

# Threat to Life Warnings

Standard Operating Procedure

This SOP provides clear direction and procedural instruction to provide a consistency of response in accordance with force policy, however it is recognised that policing is a dynamic profession and the standard response may not be appropriate in every circumstance. In every situation, your decisions and actions should be supported by the National Decision Model and based on the values and ethics of Police Scotland. You may be expected to provide a clear and reasonable rationale for any decision or action which you take.

## Notice:

This document has been made available through the Police Service of Scotland Freedom of Information Publication Scheme. It should not be utilised as guidance or instruction by any police officer or employee as it may have been redacted due to legal exemptions

Owning Department: Specialist Crime Division

Version Number: 5.0

Date Published: 06/02/2023

Contents

[Threat to Life Warnings 1](#_Toc141426487)

[Notice: 1](#_Toc141426488)

[1. Introduction/purpose 4](#_Toc141426489)

[2. Aims and objectives 5](#_Toc141426490)

[3. Scope 5](#_Toc141426491)

[4. Responsibilities 8](#_Toc141426492)

[Initial owners of threat (police officer or police staff) 8](#_Toc141426493)

[Detective Inspector 9](#_Toc141426494)

[5. Time-critical intelligence 10](#_Toc141426495)

[6. Detective Superintendent 10](#_Toc141426496)

[7. Senior Investigating Officer / enquiry team 12](#_Toc141426497)

[PNC examples 14](#_Toc141426498)

[8. Review process 15](#_Toc141426499)

[9. Threat to life – force/divisional ownership 16](#_Toc141426500)

[10. Command protocols 17](#_Toc141426501)

[11. Nature and sensitivity of intelligence sources 18](#_Toc141426502)

[12. Threat level and response 19](#_Toc141426503)

[Low – no real threat and/or immediate risk 19](#_Toc141426504)

[Medium – Threat considered conditional 19](#_Toc141426505)

[High – real and immediate threat to life, risk of personal injury or indication of commission of a serious crime 19](#_Toc141426506)

[13. Resolution – proactive/disruptive responses 20](#_Toc141426507)

[Resolution of low risk threats 20](#_Toc141426508)

[Resolution of medium risk threats and high risk threats 21](#_Toc141426509)

[Proactive response 21](#_Toc141426510)

[Disruptive response 21](#_Toc141426511)

[Investigative response 22](#_Toc141426512)

[Option to issue warning notice - threat to life warning notice/ personal safety advice warning notice 22](#_Toc141426513)

[Option to issue disruption notice - threat to life disruption notice/ crime disruption notice 23](#_Toc141426514)

[Disruptive strategy 24](#_Toc141426515)

[14. Considerations for Scottish Prison Service 25](#_Toc141426516)

[15. Threat to life – Process Summary 26](#_Toc141426517)

[16. Tactical Options for Disruption and/or Prevention 28](#_Toc141426518)

[17. Key contacts 28](#_Toc141426519)

[Compliance record 29](#_Toc141426520)

[Version control table 29](#_Toc141426521)

[Feedback 30](#_Toc141426522)

## Introduction/purpose

This Standard Operating Procedure (SOP) supports the following Police Service of Scotland (hereafter referred to as Police Scotland) Policies:

* Intelligence Policy
* Crime Investigation Policy
* Serious and Organised Crime Policy
* Data Protection Policy

This SOP provides guidance on courses of action to be considered when information, from whatever source, comes to the notice of the police that there is a specific ‘Threat to Life’ (TTL), risk to personal safety or indication of the commission of a serious crime to an individual (whether that person has been identified or not).

Instruction and guidance includes investigative points to consider, protection of intelligence sources, preparation and issue of TTL warning and/or TTL disruption notices, preparation and issue of personal safety advice notices and crime disruption notices.

Consideration and issue of crime disruption notices, TTL warning and/or TTL disruption notices or personal safety advice notices does not absolve responsibility to conduct all reasonable lines of enquiry where specific threat exists. Adherence to this SOP should provide police officers with consistency and robustness in their decision-making and encourage a positive approach to managing risks when making a decision based on an intelligence assessment.

Maintaining or achieving the safety and well-being of individuals and communities is a primary consideration in decision-making. Circumstances must be reviewed and monitored at all stages, with a view to ensuring that any changes to the nature of a threat are properly assessed and managed, and that any issues surrounding the protection of an intended victim are met.

Importantly, it has been learned from previous experience that clarity of the threat, communication across police structures and managerial ownership of the risk until this has been mitigated are essential to respond coherently, consistently and professionally to a TTL.

## Aims and objectives

The primary objectives of this SOP are to:

* Preserve the lives of all assessed as immediately involved;
* Ensure public safety;
* Maintain the safety of those involved in attempting to mitigate the risks;
* Assess the risk of exposing intelligence sources against the risk of harm to the victim;
* Provide a generic process for dealing with such incidents; and
* Where crimes and offences have or are being committed, ensure that investigative opportunities are fully exploited.

