Intelligence report

This page is from APP, the official source of professional practice for policing.

First published 24 August 2015 Updated 26 January 2022
Written by College of Policing
10 mins read

Intelligence report

The intelligence report (IR) is used to submit and evaluate information, and to manage dissemination of intelligence. It protects the source and contributes to an **audit trail** of the intelligence. Standardisation of reporting provides a shared confidence between law enforcement communities and partner agencies.

The IR evaluation reference material provides guidance on the 3x5x2 process and on how to apply it to intelligence that is graded under this system. This reference material will support forces where intelligence/products make reference to historic intelligence graded under the 5x5x5 system.

Introduction

The following guidance covers each section of the IR.

Duty of care

The ownership of the risk to the source always remains within the originating organisation. When intelligence is disseminated outside the originating organisation, any handling conditions must be adhered to by the receiving organisation. When this doesn't happen, both organisations may be held accountable for any consequences.

Government security classification

Once populated, the report should be allocated an appropriate protective marking. The majority of information/intelligence that the law enforcement agency holds contains **personal** or **sensitive data**.

It is important that the **government security classification (GSC)** reflects the level of sensitivity and degree of protection required by the IR.

Reporting member of staff and date/time of report

These fields record the name, rank or position, and the station or office of the person who completes the IR, together with the date and time of submission.

Person providing information (source)

The source of the information can be either the name and address of the person providing the information or an intelligence source reference (ISR) number.

In order to avoid any chance of compromise, the details of the person providing the information should not be placed in the main body of the IR. The final, sanitised version of an IR to be seen by operational officers and staff (for example, those expected to act upon intelligence) should not detail the true identity of any source, either within a source field or the main body of the text; this includes law enforcement officers and staff as information sources. Organisations must have measures in place to ensure that the correct identity of the source is not revealed.

A unique reference number (URN) is added to the submitted report either electronically or by the receiving intelligence unit in order to provide an **audit trail** of received information. The intelligence unit will create a second sanitised version of the report if editing or sanitisation is required. They should ensure the removal of the source details and allocate a further URN to this report, and cross-reference it to the original. Local policy determines who specifically has access to unsanitised reports. The original report must be retained and stored securely to ensure that source information is not revealed.

Items of information from the same source but concerning totally different matters should be recorded on separate IRs. If a single source of information provides several items of intelligence relevant to the same issue that could potentially compromise the source, separate IRs can be considered. This is to avoid a single source being identified who may be the only one to know the sum total of the information submitted.

Collection

Source evaluation

The source evaluation is made by the person submitting the information to describe the reliability of the source. This enables the credibility of the information to be established and informs the proportionality of tactical options.

Everyone submitting intelligence has a duty to ensure it is accurate and is corroborated where possible.

There are three source gradings.

1. Reliable – this grading is used when the source is believed to be both competent and information received is generally reliable. This may include information from human intelligence, technical, scientific and forensic sources. It is important that the two tests of competence and veracity of past intelligence are both met before a source is considered to be reliable.

   Where either test is not met, not reliable should be selected and the ground to doubt the reliability is specified.

2. Untested – this relates to a source that has not previously provided information to the person receiving it or has provided information that has not been substantiated. The source may not necessarily be unreliable, but the information provided should be treated with caution.

   Before acting on this information, corroboration should be considered. This would apply to information when the source cannot be determined, for example, Crimestoppers.

3. Not reliable – this should be used where there are reasonable grounds to doubt the reliability of the source. These should be specified within the IR risk assessment and may include concerns regarding the authenticity, trustworthiness, competence or motive of the source or confidence in the technical equipment. Corroboration should be sought before acting on this information.

Information/intelligence assessment

This grading describes the reliability of the information based on how it became known to the source and from other available intelligence.

- A – Known directly to the source. Refers to information obtained first-hand, for example, through witnessing it. Care must be taken to differentiate between what a source witnessed themselves

and what a source has been told or heard from a third party.

