POLICE SCOTLAND
Keeping people safe
POILEAS ALBA

Threats to Life Warnings

Standard Operating Procedure

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:	4.00 (Publication Scheme)
Date Published:	25/05/2018

Compliance Record

Equality and Human Rights Impact Assessment: Date Completed / Reviewed:	16/11/2017
Information Management Compliant:	Yes
Health and Safety Compliant:	Yes
Publication Scheme 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

Contents

Appendices

1. Purpose

1.1 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

1.2 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) to an individual (whether that person has been identified or not).

1.3 Instruction and guidance include 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 Disruption Interview Notices.

1.4 Consideration and issue of TTL Warning and/or TTL Disruption Notices does not absolve responsibility to conduct all reasonable lines of enquiry where specific 'Threats to Life' exist. 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.

1.5 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.

1.6 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.

2. Aims and Objectives

2.1 The primary objectives of this SOP are to:

- Preserve the lives of all assessed as immediately involved;
- Ensure public safety;
- **Information has been removed due to its content being exempt in terms of the Freedom of Information (Scotland) Act 2002, Section 39, Health, Safety and the Environment.**
- 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.

2.2 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 TTL within the meaning of that phrase as provided in this document.

2.3 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.

2.4 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.

2.5 Key Points

2.5.1 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.

2.5.2 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 of an individual exists, and consequently to take appropriate action.

2.5.3 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.

2.5.4 Additionally, intelligence may exist without sufficient evidence to reasonably suspect criminality and therefore no arrests can be made in the meantime.

2.5.5 Following the recommended procedures in this SOP will ensure that all ‘Threats to Life’ are properly assessed and that all reasonable steps are taken to preserve life.

2.5.6 This will ensure that resources are employed where there is greatest need, and specific threats are considered and where necessary, action taken that will diminish or negate risk.

2.5.7 **Information has been removed due to its content being exempt in terms of the Freedom of Information (Scotland) Act 2002, Section 35, Law Enforcement.**

2.5.8 **Information has been removed due to its content being exempt in terms of the Freedom of Information (Scotland) Act 2002, Section 35, Law Enforcement.**

3. Introduction

3.1 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.

3.2 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.

3.3 The definition of 'real and immediate' risk to life has been interpreted liberally. For the purposes of this document the phrase has two aspects; firstly that it is a risk that has been reasonably assessed to be credible, and that the potential assailant has the intention and the ability to carry out the threat. Secondly, the risk should have the character of 'immediacy' – being 'right now' or 'very soon'.

Note: The definition of 'real' is 'objectively verifiable'. The definition of 'immediate' is 'present and continuing'.

3.4 Although each incident must be dealt with on a case-by-case basis, this document sets out guidance for all officers, determines ownership and responsibility, and places a greater onus on investigative or disruptive tactics to manage and resolve such incidents.

3.5 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.

3.6 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. To this end, 'ownership' of the threat is a key area to this SOP and one that will be discussed in more detail later on in this document.

3.7 The actual meaning of a 'real and immediate TTL' is assessed as being a viable 'threat to life'. This wording should not be used when considering, for example, action that is required to be taken to mitigate a threat in respect of intelligence received about a proposed robbery, that requires some form of disruption work, and/or a warning to the perpetrators, if known. This type of warning is to be considered as a Disruption Interview Notice and not a TTL Warning Notice.

3.8 Similarly, a TTL Warning Notice should not be administered to a potential victim if the threat is not assessed as being a 'real and immediate' risk of harm. 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.

3.9 Finally, for absolute clarity on this matter, TTL Warning Notices and Personal Safety Advice Warning Notices are only issued to potential victims who have been fully identified. TTL Disruption Notices and Disruption Interview Notices are only issued to potential perpetrators, again, when they have been fully identified. Templates of these Notices can be accessed via the hyperlinks at Appendix C.

4. Procedure – Generic Process

4.1 Receipt of a Threat to Life

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

(a) 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

(b) A threat coming to the attention of Police Scotland or other LEA from an intelligence source(s), either anonymous or evaluated.

4.1.2 While the separate categories above eventually entail different considerations, all reports of a TTL must be assessed in the same way according to this SOP.

4.1.3 In any event, dealing with a TTL will follow a logical path, although the urgency of any given situation will sometimes compress the separate stages of the process. The TTL Flowchart summarising the sequence of events for the generic process is provided at Appendix 'H'.

