CENTREX
HELPING TO DEVELOP POLICING

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 pages 4, 5, 6, 7, 8 and 9) will take you directly to the page listed. Or click on any item in the list of Contents at the start of each Section. You may also access full Checklist details by clicking on the top of any Checklist box.
- 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 link.

GUIDANCE ON
THE NATIONAL INTELLIGENCE MODEL
2005

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

CENTREX
HELPING TO DEVELOP POLICING

GUIDANCE ON THE NATIONAL INTELLIGENCE MODEL

This document has been produced by the National Centre for Policing Excellence (NCPE) on behalf of the Association of Chief Police Officers (ACPO).

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

This guidance underpins the NIM Code of Practice which is the statutory code for all police forces.

All enquiries about this guidance should be addressed to:

Doctrine Development (supply request)
National Centre for Policing Excellence
Wyboston Lakes
Great North Road
Wyboston
Bedford
MK44 3BY

Telephone: 0870 241 5641
Email: ncpe.enquiries@centrex.pnn.police.uk

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

Acknowledgments
ACPO and the NCPE would like to express their thanks to all those involved in the drafting of this document, to members of the ACPO NIM Project Board in producing the original manual and to members of the ACPO NIM Working Group who gave their advice. All of the responses during the consultation phase of this project were appreciated and contributed to the final document.

CONTENTS

CONTENTS

CONTENTS

CONTENTS

Summary of Checklists

Summary of Figures

INTRODUCTION

The Police Reform Act 2002 is the statutory basis for the establishment of the National Intelligence Model (NIM), which complies to minimum standards, in all areas of policing.

Information on the content, structure, status, background, supporting material and legislative framework in which it was produced is provided in this section.

CONTENTS

BACKGROUND TO NIM

NIM is a business model for law enforcement. It became the policy of the Association of Chief Police Officers (ACPO) in 2000 and many forces underwent major restructuring and were allocated new resources in order to implement it. NIM takes an intelligence-led approach to policing. The government acknowledged its benefits and all forces in England and Wales were required to implement NIM to national minimum standards from April 2004. Additional minimum standards, which are incorporated in this guidance, have been developed for implementation by November 2005.

THE CODE OF PRACTICE FOR NIM

The *ACPO (2005) Code of Practice on the National Intelligence Model,* issued in January 2005 by the Home Secretary under the Police Reform Act 2002, provides a statutory basis for the introduction of NIM minimum standards and its basic principles. Chief officers must have regard to the code and ensure that their forces adopt the practices of NIM and implement the required minimum standards. Her Majesty's Inspectorate of Constabulary (HMIC) is responsible for inspecting the application of NIM in all police forces and for ensuring that these minimum standards are met. The full text of the code can be found in Appendix 1.

MINIMUM STANDARDS

An initial set of minimum standards was published in April 2003, and all police forces now comply with them. In order to maintain the impetus of NIM implementation, a revised edition of the minimum standards document was published in November 2004. The principles contained in that document underpin the NIM code, and **all of the standards must be implemented nationally by November 2005.** These minimum standards, together with descriptions of how to meet them and the impacts and benefits of implementation, can be found in Appendix 2.

NIM requires all forces to implement the National Briefing Model (NBM) and the HMIC will inspect its application. While the NBM is not listed as one of the elements of the NIM business process, its principles have application in each of the key business areas. The principles of the NBM are covered in *ACPO (forthcoming) Guidance on the National Briefing Model.*

SUPPORT

This guidance provides support and advice to assist police officers and staff to achieve and maintain the minimum standards required for compliance.

The National Centre for Policing Excellence (NCPE) prepared this guidance by drawing on the original NIM source document referred to as the National Criminal Intelligence Service (NCIS) NIM Blue Book and CD-Rom. It also draws on the work of the ACPO NIM Implementation Team. The NCPE doctrine team, on behalf of ACPO, is responsible for maintaining the content of this guidance and the associated practice advice. All NIM products released by the NCPE are commissioned and endorsed by the ACPO Intelligence Portfolio.