- B – Known indirectly to the source but corroborated. Refers to information that the source has not witnessed themselves, but the reliability of the information can be verified by separate information that carries the information/intelligence of assessment of A. This corroboration could come from technical sources, other intelligence, investigations or enquiries. Care should be taken when ascertaining corroboration to ensure that the information that is presented as corroboration is independent and not from the same original source.
- C – Known indirectly to the source. Applies to information that the source has been told by someone else. The source does not have first-hand knowledge of the information as they did not witness it themselves.
- D – Not known. Applies where there is no means of assessing the information. This may include information from an anonymous source, or partners such as Crimestoppers.
- E – Suspected to be false. Regardless of how the source came upon this information, there is a reason to believe the information provided is false. If this is the case, the rationale for why it is believed to be false should be documented in the IR risk assessment.

Information content

The information content should comply with the basic principles of **5WH**, namely, what, when, where, why, who and how.

Information should be for a policing purpose. It should be clear, concise and without abbreviations. The information must be of value and understood without the need to refer to other information sources.

The body of the report should give no indication of the nature of the source, whether human or technical, or the proximity of the source to the information.

Where possible, the information should be corroborated and its provenance established. This could be done through interrogation of information already held in other business areas, for example, PNC. Where that research has been done this should be recorded and contained within the initial IR and clearly labelled. It should indicate the databases that have been researched.

For ongoing operations, the operational name or number may be added. A separate IR must be submitted when new intelligence is identified from any research, for example, that carried out on non-law enforcement agency databases (including the internet).

Dissemination

Handling codes and conditions

Handling codes are a control mechanism for intelligence sharing. The risks associated with sharing intelligence must always be weighed against the potentially greater risk of not sharing. Handling codes are supported by **conditions for intelligence sharing**.

Before disseminating intelligence, the person disseminating should ensure they are familiar with the appropriate legislation and their organisation's policies, standard operating procedures and other frameworks.

For further information see APP information management on **data protection/disclosure and information sharing.**

Lawful sharing permitted (P)

In order to share this intelligence there must be:

- a policing purpose
- local protocols in place
- a legitimate need to receive it

Lawful policing purpose is defined as to:

- assist others to protect life or property
- assist to preserve order
- prevent the commission of offences
- assist others to bring offenders to justice
- linked to any duty or responsibility arising from common or statute law

Lawful sharing includes other government departments, private and voluntary sectors.

Specific questions need to be asked when considering dissemination of code P intelligence. For example:

- are there legal obligations?
- who is asking for it?

- why do they want it?
- what are they going to do with it?

Dissemination to European Economic Area (EEA) law enforcement agencies is permitted without any additional IR risk assessment.

If there are concerns around how widely the intelligence may be disseminated, code C applies. It may not be appropriate to disseminate all of the intelligence and the merits of redaction should be considered.

Dissemination to (non-EEA) foreign law enforcement agencies should be risk assessed on an individual basis. The Data Protection Act 1998 allows for personal information to be disseminated outside the EU only after the risks have been assessed and on the grounds of substantial public interest. Public interest in this context includes tackling serious crime and the maintenance of the security and integrity of law enforcement agencies.

Care should be taken when handling intelligence received from HMRC as further unauthorised dissemination may result in the commission of a criminal offence. If this is likely to happen, HMRC will provide a warning within the intelligence report.

Lawful sharing permitted with conditions (C)

This code permits dissemination but requires the receiving agency to observe conditions as specified. Application of this code means the originator has applied specific handling instructions in respect of this information. An IR risk assessment may be required in respect of the intelligence concerned. An application for public interest immunity should be considered if the intelligence is subsequently used in court.

Handling conditions should be contained within the appropriate section of the IR.

The recipient must abide by the handling conditions. The originator must be contacted by the recipient before they conduct any further activities outside the conditions.

Any intelligence report with conditions should remain under review to ensure that wider dissemination can occur as soon as is feasible, such as when an operation has been concluded or is no longer being pursued.