This SOP seeks to provide a standardised and structured framework upon which to record, assess, manage and make a decision, take appropriate action and resolve matters that constitute a risk to personal safety, crime disruption or TTL within the meaning of these phrases as provided in this document.

Some threats may be made which are explicitly to cause serious injury but which may prove fatal (e.g. threat to shoot someone in the legs, threats towards a child or the escalation of minimal threats) and in such cases it may be appropriate to follow this guidance.

Allegations where specific threats to kill are made, are classed as crimes. Where there is a sufficiency of evidence to support the arrest of the identified potential perpetrator(s), then deployment of that as a tactic, which would also preserve life, is in accordance with this document. Otherwise this document provides guidance on tactics, and procedure, for those instances where the arrest of the perpetrators is not available immediately as an option to deploy where, accordingly, alternatives must be considered.

## Scope

The procedures to be followed in this SOP determine ownership and accountability and place a responsibility on officers to take reasonable steps to protect the lives of:

* Persons subject to such risks; and Third parties whose proximity to those persons means that it would be reasonable to believe that they too may suffer as a result of those risks.

The right to life is enshrined in Article 2 of the European Convention on Human Rights (ECHR) and is a right which is enforceable in the United Kingdom (UK) in terms of the Human Rights Act 1998. There is an obligation on the Police Service and Law Enforcement Agencies (LEAs) to take all reasonable steps to protect the lives of people where there is a ‘real and immediate’ risk to them from the criminal acts of another.

Case law, most notably Osman v UK (1998), provides that where the police knew, or ought to have known at the time, of the existence of a real and immediate risk to the life of an identified individual or individuals from the criminal acts of third parties, they are under a duty to take reasonable measures to avoid that risk.

Responsibility is placed on officers to consider all relevant information and whether or not it is reasonable to conclude that a real and immediate threat to the life/risk to personal safety of an individual or indication of commission of a serious crime exists, and consequently to take appropriate action.

The definition of ‘real and immediate’ threat has been interpreted liberally. For the purposes of this document the phrase has two aspects:

* Real: the risk has been reasonably assessed to be credible, and that the potential assailant has the intention and the ability to carry out the threat.
* Immediate: the risk should have the character of ‘immediacy’ – being ‘right now’ or ‘very soon’.

The actual meaning of a ‘real and immediate TTL’ is assessed as being a viable ‘threat to life’.

* The definition of ‘real’ is ‘objectively verifiable’.
* The definition of ‘immediate’ is ‘present and continuing’.

The information and intelligence around a TTL can be summarised under the following category in order to consider tactical options:

* Threat to life: When an intelligence assessment concludes that a specific real and immediate threat to life of an identifiable victim and/or by an identifiable perpetrator exists. This includes threats that are dependent on some enabling factor.

The tactical options under this category can involve a TTL warning notice and or a TTL disruption notice.

Each case must be managed using tactics designed to protect the life of those at risk or third parties whose proximity to those persons means that it would be reasonable to believe that they too may suffer as a result of those risks. It is essential to consider the credibility and immediacy of the threat and to take action to diminish or remove the threat.

There is a need for consideration and assessment of the impact of such a threat on individuals (which could be a child) and those associated to persons(s) receiving the TTL including partners, children, family members and the wider community. This is required to ensure that any vulnerable adult or child is safeguarded. For the purposes of the TTL risk assessment, a child is considered to be any persons under the age of 18 years old as outlined within Section 93 (2)(B) Children (Scotland) Act 1995. To ensure the safety of all, there is a need for a multi-agency response to ensure that all partners contribute to the risk assessment, enabling a robust safeguarding plan, ensuring that any action and vulnerability identified is recorded on the Vulnerable Persons Database (iVPD).

At every stage of the process, officers will be required to consider the threat to be ‘real and immediate’ until it is established that it is not.

A TTL warning notice should not be administered to a potential victim if the threat is not assessed as being a ‘real and immediate’ TTL. If the intelligence provides that there is a risk of personal injury to a potential victim, that person should be issued with a personal safety advice warning notice.

Action is required to be taken to mitigate the risk in respect of intelligence received indicating the real and immediate commission of a serious crime, for example a proposed robbery that requires some form of disruption work, and/or a warning to fully identified perpetrators, if known. In this instance, the type of warning to be considered is a crime disruption notice.

* Crime disruption notice: A notice served to an identified individual whereby it has been assessed that there is a real and immediate suggestion that the individual is going to be involved in the commission of a serious crime and there in no available evidence to initiate an investigation.

## Responsibilities

### Initial owners of threat (police officer or police staff)

The initial report of a threat may be received in a number of ways, but it will inevitably fall into one of two categories, either:

* A threat coming to the attention of Police Scotland or other Law Enforcement Agency (LEA) that operates in Scotland, through an evidential or investigative process; or
* A threat coming to the attention of Police Scotland or other LEA from an intelligence source(s), either anonymous or evaluated.