The NCPE Implementation Team is a resource deployed to assist forces to implement NIM. This team provides guidance and conducts audits to assist forces to comply with the minimum standards prior to HMIC assessment. An Implementation Support Plan has been developed to assist this process. Contact details for the NCPE Implementation Team can be found in Appendix 6.

THE STRUCTURE OF THIS GUIDANCE

NIM consists of eleven individual elements. Each section of this document focuses on a single element of the NIM business process. Each element has a set of minimum standards associated with it, and a checklist of them is provided at the end of each section. Forces must take appropriate action to ensure that they comply with all 135 standards within the time frame given. The minimum standards are discussed in detail in Appendix 2.

NIM AS THE CORE BUSINESS MODEL AND OTHER RELATED PUBLICATIONS

NIM is the core business model for policing but there are other manuals of guidance and practice advice and these should be read in conjunction with this document. They provide additional information on specific aspects of the model. The key elements of the NIM business process to which these publications are linked are as follows.

Assets (1-4)

- *ACPO (forthcoming) Practice Advice on Resources and the People Assets of NIM.*
- *ACPO (2005) Code of Practice on the Management of Police Information.*

Information Sources and Intelligence/Information Recording (5-6)

- *ACPO (forthcoming) Guidance on the Management of Police Information.*
- *ACPO and HMCE (2004) Manual of Standards for Covert Human Intelligence Sources.*

Research, Development and Analysis (7)

- *ACPO (forthcoming) Practice Advice on Tasking and Co-ordination.*

Tasking and Co-ordination, Intelligence Products, Tactical Resolution and Operational Review (8-11)

- *ACPO (forthcoming) Practice Advice on Tasking and Co-ordination.*
- *ACPO (2005) Practice Advice on Professionalising the Business of Neighbourhood Policing (Draft).*
- *ACPO (forthcoming) Guidance on the National Briefing Model.*

Additional related manuals of guidance and practice advice publications, particularly regarding tactical resolution considerations, eg, surveillance, are listed in Appendix 5.

This guidance provides the primary source of reference for the application of NIM within the Police Service together with the NCPE Implementation Support Plan and supporting practice advice publications.

ACCESS TO THE GUIDANCE

This guidance should be readily available at local police organisational level, ie, basic command unit (BCU) or operational command unit (OCU), and the force level. It should also be available to other law enforcement agencies who request access to it through the NCPE. Copies of the guidance will only be made available to other outside agencies through the NCPE and with the sanction of the ACPO NIM Working Group. Currently, the guidance is accessible in hard copy format or CD-Rom. An interactive version on the Genesis system, supporting links to other associated doctrine and allowing for easier amendment and future updates, will be available in the future.

THE NATIONAL INTELLIGENCE MODEL

NIM is an intelligent means of conducting police business. Although NIM can appear complex, when broken down into key elements it is relatively straightforward.

This section introduces the eleven elements of the NIM business process, and explains how this intelligence-led approach should operate in practice.

CONTENTS

THE NATIONAL INTELLIGENCE MODEL

NIM is an information-based deployment system and a cornerstone for the management of law enforcement operations in England and Wales. Historically most policing has been driven by the need to respond to calls from the public. This is necessary police business but crime and incident patterns are not identified. NIM identifies patterns of crime and enables a more fundamental approach to problem solving in which resources can be tasked efficiently against an accurate understanding of crime and incident problems.

NIM promotes a cooperative approach to policing and many of the solutions to problems will require the participation of other agencies and bodies. It is further strengthened when used in conjunction with other partner agencies, eg, joint tasking and co-ordination processes, and when it incorporates community information into the strategic assessment. For further information see *ACPO (2005) Practice Advice on Professionalising the Business of Neighbourhood Policing (Draft).*

LEVELS OF OPERATION

NIM requires that a number of capabilities are defined and built in order to professionalise and improve intelligence work, and to enable the compilation of standardised intelligence products. Intelligence products inform staff of significant threats, including those arising from less serious and serious crime. For example, road safety, anti-social behaviour and community tensions present significant problems which can be addressed through an appropriate use of intelligence. Risk management, the allocation of resources (including finance and technology), engagement with partner agencies and a review of tactics are all systems driven by NIM. This is equally the case whether the system is operating within a BCU or dealing with an international crime threat.

