



**This PDF file contains interactive links that help you to navigate the document quickly, and to enable you to gain immediate access to all websites listed.**

- ▶ Clicking on any of the items in the main list of Contents (screen page 4 ) will take you directly to the page listed. Or click on any item in the list of Contents at the start of each section. To immediately access cross-referred items contained in this practice advice, click on any cross-references shown in purple.
- ▶ To return to the list of Contents, simply click on the line “NOT PROTECTIVELY MARKED...” at the foot of each page.
- ▶ Where you see a website address featured in purple, click on it to make a direct online link.

# PRACTICE ADVICE INTRODUCTION TO INTELLIGENCE-LED POLICING

## 2007

Produced on behalf of the  
Association of Chief Police Officers  
by the National Centre for Policing Excellence



**CENTREX**  
HELPING TO DEVELOP POLICING

**This practice advice contains information to assist policing in the United Kingdom.**

**It is not protectively marked under the Government Protective Marking Scheme.**

**The decision to make the content, or any part of it, publicly available or not, rests with the copyright holders. They have agreed to make it available to the police and partner agencies on condition that these agencies do not make it publicly available, for example, on internet sites.**

**Application for disclosure under the Freedom of Information Act 2000 should be sent to the Centrex Security and Business Continuity Unit at <SecurityBusinessContinuity@centrex.pnn.police.uk>. The Security and Business Continuity Unit will be responsible for notifying ACPO and the Police Central Referral Unit.**

#### PRACTICE ADVICE: INTRODUCTION TO INTELLIGENCE-LED POLICING

This document has been produced by the National Centre for Policing Excellence (NCPE) on behalf of the Association of Chief Police Officers (ACPO). It will be updated according to legislative and policy changes and re-released as required.

The NCPE was established by the Police Reform Act 2002. As part of its remit the NCPE is required to develop policing doctrine, including practice advice, in consultation with ACPO, the Home Office and the Police Service. Practice advice produced by the NCPE should be used by chief officers to shape police responses to ensure that the general public experience consistent levels of service. The implementation of all practice advice will require operational choices to be made at local level in order to achieve the appropriate police response.

All enquiries about this practice advice should be addressed to:

Opsline  
National Centre for Policing Excellence  
Wyboston Lakes  
Great North Road  
Wyboston  
Bedfordshire MK44 3BY

Tel: 0870 241 5641  
Email: opsline@centrex.pnn.police.uk

A printed version of this CD-Rom is available on request from the above address.

#### Acknowledgements

ACPO and the NCPE would like to express their thanks to all those involved in the drafting of this document and to members of the ACPO NIM and CHIS Working Groups who gave their advice. All of the responses during the consultation phase of this project were appreciated and contributed to the final document.

© Association of Chief Police Officers (2007) © Centrex (2007)

All rights reserved. No part of this publication may be reproduced, modified, amended, stored in any retrieval system or transmitted, in any form or by any means, without the prior written permission of Centrex and ACPO or their duly authorised representative.

**Centrex is committed to providing quality products and services which comply with the Centrex Quality Assurance Framework and encompass diversity.**

# CONTENTS

<b>Foreword</b> .....	<b>3</b>
<b>Section 1 THE NATIONAL INTELLIGENCE MODEL</b> .....	<b>5</b>
1.1 What Is NIM and How Is It Used? .....	6
1.2 The Benefits of NIM .....	6
1.3 How Does NIM Work? .....	6
<b>Section 2 SOURCES OF INFORMATION</b> .....	<b>17</b>
2.1 What Is Police Information? .....	18
2.2 Types of Sources .....	18
2.3 The Collection of Information .....	19
2.4 Dealing with Human Sources of Information .....	20
2.5 Sensitive Sources .....	20
2.6 Frequent Contact .....	21
2.7 Tasking Sources .....	21
2.8 What Is a CHIS? .....	22
2.9 Recognising Issues Related to CHIS .....	22
<b>Section 3 THE 5x5x5 PROCESS</b> .....	<b>25</b>
3.1 What Is a 5x5x5 Form? .....	26
3.2 When Should a 5x5x5 Be Used? .....	26
3.3 How to Complete the 5x5x5 .....	27
3.3.1 Reporting Member of Staff .....	27
3.3.2 Person Providing Information (Source) .....	27
3.3.3 Source Evaluation .....	28
3.3.4 Information/Intelligence Evaluation .....	29
3.3.5 Completing the Report .....	30
<b>Appendix 1 5x5x5 TEMPLATE</b> .....	<b>33</b>
<b>Appendix 2 STAFF RESPONSIBILITIES CHECKLIST</b> .....	<b>37</b>
<b>Appendix 3 ABBREVIATIONS AND ACRONYMS</b> .....	<b>41</b>
<b>Appendix 4 REFERENCES AND FURTHER INFORMATION</b> .....	<b>43</b>
<b>Summary of Figures</b>	
Figure 1 The Three Levels of NIM .....	7
Figure 2 NIM in Practice .....	8
Figure 3 The Eleven Elements of NIM .....	9
Figure 4 Three Methods for Collecting Information .....	19
Figure 5 Identifying CHIS Status .....	23
Figure 6 Gradings for Source Evaluation .....	28
Figure 7 Gradings for Information/Intelligence Evaluation .....	29



# FOREWORD

The concept of intelligence-led policing underpins all aspects of policing, from neighbourhood policing and partnership work to the investigation of serious and organised crime and terrorism. Within the framework of the National Intelligence Model, the effective and efficient collection, recording, dissemination and retention of information allows for the identification of material which can be assessed for intelligence value and enables decision-making about priorities and tactical options. Where information has been derived from human sources, whether members of the public, criminals or police staff, additional risks and considerations arise about the management of such material. It is, therefore, important that staff understand the role that they play in the intelligence-led policing process, and how they can achieve the best results through knowledge of the following key aspects:

- The National Intelligence Model (NIM);
- The collection of information, including Covert Human Intelligence Source (CHIS) issues and;
- The national Information/Intelligence Report (ie, the 5x5x5 process).

This practice advice assumes no previous knowledge or experience of intelligence-led policing. It is designed as a quick reference guide for staff who are not intelligence specialists, but require an understanding of intelligence-led policing processes as part of their day-to-day duties. This includes team leaders/managers who have a key role ensuring that staff are fully briefed on their specific responsibilities. Staff involved in specialist intelligence roles, however, may also find the publication useful as an aide-memoir.

Staff engaged in a training capacity can use the content to inform training products in relation to intelligence-led policing. This includes such national programmes as the Initial Police Learning and Development Programme (IPLDP), the Core Leadership and Development Programme (CLDP) and neighbourhood and community policing training.

A checklist of responsibilities in relation to intelligence-led policing is presented in [Appendix 2](#).

This practice advice highlights publications for further reading on particular aspects of intelligence-led policing:

- *ACPO (2005) Guidance on the National Intelligence Model;*
- *ACPO (2006) Guidance on the Management of Police Information;*
- *ACPO (2006) Guidance on the Management of Covert Human Intelligence Sources.*



Sara Thornton  
Chair Intelligence Portfolio  
Chief Constable, Thames Valley Police



# Section 1

## THE NATIONAL INTELLIGENCE MODEL

**T**his section provides an introductory explanation of the National Intelligence Model (NIM).

### CONTENTS

1.1	What Is NIM and How Is It Used? .....	6
1.2	The Benefits of NIM .....	6
1.3	How Does NIM Work? .....	6

## 1.1 WHAT IS NIM AND HOW IS IT USED?

The NIM is a business model used by the Police Service, and increasingly by other partners, to ensure that policing is delivered in a targeted manner through the development of information and intelligence. It is used to prioritise issues and allocate resources to deal with them. NIM is applicable to all aspects of operational policing and is used, for example, to:

- Direct patrols;
- Target prolific and priority offenders, and resolve crime and disorder problems;
- Work effectively with partner agencies;
- Drive problem solving;
- Improve road safety;
- Manage priority locations and high-risk issues;
- Guide neighbourhood policing activity;
- Increase the understanding of criminality and anti social behaviour issues.

NIM is based on proactive policing which involves identifying, understanding and addressing underlying problems and trends. This broader perspective allows for prioritisation of police activity which makes it easier to respond to the increasing demands placed on the Police Service. Elements of NIM, however, may be used in reactive investigations, for example, to direct resources and establish a full picture of an issue under investigation.

## 1.2 THE BENEFITS OF NIM

Every member of staff has a role to play in making NIM work. When working effectively, NIM enables staff to:

- Receive better tasking and direction (eg, staff are deployed to a location or to deal with a problem where they can have most impact);
- Contribute to effective policing by collecting and recording relevant information which is used to create greater understanding of crime and non-crime problems.

As a result, an improved service is provided to the public, public confidence is increased and more offenders are brought to justice.

## 1.3 HOW DOES NIM WORK?

The following pages outline how NIM works through a series of three figures:

- **Figure 1** illustrates how NIM works on three levels.
- **Figure 2** describes how NIM works in practice, by presenting the eleven elements of the model alongside a relevant policing example.
- **Figure 3** explains each of the eleven elements of NIM.