On receiving information that notifies Police Scotland of a threat to life, risk of personal injury or commission of a serious crime, the police officer or police staff must take immediate and reasonable action to obtain all available details regarding that threat. In doing so they become the initial owner of that threat.

Details obtained should include, but are not limited to:

* Suspect(s) details;
* Victim(s) details;
* Reporter(s) details;
* Time of report of the TTL;
* Timescale of the TTL;
* Locus;
* Method and
* Motive.

At this point all necessary steps to seize, obtain or preserve any evidence relating to the threat should be considered and, where possible, undertaken.

An officer of at least Detective Inspector rank must be informed without delay. Out with normal business hours, the on-call Divisional DI should be informed.

### Detective Inspector

On receipt of the information that initially indicates a real and immediate threat to Life, risk to personal safety or commission of a serious crime, the Detective Inspector (DI), (or Detective Chief Inspector (DCI) or Detective Superintendent (DSU) in their absence) takes ownership of the threat.

Consideration should be given at this stage to contacting the on call senior intelligence officer within SCD for any clarity required around assessment of intelligence.

In the case of TTL, the DI (or when applicable DCI or DSU) must instruct the completion of Section 1 of the Threat Risk Assessment Document, Form 139-007 (TRAD) by the National Intelligence Bureau (NIB 24/7), ensuring that source protection is considered. The NIB will ensure that the DI is fully sighted on all relevant intelligence.

In the case of the indication of the commission of a serious crime or indication of risk of personal injury, the DI must instruct the completion of Section 1 of the TRAD by a suitably trained intelligence officer, with consultation with the NIB to ensure that they are fully sighted on all relevant intelligence and source protection is considered.

The information contained within the initial report which highlighted the threat must be committed to Scottish Intelligence Database (SID) utilising the appropriate grading and ‘THREATS’ header. This intelligence log must be updated in the ‘Action Taken’ field with the outcome of the TRAD process.

Following completion of Section 1 of the TRAD, the DI will provide their assessment whether there is a real and immediate threat to Life, risk of personal injury or indication of the commission of a serious crime, recording the decision making process within Section 2 of the TRAD document.

The threat(s) will then be graded by the DI as:

* Low – no real and/or immediate threat identified (including a threat where the victim and/or suspect are identifiable but the assessment is that the threat is not adjudged credible );
* Medium – the threat is conditional upon another factor/s; or
* High – the victim, suspect and/or location are identifiable and the threat is assessed as real and immediate.

Previous indicators of violence, other known threats and connectivity to serious organised crime are significant considerations at this initial phase.

The assessing DI must outline their assessment and rationale. The time and date of the assessment and subsequent actions should be noted within the TRAD.

This information must be presented to a DSU or on-call DSU without delay, for agreement and subsequent authorisation. If attempts to identify a DSU have been exhausted then a nominated deputy of no less than the rank of DCI must be informed. The policy decision to nominate the DCI must be recorded within the TRAD.

## Time-critical intelligence

Where a delay in acting on the information and/or intelligence may increase the risk of death or serious injury to any person, this process may be carried out verbally and later recorded within the TRAD document, recording decision making and rationale behind the time critical nature.

## Detective Superintendent

Once briefed by the DI, the DSU assumes ownership of the threat and will review the assessment and rationale, allowing them to determine if there is a real and immediate threat to Life, risk to personal safety or indication of commission of a serious crime. Tactics for disruption and/or prevention will be considered and threat mitigation decisions made. These may include overt means of disruption and prevention.

Based on the information contained in the TRAD, the DSU will ensure that the recommended actions proposed are appropriate and add any subsequent actions deemed necessary to mitigate the threat, risk and harm posed.

The decision as to what operational response is to be undertaken should be based on the following factors:

* The stated and/or assessed intention of the perpetrator(s)
* The stated and/or assessed capability of the perpetrator(s)
* The likelihood that the perpetrator/s will act; and
* Risk and impact of failure by the police to take action.

TTL Warning Notice Form 139-004, [TTL Disruption Notice Form 139-005](https://spi.spnet.local/policescotland/guidance/Force%20Forms/Police-Scotland/Threat%20to%20Life%20Disruption%20Notice.docx) and/or Crime Disruption / Personal Safety Advice Warning Notice Form 139-008 must also be considered at this stage. Where the threat has been assessed as being real and immediate, warnings must be given unless there are reasonable grounds not to do so.

The DSU will document their overall decision and rationale including authorisation of the working strategy and tactical options proposed within Section 3 of the TRAD document.

If it is assessed by the DSU that there is a low threat and no real and immediate threat to Life, risk to personal safety or indication of the commission of a serious crime, Section 3 (Threat Closure) of the TRAD must be completed.

If the DSU assesses that there is a medium or high threat and a real and immediate threat to Life, risk to personal safety or commission of a serious crime, they will appoint a Senior Investigating Officer (SIO) of DI rank or above, to implement the actions, including the issuing of any notices (where appropriate, it is recommended that the SIO is the original assessing DI for first-hand knowledge and continuity).