4.2 Action on Receipt of the Threat

4.2.1 Any officer or member of staff receiving first notification of any TTL will take immediate reasonable action as necessary to obtain all available information where possible concerning the threat, such as details of the suspect, victim, location, timescale, method etc., taking any immediate and reasonable steps to reduce the associated risk before the matter is referred to an officer of Inspecting Rank.

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

4.3 Assessment of the Threat

4.3.1 Immediate action must be taken by any police officer or member of staff receiving notification of a TTL or to cause serious injury. The first person receiving the information will initially become the owner of the threat. This person should notify an officer of Inspecting rank who, once apprised of the information, will brief the relevant Divisional Detective Superintendent (Det Supt) who then becomes the initial "owner" of the threat.

4.3.2 Intelligence checks on the Scottish Intelligence Database (SID) will be made immediately to obtain further information to assist the risk assessment process regarding the threat, with additional checks being carried out on the Police National Database (PND), Criminal History System (CHS), Police National Computer (PNC) and other local systems.

4.3.3 An intelligence based threat assessment using all available information will be undertaken at the first opportunity. The threat(s) will then be graded 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 – see section 13.3);
- Medium – the threat is conditional upon another factor/s (section 13.4); or
- High – the victim, suspect and/or location are identifiable (section 13.4) and the threat is assessed as real and immediate.

4.3.4 If the threat is assessed as being credible, an ‘incident’ should be created on Command and Control by the Duty Officer, a SID log created and the Det Supt (as determined by the relevant Division) notified. (In the absence of the Det Supt it should be the senior detective officer on duty, i.e. Detective Chief Inspector (DCI)).

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

4.3.6 Officers should always consider a threat to be real, unless compelling information exists to the contrary.

4.3.7 Where the TTL intelligence is perceived as credible and identifies a potential victim in a Force outwith Police Scotland or who is known to be someone for whom responsibility may rest with some other UK LEA, immediate notification of this threat must be undertaken and the threat and the mitigation of this is then owned and coordinated by that Force or LEA.

4.4 Decision on Response

4.4.1 The relevant Det Supt, (or DCI in the absence of the Det Supt), now owns the threat and consults as necessary. Tactics for disruption and/or prevention will be considered and threat mitigation decisions made. These may include overt means of disruption and prevention.

4.4.2 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.

4.4.3 TTL Warning Notices/Personal Safety Advice Warning Notices and/or TTL Disruption Notices/Disruption Interview Notice's 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.

4.4.4 It is also particularly important at this stage to consider the process to be used for the assessment and dissemination of time critical TTL intelligence, which often may be outwith normal office hours. Out of hours the default position should be the on call Detective Inspector (DI) for the relevant Division concerned. The on call DI should also update the on call Det Supt from Specialist Crime Division (SCD).

4.4.5 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.

4.4.6 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.

4.4.7 A combination of any or all of these options may be the most suitable according to the circumstances (see Section 13 for further information).

4.5 Action

4.5.1 The SIO will direct the agreed action, monitor the threat and refresh the intelligence picture. Any developments are notified to the appropriate Divisional Det Supt, who retains ownership and any updates are to be recorded on the Incident Log. Once all agreed action has been undertaken, the Command and Control Incident can be closed and the SID log updated accordingly. With respect to High Risk threats, the TTL central record should also be updated at the National Intelligence Bureau (NIB).

4.6 Ownership

4.6.1 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 appointed Det Supt (or DCI in the absence of the Det Supt).

5. Command Protocols

5.1 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.

5.2 That said, the Det Supt 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 to the life of a person as a result of the criminal acts of another (i.e. High Risk Threats). A 'Gold' commander may hold a strategic coordinating meeting with all the stakeholders involved in the enquiry.

5.3 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.

5.4 To ensure consistency of approach when dealing with a TTL scenario, the Det Supt 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. **Note**: If the threat emerges from an ongoing Force Operation / Major Inquiry then the SIO for that operation or inquiry, will have the responsibility for assessing the risk and the decision process as how to manage the TTL. That said, the Det Supt or DCI from the relevant Territorial Division still owns the threat and the SIO will liaise with the Det Supt or DCI accordingly. A separate flowchart has been produced to manage this process and is attached at Appendix 'I'.

5.5 The SIO will be accountable for 'Bronze' responsibilities - the implementation of the tactical plan to minimise or eliminate the TTL and to apprehend any suspect.

6. Nature and Sensitivity of Intelligence Sources

6.1 **Information has been removed due to its content being exempt in terms of the Freedom of Information (Scotland) Act 2002, Section 35, Law Enforcement.**

6.2 **Information has been removed due to its content being exempt in terms of the Freedom of Information (Scotland) Act 2002, Section 35, Law Enforcement.**

6.3 **Information has been removed due to its content being exempt in terms of the Freedom of Information (Scotland) Act 2002, Section 35, Law Enforcement.**

6.4 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.