Figure 1 The Three Levels of NIM

Staff need to be aware that NIM operates on three levels. Any crime, incident or neighbourhood priority that is evident at a local level, ie, Level 1, could originate from, or have implications for, other levels. A key component of NIM is to ensure that communication and information flows exist between all three levels. This enables the Police Service to maximise the effectiveness and efficiency of any formulated response, whatever the level. Level 2 and Level 3 will invariably require additional specialist resources which must be accessible to Level 1 when necessary.

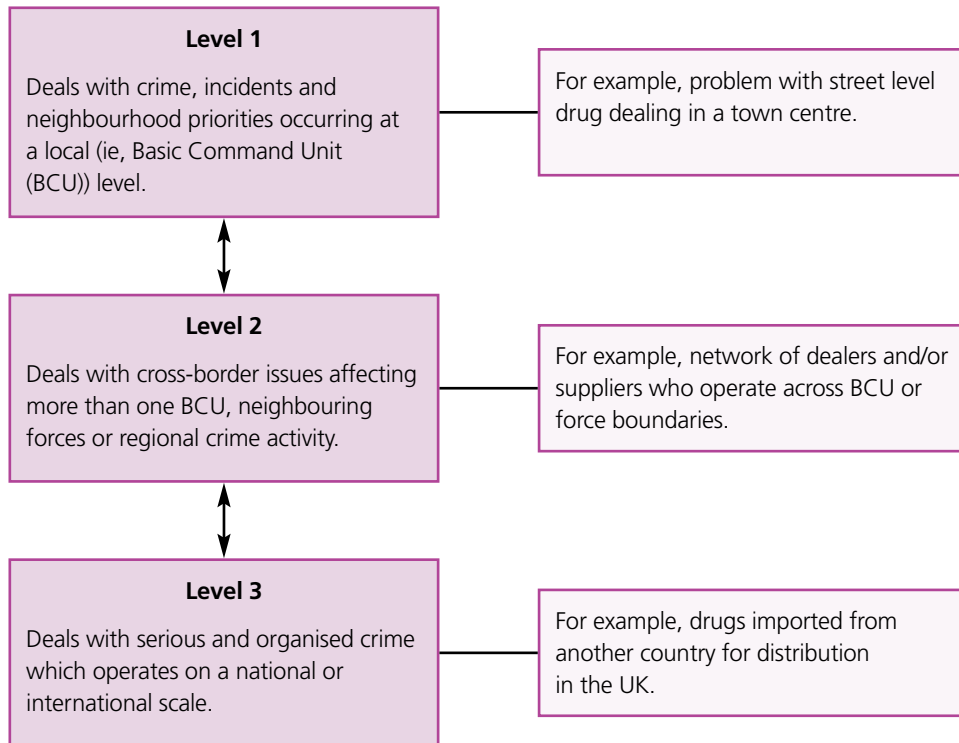


Figure 2 NIM in Practice

The NIM comprises of eleven elements and this figure illustrates how they relate to one another.

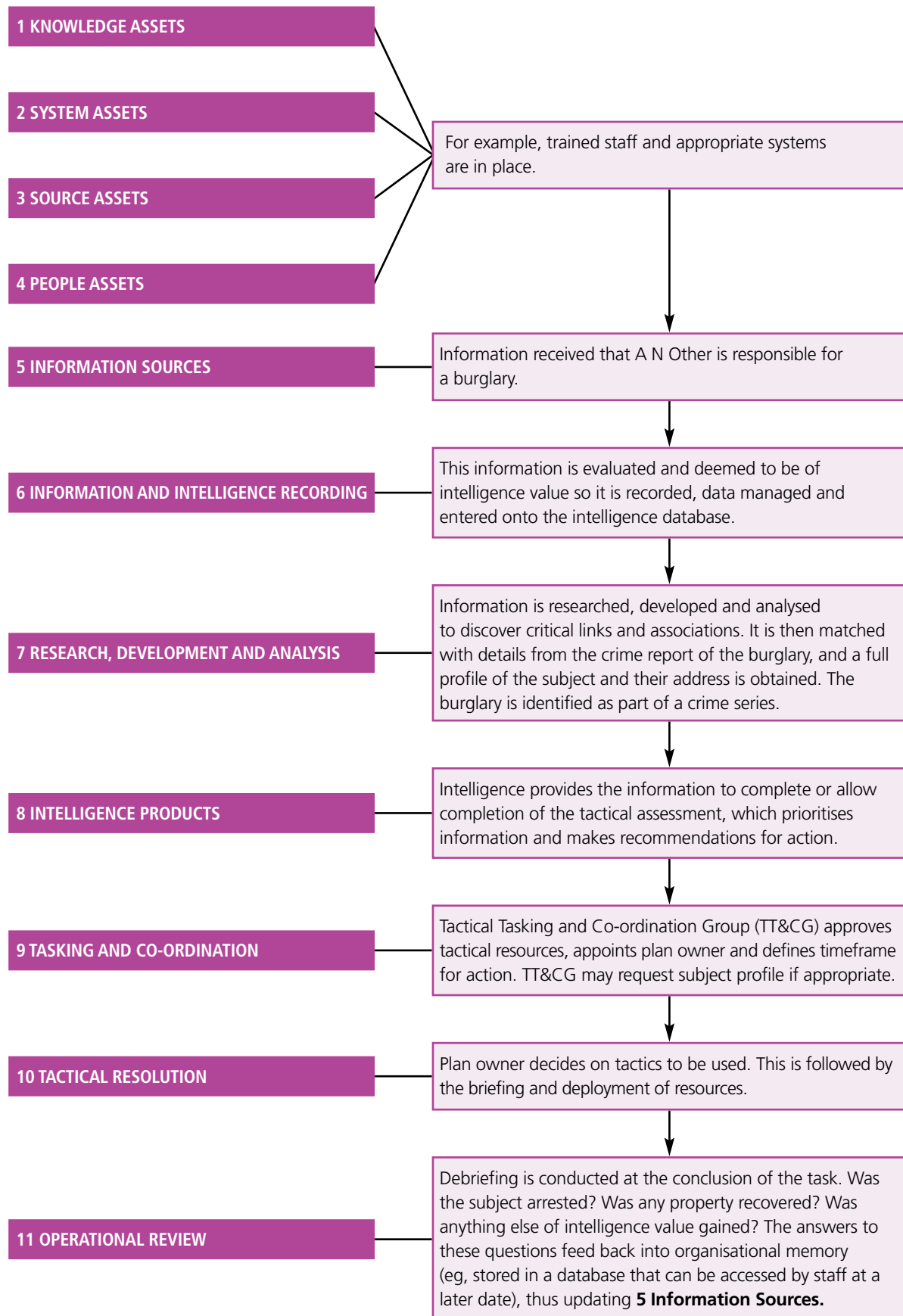


Figure 3 The Eleven Elements of NIM

The first four of the eleven NIM elements are the assets, which are shown below. These represent the foundation of NIM at all levels. These four assets must, therefore, be in place for NIM to be effective.

#### 1 KNOWLEDGE ASSETS

**Description:**

Knowledge assets refer to the professional knowledge needed by staff to enable them to work effectively. The dissemination and accessibility of knowledge assets makes this possible. Examples of knowledge assets include current legislation, ACPO guidance and force policies.

**Impact on Staff:**

Knowledge assets can be obtained through training, accessing force intranets, and accessing police libraries.

#### 2 SYSTEM ASSETS

**Description:**

Staff must be aware of the rules and policies that are associated with the secure capture, recording, storage and use of information and the infrastructure required to enable intelligence activity. Examples include physical and technical security policies (eg, secure access to buildings, computer firewalls and passwords).

**Impact on Staff:**

Staff must follow relevant security procedures, for example, logging on and off computers, and complying with building access policies.

#### 3 SOURCE ASSETS

**Description:**

To work effectively, NIM needs information. Source assets, therefore, refer to sources of information which can be both overt and covert. Examples include witnesses, partner agencies, forensic information and human intelligence sources.

**Impact on Staff:**

Staff must be aware of how different types of information can be collected. This includes knowing where different sources exist, and how they can be accessed. For further information see [2 Sources of Information](#).

#### 4 PEOPLE ASSETS

**Description:**

NIM relies on all staff knowing their roles and responsibilities in relation to the model. People assets recognise that staff need to be trained to the relevant level to carry out these roles and responsibilities effectively.

**Impact on Staff:**

Staff must ensure that they understand the training they receive on NIM so that they can carry out their roles and responsibilities effectively. This document, in conjunction with training, will help staff to achieve this.

### Figure 3 The Eleven Elements of NIM (continued)

Elements 5, 6 and 7 of the NIM, see below and overleaf, explain the process of turning information into useful intelligence. The role of the analyst is outlined in detail in **7 Research, Development and Analysis**.

#### 5 INFORMATION SOURCES

**Description:**

Information can come from a number of sources, eg, witnesses, databases and briefings. Information which has been processed may become actionable intelligence.

