SCU outside of business hours. In the event that there is no resolution the decision should be escalated to the Assistant Commissioner, Communications Services Command.

All information/requests to and from the State Coordination Unit regarding Triangulation Requests are recorded in the following way:

- Recorded telephone calls The State Coordination Unit is a declared "Emergency Service Facility" for the purpose of the Telecommunications (Interception & Access) Act 1979.
 Accordingly, all calls made to and from the SCU are recorded and saved for a minimum of 7 years.
- Handwritten Log Book or Indigo System or S287 Request Form- State Coordinators will
 make written records of requests made to them in a Log Book, the Indigo System or on a
 S287 Request Form. A NSW Police Force Radio Log Book is a legal and accountable
 document and may be used in court proceedings. A S287 Request Form may be completed
 to facilitate requests with those telecommunication carriers that require them. These forms
 are saved electronically on the NSWPF P Drive.

Threat	Is it serious?
Notification from a mental health service line or other external organisation that a person intends to kill himself/herself.	This is likely to be considered serious.
A person has committed a murder or a crime of serious violence and their geographical location is unknown.	If there are family members or other persons who may be at risk, or the suspected offender has done or said anything to indicate a risk of self-harm, then this is likely to be considered a serious threat.
	If there are no such indications (for example, where the request is made by investigative police a number of days after the incident), the case may nevertheless amount to a serious threat, however, further consideration will be required as to the possibility that the suspected offender may engage in further conduct that threatens the life or health of other persons.
A bomb threat.	This is likely to be considered serious.
A family member calls NSWPF or another emergency services agency about a person who intends to kill himself/herself or to kill other people.	This is likely to be considered serious.
Investigative police receive a telephone call from a private number.	This will depend on information provided during the call.
A bushwalker who calls NSWPF stating he is lost or where a bushwalker has not returned from a walk and a report is made that he is missing.	If the call is from the bushwalker, then disclosure of geographical position could be sought under s.290 in that they have given implied consent for the release of this information.
	It could also be argued that there is serious threat to the person's life or health given that they are lost and it is not known whether they are injured.
A call to NSWPF from a person advising that he is going to drive his car through a politician's office.	This is likely to be considered serious.

• <u>PoliceCAD</u> - Requests and updates concerning the utilisation of the S287 are recorded in the CAD incident log using the S287 deployment form.

Basic Examples of Threats Against a Person

A call to NSWPF advising a person is going to kill themselves.	This is likely to be considered serious.
A threat to blow up Sydney Harbour Bridge where a time frame is given, (e.g. 1 hour, 1 week, 6 months)	1 hour - This is likely to be considered serious. Although 'imminency' is no longer a consideration in S287, a common sense approach should be used, (is the information required for investigative purposes or is there a reasonable belief that a person's life or health is at serious risk?).
A call to NSWPF that a person is going to kill 5 people in 10 minutes.	This is likely to be considered serious.
A victim's phone is stolen in a robbery and investigative police request that geographical position of the phone.	This would require consideration of whether the person is thought to be dangerous and is likely to commit another crime that would threaten the health and safety of another person or persons.
Where a call to Lifeline is made on Skype.	If details are held by an overseas company, then we do not consider that the company would be bound to provide that information under section 287.
An anonymous telephone call stating that the caller is going to release damaging information about a particular person.	This is unlikely to meet the test as the risk is to the person's reputation rather than to their life or health.

Other Threats

Other situations that could be considered to be a serious threat to the life or health of a person could include the threat of:

- (a) Bodily injury, illness or death
 - (i) Where a person is being threatened with a weapon, including NSWPF;
 - (ii) Hostage situations;
 - (iii) Where a credible threat has been received, i.e. an explicit / specific threat of murder or assault relating to a particular person, group of persons or the community at large;
 - (iv) At an accident, incident or a disaster where people have been seriously injured.
- (b) Contracting or being denied effective treatment for a serious medical condition:
 - (i) Where NSWPF are involved in a situation where a person is being denied effective treatment for an illness or trauma;
 - (ii) NSWPF may be investigating the release of a toxic substance such as anthrax on public transport;
 - (iii) In a situation where a person is deliberately infecting others with a life-threatening condition such as HIV.