6.5 **Information has been removed due to its content being exempt in terms of the Freedom of Information (Scotland) Act 2002, Section 35, Law Enforcement.**

6.6 **Information has been removed due to its content being exempt in terms of the Freedom of Information (Scotland) Act 2002, Section 34, Investigation by Scottish public authorities and proceedings arising out of such Investigations.**

6.7 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.

6.8 Where firearms are likely to be involved in the assessed threat and/or firearms may be deployed as part of the police tactical response then in addition to risks associated with operational officers' own safety, consideration should always be given to the dangers that may be caused to the general public.

6.9 Officers should follow the guidance contained within the Armed Policing Operations SOP in relation to firearms related incidents.

7. Intelligence from other Law Enforcement Agencies

7.1 LEAs have established protocols for dissemination of intelligence. These protocols seek to ensure that, where there is a TTL or serious injury to any person, operational officers are provided with all necessary information to ensure their own safety as well as protection of the source of the intelligence.

7.2 Such protocols will not prevent the dissemination of intelligence regarding a TTL. Operational officers should therefore act in accordance with the guidance in this SOP in the knowledge that the intelligence has been gathered according to those protocols and has been provided to coordinate a proper policing response, aimed at protecting public safety.

8. Time Critical Intelligence

8.1 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).

9. Creation of a Command and Control Incident

9.1 The principles of Command and Control are highly relevant to dealing with a TTL. An established, tested and recognisable process for responding to and managing a dynamic incident provides a platform for uniformity, consistency and visibility in regard to how TTLs are mitigated.

9.2 On receipt of TTL information being received at an Area Control Room, a command and control incident should be created and this will ensure that Police Scotland has an overview of the matter.

9.3 Creation of a Command and Control incident will ensure that the threat is properly monitored throughout the duration of the threat. Staff at the relevant Intelligence Unit of the Territorial Division, who should be involved in the assessment of the threat and who have an enhanced level of intelligence access, will research SID and other available databases and systems and update the relevant Det Supt.

9.4 The command and control incident must include policy decisions made by the officer with ownership, after consultation with the DIM, SIO, and/or other departments.

9.5 This will provide an accurate flow of information, research undertaken, decisions made and resources allocated. Where the intelligence stems from a sensitive source the command and control incident should be marked 'VIEW RATED' (RESTRICTED).

9.6 If it is established that a report is malicious or false, or a decision has been taken not to issue any TTL Notices as other action has been undertaken, i.e. proactive or disruption measures, the incident must still be fully updated, appropriate markers placed on the command and control incident and a SID log created outlining the circumstances as directed by either the Det Supt or the SIO.

10. Threat/Risk Assessment

10.1 Once the officer of Inspecting rank has been notified and briefs the Det Supt, who becomes the initial owner of the threat, the person tasked with making the initial assessment will be responsible for ensuring that this is coherent and that all available information has been taken into account.

10.2 A threat assessment must take into account all known information regarding the victim, the perpetrator and the source, including any new intelligence or information received after the initial report.

10.3 **Information has been removed due to its content being exempt in terms of the Freedom of Information (Scotland) Act 2002, Section 35, Law Enforcement.**

10.4 The risk to the local community, or police officers that may come into contact with a known perpetrator on unrelated operational matters, must also be assessed.

10.5 **Information has been removed due to its content being exempt in terms of the Freedom of Information (Scotland) Act 2002, Section 35, Law Enforcement.**

10.6 For those instances where the initial report of a TTL is being handled by call centre staff or front line Police Officers, then initial intelligence checks should be made with the relevant DIM or his/her deputy for the relevant area. Please note that in any instance where the DIM or his/her deputy is involved in making a risk assessment, the threat is not owned by the DIM, but by the identified Det Supt or DCI.

10.7 It is recommended that a Risk Assessment Form be completed when dealing with a 'High Risk' TTL incident. In circumstances where Police Scotland receives the initial report of a TTL then passes the threat to another Force for ownership, this risk assessment form should be completed to offer a standardised product to assist that Force in managing the overall threat.

10.8 The risk assessment form gives consideration to the under noted process:

- Assessment of threat;
- Analysis of the risk;
- Probability of the risk occurring;
- Control Strategy (considering Tactical menu of options); and
- Risk assessment post control strategy.