**Impact on Staff:**

Staff need to know what information to collect and how to access it from different sources. For further information, see [2 Sources of Information](#).

#### 6 INFORMATION AND INTELLIGENCE RECORDING

**Description:**

Once relevant information is obtained, it needs to be recorded and evaluated. Recording information on standardised systems allows it to be processed and retrieved efficiently. Information evaluation is conducted through an initial assessment which determines the reliability of both the source and the information, and the level at which the information can be disseminated.

**Impact on Staff:**

To record and evaluate information/intelligence, staff must know how to complete a 5x5x5 form. This is outlined in [Section 3 The 5x5x5 Process](#).

Figure 3 The Eleven Elements of NIM (continued)

**7 RESEARCH, DEVELOPMENT AND ANALYSIS**

**Description:**  
Information that has been recorded and evaluated using a 5x5x5 needs to be processed, along with other information, so that it becomes intelligence which directs decision making. This is achieved through research and analysis that is conducted by trained staff in the intelligence unit.

**Impact on Staff:**  
The work of researchers and analysts is important in maximising the effectiveness of NIM. Their work will eventually impact on staff through briefings relating to crime and non-crime priorities. Staff will also become involved in contributing towards problem solving through the production of intelligence products, see **8 Intelligence Products**.

**The Role of the Analyst:**  
Analysis is the process of collecting, reviewing and interpreting a range of data and making inferences and recommendations. Intelligence analysts use defined analytical techniques to identify and explain patterns of crime and incidents, and infer who or what may be responsible. For more information on the use of analytical techniques, see *ACPO (forthcoming) Analytical Tools and Techniques*. Analysis supports strategic decision making and the tactical deployment of resources to prevent crime, detect and disrupt criminal activity, and solve problems.

Intelligence analysts work to the 'intelligence cycle'. The components of the cycle are: Direction, Collection, Collation, Evaluation, Analysis, Dissemination and back to Direction. Direction is the tasking stage of the process and directly links to Tasking and Co-ordination, **9 Tasking and Co-ordination**.

The analysis component of the intelligence cycle identifies facts and draws conclusions and inferences from the information, making recommendations for further data collection, reduction opportunities or enforcement activity. These findings are disseminated in written form or through verbal briefings with accompanying charts and maps. The outcome of the cycle may lead to further tasking in response to the findings and is, therefore, a continuous process.

The aim of crime analysis is to interpret a range of information to develop inferences, which are conclusions about what is known or what is believed to be happening. In order to develop a greater understanding of a problem, an inference will attempt to answer questions such as:

- Who are the key individuals?
- What are the key criminal activities?
- When, where and how are these criminals taking part in these activities?
- Why?

This will enable the analyst to proactively identify problems and targets which may include crime series, hotspots, key networks or markets, and high-risk issues.

These inferences can then be fed into the tasking and co-ordination process via the intelligence products. For example, inferences in the tactical assessment should be fed into the weekly intelligence unit meeting, see **9 Tasking and Co-ordination**, so that that specialists can collaborate with the intelligence unit to identify prevention, intelligence and enforcement recommendations. These recommendations are then disseminated via the tactical assessment for action at the TT&CG.

Figure 3 The Eleven Elements of NIM (continued)

Research and development culminates in the development of four types of intelligence product, which are outlined below. Intelligence products are closely associated with tasking and co-ordination, see **9 Tasking and Co-ordination**, and they are commissioned by the chair of the Tasking and Co-ordination Group.

8 INTELLIGENCE PRODUCTS	
<b>Strategic Assessment</b>	<p><b>Description:</b></p> <p>This product, which is created every twelve months, drives the business of the Strategic Tasking and Co-ordination Group (ST&amp;CG), see <b>9 Tasking and Co-ordination</b>. It provides an assessment of the current, emerging and long-term issues affecting a BCU, force or region. The strategic assessment will make key judgments and recommendations concerning the direction of future policing strategy and tactics. It is then used to set a control strategy and intelligence requirement, see <b>9 Tasking and Co-ordination</b>.</p>
<b>Tactical Assessment</b>	<p><b>Description:</b></p> <p>This product, which is created every fortnight, drives the business of the Tactical Tasking and Co-ordination Group (TT&amp;CG), see <b>9 Tasking and Co-ordination</b>. The assessment identifies the shorter-term issues in a police force, BCU or region in accordance with the control strategy. It defines problems and targets, and suggests recommendations for tactical resolution, see <b>10 Tactical Resolution</b>, to be considered for tasking at the TT&amp;CG. The TT&amp;CG also uses the assessment to amend the intelligence requirement where necessary.</p>
<b>Problem Profiles</b>	<p><b>Description:</b></p> <p>A problem profile is a report produced during a detailed investigation of a problem faced within a force, BCU or region. It is used to gain a greater understanding of a problem, and to target the problem tactically through prevention, intelligence and enforcement opportunities, see <b>10 Tactical Resolution</b>. A problem profile is a continuously evolving product which is added to and updated until the problem is resolved. It is then stored to enable retrieval if the problem reoccurs.</p>
<b>Subject Profiles</b>	<p><b>Description:</b></p> <p>A subject profile (formerly known as a 'target profile') is a report produced during a detailed investigation of a subject (suspect or victim). It is used to gain a greater understanding of an individual and to target or protect the individual(s) through prevention, intelligence and enforcement opportunities. The subject profile is a continuously evolving product which is added to and updated until the subject is apprehended or protected. It is then stored to enable it to be retrieved, especially if the subject reoffends.</p>

Figure 3 The Eleven Elements of NIM (continued)

**9 TASKING AND CO-ORDINATION**

**Description:**

The purpose of tasking and co-ordination is to make and communicate decisions based on the development of intelligence products, see **8 Intelligence Products**. Staff should be aware that tasking and co-ordination processes are associated with five types of meetings, which are outlined below. The outcome of these meetings will impact on the work that is assigned to staff through taskings and briefings. For further information on briefings, see *ACPO (2006) Guidance on the National Briefing Model*. Tasking and co-ordination will also include the setting, reviewing and revision, where necessary, of a control strategy and intelligence requirement. The purpose of the control strategy is to prioritise the work of the BCU, force or region according to an agreed, manageable range of issues against which resources can be allocated for the forthcoming twelve months. There will be significant issues that do not appear on the control strategy. This does not mean that they cannot be dealt with, but control strategy issues should be given priority when resources are allocated. The intelligence requirement is simply a series of facts that are required, or questions that need answering, about policing problems. The purpose of an intelligence requirement is to gain more information about crime and disorder problems. The intelligence requirement will direct staff to focus on key areas, but it should not prevent them from collecting information on a wide range of issues. For example, a control strategy priority may be to focus on theft from motor vehicles, while the intelligence requirement could be to find likely disposal points for the property stolen from such crimes. Control strategies are likely to remain constant throughout a current strategic assessment period, however, intelligence requirements will be constantly reviewed and amended where necessary.

**Impact on Staff:**

The decisions made during the tasking and co-ordination process influence all policing activity. These decisions, in conjunction with those made during the tactical resolution, see **10 Tactical Resolution**, will determine the nature of the tasks that are communicated to staff through briefings.

**Tasking and Co-ordination Meetings:**

Strategic Tasking and Co-ordination Group (ST&CG) – The ST&CG meets every twelve months to set the control strategy and intelligence requirement based on the strategic assessment, see **8 Intelligence Products**. Senior managers from the Police Service and partner agencies attend this meeting and will decide on resource allocation and strategic ownership to meet the needs of the control strategy and intelligence requirement.

Tactical Tasking and Co-ordination Group (TT&CG) – The TT&CG meets every two weeks and it is driven by the tactical assessment, see **8 Intelligence Products**. Intelligence staff meet on a weekly basis to discuss and agree the content of the tactical assessment. The control strategy is used by the TT&CG to prioritise issues highlighted in the tactical assessment and, if necessary, it will also review the intelligence requirement. The TT&CG will then decide on the best methods for dealing with prioritised crime and non-crime problems. This process is called tactical resolution, see **10 Tactical Resolution**. Once this is done, plan owners are identified and relevant resources are allocated. As with the ST&CG, partners will attend and contribute to TT&CG meetings.

**9 Tasking and Co-ordination** *continued overleaf*

Figure 3 The Eleven Elements of NIM (continued)

### 9 Tasking and Co-ordination *continued*

Intelligence Unit Meetings (IUMs)– The intelligence unit meets on a weekly basis to develop the tactical assessment and consider options for tactical resolution prior to the TT&CG. The weekly meeting will include input from analysts and others, for example, plan holders, neighbourhood policing teams, crime investigators, crime management units and response policing. The intelligence unit also meets on a daily basis to provide relevant information to the daily management meeting.

Daily Management Meetings (DMMs) – These meetings consider the incidents and actions which have occurred, or may occur, over a twenty-four hour period in line with the control strategy and the requirements of the TT&CG. To achieve this, relevant information from the intelligence unit is passed to the DMM on a daily basis. In addition to this work, the DMM can also make decisions on issues that arise at short notice, for example, to act on important intelligence that has been received from staff during a shift.