Basic Investigation Questionnaire Sheet

Information required by the SCU for consideration of activating a triangulation

- Which PAC has ownership of the missing/abducted/suicidal person?
- Contact number
- Contact number on change over
- Reason for the request
- What is the serious threat to the life or health of a person?
- Have we established the person is not at their residential address?
- Is it confirmed the person has the mobile phone with them and is it switched on?
- Is the number confirmed as being theirs and who is their Telco Provider?
- Have you called the number?
- If not, why not?
- What happens when you call it?
- Goes straight to message bank
- Rings and then goes to message bank
- Rings out

- Phone answers refuses to say where they are
- Where did the information come from?
- Who is the informant?
- What is their relationship with the person?
- Have you met with them or spoken to them directly?
- How credible is the information?
- Where and when was person last seen?
- How long ago did they last make contact?
- Is it feasible that they may have already committed suicide/reached their destination?
- What is their mode of transport?
- Do we have a description good enough to look for the person?
- Is there a mental health or self-harm history?
- Have they been reported missing?
- Is there a PoliceCAD message on channel?
- Has a nemesis message been forwarded?
- In the event the person has been missing for a considerable time, have you made any requests through RFI or BluePortal?
- If the matter involves violence or serious injury, are there family members or others who may be at risk, or has the person done or said anything to indicate to risk of self harm?

SERVICES PROVIDED BY TELECOMMUNICATIONS AUTHORITIES - SCU

CONTACT THE SCU IN "SERIOUS LIFE-THREATENING SITUATIONS" ONLY

Malicious Call Trace Facility (MCT)

All Police Stations should have a MCT facility on their telephone switch boards.

If a threatening phone call, a violent incident such as a domestic or medical emergency is occurring, and your caller does not provide a location – activate the MCT / trace button.

You need to provide the SCU with a start and finish time as well as the time the pressed the MCT button.

If it is a location other than a police station you need to provide the SCU with the name of the Telco and the number that received the call.

Emergency Life Threatening Trace

Didn't activate the MCT – the SCU can try a call trace which will give you the last call or a recent call.

Best results are when you can give exact call start and finish times. It is useful to determine from the person receiving the call, how many calls were received before and after the call you are tracing.

Mainly used for landlines but can be done on mobiles – examples of use, not limited to;

premises who receive bomb threats, distressed callers who leave a message on an answering machine, stressed callers who misdial, medical issues, police stations who receive a threat to an officer, calls which sound like a violent domestic is occurring (leave the phone off the hook and best to answer on switch)

Customer details (Life Threatening Only)

Got only a number but no address and it is "life threatening"? The SCU can obtain customer details which includes the name of the person they bill and the address they send the bill to.

Investigative issues are done through RFI on BluePortal

Mobile Location (Triangulation)

Ownership of the triangulation by a PAC is important. This ensures a liaison officer for the SCU and a managed response to locate the subject. The mobile needs to have a SIM card and must be turned on. You should consider trying to call the number yourself to see what happens. You can't absolutely be sure it is off unless you check with the Telco. Traditional investigative methods must be adopted in conjunction with a triangulation. Triangulations do not substitute for direct enquiries by Officers attending known residential addresses or speaking with NOK and getting KLO4 memo's out. A CAD job should be generated and circulated with description of the person for others to KLO4 and the SCU tagged in CAD.

DO NOT REQUEST A TRIANGULATION TO LOCATE OFFENDERS

IF YOU ARE CONSIDERING A TRIANGULATION FOR AN ABDUCTION YOU NEED TO DETERMINE IF A STATE CRIME COMMAND RESPONSE IS NECESSARY AND/OR ACTIVATION OF THE AMBER ALERT SOPS WITH REGARDS TO CHILDREN UNDER 16 YEARS

https://intranet.police.nsw.gov.au/ data/assets/file/0003/527943/Final Amber Alert SOPS - Dec 2021.pdf

ANNEXURE A – Public Interest Consideration Checklist

IMPORTANT

There is an overriding public interest against disclosure only when, having considered the reasons in favour of disclosure and those reasons against disclosure of government information, on balance those reasons against disclosure outweigh those in favour of disclosure.