11. Intelligence Evaluation

11.1 The objective of the 5x5x5 intelligence evaluation system is to ensure the best possible protection for, and assessment of, sources of intelligence, while at the same time safeguarding the rights of individuals. It is also designed to enable an objective judgement to be made of the value and reliability of the intelligence contained within the report.

11.2 The dissemination codes were added to meet requirements of the Human Rights Act and the Data Protection Act (DPA 2018). It is important when considering a response to a TTL that the dissemination code, if included, is taken into account and met.

11.3 **Information has been removed due to its content being exempt in terms of the Freedom of Information (Scotland) Act 2002, Section 35, Law Enforcement.**

11.4 Further advice and guidance on intelligence evaluation and its assessment can be obtained from the relevant DIMs and/or NIB.

12. Threat Level and Response

12.1 Low – No Real Threat and/or Immediate Risk

12.1.1 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 officer with ownership (i.e. Det Supt) 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.

12.1.2 The command and control incident must include policy decisions made by the Det Supt with ownership of the threat, after consultation as necessary with the relevant DIM or other intelligence departments. This will provide an accurate flow of information, research undertaken, decisions made and resources allocated.

12.1.3 If any additional information comes to light at a later stage that indicates the threat has increased, the owner of the threat will be responsible for ensuring that the matter is reassessed and any necessary action is taken. Should the level of threat decrease, resulting in the decision to reduce or withdraw resources, the command and control incident must be updated.

12.1.4 In addition a SID log, containing as much information as possible, must be created on the instructions of the Det Supt.

12.2 Medium – Threat Considered Conditional

12.2.1 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 credible immediate threat to life 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.

12.2.2 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?

12.2.3 Where a threat is considered medium risk, the appropriate Det Supt should be advised. The Det Supt will maintain ownership of the threat, and after the appropriate risk assessment has taken place, that officer should ascertain any levels of intervention or disruption that should be undertaken.

12.2.4 The Command and Control incident must include policy decisions made by the officer with ownership, after consultation with the Intelligence Manager, SIO or

other departments. This will provide an accurate flow of information, research undertaken, decisions made and resources allocated.

12.2.5 The Det Supt will ensure that steps are taken for any new intelligence to be reviewed as it arises. Any change in the intelligence will require a reassessment of the threat. The Det Supt will consider any of the range of tactical options available, to eliminate or minimise the threat to the intended victim, the community or police officers.

12.2.6 The Det Supt will be responsible for managing, reviewing the risk and threat and ensuring all necessary action is taken to minimise the threat. Consideration should also be given to notifying the 'on call' Chief Officer at the first available opportunity and in any event within 24 hours.

12.2.7 Should the level of threat decrease, resulting in the decision to reduce or withdraw resources, the Command and Control incident must be updated. In addition a SID log to this effect containing as much information as possible must be created.

12.3 High – Real and Immediate Threat to Life

12.3.1 A High threat, assessed as being specific, is a credible immediate threat to life 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.

12.3.2 The appropriate Det Supt should be advised of all High Risk TTLs. He/she will maintain ownership of the threat. After the appropriate risk assessment has taken place that officer should ascertain any levels of intervention or disruption that should be undertaken to minimise the threat to the intended victim, the community and police officers, and declare this as a critical incident.

12.3.3 The Command and Control incident must include policy decisions made by the Det Supt, after consultation with the DIM or other departments. This will provide an accurate flow of information, research undertaken, decisions made and resources allocated.

12.3.4 The Det Supt remains the 'owner' of the threat, and it is good practice to also advise the 'on call' Detective Superintendent, SCD. Consideration should also be given to notifying the 'on call' Detective Chief Superintendent and, as appropriate, the 'on call' Chief Officer at the first available opportunity and in any event within 24 hours.

13. Resolution – Proactive/Disruptive Responses

13.1 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.

13.2 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.

13.3 Resolution of Low Risk Threats

13.3.1 As owner of the threat, the Det Supt will ensure that the Command and Control incident is updated so that any subsequent information concerning the threat will be brought to his/her attention. Additionally, a SID log should be submitted. No further action need be taken unless more information comes to light.

13.3.2 **However, 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**.

13.3.3 **Information has been removed due to its content being exempt in terms of the Freedom of Information (Scotland) Act 2002, Section 35, Law Enforcement.**

13.4 Resolution of Medium Risk Threats and High Risk Threats to Life

13.4.1 It is recommended that the police response to resolve a Medium Threat or High Risk TTL is for the Det Supt 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 TTL 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 TTL.