Neighbourhood Co-ordination Meetings (NCMs) – The introduction and roll-out of neighbourhood policing has added an additional tasking and co-ordination function to NIM. NCMs are held to address local crime, disorder and neighbourhood priorities. The results of these meetings will be addressed at TT&CG meetings. For further information on the neighbourhood co-ordination process, see *ACPO (2006) Practice Advice on Tasking and Co-ordination*.

The final two elements of NIM outline the tactical options for resolving problems, and how evaluation is conducted to ensure that chosen interventions work. Briefing and debriefing are important processes in ensuring these elements are communicated to staff and subsequently evaluated. For further information see *ACPO (2006) Guidance on the National Briefing Model*.

## 10 TACTICAL RESOLUTION

### Description:

The purpose of tactical resolution is to identify the relevant tactics that can resolve a crime or non-crime problem. This is achieved by identifying any relevant Prevention, Intelligence and Enforcement (PIE) opportunities that will help resolve a problem. The nature of the problem will dictate which elements of PIE are most appropriate – it is possible that all three are relevant. Partners and community groups will also be involved in contributing to this process.

Specialists and plan owners will meet with staff from the intelligence unit to discuss and recommend relevant tactical resolutions arising from the tactical assessment, see

**8 Intelligence Products**. These recommendations are then discussed and actioned to individuals at the TT&CG.

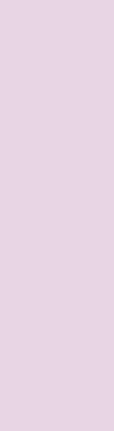
### Impact on Staff:

Tasking and co-ordination processes prioritise crime and non-crime problems that require action. Tactical resolution identifies the action necessary to resolve problems. These two processes direct the day-to-day activities of staff. This is achieved through briefing and task allocation which may consist of conducting prevention, intelligence and/or enforcement-related duties.

Staff will be tasked to carry out actions or contribute to the tactical resolution process, depending on their own areas of expertise. Staff from a neighbourhood policing team, for example, could be tasked to execute a search warrant, or asked to recommend potential prevention opportunities in relation to an identified and prioritised problem.

Figure 3 The Eleven Elements of NIM (continued)

11 OPERATIONAL REVIEW
<p data-bbox="730 376 865 405"><b>Description:</b></p> <p data-bbox="331 423 1230 517">This final element of NIM is concerned with evaluating the effectiveness of tactical activity on identified problems and targets. This is done through a number of processes including results analysis and debriefing. The aim of results analysis is to determine, for example:</p> <ul data-bbox="360 535 1262 725" style="list-style-type: none"><li data-bbox="360 535 1177 595">– The impact of tactical activity on a problem or subject (eg, were objectives met successfully?);</li><li data-bbox="360 600 1262 660">– The nature of any repercussions (eg, the impact of unintentional side effects associated with tactical activity);</li><li data-bbox="360 665 1187 725">– Conclusion and recommendations (eg, what did and did not work in relation to resolving the problem, and why?).</li></ul> <p data-bbox="331 743 1262 869">This information forms part of the organisational memory which includes, for example, a database of which tactics have worked, impact assessments, results analysis, debriefing records and performance outcomes. These can be consulted when dealing with future crime and non-crime problems.</p> <p data-bbox="708 887 887 916"><b>Impact on Staff:</b></p> <p data-bbox="331 920 1227 1014">Staff will contribute to the operational review through debriefing. Debriefing should be conducted after completing a task and/or shift to capture progress made and any lessons learned.</p> <p data-bbox="331 1032 1262 1126">Staff must also be made aware of where operational review information is held. This information should then be referred to when staff are assigned a task as it could offer useful recommendations on how the task could be carried out effectively.</p>



# Section 2

## SOURCES OF INFORMATION

**T**his section presents examples of different sources of information that staff have access to in their day-to-day roles. It also describes how information, deemed sensitive or confidential, should be managed.

### CONTENTS

2.1	What Is Police Information? .....	18
2.2	Types of Sources .....	18
2.3	The Collection of Information .....	19
2.4	Dealing with Human Sources of Information .....	20
2.5	Sensitive Sources .....	20
2.6	Frequent Contact .....	21
2.7	Tasking Sources .....	21
2.8	What Is a CHIS? .....	22
2.9	Recognising Issues Related to CHIS .....	22

## 2.1 WHAT IS POLICE INFORMATION?

The police gather information that is required for a policing purpose. Policing purposes 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.

These five policing purposes provide the legal basis for collecting, recording, evaluating, sharing and retaining police information. They will include information relating to key policing functions such as crime investigation, racial and community tension, anti-social behaviour, roads policing, public order, counter-terrorism, or protection of children and other vulnerable groups. For further information on police information, ranging from community information through to information in relation to serious crime, see *ACPO (2006) Guidance on the Management of Police Information* and *ACPO (2006) Practice Advice on Professionalising the Business of Neighbourhood Policing*.

Intelligence management involves linking information from a wide range of sources in order to fulfil an intelligence requirement (see **Figure 3, 9 Tasking and Co-ordination**). This will include publicly available information, and information that is obtained covertly. This allows the police to highlight links between people, objects, locations and events that are essential in supporting the policing purposes described.

Identifying these links enables decisions to be made about the priorities and resources needed to manage risk and provide an efficient and effective service.

## 2.2 TYPES OF SOURCES

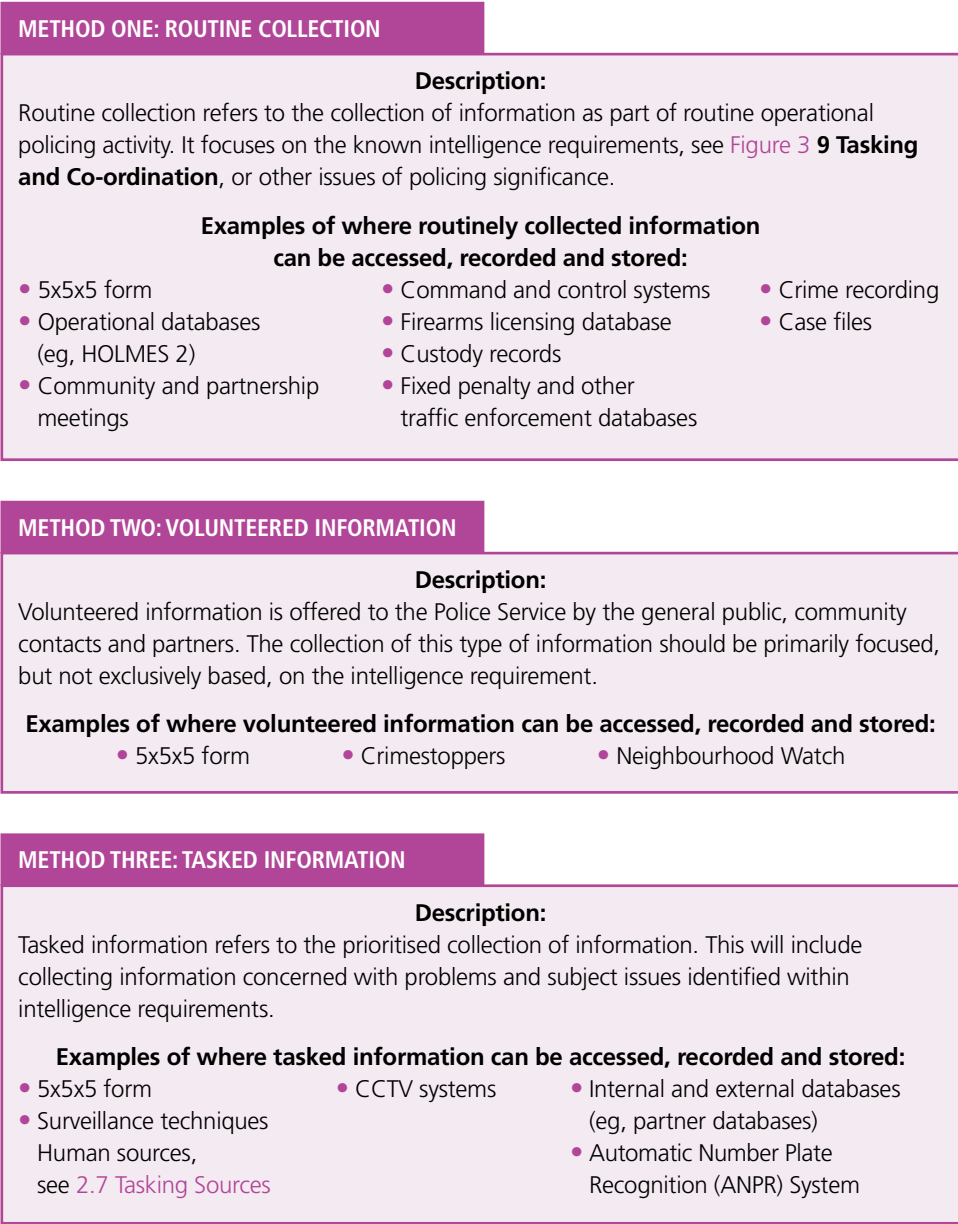
Before searching for and obtaining information, staff should consider the type of information that may be available and the likelihood of it having value as intelligence. This may be achieved by referring to current BCU or force intelligence requirements. This should not, however, prevent staff from submitting information that is required for a policing purpose but may not be contained in the relevant intelligence requirement. Sources of information available to the Police Service include:

