Intelligence collection, development and dissemination

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

First published 23 October 2013 Updated 16 March 2015
Written by College of Policing
5 mins read

The collection, development and dissemination of intelligence allow decisions to be made about priorities and tactical options. Intelligence collection is a continuous process and there may be specific requirements for its recording and use.

Collection

The police collect information that is required for policing purposes. Policing purposes provide the legal basis for the collection, recording, evaluation, sharing and retention of information and may include one, or a combination, of the following:

- protecting life and property
- preserving order
- preventing the commission of offences
- bringing offenders to justice
- any duty or responsibility arising from common or statute law

Information is collected in one of three ways:

- **routine collection**
- **tasked information**
- **volunteered information**

Staff should consider the type of information that may be available and the likelihood of it having value as intelligence, based on the **intelligence requirement**. Collection should be managed by using intelligence collection plans to ensure that it remains focused. This should not prevent staff from submitting information for a policing purpose that is not contained in a current intelligence

requirement.

Tasked information

Is the prioritised collection of information, for example, information concerned with problems and subjects (suspect or victim) identified in the **intelligence requirement**.

Tasked information may be accessed from many **sources** including:

- internal and external databases
- CCTV systems
- **covert human intelligence sources (CHIS)**
- automatic number plate recognition systems

Intelligence collection plans

These plans help to close gaps in knowledge. They focus on the **intelligence requirement** and provide a structure for the collection of information.

The content of an intelligence collection plan varies according to the intelligence that is required. Intelligence may be collected from a variety of data sources, including:

- community intelligence
- forensic intelligence product
- communications data
- CHIS

Intelligence collection plans should:

- be updated regularly so that information collection can be properly managed, ensuring gaps, additional potential sources and possible access difficulties are identified
- contain the necessary information requirements in order to inform a comprehensive and accurate intelligence picture
- justify the proportionality and necessity of the activities that will be used for collecting the information

Open sources

Open sources of information are widely available but may not be accurate, reliable or valid.

The main uses of open-source information are to:

- develop an understanding of the locations relevant to a piece of **analysis**
- identify the potential impact of social and demographic changes
- identify external factors that may impact on crime, disorder and community concerns
- support and develop investigations by indicating lines of enquiry or corroborating other information
- support the development of **subject profiles** and **problem profiles**

There are several factors to take into account when using open-source information:

- access may require the user to register or pay a fee (for example, online news media, the electoral roll)
- the use of open-source information should be audited
- the effect of local security policies on access to open-source information (for example, some sites are not available to local users)
- it is not subject to the same quality standards as **closed sources**
- it should be corroborated by supporting information

When accessing open-source information online, a footprint identifying the police address is left on the website. A non-attributable IT identity is sometimes required to avoid law enforcement being identified as the originator of the enquiry. An accredited covert internet investigator should be asked to advise in these instances.

Closed sources

Closed sources of information are those with restricted access, for example, police crime recording systems and information available through **information sharing agreements (ISAs)** with partners.

Information from police closed sources is not evaluated through the **intelligence report** process and is usually assessed to be reliable. Users should, however, still critically view the information and understand the context in which it has been collected, and its purpose.

Closed-source information is also available from:

- other police forces

- specialist closed sources, for example, financial intelligence, special branch intelligence, **prison intelligence**
- existing intelligence and analytical products
- information from partners, including the National Crime Agency (NCA), Her Majesty's Revenue & Customs (HMRC) and the UK Border Agency (UKBA)
- organisations that are part of the local community safety partnership

A covert internet investigator may be required to access some closed-source information.

Prison intelligence

Prison intelligence officers (PIOs) are responsible for managing prison intelligence collection. They are usually based in prison establishments which are located within the force area, and act as the single point of entry into the prison security unit. PIOs oversee law enforcement agency intelligence and evidence requests received through either the nationally approved operational partnership team (formerly known as Operational Partnership Team) form process, or prison voluntary disclosure. They liaise with a prison's security unit to obtain advice, secure authorisations and facilitate access to prisoner-related information.

PIOs can provide:

- offender sentence planning, movement and release information
- updates on current and emerging organised crime networks and individuals, including alliances, tensions, continued activity and future intent
- advice on **CHIS** tasking opportunities in support of a law enforcement agency intelligence requirement
- intelligence collection to support the development of subject profiles
- logistical and planning support for debriefing within prisons
- guidance on the use of prison intelligence products
- overt and covert tactical advice and support for prison production order applications
- access to information on special interest prisoner groups such as extremist prisoners, assisting offenders, protected witnesses, category A prisoners and multi-agency public protection arrangements nominals

Development

Intelligence collection should continue throughout prevention or enforcement activity. All methods of intelligence development should be considered, including data research, communications data analysis, CHIS tasking, covert deployments and the use of **analytical techniques**.

Dissemination

Intelligence **sharing** should be proportionate and carried out in accordance with principles of the **Human Rights Act 1998**.

Protocols should be in place for disseminating confidential intelligence or sensitive intelligence.

Organised crime group mapping

In order to exploit the benefits of organised crime group mapping (OCGM), data must be shared locally, regionally and nationally within and between partners. If information development shows an organised crime group as having a criminal impact outside a partner's area of responsibility, the identifying partner should:

- record the impact upon the partner's area of responsibility
- harm assess that impact
- disseminate all appropriate information or intelligence to the relevant partner for action

All OCGM partners have **information sharing agreements** and memorandums of understanding relating to OCGM. Each partner should ensure that the 'not for dissemination' marking in the OCGM system is used only in exceptional cases.

OCGM information may be shared outside UK law enforcement agencies if a statutory purpose or proven business purpose exists. Dissemination may involve sanitisation of the original information and/or imposing certain conditions restricting its further dissemination or use without reference to the originator.

Tags

Intelligence management