13.4.2 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 at Appendix 'E'.

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

13.4.4 **Information has been removed due to its content being exempt in terms of the Freedom of Information (Scotland) Act 2002, Section 39, Health, safety and the environment.**

13.4.5 As previously documented, among the options available to resolve a threat are proactive responses, disruptive responses, an option to warn the intended victim or perpetrator, or the pursuit of investigative opportunities where crime or offences have been committed.

13.5 Proactive Response

13.5.1 A proactive response may entail measures such as removing the victim to a place of safety or offering protection, while conducting covert and/or overt investigations to identify the perpetrator/potential perpetrator. Other options may include deployment of covert sources and techniques to obtain evidence or intelligence on the potential perpetrator, or in some circumstances to mount a wide ranging operation in response to developments as they arise. In any proactive response, the strategy must be clear and understood by those entrusted with its implementation and it must be formally agreed and documented by the officer responsible for oversight of the response to a High Risk threat, who will usually be of Det Supt rank.

13.6 Disruptive Response

13.6.1 A disruptive response is designed to prevent the intended / potential attack from occurring. Options for disruptive tactics are found within Appendix 'E'.

13.6.2 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.

13.6.3 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.

13.6.4 The Det Supt 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.

13.7 Investigative Response

13.7.1 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.

13.8 Option to Issue Warning Notice - Threat to Life Warning Notice/ Personal Safety Advice Warning Notice

13.8.1 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. 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.

13.8.2 The Warning Notice can be for two purposes. The TTL Warning Notice is to be issued where the threat is considered as being 'real' and 'immediate'. A Personal Safety Advice Warning Notice is to be issued where there is intelligence to suggest that the individual's personal safety is at risk, but the threat is not 'real' and 'immediate', but may involve some form of lesser violence.

13.8.3 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 Det Supt/or DCI to decide whether a further TTL Warning Notice or Personal Safety Advice Warning Notice has to be issued. The Command and Control Incident and associated SID log needs to be updated with the decision process accordingly.

13.9 Option to Issue Disruption Notice - Threat to Life Disruption Notice/ Disruption Interview Notice

13.9.1 The TTL Disruption Notice can also be for two purposes. The TTL Disruption Notice 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 Disruption Interview Notice 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.

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

13.9.3 **Information has been removed due to its content being exempt in terms of the Freedom of Information (Scotland) Act 2002, Section 35, Law Enforcement.**

13.9.4 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?
- **Information has been removed due to its content being exempt in terms of the Freedom of Information (Scotland) Act 2002, Section 35, Law Enforcement.**
- 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?

13.9.5 A Det Supt who decides to issue a Warning Notice to a potential victim and/or a Disruption Notice to a perpetrator should consult with the SIO if the incident relates to an ongoing major investigation, as a means to establish the risk and impact to that enquiry by such action.

13.9.6 If the Det Supt decides not to warn an intended victim or the perpetrator, the rationale for doing so must be documented and, if the matter is assessed as being a High Threat to Life 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 Det Supt 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.

13.9.7 Where a warning is not issued, the intelligence must be monitored and the assessment must be reviewed accordingly. The Command and Control incident must also be updated to that effect.

13.9.8 Likewise, if a Warning or Disruption Notice is administered then that must be updated on the Command and Control incident.

13.9.9 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. It is also recommended that experienced officers are selected for this task and that the Warning and/or Disruption is issued as per the contents of the Warning or Disruption Notice to the intended victim/assailant.

13.9.10 **The potential victim/perpetrator will not be given a copy of the Warning or Disruption Notice under any circumstances. Officers should record the delivery of the Warning or Disruption Notice and the response, if any, from the recipient**.

13.9.11 Points to consider in respect of Warning and Disruption Notices are documented in Appendix 'F'.

13.9.12 Special consideration must be given to instances in which the recipients of such notices are incapable of signing the notices in acknowledgement of their content (for example if the recipient suffers from a relevant disability or they are unable to read and/or write). Consideration should also be given to utilising Language Line or the Interpreting Service where a Notice is to be issued to a non English speaker.

13.9.13 In out of hours circumstances where the on call DI for the relevant Division is involved in making a decision as to whether a Warning or Disruption Notice is issued, and the Warning or Disruption Notice is to get signed in another Division, then the relevant Notice can get signed retrospectively as long as the decision was logged on the Command and Control incident at that time.

13.9.14 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 SFRS NOLO can be contacted for advice and covert options including an enhanced response by fire service, without the intelligence being more widely disseminated.