- Victims and witnesses;
- Communities and members of the public;
- Crimestoppers;
- Prisoners;
- Covert Human Intelligence Sources (CHIS);
- Covert operations, eg, surveillance;
- CCTV and Automatic Number Plate Recognition (ANPR);
- Crime and disorder reduction partnerships;
- Commercial agencies, eg banks and credit card agencies;
- Fixed Penalty Tickets database;
- Forensic Science Service (FSS);
- Internet – Open Sources (eg, <http://www.homeoffice.gov.uk>)
- Media;
- NCPE Opsline;
- Neighbourhood Watch Scheme;
- Police IT systems, eg, Police National Computer (PNC);
- Other law enforcement agencies, eg, Serious Organised Crime Agency (SOCA);
- Primary Care Trusts (PCTs);
- Local Education Authorities (LEAs);
- National Firearms License Management System (NFLMS).

## 2.3 THE COLLECTION OF INFORMATION

There are three different methods commonly associated with the collection of information: routine, tasked and volunteered. These methods are presented in [Figure 4](#). Whatever the information collection method, staff should be aware that in some circumstances the source of the information may need to be treated in confidence or in a sensitive manner.

Figure 4 Three Methods for Collecting Information



## 2.4 DEALING WITH HUMAN SOURCES OF INFORMATION

It is the duty of the Police Service to openly engage with the community in order to gather information about issues which affect a BCU or force. Effective community engagement gives the public confidence when providing the police with information and encourages them to assist the police when required. This is a civic, rather than a legal, duty. The police have, in turn, a duty of care to protect the confidentiality of an individual who provides them with information. It is, however, recognised that some individuals may be at additional risk because of their personal or professional circumstances.

Where an increased risk of harm is so great, specific action must be taken. Such situations may include the following:

- The nature of the information, the way it was obtained, or the circumstances of the person providing the information indicates that the information should be treated in confidence or in a sensitive manner, see [2.5 Sensitive Sources](#).
- The frequency of contact between an individual and the police indicates that the information should be treated in confidence or in a sensitive manner, or that the individual may be maintaining a relationship in order to obtain that information, see [2.6 Frequent Contact](#).
- A member of the public has been tasked to provide the information by a member of staff, see [2.7 Tasking Sources](#). This does not include the requirement to provide statements or the completion of diaries to record witness or victim experiences of a particular problem.

## 2.5 SENSITIVE SOURCES

Information of intelligence value may sometimes need to be handled with a high level of confidentiality and sensitivity, for example:

- Because of the vulnerable environment in which an individual lives (eg, a person living in an area with a history of witness intimidation);
- Due to the individual's close proximity to the subject of the information (eg, a family member, neighbour or employee);

OR

- During the deployment of technical or other surveillance activity, and for any resulting material.

For further information on dealing with sensitive sources, see [Figure 5](#).

## 2.6 FREQUENT CONTACT

Individuals or organisations, for example, travel agents, housing associations and taxi companies, who, because of their work or role have access to personal information, may provide information to the police on a repeated basis. They, therefore, need to be managed appropriately. These individuals or organisations may have previously been referred to as confidential contacts or trade sources. This terminology is no longer recognised.

Information provided by individuals or organisations on a repeated basis are now referred to as frequent contacts. A review by the intelligence unit must take place after an individual or organisation has had a maximum of three repeated contacts with the police.

The purpose of the review is to determine whether an individual or organisation:

- Is being managed with an appropriate level of sensitivity and confidentiality;
- Should be considered for registration as a CHIS.

There is no specified time period to becoming a frequent contact. Determining the status of an individual or organisation is a matter of judgement by the intelligence unit and will be considered in consultation with the reporting member of staff.

Individuals who are deemed suitable for registration as a covert human intelligence source will be referred to a dedicated source unit (DSU). DSUs are resourced by specialist staff who are trained to manage covert human intelligence sources.

It is important that all staff are aware of these issues concerning frequent contact. This will help avoid the potential implications of status drift, which could include breaches of the Regulation of Investigatory Powers Act 2000 and the Human Rights Act 1998.

'There are clearly other ways in which a source may over time develop and change in the way in which he obtains the information he provides so as to fall within the statutory definition of a CHIS. It is vitally important that such a change [status drift] is identified, and the source authorised and thereafter properly managed and controlled.'

*Butterfield Review, 2003, Paragraph 10.79*

## 2.7 TASKING SOURCES

Asking a member of the public to provide information that is within their knowledge, for example, maintaining a diary of events or providing witness evidence does not require any specific authorisation.

The risk to an individual is greatly increased when, without disclosing their true intentions (ie, to obtain information and then pass it on to the police), they start or maintain a relationship with someone in order to obtain or access information which they then pass on to the police, without the knowledge of their source.

If a member of staff identifies that such a situation has occurred, or where tasking someone in these circumstances would be useful, they must seek advice from, for example, the DSU as this person is likely to require authorisation as a CHIS. Trained covert source handlers will then take responsibility for assessing their suitability as a CHIS.

## 2.8 WHAT IS A CHIS?

A CHIS represents a potentially useful source of information and a valuable tool for law enforcement. All staff must have a basic understanding of how, and under what circumstances, someone becomes a CHIS.

The legal definition of a CHIS is provided by the Regulation of Investigatory Powers Act 2000.

### **Section 26(8) of RIPA classifies a person as a covert human intelligence source (CHIS) if:**

- (a) he establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph (b) or (c);
- (b) he covertly uses such a relationship to obtain information or to provide access to any information to another person; or
- (c) he covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

### **Section 26(9) of RIPA defines a covert relationship as follows:**

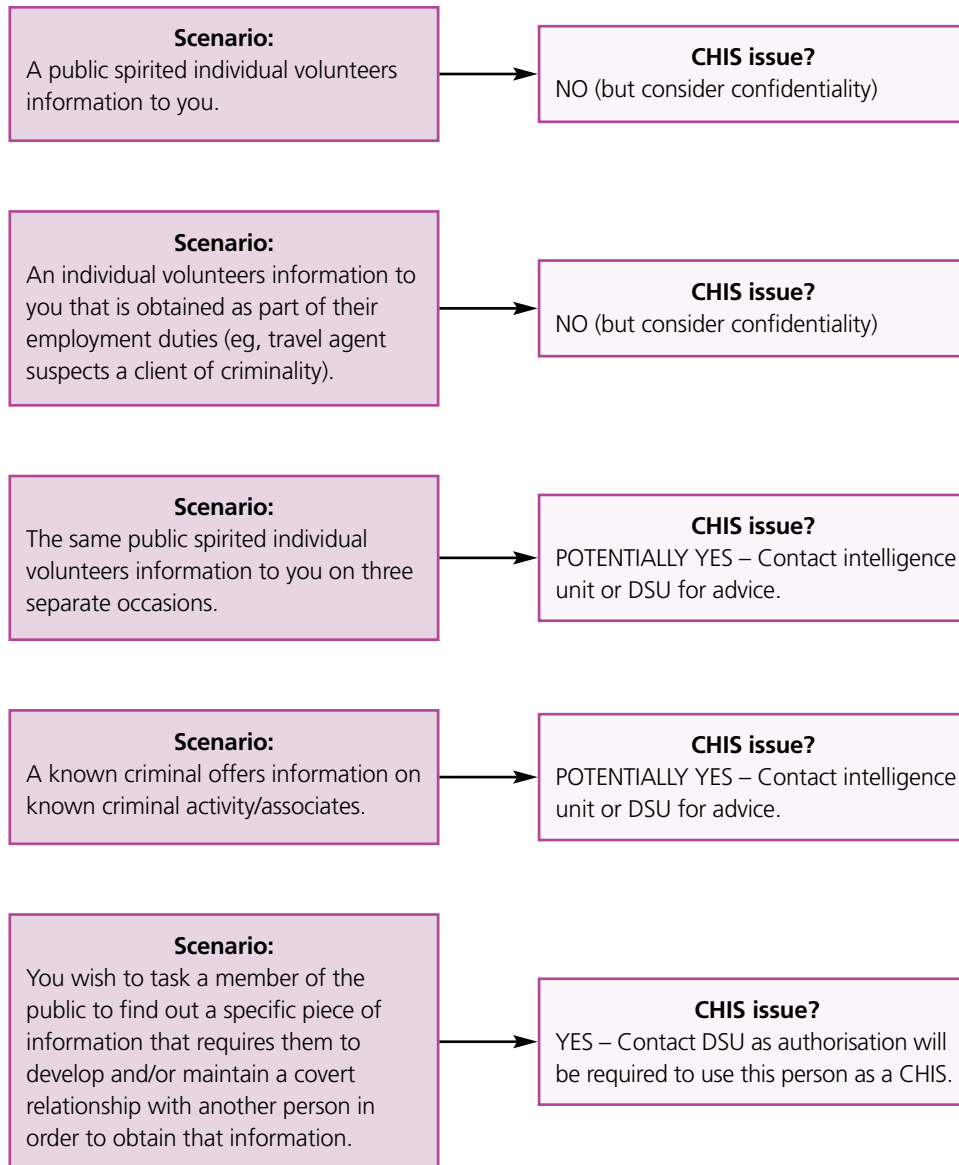
- (c) a relationship is used covertly, and information obtained as mentioned in subsection (8)(c) is disclosed covertly, if and only if it is used or, as the case may be, disclosed in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the use or disclosure in question.