While the Government Information Public Access Act (GIPAA) allows for unlimited factors in favour of disclosure to be considered, it only allows certain factors against disclosure to be considered.

Those factors are specified in a table within section 14 of the GIPAA. There are also some limited circumstances in which information simply cannot be released under the GIPAA. The GIPAA has identified particular classes of information for which there is a conclusive presumption against disclosure. Schedule 1 of the GIPAA lists the information for which the conclusive presumption applies. Where information falls within a class of information to which the schedule applies, it cannot be released.

GIPAA Schedule 1

IMPORTANT

Schedule 1 of the Government Information (Public Access) Act 2009 lists certain matters for which the is conclusive presumption of overriding public interest **AGAINST** disclosure. Please check the link to confirm if your policy relates to any of the following:

Does your corporate policy document (or any part thereof) relate to any of the following:

GIPAA Reference	Area	Does your policy relate?
1	Overriding secrecy laws	N
2	Cabinet information	N
3	Executive Council information	N
4	Contempt	N
5	Legal professional privilege	N
5A	Privilege generally	N
6	Excluded information	N
7	Documents affecting law enforcement and public safety	N
8	Transport safety	N
9	Adoption	N
10	Care and protection of children	N
11	Ministerial Code of Conduct	N
12	Aboriginal and environmental heritage	N
13	Information about complaints to Judicial Commission	N
14	Information about authorised transactions under Electricity Network Assets (Authorised Transactions) Act 2015	N
15	Information about authorised transaction under Land and Property Information NSW (Authorised Transaction) Act 2016	N
16	Information provided to High Risk Offenders Assessment Committee	N
-	orate policy document (or part thereof) covered under of the GIPAA?	N

GIPAA - Table 1 in Section 14

<u>Section 14 of the GIPAA</u> outlines public interest considerations against disclosure. Does your corporate policy document relate any of the following:

Clause	Sub-Section	Does your policy relate? Y/N
	prejudice collective Ministerial responsibility,	N
	prejudice Ministerial responsibility to Parliament,	N
	prejudice relations with, or the obtaining of confidential information from, another government,	N
Responsible and Effective Government	prejudice the supply to an agency of confidential information that facilitates the effective exercise of that agency's functions,	N
There is a public interest consideration against disclosure of	reveal a deliberation or consultation conducted, or an opinion, advice or recommendation given, in such a way as to prejudice a deliberative process of government or an agency,	N
information if disclosure of the information could	prejudice the effective exercise by an agency of the agency's functions,	N
reasonably be expected to	found an action against an agency for breach of confidence or otherwise result in the disclosure of information provided to an agency in confidence,	N
	prejudice the conduct, effectiveness or integrity of any audit, test, investigation, or review conducted by or on behalf of an agency by revealing its purpose, conduct or results (whether or not commenced and whether or not completed).	N
Law Enforcement and Security	reveal or tend to reveal the identity of an informant or prejudice the future supply of information from an informant,	N
There is a public interest consideration against disclosure of information if disclosure of the information could reasonably be expected to	prejudice the prevention, detection or investigation of a contravention or possible contravention of the law or prejudice the enforcement of the law,	N
	increase the likelihood of, or prejudice the prevention of, preparedness against, response to, or recovery from, a public emergency (including any natural disaster, major accident, civil disturbance, or act of terrorism),	N
	endanger, or prejudice any system or procedure for protecting, the life, health, or safety of any person,	N