13.10 Disruptive Strategy

13.10.1 If a potential victim/perpetrator acknowledges the Warning or Disruption Notice, the associated Command and Control incident must remain open. Any handover to other Officers must be noted within the log of the incident.

13.10.2 If the Det Supt or SIO is satisfied that an assessed level of threat appears to have diminished, the incident may be closed on their instruction, although any investigation into the crime of threats should continue. Where such an incident is closed, a full update must be included and a relevant SID log detailing the full circumstances **will** be created on the instructions of the Det Supt/SIO.

13.10.3 An 'occurrence' marker should be created on Command and Control for the information of officers who may be asked to attend further calls, related or not, at any specified location.

13.10.4 The Chief Officer must also be advised of the result of an enquiry if it is in relation to a High threat involving the use of firearms.

13.10.5 In the event that the Warning or Disruption 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.

13.10.6 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.

14. Cross Force / Border or Inter Agency Operations

14.1.1 Where an incident is cross-boundary or cross-border, all relevant parties must be made aware of the risk and the extent of the threat.

14.1.2 Where an incident traverses divisional boundaries but does not extend beyond Scotland, the relevant Det Supt for that Division or nominated deputy will initially act as SIO and will assume tactical responsibility for the matter.

14.1.3 If the matter involves cross-border implications and identifies a potential victim in another Force area outwith Scotland, immediate notification of this must be undertaken and the mitigation of the risk is then owned and coordinated by that Force.

15. Monitor and Review / Ownership

15.1 Administration

15.1.1 The Det Supt / SIO combination managing each threat will retain original documents at all times. Copies of TTL Disruption and/or TTL Warning Notice (in respect of High Risk TTLs) are to be submitted to the NIB once the threat no longer exists. All such communication should be handled as RESTRICTED under the Government Protective Marking Scheme (GPMS).

15.1.2 Copies of all original documents used to record and manage High Risk TTL incidents should be forwarded to the NIB who will act as a central record keeping unit for High Risk TTLs. As part of the administration process, it is assessed that the generation of a unique reference number for each High Risk TTL will be best practice. In view of the significant role played by intelligence, particularly intelligence derived from covert practice, it is further assessed that any central record keeping be vested in an intelligence unit well-versed in handling sensitive material relating to TTLs. The administration of Low and Medium Risk TTLs is a local responsibility.

15.1.3 The same process should be used to record the decision not to issue a TTL Warning/TTL Disruption Notice. It is useful to structure the rationale and context of the decision made.

15.1.4 This may be required at a future date in any judicial inquiry into the management of a threat to a third party, but also provide useful intelligence that links in with other information relating to criminal activity.

15.1.5 These policy decisions should also be filed in the designated record keeping unit and marked RESTRICTED under GPMS.

15.1.6 Where a Warning or Disruption Notice has been issued, the recipient will be invited to sign a notice and this will be witnessed by the serving officers.

15.1.7 Not all parties will be amenable to the police and where the recipient refuses to sign the notice the serving officers will record the fact of refusal on the notice and sign it themselves.

15.1.8 Copy TTL Warning/ TTL Disruption Notices and copies should be forwarded to NIB and marked RESTRICTED under GPMS.

15.2 Managing Ongoing Threat to Life Incidents - Ownership

15.2.1 In all cases, particularly where a Warning or Disruption Notice has been given, a review is to be carried out by the Det Supt as follows:

- Initial review to be made within 48 hours after the issue of the Notice, 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 the appropriate response.

15.2.2 Any subsequent review to be made no longer that 7 days after the previous review and every 7 days thereafter until there is deemed to be no longer a threat (see update in paragraph 17 below for SID flags). Only once the threat has been reduced and signed off by the Det Supt, should the threat be deemed to be no longer viable at that particular time.

16. Considerations for Scottish Prison Service

16.1.1 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 /Disruption Notice.

16.1.2 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 /Disruption Notice should be progressed by Police Scotland as would have been the case if the victim/perpetrator were out in the community.

16.1.3 During office/prison operational hours in circumstances where Police Scotland require to assess the risks to the source, re 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:

- **Information has been removed due to its content being exempt in terms of the Freedom of Information (Scotland) Act 2002, Section 35, Law Enforcement.**
- Is there an opportunity to develop this intelligence?
- **Information has been removed due to its content being exempt in terms of the Freedom of Information (Scotland) Act 2002, Section 35, Law Enforcement.**

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

16.1.5 Outwith 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

17. SID Entries

17.1.1 Officers will ensure that on every occasion an intelligence entry is created in SID with the subject heading THREATS - TTL. An A11 log will detail circumstances surrounding the issue of the Threat to Life Warning Notice with the subject heading THREATS - TTL - TTN or in the case of a Disruption Notice THREATS - TTL - DTTN. Should the recipient provide explanation as to why they are under threat a witness statement and separate intelligence entry should be created and graded appropriately.