It is the actions of the individual, on behalf of a law enforcement agency and in the manner described, that constitutes their status as a source that requires authorisation. Merely providing information to a law enforcement agency that is already within the individual's possession does not necessitate authorisation.

## 2.9 RECOGNISING ISSUES RELATED TO CHIS

The key issue for staff relates to identifying a potential CHIS. [Figure 5](#) overleaf outlines different situations that staff may face in their day-to-day duties, along with whether the source of the information holds potential CHIS status. If someone is potentially a CHIS, further advice should be sought from the intelligence unit or DSU.

Figure 5 Identifying CHIS Status



CHIS awareness training is available for all non-specialist staff. This is currently delivered through the Initial Police Learning and Development Programme (IPLDP) to all student officers. Advice regarding the identification of a potential CHIS can be obtained from any DSU or Central Authorities Bureau that has access to *ACPO (2006) Guidance on the Management of Covert Human Intelligence Sources*. This is a RESTRICTED document.



# Section 3

## THE 5x5x5 PROCESS

**T**his section details the processes associated with the 5x5x5 form.

### CONTENTS

3.1	What Is a 5x5x5 Form? .....	26
3.2	When Should a 5x5x5 Be Used? .....	26
3.3	How to Complete the 5x5x5 .....	27
3.3.1	Reporting Member of Staff .....	27
3.3.2	Person Providing Information (Source) .....	27
3.3.3	Source Evaluation .....	28
3.3.4	Information/Intelligence Evaluation .....	29
3.3.5	Completing the Report .....	30

### 3.1 WHAT IS A 5x5x5 FORM?

The 5x5x5 is the national Information/Intelligence Report which allows the Police Service and other agencies to record, evaluate and disseminate information. A 5x5x5 can also be used to assess the risk of exposure to the source of the information or to the use of the material and, therefore, protect the individual or police operation to which the information relates to. The use of a 5x5x5 also starts an audit trail and ensures consistency between forces, thus enabling them to share intelligence more easily.

The 5x5x5 consists of three forms:

<b>Form A</b>	Information/Intelligence Report which covers the three elements of: <ul style="list-style-type: none"> <li>• Source evaluation;</li> <li>• Information/intelligence evaluation;</li> <li>• Handling code.</li> </ul> This form also contains risk management processes.
<b>Form B</b>	Information/Intelligence Report continuation form.
<b>Form C</b>	A further risk assessment process. This is a more comprehensive risk assessment record that is used in particular circumstances where the handling codes alone are not sufficient to manage the risk of dissemination of the information.

A template of the 5x5x5 Information/Intelligence Report is presented in [Appendix 1](#).

### 3.2 WHEN SHOULD A 5x5x5 BE USED?

The 5x5x5 should be used to record any information for a policing purpose that is generally not recorded on other systems. The 5x5x5 can be used during routine, volunteered and tasked information collection, see [2.3 The Collection of Information](#). Examples of when to use a 5x5x5 include:

- Information given to the police, in confidence, by a member of the public;
- Information from anonymous sources, for example, Crimestoppers, Anti-Terrorism Hotline;
- Information of a personal or confidential nature received from someone who has access to it because of their occupation, for example, hotel, airline, ticket office or currency exchange staff;
- Sanitised information derived from a CHIS, see [2.8 What is a CHIS?](#);
- Sanitised information obtained by covert means, for example, the product of technical or other surveillance activity;
- Information from other law enforcement agencies that is supplied in confidence, or is from a sensitive source (and would, therefore, be recorded on a 5x5x5 had it originated from the Police Service);
- Information from liaison with other partner agencies, for example, Crime and Disorder Reduction Partnerships, Youth Offending Teams;
- Information obtained by police officers and staff in the course of their duties, for example, patrol officers, front desk staff, PCSOs and interviewing officers.

The 5x5x5 should not generally be used when information is recorded through other systems, for example:

- Crime reports;
- Incident records;
- Custody records;
- Neighbourhood problem-solving file.

Other examples of when to use the 5x5x5, however, may include recording the following information:

- Reasons for the revocation of a firearms licence;
- Details about a person who may be a risk to children or vulnerable adults;
- Details about a known or suspected domestic violence perpetrator;
- Allegations of threats to life or of serious harm;
- Details of potentially dangerous people who pose a threat to the public;
- Where it is necessary to restrict or control the subsequent dissemination of the information;
- Information contained in other formats, for example, crime reports, custody records and case files, that may not be readily searchable or identifiable as having relevant intelligence value.

The 5x5x5 report contains basic details identifying the person completing and submitting the report. It also contains the time and date of submission and, if a paper copy is used, the signature of the person submitting the report will also be included. Electronic submission of a 5x5x5 usually contains automatic identifiers and does not, therefore, require a signature. An audit trail of the information recorded on the 5x5x5 is essential and all staff **must** ensure that these details are completed.

### 3.3 HOW TO COMPLETE THE 5x5x5

Staff should follow the process outlined below when completing a 5x5x5 form. This will ensure it is accurate and comprehensive. This section should also be read in conjunction with the template that is provided in [Appendix 1](#).

#### 3.3.1 REPORTING MEMBER OF STAFF

The person completing the 5x5x5 must record their name and organisation. The time and date of the submission must also be recorded. These details are important for auditing purposes and a potential evidential chain.

#### 3.3.2 PERSON PROVIDING INFORMATION (SOURCE)

The identification of the source of the information can either be the name and address of the person providing the information, if appropriate, or a unique intelligence source reference (ISR) number, where increased risk has been identified, see [2.4 Dealing with Human Sources of Information](#). Details of the person providing the information should be placed in these sections and not in the body of the text of the report.

Providing this information on the 5x5x5 allows for transparency in the possible identification of an unauthorised CHIS and also for the continuation of the audit trail. For advice on obtaining an ISR contact the local intelligence unit. A 5x5x5 report derived from sensitive sources such as a CHIS, covert or technical deployments and surveillance, will always use an ISR.

### 3.3.3 SOURCE EVALUATION

Source reliability refers to the assessment made of the person, agency or technical equipment providing the information or intelligence. The source reliability is initially assessed by the person recording the information and should be completed in all circumstances. The source evaluation, however, is not a static process and must be subject to constant review. This will affect the whole of the information management process, in particular sharing information and the need for retaining it. The assessment of the source must be accurate as it will affect both the evaluation of the information recorded, and the potential action of that information as intelligence. The 5x5x5 provides five gradings for source evaluation, see Figure 6.

Figure 6 Gradings for Source Evaluation

#### **A – ALWAYS RELIABLE**

There is no doubt about the authenticity, trustworthiness and competence of the source. Information has been supplied in the past and has proved to be reliable in all instances. This grading should only apply to cases where reliability can be assured. It will NOT be used frequently as a source evaluation.

**Example:** this could include information received from technical products, eg, DNA, interceptions, fingerprints. **This does not include information received from officers or staff, as they are subject to human error.**

#### **B – MOSTLY RELIABLE**

Information has been received from this source in the past and in the majority of instances has proved to be reliable. This could be the majority of law enforcement and other prosecuting agencies.

**Example:** information received from police officers, covert human intelligence sources and agencies, eg, United Kingdom Immigration Service (UKIS).

#### **C – SOMETIMES RELIABLE**

Some of the information received from this source has proved to be both reliable and unreliable. Any information with this grading should generally not be acted on without corroboration. Where a potential risk demands a response, the intelligence manager will need to obtain as much corroboration as possible before commissioning action.

**Example:** this grading may apply to CHISs or information received from the media or product of a technical deployment where the quality of the product is poor.

#### **D – UNRELIABLE**

Information under this grading will refer to individuals who have provided information in the past which has routinely proved unreliable. There may be some doubt regarding the authenticity, trustworthiness, competency or motive of the source. Any information with this grading should not be acted on without corroboration.

**Example:** this grading could apply to information received from members of the public with a potentially malicious motive, eg, in neighbourhood disputes, or to information received from an individual with a history of making false allegations.