In the case where the on-call DSU has taken responsibility, the Divisional DSU with investigative responsibility will assume ownership from the on-call DSU as soon as reasonably practical.

## Senior Investigating Officer / enquiry team

A Senior Investigating Officer (SIO) of the rank of DI or above is then responsible for setting and then oversight of the delivery of the tactical options. Any associated criminal investigation will also be directed by the same SIO.

Among the tactical options available to resolve a threat are:

* A proactive response;
* A disruptive response;
* An option to warn the intended victim and/or perpetrator; or
* The pursuit of investigative opportunities where crimes or offences have been committed.

Following authorisation by the DSU to serve any notice, the SIO must contact NIB who will allocate a unique reference number (URN) which must be added to the Action Taken field on the initial intelligence log(s) and cross referred on all subsequent intelligence logs relative to each threat entry.

While the SIO features significantly in relation to directing the investigation and warnings, ownership and responsibility for implementing control measures to minimise the threat, remains with the relevant DSU.

The SIO must arrange for the control room to be informed and a STORM incident raised for each notice to be issued (there can be multiple incidents created dependent on the number of nominals and locations). Incidents will remain open during the initial critical period but will not remain open indefinitely. When an incident is closed the owning division and SIO will be informed.

Policy decisions made by the DSU with ownership, after consultation with the SIO, and/or other departments must be recorded within the TRAD.

In addition to each incident raised, a SID log outlining the notice being served and any subsequent response must be submitted, one SID log must be raised per notice issued using the following headers:

* TTL warning notice - header- ‘THREATS-TTLW’
* TTL disruption notice - header - ‘THREATS-TTLD’
* personal safety advice notice – header – ‘THREATS – PSA’
* Crime disruption notice – header – ‘THREATS – CDN’

Any notice served must be filled out by the officers serving the notice. Their details must be clearly printed and their signature added as police witnesses, with the time and date of service noted.

Where possible, the police witnesses must read out the relevant notice to ensure that it is understood by the recipient. Consideration should be given to utilising an interpreting service or appropriate adult if necessary.

* The intended recipient of the notice must be requested to sign the notice. If the recipient refuses, this must be recorded on the notice by the police witnesses.
* The intended recipient must not be provided with a copy of the notice under any circumstances.
* Police witnesses issuing the delivery of the notice should record it within their police notebooks, including any response from the recipient.
* Once served, the police witnesses should thereafter return the notice to the DSU who has the responsibility to review, sign and return the notice.

The NIB will act as the central register for all threat to Life documentation including TRAD and subsequent notices served.

In the case of the indication of the commission of a serious crime, or risk of personal injury the original notice and completed TRAD must be retained at the relevant division with ownership.

The completed TRAD document mustalsobe forwarded to the NIB mailbox:

**‘Information has been removed due to its content being exempt in terms of the Freedom of Information (Scotland) Act 2002‘**

**Exempted Section 30 (c) - Prejudice to the Effective Conduct of Public Affairs.**

The completed TRAD must be converted into PDF format and attached within SID to the intelligence log highlighting the initial threat. In addition, any subsequent notices issued must be scanned and attached within SID to the intelligence log relating to the issue of the notice.

The presence of a TTL warning must be recorded on Police National Computer (PNC) using an appropriately worded ‘information’ entry under the following categories:

* The subject has or is to be served with a TTL warning and or TTL disruption notice.
* The person is the subject of a TTL enquiry, enquiries now concluded, no requirement for TTL warning and or TTL disruption notice.

As the threat to life scenario progresses at each review, the content of the PNC locate information must also be reviewed.

### PNC examples

Subject of a “Threat to Life” warning/disruption notice:



Subject of a “Threat to Life” enquiry:



## Review process

In all cases where there is deemed to be a real and immediate threat to Life, risk of personal injury or indication of the commission of a serious crime, a review must be carried out by a Detective Inspector and authorised by the DSU owning the risk as follows:

Consideration must be given for the review to be carried out by the original SIO or Divisional Intelligence Manager.

Initial review to be made within 48 hours after receipt by the DSU, or as soon as is reasonably practicable.

* Intelligence updates and threat assessments should be monitored accordingly.
* Record the decision making process.
* Consider the re-assessed risk factor to determine if the response is still appropriate.

Subsequent reviews of the threat must be made no more than 7 days apart, and every 7 days thereafter until it is deemed no longer a real and immediate threat.

In the instance whereby the recipient of a notice is overseas and all reasonable efforts have been made to serve said notice, consideration may be given to archiving the TRAD subject to the notice being served.

The DI must ensure that any review is recorded in Section 4 of the TRAD documenting any decision making and assessment based on new information or intelligence updates.

The DI must brief the DSU at each stage of the review. The DSU will review the assessment and authorise any subsequent action.