17.1.2 To ensure that subsequent reviews of the threat are maintained, a flag on the SID log should be created to appear in the Local Intelligence Office (LIO) queue for review, thereafter the log will be updated (including action taken etc) and a new review period set.

18. Recording Threats to Life on PNC

18.1.1 The presence of a TTL warning will be recorded on PNC using an appropriately worded Locate Information entry. These entries fall into two different categories:

(i) The subject has been served with a TTL Warning/ TTLDisruption Notice;

(ii) The person is the subject of a TTL Enquiry, enquiries now concluded, no requirement for TTL Warning/TTL Disruption Notice.

18.1.2 As the threat to life scenario progresses at each review, the content and the PNC Locate Information entry must also be reviewed.

18.1.3 Close liaison is required with NIB who is responsible for managing the Threat to Life on PNC to implement an administration process.

18.1.4 There will also need to be a robust audit process in place to avoid inadvertent weeding of the entry.

18.1.5 Examples of TTL PNC entries are provided in Appendix 'G'.

19. Summary of Rank / Role Specific Responsibilities

19.1 The Det Supt is responsible for assessing the extent of a TTL and for ensuring that appropriate action is taken to minimise the risk. If the threat emerges from an ongoing major investigation, the SIO will have responsibility for the risk assessment and TTL decision. The implementation of control measures to minimise the risk is the responsibility of the relevant Division.

19.2 The NIB is responsible, on behalf of the Det Supt, NIB, SCD, for managing and providing advice on all matters associated with the issue, preparation, content and retention of TTL Warning and TTL Disruption Notices. These TTL Notices will not be issued until discussion with staff within the designated intelligence unit has taken place. For control and auditing purposes, all TTL Notices will be allocated a unique reference number (URN).

Appendix 'A'

List of Associated Legislation

- Human Right Act 1998
- Data Protection Act 2018

Appendix ‘B’

List of Associated Reference Documents

Policies

- Intelligence Policy
- Crime Investigation Policy
- Serious and Organised Crime Policy

Standard Operating Procedures

- Scottish Protected Persons Unit SOP
- Armed Policing Operations SOP

Appendix ‘C’

List of Associated Forms

Forms

- PSoS Form 139–004 Threat to Life Warning Notice / Personal Safety Advice Warning Notice
- PSoS Form 139–005 Threat To Life Disruption Notice / Disruption Interview Notice
- PSoS Form 139–006 TTL Risk Assessment Process and Template

Appendix ‘D’

Glossary of Terms

ACC	Assistant Chief Constable
CHS	Criminal History System
DIM	Divisional Intelligence Manager
ECHR	European Convention on Human Rights
GPMS	Government Protective Marking Scheme
LEA	Law Enforcement Agency
LIO	Local Intelligence Office
NIB	National Intelligence Bureau
PNC	Police National Computer
PND	Police National Database
SCD	Specialist Crime Division
SID	Scottish Intelligence Database
SIO	Senior Investigating Officer
SPS	Scottish Prison Service
TTL	Threat to Life
UKBA	United Kingdom Border Agency
URN	Unique Reference Number

Appendix ‘E’

Information has been removed due to its content being exempt in terms of the Freedom of Information (Scotland) Act 2002, Section 35, Law Enforcement.

Appendix 'F'

Threats to Life Warning / TTL Disruption Notice – Points to Consider

Where consideration is being given to issuing a TTL Warning or TTL Disruption notice to an intended victim/perpetrator, all available information must be monitored and assessed.

Information has been removed due to its content being exempt in terms of the Freedom of Information (Scotland) Act 2002, Section 35, Law Enforcement.

The administration relevant to TTL Warning and TTL Disruption Notices will be governed by NIB, who will allocate a URN and retain copies of the documentation.

Officers instructed to issue a TTL Warning or TTL Disruption Notice must be briefed by the SIO regarding the circumstances surrounding the threat and where appropriate, health and safety risk assessments must be conducted. It must be made clear that the warning should not deviate from the contents of the notice.

The intended victim/perpetrator will be asked to acknowledge and sign the TTL Warning or Disruption Notice. The Command and Control incident will be updated accordingly and the original notice retained within NIB. A copy of the Notice must be retained by the SIO for reference purposes. The intended victim/perpetrator must not be given a copy of the Notice.