#### **E – UNTESTED SOURCE**

This grading refers to information received from a source that has not previously provided information to the person recording. The information may not necessarily be unreliable but it should be treated with caution. Corroboration of this information should be sought.

**Example:** this grading will usually apply to members of the public, and the majority of information received from Crimestoppers.

### 3.3.4 INFORMATION/INTELLIGENCE EVALUATION

It is essential that any information received or recorded must be evaluated for reliability. The evaluation will involve using an objective professional judgement, and the value of the information must not be exaggerated to encourage action to be taken. The assessment of the reliability of the information will be based on the person recording it and their knowledge of the circumstances at that time. The 5x5x5 provides five information/intelligence evaluation gradings, see Figure 7.

Figure 7 Gradings for Information/Intelligence Evaluation

#### 1 – KNOWN TO BE TRUE WITHOUT RESERVATION

This could be information generated from a technical deployment or an event which was witnessed by a law enforcement officer or prosecuting agency. Information received from technical deployments must be treated with caution as the information may have been recorded accurately but the content may be misinterpreted. This grading refers to first-hand information.

**Example:** an officer witnessed an incident or refers to live evidence.

#### 2 – THE INFORMATION IS KNOWN PERSONALLY BY THE SOURCE BUT NOT TO THE PERSON REPORTING

Information under this grading will be believed to be true by the source although is not personally known by the person recording the information. The information is provided second-hand.

**Example:** a CHIS giving information which they know of first-hand, to the person recording the information.

#### 3 – THE INFORMATION IS NOT KNOWN PERSONALLY TO THE SOURCE BUT CAN BE CORROBORATED BY OTHER INFORMATION

Information given may have been received by a source from a third party; its reliability has been corroborated by other information, eg, CCTV, other force systems.

**Example:** a CHIS has been told that Michael Brown has been seen driving a car, registration number ABC 123. The PNC checks that Michael Brown is the registered keeper of car registration number ABC 123.

#### 4 – THE INFORMATION CANNOT BE JUDGED

The reliability of this information cannot be judged or corroborated. Information with this grading must be treated with caution.

**Example:** anonymous information received from members of the public that a crime has occurred but it is not possible to corroborate.

#### 5 – SUSPECTED TO BE FALSE

Information with this grading should be treated with extreme caution. This information should be corroborated by a reliable source before any action is taken. Any person applying this grade must justify within the body of the report why it is appropriate to use this grading.

**Example:** malicious/non-malicious callers or a CHIS, who is engaged in criminal activity and provides exaggerated information against others in order to deflect attention from themselves, or to prepare a defence of working for the police should they be arrested.

### 3.3.5 COMPLETING THE REPORT

---

#### **Government Protective Marking Scheme (GPMS)**

Once the 5x5x5 has been completed, it needs to be allocated an appropriate level of protective marking. The majority of information/intelligence held within the Police Service contains personal or sensitive data. This data, therefore, needs a level of protective marking and this is normally RESTRICTED. For further information on the GPMS, see *ACPO, ACPOS, PITO and NPT (2001) Handing of Protectively Marked Material – A Guide for Police Personnel*.

#### **Information Content**

This refers to the body of the text within the report. The information provided must be clear, concise and without abbreviations. The report should contain all information, whether or not the person submitting it believes it to be relevant. Where possible, the information should be corroborated and provenance established by cross-checking with other systems. For example, Michael Brown is confirmed on the PNC as being the registered keeper of a red Ford Escort car registration number ABC 123.

The information content will commence with the full name of the subject nominal, if known, together with their date of birth and/or age and, where possible, any national identification number, eg, National Identification Bureau Criminal Records Office number. For ongoing operations the operational name or number may be added. Having identified who the information relates to, it should then clearly describe what is likely to occur, where, when, why and how, if known. If this information is not known, then this fact should be clearly stated.

Information from the same source but concerning totally different issues should be recorded on separate information/intelligence reports. A 5x5x5 report may, nevertheless, contain several items of information relevant to a single issue but they must all come from the same source. This is particularly important when intelligence reports are prepared from a sensitive source, for example, a CHIS or a technical device. The purpose of this procedure is to ensure that an adverse decision on disclosure of a 5x5x5 would only put a single sensitive source or a single record at risk of compromise.

#### **Sanitisation**

Sanitisation of information occurs when material is removed which explicitly or implicitly identifies a source. It also occurs when identifying details of a data subject are removed. This process will be undertaken by the intelligence unit prior to the dissemination or inputting onto an intelligence system. Staff can help this process, however, by ensuring that only relevant information is included in the 5x5x5.

#### **Handling Codes**

Handling codes are designed to provide an initial risk assessment prior to recording material into an intelligence system. Staff completing the 5x5x5 will not generally complete the handling code unless they are involved in the intelligence discipline as, for example, trained intelligence officers or specialists. The handling codes allow recording staff and others involved in the dissemination of intelligence material to clearly record their decisions on the suitability, or otherwise, of sharing the intelligence with other parties. If, however, the person submitting the 5x5x5 has specific concerns over disseminating the information (eg, ethical, personal or operational risks), Risk Assessment Form C should be completed. For guidance on when and how to complete Risk Assessment Form C, contact the local or force intelligence unit.

### Submission of the 5x5x5

The timely submission of recorded information will ensure that intelligence systems are kept up to date. Once information has been recorded on a 5x5x5, the report should be submitted to the local or force intelligence unit by secure electronic or manual means. It will then be considered for its intelligence value based on research, source reliability, the content of the information and its actionable value against the BCU or force control strategy, intelligence requirement or other policing purpose.

### Priority Assessments

The intelligence unit will conduct a priority assessment once information from the submitted 5x5x5 has been reviewed. Information will be assessed as being of a HIGH, MEDIUM or LOW priority and will be actioned accordingly. There are occasions, however, when staff may receive information that indicates:

- A risk of death and/or serious harm;
- A serious crime is about to be committed.

**Example:** A reliable source states that Michael Brown, a known offender, has a shotgun (confirmed on the firearms licensing register) and intends to go out that same evening to shoot Simon Smith. The name of the victim is known, the name of the offender is known and there is, potentially, a public and officer safety issue here.

This situation potentially becomes one of immediate response and, therefore, a command and control issue. Staff should bring the information to the attention of an appropriate supervisor immediately, in order for it to be actioned. Such an incident or information report would also receive high priority action to ascertain the accuracy of the content and any supporting intelligence.



# APPENDIX 1

## 5x5x5 TEMPLATE

## Template 1

NOT PROTECTIVELY MARKED UNTIL COMPLETED

<b>GPMS:</b>	<b>RESTRICTED</b> <input type="checkbox"/>	<b>CONFIDENTIAL</b> <input type="checkbox"/>	<b>SECRET</b> <input type="checkbox"/>
--------------	--	--	--

### 5x5x5 Information Intelligence Report Form A

ORGANISATION AND OFFICER	DATE/TIME OF REPORT
INFORMATION/INTELLIGENCE SOURCE/INTELLIGENCE SOURCE REF NO. (ISR)	REPORT URN

**SOURCE AND INFORMATION/INTELLIGENCE EVALUATION TO BE COMPLETED BY SUBMITTING OFFICER**

SOURCE EVALUATION	A Always Reliable	B Mostly Reliable	C Sometimes Reliable	D Unreliable	E Untested Source
INFORMATION/INTELLIGENCE EVALUATION	1 Known to be true without reservation	2 Known personally to the source but not to the person reporting	3 Not known personally to the source, but corroborated	4 Cannot be judged	5 Suspected to be false

**REPORT**

PERSON RECORD: <input type="checkbox"/>	DoB: <input type="checkbox"/>	NIB CRO: <input type="checkbox"/>
---	-------------------------------	-----------------------------------

OPERATION NAME/NUMBER: <input type="checkbox"/>	S	I	H

**INTELLIGENCE UNIT ONLY**

HANDLING CODE	1	2	3	4	5
To be completed by the evaluator on receipt and prior to entry onto the intelligence system.  <b>To be reviewed on dissemination.</b>	<b>Default:</b> Permits dissemination within the UK police service AND to other law enforcement agencies as specified  [see guidance]  <input type="checkbox"/>	Permits dissemination to UK non prosecuting parties  [conditions apply see guidance]  <input type="checkbox"/>	Permits dissemination to (non EU) foreign law enforcement agencies  [conditions apply see guidance]  <input type="checkbox"/>	Permits dissemination within originating force/agency only: specify reasons and internal recipient(s) Review period must be set  [see guidance]  <input type="checkbox"/>	Permits dissemination but receiving agency to observe conditions as specified  [see guidance on risk assessment]  <input type="checkbox"/>

5x5x5 REVIEWED BY: RE-EVALUATED: Yes <input type="checkbox"/> No <input type="checkbox"/>	CROSS-REF URN:	TIME/DATE OF REVIEW:
--	----------------	----------------------