If it is assessed by the DI during the review process that there is no longer a real and immediate threat, Section 4.2 of the TRAD (Threat Closure) must be updated and authorised by the DSU. The NIB must be notified to ensure that the National TTL Register is updated.

## Threat to life – force/divisional ownership

Ownership of a threat to Life, risk of personal injury or crime disruption and the implementation of the tactics to mitigate the threat lies directly with the Division where the potential victim resides unless the victim cannot be identified. In such circumstances, ownership moves to the Division where the perpetrator resides. In the absence of this information, ownership falls to the Division where it is indicated that the threat or act will take place.

Where the DI or DSU owning the risk has taken the responsibility whilst on call, they will brief the Divisional DSU as soon as reasonably practical and in doing so will transfer the ownership to them.

If the threat to Life emerges from or impacts on an ongoing Force Operation or Major Enquiry, early discussion should be considered between the operational or enquiry DSU and Divisional DSU to ascertain ownership and responsibilities if appropriate.

If a potential victim is residing in another force area out with Scotland (including overseas), immediate notification of this must be undertaken. Ownership will thereafter transfer to the force in which the potential victim is residing. It is the responsibility of the DSU to notify the relevant force area. This process should be done in conjunction with the NIB to ensure the recording of the threat and the dissemination of all relevant information and intelligence. Consideration should be given to the creation of a STORM incident outlining the details of the notification and transfer of ownership.

## Command protocols

Where there is an interdisciplinary element or even a multi-agency element to an operation, then command protocols can assist in clarifying areas of responsibility and command function, channels of communication and primacy of command at various stages of the investigation.

That said, the DSU who owns the threat will remain as the officer who is accountable for ‘gold’ responsibilities and will ultimately be responsible for the strategic response to ‘real and immediate’ threats. A ‘gold’ commander may hold a strategic coordinating meeting with all the stakeholders involved in the enquiry.

If proportionate to the threat, and when activated, a command protocol can assist in identifying:

* The desired outcome of the investigation;
* Who is responsible for achieving each of the tasks allocated;
* Who is responsible for minimising each risk identified;
* Who controls each of the resources;
* Who commands each separate geographic area (particularly important where multiple divisions within a force are involved);
* Procedures for the transfer of command (if necessary), how communicated and recorded; and
* How each of the functions will operate during the planning, operational and post deployment stages of the investigation.

To ensure consistency of approach when dealing with a TTL scenario, the DSU will be accountable for both ‘silver’ and ‘gold’ responsibilities - assessing the extent of a TTL and ensuring that an appropriate tactical plan is formulated to minimise or eliminate risk.

The SIO will be accountable for ‘bronze’ responsibilities - the implementation of the tactical plan to minimise or negate the threat and to apprehend any suspect.

## Nature and sensitivity of intelligence sources

All references to relevant intelligence in this SOP will mean information that is made known to the police and assessed as sufficiently reliable to indicate immediately the occurrence of conduct that may jeopardise life, or that may result in serious injury to a person or persons.

Some of the persons under threat (or those posing the threat) will be involved in serious and organised crime or other criminal activity. Some may be aware that a threat exists against them. A duty of care to take reasonable steps to protect such persons is not lessened by their involvement in serious crime. The police must be cognisant that warning such persons of a threat to their life may, in itself, heighten tensions, provoke repercussions or expose intelligence sources. Consequently, a balance has to be struck and maintained when determining what disruptive or proactive action, if any, should be taken.

Where it is decided that intelligence should not be disclosed and no specific action is to be taken, other specific disruption action needs to be taken to protect the potential victim of the threat. The decision and the rationale underpinning it will be documented by the SIO, in conjunction with the relevant DSU.

It should be noted therefore, that on all occasions, preservation of the life of the person subject to the threat which is deemed to be ‘real and immediate’ must take precedence over the protection of the sensitive intelligence/source protection issues.

Intelligence may suggest use of firearms or other weapons and therefore, officers being tasked to take action on that intelligence must be made aware of the risks. In such circumstances, to allow appropriate risk and impact assessments to be conducted a Firearms Silver Commander will be appointed in addition to the incident Silver Commander, and officers will be made fully aware of the specific risk(s) and associated intelligence.

Where delay in acting on intelligence may increase the risk of death or serious injury to any person, information or intelligence will be disseminated immediately (un-assessed if necessary).

## Threat level and response

### Low – no real threat and/or immediate risk

When a TRAD concludes that there is no real or immediate threat or risk, the threat can be regarded as low and the DSU with ownership will record the fact that the threat is not considered real and/or as immediate. However, the threat must continue to be monitored and any additional intelligence or information used to reassess the threat level.

### Medium – Threat considered conditional

A medium threat is a threat that is conditional (i.e. it is dependent on some enabling factor that is not currently satisfied), or one where the perpetrator does not have the current ability or opportunity to carry it out, and there is no real immediate threat to an identifiable victim, or by an identifiable perpetrator, or at an identifiable location. A medium threat can escalate rapidly if any of the prevailing circumstances change.