Clause	Sub-Section	Does your policy relate? Y/N
Law Enforcement and Security There is a public interest consideration against disclosure of information if	endanger the security of, or prejudice any system or procedure for protecting, any place, property, or vehicle,	N
	facilitate the commission of a criminal act (including a terrorist act within the meaning of the <i>Terrorism</i> (<i>Police Powers</i>) <i>Act 2002</i>),	N
disclosure of the information could	prejudice the supervision of, or facilitate the escape of, any person in lawful custody,	N
reasonably be expected to	prejudice the security, discipline, or good order of any correctional facility.	N
	reveal an individual's personal information,	N
Individual rights, judicial processes and natural justice There is a public interest consideration against disclosure of information if	contravene an information protection principle under the <i>Privacy and Personal Information Protection Act</i> 1998 or a Health Privacy Principle under the <i>Health</i> <i>Records and Information Privacy Act</i> 2002,	N
	prejudice any court proceedings by revealing matter prepared for the purposes of or in relation to current or future proceedings,	N
	prejudice the fair trial of any person, the impartial adjudication of any case or a person's right to procedural fairness,	N
disclosure of the information could	reveal false or unsubstantiated allegations about a person that are defamatory,	N
reasonably be expected to	expose a person to a risk of harm or of serious harassment or serious intimidation,	N
	in the case of the disclosure of personal information about a child—the disclosure of information that it would not be in the best interests of the child to have disclosed.	N
Business interests of agencies and other persons There is a public interest consideration against disclosure of information if disclosure of the	undermine competitive neutrality in connection with any functions of an agency in respect of which it competes with any person or otherwise place an agency at a competitive advantage or disadvantage in any market,	N
	reveal commercial-in-confidence provisions of a government contract,	N
	diminish the competitive commercial value of any information to any person,	N

Clause	Sub-Section	Does your policy relate? Y/N
information could reasonably be	prejudice any person's legitimate business, commercial, professional, or financial interests,	N
expected to—	prejudice the conduct, effectiveness, or integrity of any research by revealing its purpose, conduct or results (whether or not commenced and whether or not completed).	N
	endanger, or prejudice any system or procedure for protecting, the environment,	N
Environment, culture, economy, and general matters	prejudice the conservation of any place or object of natural, cultural or heritage value, or reveal any information relating to Aboriginal or Torres Strait Islander traditional knowledge,	N
There is a public interest consideration against disclosure of information if disclosure of the information could reasonably be expected to	endanger, or prejudice any system or procedure for protecting, the life, health or safety of any animal or other living thing, or threaten the existence of any species,	N
	damage, or prejudice the ability of the Government or an agency to manage, the economy,	N
	expose any person to an unfair advantage or disadvantage because of the premature disclosure of information concerning any proposed action or inaction of the Government or an agency.	N
Secrecy provisions	There is a public interest consideration against disclosure of information if disclosure of the information by any person could (disregarding the operation of this Act) reasonably be expected to constitute a contravention of a provision of any other Act or statutory rule (of this or another State or of the Commonwealth) that prohibits the disclosure of information, whether the prohibition is subject to specified qualifications or exceptions.	N
	The public interest consideration under this clause extends to consideration of the policy that underlies the prohibition against disclosure.	N

Clause	Sub-Section	Does your policy relate? Y/N
Exempt documents under interstate Freedom of Information legislation	There is a public interest consideration against disclosure of information communicated to the Government of New South Wales by the Government of the Commonwealth or of another State if notice has been received from that Government that the information is exempt matter within the meaning of a corresponding law of the Commonwealth or that other State.	N
	The public interest consideration under this clause extends to consideration of the policy that underlies the exemption.	N
	In this clause, a reference to a corresponding law is a reference to - (a) the <i>Freedom of Information Act 1982</i> of the Commonwealth, or (b) a law of any other State that is prescribed by the regulations as a corresponding law for the purposes of this clause.	N

If your corporate policy document (or any part thereof) relates to any matters listed in Section 14 of the GIPAA, you must consider whether those considerations outweigh the public interest in allowing the community to have access to the information (see section 12 of the GIPAA). Please provide your decision and reasons below. Note: to the extent that only part of the document relates, please indicate which part:

SEE FACT SHEET: WHAT IS THE PUBLIC INTEREST TEST?

Should the corporate policy document (or part thereof) be withheld based on there being an overriding public interest against disclosure?	N	

Nil

Endnote References

¹ Key Operational Change references: In August 2023 the CET met and agreed that corporate policy documents must include Document Modification References whenever there is a *key operational change* to the document. D/2023/788992