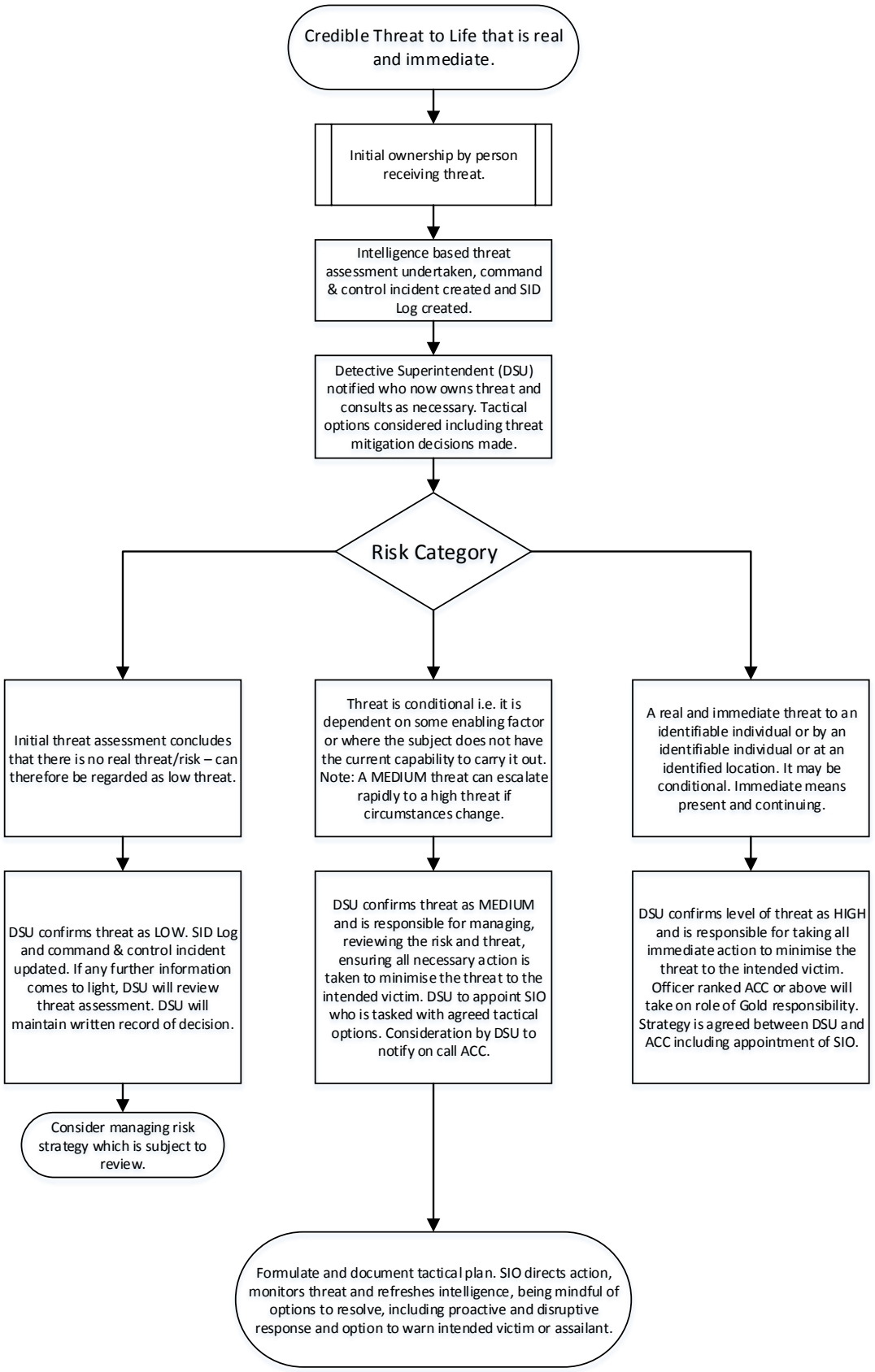
Appendix ‘G’

Recording Threats to Life on PNC – Examples

Information has been removed due to its content being exempt in terms of the Freedom of Information (Scotland) Act 2002, Section 35, Law Enforcement.

Appendix 'H'

Threat to Life Generic Flowchart



Appendix 'I'

Threat to Life Warnings – Information has been removed due to its content being exempt in terms of the Freedom of Information (Scotland) Act 2002, Section 35, Law Enforcement.