When considering therefore, whether a threat is medium risk, all material factors must be considered; for example, the nature of the threat and the capability of those thought to be involved in carrying out the alleged threat. At all times, the police response must be proportionate and engage any known or suspected time scales. Additionally, the potential perpetrator’s opportunity must be examined, for example, is either party within a police/prison establishment?

### High – real and immediate threat to life, risk of personal injury or indication of commission of a serious crime

A high threat, assessed as being specific, is a real immediate threat to an identifiable victim, or by an identifiable perpetrator, or at an identifiable location. It may be conditional. If neither victim nor perpetrator can be identified, then the threat should be termed non-specific and responded to accordingly.

## Resolution – proactive/disruptive responses

Threats that have been assessed as low risk or medium risk fall short of the definition of threat To Life in its truest form (where there is a real and immediate threat to life); however it is useful to consider the responses to these threats alongside the response to high risk TTLs as there are some similar and some common practices for dealing with all levels of threat.

For clarity, initial reports that have subsequently been assessed as a low risk threat or medium risk threat cease to be classified as a ‘Threat to Life’ (TTL) at the point the assessment has been completed. These threats should be dealt with as per the instructions below and reviewed as appropriate in consideration of any change to the threat level assessment.

### Resolution of low risk threats

When an initial risk assessment concludes that there is no real or immediate threat or risk, the threat can be regarded as low and the DSU will record the fact that the threat is not considered real and/or as immediate. However, the threat must continue to be monitored and any additional intelligence or information used to reassess the threat level

Should it become apparent that a person is being repeatedly subjected to low level threats, there may be a need to initiate action to counter possible harassment or underlying domestic incidents.

The DSU will ensure that the person making the intelligence entry onto SID conducts a search to establish if previous incidents have been recorded on ViSOR or the Vulnerable Persons Database (or equivalent). There is nothing to prevent the officer dealing, or any other officer involved with the repeated minimal threats, to escalate the threat to medium if they feel that the number of such threats is likely to impact on the risk to the victim or community.

### Resolution of medium risk threats and high risk threats

It is recommended that the police response to resolve a medium threat or high risk threat is for the DSU to appoint an appropriate SIO to take charge of the incident. An appropriate ACC should be notified if the planned response to a high risk threat incident involves the use of a Tactical Firearms Advisor (TFA), as from the evaluation of all available information it is assessed that the use of firearms could be involved in the threat.

Primary concerns are the safety of the intended victim of the threat and the safety of the community and police officers. It will be the responsibility of the senior officer dealing with the threat to ensure that all immediate steps have been taken to minimise the risk. A menu of tactical options to assist in determining the measures is provided in Section 16.

This is not a definitive list. Tactics for each threat to life situation must be considered on a case-by-case basis.

The safety and integrity of intelligence sources is also of major importance and extensive consultation should take place with the source of the intelligence in all high and medium threat cases where a warning is to be given to the victim or perpetrator of the threat, or where any overt disruptive action is intended.

### Proactive response

**‘Information has been removed due to its content being exempt in terms of the Freedom of Information (Scotland) Act 2002‘**

**Exempt under Section 35 (1) (a) & (b) – Law Enforcement and Section 39 (1) – Health, safety and the environment**

### Disruptive response

A disruptive response is designed to prevent the intended/potential attack from occurring. Options for disruptive tactics are found within Section 16 – Tactical Options.

They are not exhaustive and in some circumstances may have little or no impact and as such, consideration should be given to contingencies in such events.

Where a disruption is planned, the SIO must take into account any collateral risks to the community or police officers, as well as considering the safety of the identified victim. It is recommended that a separate risk assessment is carried out for this disruption operation by the SIO.

The DSU and SIO will be responsible for obtaining appropriate advice and guidance from specialists when planning to disrupt a TTL which has been assessed as being either medium or high. Such specialists may include Tactical Firearms Advisors, local patrol / community officers or Roads Policing officers.

### Investigative response

Occasionally, intelligence that is received in respect of threats of violence or of an individual’s intention to become involved in criminality will provide the SIO with investigative opportunities. It is essential that where these opportunities exist that they are prioritised and pursued and that every line of enquiry is exploited with a view to establishing a sufficiency of evidence that would lead to arrest and prosecution. Such crimes may include conspiracy offences. It is of course essential that source protection issues are fully considered where an investigative response is followed.

### Option to issue warning notice - threat to life warning notice/ personal safety advice warning notice

A warning to an identified victim may be issued when the officer in charge of the threat, believes that the identified victim should be made aware of the threat/risk against them. This warning process is known as the service of a TTL Warning Notice Form 139-004. The purpose of a warning notice is to notify the potential victim of the existence of a threat or risk towards them and to allow the potential victim to take precautionary steps to protect themselves, or to allow the victim an opportunity to consider the protective measures proposed by the police.