Conditions – intelligence unit only

- A1 covert development – intelligence may be combined or corroborated with other intelligence but action cannot be taken directly. Permission must be sought from the originator before action is taken on any derived intelligence.
- A2 covert use – covert action may be taken on this intelligence although the source, technique and any wider investigative effectiveness must be protected. This intelligence may not be used in isolation as evidence, in judicial proceedings or to support arrest.
- A3 overt use – overt action is permitted on this intelligence. This information can be used for: TO BE SPECIFIED BY SOURCE INTELLIGENCE OWNER.
- S1 delegated authority – the originator of the intelligence permits the unsupervised sanitisation of the material in order to allow dissemination to a wider audience.
- S2 consult originator – the originator of the intelligence does not permit the sanitisation of the material for wider dissemination without consultation being sought.

Government security classifications	Acquisition		Exploitation		
Top Secret	Source	Intelligence	Handling	Inteligence unit only	
Secret	1 – Reliable	A – Known directly	P - Lawful sharing permitted	Action	Sanitisation
Official	2 – Untested	B – Known indirectly but corroborated	C - Lawful sharing permitted with conditions	A1 - Covert development A2 - Covert use A3 - Overt use	S1 - Delegated authority S2 - Consult originator
	3 – Not reliable	C – Known indirectly			
		D – Not known			
		E – Suspected to be false			

Audit trail

This is necessary when intelligence is disseminated. The following information should be recorded:

- recipient
- material disseminated
- purpose of dissemination
- authorisation
- restrictions on the use or further dissemination of the information
- additional IR risk assessment form if appropriate

Evaluation and quality assurance of the intelligence report

Once an IR has been received by the intelligence unit, it should be further assessed for:

- risks and duty of care issues
- intelligence value
- accurate and full provenance of the information
- consideration for further research and development
- quality assurance of data standards
- consideration for dissemination and requirements for sanitisation

Any amendment to the report should have an audit trail. This may include the resubmission of a sanitised IR linked directly to the original report.

The person recording the report should be considered as credible with regards to the source reliability and information evaluation unless there is an obvious discrepancy or incompatibility. The person who submitted the report should be contacted if further clarity or corroboration is required on any issue

Sanitisation

Reports should be sanitised for onward transmission by removing material which explicitly or implicitly identifies a source or sensitive law enforcement methodology.

Intelligence report risk assessment

This form records the risks associated with the dissemination of intelligence held within the report.

It should:

- consider ethical, personal and operational risks in respect of the source, the intelligence content, its use and dissemination
- consider compliance with a legislative requirement or policing purpose
- record the justification for decisions made
- record the authority of the person making decisions
- consider the proportionality, accountability and necessity for disseminating the intelligence

Considerations:

- the IR risk assessment should not be disseminated outside the intelligence or confidential unit environment. Handling conditions should be recorded in the IR
- a review of any IR risk assessment should take place when the report is evaluated for dissemination

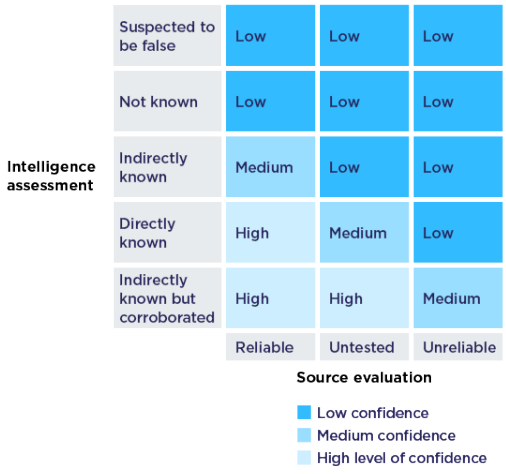
Authorisations

Each organisation should develop a policy to ensure suitable levels of authorisation for the dissemination of intelligence. Consideration should be given to dissemination to non-prosecuting parties.

Dissemination to non-EEA countries is to be authorised by at least a police inspector or equivalent grade.

Intelligence confidence matrix

The following matrix provides an indication of the level of confidence that can be taken in the intelligence dissemination. This informs decision-making and supports interoperability between agencies or organisations.



Tags

Intelligence management