NIM, therefore, operates at three levels of policing.

- **Level 1** – Local crime and disorder, including anti-social behaviour, capable of being managed by local resources, eg, crimes affecting a BCU or small force area. Level 1 policing activity in large BCUs is often handled through local neighbourhood policing teams. Where the BCU deploys resources at a neighbourhood level, appropriate arrangements have to be made for intelligence collection and dissemination and the allocation of tasks.

- **Level 2** – Cross-border issues affecting more than one BCU within a force or affecting another force or regional crime activity and usually requiring additional resources.

- **Level 3** – Serious and organised crime usually operating on a national and international scale, requiring identification by proactive means and a response primarily through targeted operations by dedicated units. It is also likely to require a preventative response on a national basis.

INFORMATION SHARING

NIM improves the opportunities to share intelligence across forces and agencies, and between local and national levels of policing. NIM has not only been adopted by police forces but also by other agencies such as the Serious and Organised Crime Agency (SOCA), United Kingdom Immigration Services (UKIS) and by Crime and Disorder Reduction Partnerships (CDRP). It reduces barriers to effectiveness by producing standardised processes and language and creates a cooperative working environment.

RELIANCE ON INFORMATION

An intelligence-led organisation, by its very nature, relies on information. Capabilities must be built which enable information to be gathered, recorded, evaluated, disseminated, retained and disclosed as necessary from a range of available information sources. Staff members often submit information with no certainty of its potential relevance. NIM allows the police to direct resources to collect information to fill identified knowledge gaps. It also requires the Police Service to consider how and why it collects information and to identify ways to convert this information into intelligence.

IMPORTANCE OF INFORMATION ANALYSIS

Information refers to all forms of information obtained, recorded or processed by the police, including personal data and intelligence. Intelligence is defined as information that has been subject to a defined evaluation and risk assessment process in order to assist with police decision making. In addition to being evaluated, information is analysed. Analysis involves identifying critical links and associations that assist in understanding crime patterns, offending behaviour and incident problems. From that analysis intelligence products are developed and considered at either strategic or tactical tasking and co-ordination group (T&CG) meetings. At these meetings priorities are identified and decisions made on the deployment of resources. A review of all the tactics employed is also undertaken to identify the lessons learnt to benefit future operational activity. This analysis is then fed into the organisational memory (see 11.9 Organisational Memory) and becomes a part of the organisation's information sources thereby enabling the Police Service to obtain an accurate overall picture of crime and criminality.

NIM ASSETS

For the Police Service to become intelligence-led, the NIM business process must become embedded in local and national levels of policing. The foundations for this are referred to as **ASSETS**. These are:

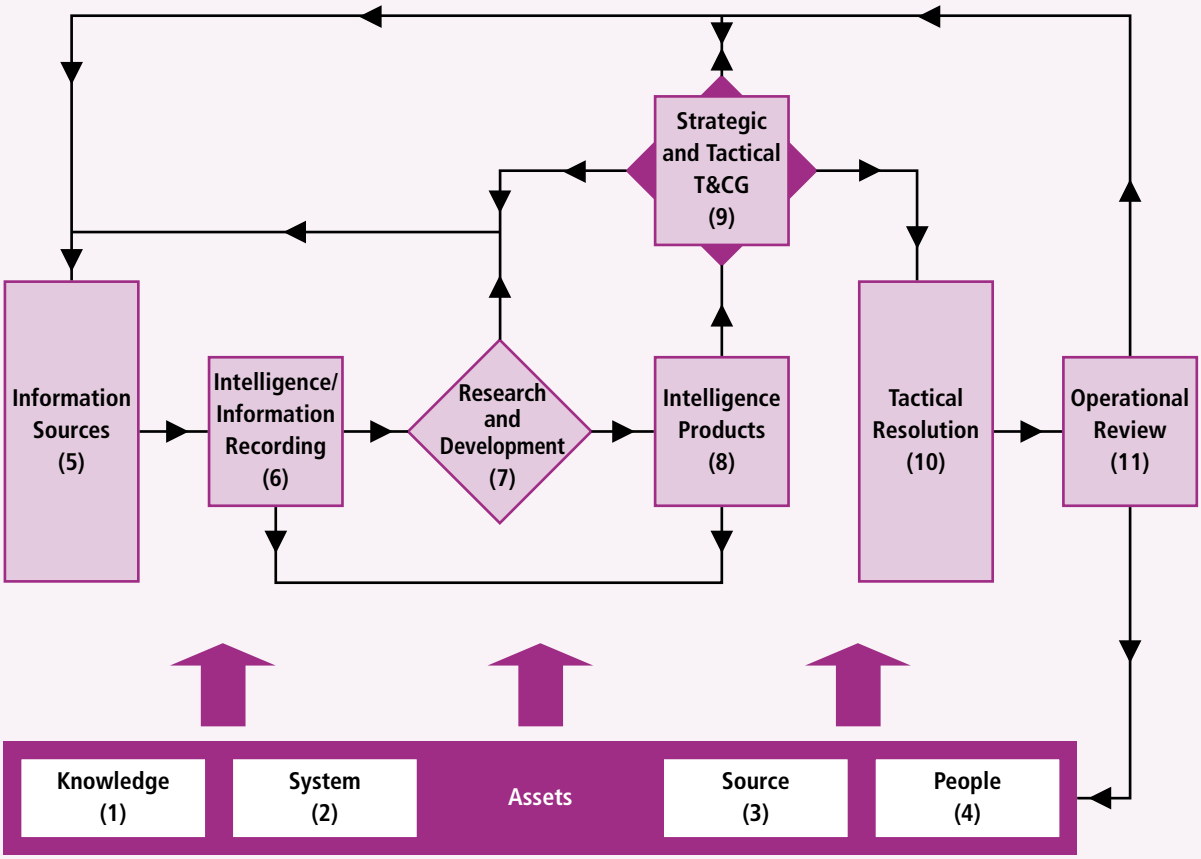
- **Knowledge assets** – Knowing the business of policing and understanding law, policy and guidance (see 1 Knowledge Assets);
- **System assets** – Having appropriate systems and structures in place, including secure environments and practices (see 2 System Assets);
- **Source assets** – Ensuring information is effectively gathered and managed from as many sources as possible (see 3 Source Assets);
- **People assets** – Establishing a professional personnel structure with trained and suitably skilled staff to carry out the required functions within the model (see 4 People Assets).

All these assets must be in place before the NIM business process can work effectively.

THE NIM BUSINESS PROCESS

Figure 1 illustrates the relationship between NIM and the intelligence cycle.

FIGURE 1 The NIM Business Process



THE NIM BUSINESS PROCESS IN ACTION

In a scenario involving burglary, the following process might take place:

ASSETS Foundation ▶ NIM platform and intelligence capability established ▶

↓

INFORMATION SOURCES Information received ▶ A N Other is responsible for a burglary ▶

↓

INFORMATION AND INTELLIGENCE RECORDING Information evaluated and deemed of intelligence value ▶ information recorded, data managed and entered onto the intelligence database ▶

↓

RESEARCH, DEVELOPMENT AND ANALYSIS Information researched, developed and analysed to discover critical links and associations ▶ information matched with details from crime report of burglary, full profile of subject and address obtained, burglary identified as part of crime series ▶

↓

INTELLIGENCE PRODUCTS Intelligence informs completion of the tactical assessment, prioritising this information for action ▶

↓

STRATEGIC AND TACTICAL TASKING & CO-ORDINATION Tactical tasking and co-ordination ▶ approve tactical resources, appoint plan owner and define timeframe for action ▶ may request target profile if appropriate ▶

↓

TACTICAL RESOLUTION Tactical manager decides on tactics to be used ▶

↓

Briefing and deployment of resources, debriefing at conclusion of task (see NBM) ▶

↓

OPERATIONAL REVIEW Commissioned by T&CG, feedback to them ▶ was suspect arrested, was property recovered, was anything else of intelligence value gained? ▶

↓

Feeds back into organisational memory ▶ **INFORMATION SOURCES**

In most cases there would be a constant flow back and forth between different elements of the process before reaching a conclusion. For example, a tactical T&CG (TT&CG) may direct further research and development before any tactical resolution. Research and development, on the other hand, may require further source tasking prior to compiling an intelligence product.