The TTL warning notice is to be issued where the threat is considered as being ‘real’ and ‘immediate’. A Personal Safety Advice Warning Notice Form 139-008 is to be issued where there is intelligence to suggest that the individual’s personal safety is at risk, but the threat is ‘real’ and ‘immediate’, but may involve some form of lesser violence.

* Note: If a victim has been subject to a previous or number of TTL warning notices or personal safety advice warning notices and/or it is assessed from all available information that the victim is aware of the threat against him/her, each scenario has to be assessed on a case by case basis and it is for the DSU to decide whether a further TTL warning notice or personal safety advice warning notice has to be issued. The TRAD and associated SID log needs to be updated with the decision process accordingly.

### Option to issue disruption notice - threat to life disruption notice/ crime disruption notice

The TTL Disruption Notice Form 139-005 is to be issued where there is intelligence which indicates that an individual (perpetrator) is going to be involved in causing serious harm to another individual (victim) and it is assessed that the threat is ‘real’ and ‘immediate’.

A Crime Disruption Notice Form 139-008 is to be issued where there is specific intelligence to suggest that individual/s are going to be involved in the commission of a serious crime and there is no available evidence to initiate an investigation.

A warning to the perpetrator may be issued when the DSU believes that the perpetrator should be made aware that the existence of the threat/risk posed by them is known.

A warning to the perpetrator is not intended to allow him/her to identify intelligence sources but remains a tactical option to consider, particularly when the identity of the potential victim or location is unknown or is unclear.

As a general rule, when the life of a person is considered to be in a real and immediate danger from the criminal actions of another, the Police should warn the intended victim of the threat. The issue of such a warning should never be regarded as the only option and the following should be considered when deciding whether or not warnings are to be issued:

* Is it likely that the warning may result in violence against another person?
* Is it likely that the warning may reveal the existence or nature of an intelligence source? If yes, is it likely that the harm caused by the revelation will be serious?
* Is this the first occasion a warning has been given or is it in a series?
* Is this a strategic attempt by either party to try and identify the intelligence source?
* Is it likely that the warning may exacerbate existing violence?
* The service of a warning may not be effective, if so, what contingencies are in place?
* Is the victim the source of the intelligence?

If the DSU decides not to warn an intended victim or the perpetrator, the rationale for doing so must be documented in the TRAD and, if the matter is assessed as being a threat involving the use of firearms, the Chief Officer having oversight must be consulted and must endorse the decision. If a warning is not issued, the Chief Officer, in consultation with the DSU must detail any alternative strategy to minimise the threat. Such measures may include a proactive investigation of the intended victim or perpetrator, or covert protective measures.

Unless circumstances alter and immediate action is required, the SIO should await the outcome of the issue of the warning and/or disruption prior to continuing with any other action, such as a disruptive strategy, therefore it must be ensured that officers tasked to deliver a warning and/or disruption are fully briefed.

Where it is assessed that the threat resulting from the TTL incident may present a risk to staff from partner agencies then consideration should be given to notifying that agency, e.g. where there may be a threat involving fire raising the Scottish Fire and Rescue Service (SFRS) can be contacted for advice and covert options including an enhanced response by fire service, without the intelligence being more widely disseminated.

### Disruptive strategy

An ‘occurrence’ marker should be created on STORM for the information of officers who may be asked to attend further calls, related or not, at any specified location.

In the event that the notice could not be served, the SIO must consider other tactics to disrupt the situation, either in terms of the perpetrator, or of the intended victim, or the locus.

It is imperative that a TTL must not be left unresolved and the SIO must devise a tactical strategy that meets the needs of both the intended victim, as well as the local community.

## Considerations for Scottish Prison Service

If the intended victim or perpetrator is in custody within a Scottish Prison Service establishment (SPS) this SOP remains applicable. The relevant intelligence should be disseminated to the Prison Public Protection Unit and the relevant Prisons Intelligence Management Unit. Thereafter consultation between both organisations should seek to mitigate any immediate risk. Arrangements can then be made to issue the TTL warning notice/TTL disruption notice /personal safety advice warning notice /crime disruption notice.

Police generated intelligence should therefore be dealt with as per the SOP – the fact persons named are within a prison is irrelevant on most/if not all occasions. The issuing of TTL warning notice/TTL disruption notice / personal safety advice warning notice / crime disruption notice should be progressed by Police Scotland as would have been the case if the victim/perpetrator were out in the community.

During office/prison operational hours in circumstances where Police Scotland require to assess the risks to the source, for example prison sourced intelligence i.e. should any action be taken against the person(s) posing the risks to others, or persons at risk of harm - SCD Prison Intelligence Unit should be contacted and will act as the conduit with the relevant Prison or SPS Public Protection Unit.

The following enquiries will be made of the SPS:

• Is there an opportunity for police to engage with the source (i.e. obtain witness statement)?

• Is there an opportunity to develop this intelligence?

• How does the source know this information/who else knows this/would the source or any other persons be at risk should the police take any action?

The result of these enquires will be provided to SIO/divisional contact thereafter for full police assessment.