DISSEMINATED TO:	PERSON DISSEMINATING TIME/DATE:
------------------	---------------------------------

DETAILED HANDLING INSTRUCTIONS:	PUBLIC INTEREST IMMUNITY:
---------------------------------	---------------------------

INPUT ON TO AN INTELLIGENCE SYSTEM Yes  No

SIGNATURE (PAPER COPY):

<b>GPMS:</b>	<b>RESTRICTED</b> <input type="checkbox"/>	<b>CONFIDENTIAL</b> <input type="checkbox"/>	<b>SECRET</b> <input type="checkbox"/>
--------------	--	--	--

## Template 2

NOT PROTECTIVELY MARKED UNTIL COMPLETED

<b>GPMS:</b>	<b>RESTRICTED</b> <input type="checkbox"/>	<b>CONFIDENTIAL</b> <input type="checkbox"/>	<b>SECRET</b> <input type="checkbox"/>
--------------	--	--	--

### 5x5x5 Continuation Form B

INFORMATION/INTELLIGENCE SOURCE/INTELLIGENCE SOURCE REF NO. (ISR)	█	REPORT URN	█
<b>REPORT</b>			
<b>NOMINAL:</b> █	DoB: █	NIB CRO: █	
OPERATION NAME/NUMBER: █			<b>S</b>   <b>I</b>   <b>H</b>
<b>GPMS:</b>	<b>RESTRICTED</b> <input type="checkbox"/>	<b>CONFIDENTIAL</b> <input type="checkbox"/>	<b>SECRET</b> <input type="checkbox"/>

## Template 3

### Risk Assessment Form C

#### FOR USE IN THE DISSEMINATION OF INFORMATION/INTELLIGENCE

<b>1</b>	Does the information contain confidential material or sensitive material as identified in law?	<b>YES/NO</b>
<b>2</b>	If yes, are there any restrictions on use, or requirements for special handling, imposed by the person submitting the report?	<b>YES/NO</b>
<b>3</b>	<p>What are the ethical, personal or operational risks which are likely to result as a consequence of any dissemination or disclosure?</p> <p>Consideration must be given to the risk to the source and the content of information within the report.</p>	<b>DETAIL THE RISKS</b>
<b>4</b>	<p>What is the purpose of dissemination or disclosure?</p> <p>Is it for a policing purpose or a legislative requirement?</p>	
<b>5</b>	<p>Having identified the risks, justify the decision making process.</p> <p>This must include the justification, authority, proportionality, accountability and necessity of a dissemination or disclosure.</p>	
<b>FOR INTELLIGENCE UNIT ONLY</b>		
<b>6</b>	In light of the risk assessment is the Handling Code correct?	<b>YES/NO</b>
<b>Risk Assessment and Management Plan authorised by ..... (Intelligence Manager)</b>		<b>Person Completing Risk Assessment:</b>
<b>Cross-ref URN:</b>		<b>Time/Date:</b>

# APPENDIX 2

## STAFF RESPONSIBILITIES

### CHECKLIST

**T**his appendix details responsibilities for staff and team leaders and managers in respect of intelligence-led policing.

## Staff Responsibilities

To carry out day-to-day duties effectively, it is important that staff:

Know their local and force control strategies (as set by the ST&CG).	
Know their intelligence requirement and gather relevant information.	
Carry out TT&CG authorised tasks and report back on results.	
Ensure that all relevant information or intelligence from all routine policing activities is gathered.	
Ensure that all relevant intelligence obtained from offenders, including how and why the offences were committed, is gathered.	
Ensure that intelligence from all victim and witness statements is captured.	
Build relationships and routinely collect information from the community. This information and intelligence could come from many sources, for example, community leaders, schools, Neighbourhood Watch schemes or shopkeepers.	
Complete crime reports clearly and accurately to ensure information can be analysed effectively.	
Use the 5x5x5 form to record accurately and submit relevant information as soon as possible (always before the end of a shift) by:	
Completing all submission fields;	
Assessing the source and the information and applying the correct grading;	
Corroborating the information, where possible, eg, conduct PNC check;	
Evaluating and grading the information given;	
Completing text of the report;	
Using the correct GPMS marker, eg, RESTRICTED, CONFIDENTIAL (see <i>ACPO, ACPOS, PITO and NPT (2001) Handing of Protectively Marked Material – A Guide for Police Personnel</i> );	
If necessary, giving specific handling instructions and applying a risk assessment to the information (Form C must be attached and sent to the intelligence unit);	
Sending the report to the appropriate intelligence unit in line with force security policy.	

### Team Leaders' and Managers' Responsibilities

Team leaders and managers have additional responsibilities to make intelligence-led policing work effectively. These include:

Making sure that their staff have access to relevant knowledge assets, eg, <i>ACPO (2006) Guidance on the National Briefing Model</i> .	
Making sure that their staff are aware of the control strategy and intelligence requirement.	
Ensuring staff routinely gather information and intelligence from all sources and feed it into the system using 5x5x5 forms.	
Delivering briefings and debriefings that comply with the <i>ACPO (2006) Guidance on the National Briefing Model</i> .	
Ensuring that tasks are allocated to staff as part of the briefing and that these are rigorously followed up.	
Ensuring that tasks are completed within the specified timescale.	
Auditing tasks to ensure compliance, and sign off tasks after completion.	
Providing timely feedback to the local intelligence unit regarding the results of tasks and other intelligence.	
Providing an explanation to the TT&CG if tasks are not completed in the specified timescale.	
Conducting a real-time handover between teams/shifts to ensure that information and intelligence is passed on.	
Monitoring the quality of 5x5x5s submitted to ensure they are correctly completed, corroborated and graded.	
Monitoring the nature of the information submitted in 5x5x5s with regard to the BCU or force intelligence requirement and control strategy.	



# APPENDIX 3

## ABBREVIATIONS AND ACRONYMS

### ABBREVIATIONS AND ACRONYMS

<b>ACPO</b>	Association of Chief Police Officers
<b>ACPOS</b>	Association of Chief Police Officers in Scotland
<b>ANPR</b>	Automatic Number Plate Recognition
<b>BCU</b>	Basic Command Unit
<b>CCTV</b>	Closed Circuit Television
<b>CHIS</b>	Covert Human Intelligence Source
<b>CLDP</b>	Core Leadership and Development Programme
<b>DMM</b>	Daily Management Meeting
<b>DNA</b>	Deoxyribonucleic Acid
<b>DSU</b>	Dedicated Source Unit
<b>FIB</b>	Force Intelligence Bureau
<b>FSS</b>	Forensic Science Service
<b>GPMS</b>	Government Protective Marking Scheme
<b>HOLMES 2</b>	Home Office Large Major Enquiry System
<b>IPLDP</b>	Initial Police Learning and Development Programme
<b>ISR</b>	Intelligence Source Reference
<b>IUM</b>	Intelligence Unit Meeting
<b>LEA</b>	Local Education Authority
<b>NCM</b>	Neighbourhood Co-ordination Meeting
<b>NCPE</b>	National Centre for Policing Excellence
<b>NFLMS</b>	National Firearms License Management System
<b>NIM</b>	National Intelligence Model
<b>NPT</b>	National Police Training
<b>PCSO</b>	Police Community Support Officer
<b>PCT</b>	Primary Care Trust
<b>PIE</b>	Prevention Intelligence Enforcement
<b>PITO</b>	Police Information Technology Organisation
<b>PNC</b>	Police National Computer
<b>RIPA</b>	Regulation of Investigatory Powers Act 2000
<b>SOCA</b>	Serious Organised Crime Agency
<b>ST&amp;CG</b>	Strategic Tasking and Co-ordination Group
<b>TT&amp;CG</b>	Tactical Tasking and Co-ordination Group
<b>UKIS</b>	United Kingdom Immigration Service



# APPENDIX 4

## REFERENCES AND FURTHER INFORMATION

### REFERENCES

ACPO (2005) *Guidance on the National Intelligence Model*. Wyboston: NCPE.

ACPO (2006) *Guidance on the Management of Police Information*. Wyboston: NCPE.

ACPO (2006) *Guidance on the Management of Covert Human Intelligence Sources*. Wyboston: NCPE.

ACPO (2006) *Guidance on the National Briefing Model*. Wyboston: NCPE.

ACPO (2006) *Practice Advice on Professionalising the Business of Neighbourhood Policing*. Wyboston: NCPE.

ACPO (2006) *Practice Advice on Tasking and Co-ordination*. Wyboston: NCPE.

ACPO (forthcoming) *Analytical Tools and Techniques*. Wyboston: NCPE.

ACPO, ACPOS, PITO and NPT (2001) *Handing of Protectively Marked Material – A Guide for Police Personnel*. London: ACPO.

The Honourable Mr Justice Butterfield (2003) *Review of Criminal Investigations and Prosecutions Conducted by HM Customs and Excise*. London: HM Treasury.

### FURTHER INFORMATION

Staff can find out more information about the NIM using the following resources:

- Your force intelligence bureau (FIB) or local intelligence unit.
- The National Intelligence Model section at: <http://www.genesis.pnn.police.uk>
- ACPO website at: <http://www.acpo.police.uk/policies.asp>