Out with office/prison operational hours - where assessed risks are such that action needs to be progressed as a priority, then the on call DI for intelligence should be contacted and will act as a conduit to share relevant information with identified SPOCs in the relevant SPS establishment.

## Threat to life – Process Summary

1. Intelligence/information is highlighted to Police Scotland suggesting threat to life, risk to personal safety or indication of the commission of a serious crime.
2. The police officer / staff receiving the information/intelligence takes initial details and ownership of the threat (see section 4)
3. The police officer / staff must brief an officer of at least the rank of DI (see section 4)
4. DI takes ownership and instructs the completion of Section 1 of the TRAD by:
	1. the NIB in the case of a threat to life (see section 4);
	2. a suitably trained intelligence officer for crime disruption / personal safety risk ([see section 4](#_Responsibilities)).
5. DI must ensure there is consultation with the NIB to ensure sight of all relevant intelligence and ensure that the initial threat information is submitted to SID (see section 4).
6. Once completed by NIB / intelligence officer, the DI:
	1. Reviews section 1 of the TRAD;
	2. Completes section 2 of the TRAD outlining rationale and assessment of threat level ([see section 4](#_Responsibilities)).
7. DI briefs DSU on the threat.
	1. DSU take ownership of the threat (see section 6).
8. DSU reviews TRAD and completes Section 3 (SIO):
	1. Outlining rationale/decision;
	2. Assessing threat level;
	3. Authorising tactical measures to mitigate threat ([see section 6](#_Detective_Superintendent)).
9. If applicable, DSU authorises TTL warning/disruption notice, contacting NIB to obtain TTL reference number (see section 7).
10. In the case of medium to high threats, DSU appoints an SIO to ensure tactical options are implemented (see section 7).
11. DSU ensures the following have been raised for each TTL notice:
	1. STORM incident log;
	2. SID log;
	3. PNC update.
12. The original notice documentation must be returned to the DSU for review / sign-off and then scanned to produce an electronic record.
	1. For TTL notices, this must be forwarded to the NIB mailbox at

**‘Information has been removed due to its content being exempt in terms of the Freedom of Information (Scotland) Act 2002‘**

**Exempted Section 30 (c) - Prejudice to the Effective Conduct of Public Affairs.**

1. DSU continues with ownership and instigates review process (completing Section 4 of TRAD):
	1. 48 hours after receipt;
	2. Every seven days (see section 8).
2. The review process is continued until the DSU decides there is no longer a real and immediate threat.
	1. DSU completes Section 4.2 of TRAD, closing the threat (see section 8).
3. For TTL only – DSU contacts NIB to highlight closure of the TTL on the national register and forwards completed TRAD to NIB for storage (see section 8).

**‘Information has been removed due to its content being exempt in terms of the Freedom of Information (Scotland) Act 2002‘**

**Exempted Section 30 (c) - Prejudice to the Effective Conduct of Public Affairs.**

## Tactical Options for Disruption and/or Prevention

The following is not designed to be a definitive list of responses to all threats but provides possible options that may then open the way to other more imaginative ways of dealing with a particular threat.

**‘Information has been removed due to its content being exempt in terms of the Freedom of Information (Scotland) Act 2002‘**

**Both Section 35 (1) (a) & (b) – Law Enforcement relating to police tactics and Section 39 (1) – Health, safety and the environment apply to this section.**

## Key contacts

**‘Information has been removed due to its content being exempt in terms of the Freedom of Information (Scotland) Act 2002‘**

**Exempted Section 30 (c) - Prejudice to the Effective Conduct of Public Affairs.**

## Compliance record

EqHIRA completion/review date: 02/02/2023

Information Management Compliant: Yes

Health and Safety Compliant: Yes

## Version control table

| Version | History of amendments | Approval date |
| --- | --- | --- |
| 1.00 | Initial Approved Version | 27/03/2013 |
| 2.00  | Cyclical Review – Amendments to Sections 5.4, 9.6, 10.5, 10.6, 12.3.4, 13.2.1, 13.3.1, 13.6.3, 13.7.6. New paragraph added at sec 16 in relation to TTL considerations for Scottish Prison Service. Flowcharts added at Appendix H and Appendix I. | 16/12/2015 |
| 3.00 | Cyclical Review, additional comment on low and medium threats (to clarify that such assessed threats fall out with the ‘real and immediate TTL definition) and minor amendments to ensure CJ(S) Act compliance | 23/01/2018 |
| 4.00 | Updated to reflect changes in data protection legislation | 24/05/2018 |
| 5.00 | Reviewed and reformatted under the parameters of the SOP Review and accessibility requirements. Crime disruption updated. | 02/02/2023 |

## Feedback

All Police Scotland service delivery Policies, Standard Operating Procedures (SOPs) and National Guidance are subject to regular reviews. It is important that user feedback is taken into account when documents are reviewed.

If any officer / staff member wishes to provide comment, or make suggestions for improvements to this or any associated document, Force Form 066-014 should be used.