The NIM business process is designed to accommodate a free flow of action between each element. These elements exert influence on the other business areas. No individual element of the NIM business process should be allowed to under-perform and the following sections discuss each of them in turn.

Section 1
KNOWLEDGE ASSETS

Knowledge is one of the four assets underpinning NIM. Knowledge assets enable staff to deliver a quality service and they may be communicated through training courses, force intranets or libraries accessible twenty-four hours a day.

CONTENTS

1.1 KNOWLEDGE ASSETS

All police staff should be aware of, and have access to, knowledge assets. Within the intelligence capability there are dedicated intelligence staff members who require specialist knowledge. Not all police staff require such detailed knowledge.

There are numerous roles and responsibilities directly related to the operational effectiveness of NIM. For further information see 4 People Assets and *ACPO (forthcoming) Practice Advice on Resources and the People Assets of NIM.*

KNOWLEDGE ASSETS INCLUDE:

- Current legislation and case law;
- Codes of practice;
- Manuals of standards and ACPO guidance;
- Force policies;
- Briefing products.

1.2 KNOWLEDGE ASSETS AND STAFF PROFILING

The level of knowledge required by police staff will be determined by the specific role they perform or duties to which they are assigned. Staff profiling is a means of conducting a gap analysis. This analysis helps to determine the levels of staff knowledge required to meet organisational needs (in line with NIM) and also to assist with succession planning and the need for knowledge to be maintained.

Profiling should be in accordance with the Skills for Justice National Occupational Standards and competency framework, and informed by organisational need. This guidance and *ACPO (forthcoming) Practice Advice on Resources and the People Assets of NIM* should be used to assist staff profiling.

Methods of communicating knowledge assets will vary considerably but can include the use of force intranets, briefings, and the development of a research library, either physical or electronic.

1.3 INVESTING IN KNOWLEDGE ASSETS

The acquisition, maintenance and delivery of knowledge assets and training materials must be continually reviewed so that the Police Service is consistently able to meet the highest standards of policing delivery. The available material must be kept up to date, particularly regarding legislation, case law and policy, and will require investment in a supportive infrastructure. Police forces must maintain their knowledge assets in line with continual changes in the business environment, and also ensure that their staff are suitably trained.

1.4 TRAINING

The capture and maintenance of all available knowledge, staff profiling and methods of communication will influence requirements for force training, intelligence and communication strategies, and the force training budget.

Recommendations in the force strategic assessment (see 8 Intelligence Products) should identify training requirements. Staff profiling will identify different training needs for specialist intelligence staff and non-specialist staff. Dedicated intelligence staff must be trained to competence levels within the Skills for Justice competency frame work. Non-specialist staff will require less training and their requirements may be met by internal delivery. The identification of training needs will drive the development of national training products through Centrex.

Information on intelligence training can be found in *ACPO (forthcoming) Practice Advice on Resources and the People Assets of NIM.*

1.5 CHECKLIST OF MINIMUM STANDARDS

Checklist 1: Minimum Standards for Knowledge Assets

Standards 1 to 11 relate to knowledge assets and must be implemented by November 2005.
For details on these requirements and how to meet them, see Appendix 2.

1. Current legislation and case law.
2. Codes of practice and secondary legislation.
3. Manuals of guidance.
4. Practice advice.
5. Force policy relevant to intelligence.
6. Access to knowledge assets.
7. Force NIM communications strategy.
8. Force IT strategy (force information strategy).
9. IT dissemination of force and local control strategy and intelligence requirements.
10. IT dissemination of T&CG actions.
11. Force training strategy.

Section 2
SYSTEM ASSETS

System assets support intelligence-led policing. They are not simply technological solutions but also include the rules and policies which control their use, and the security measures necessary to protect them.

CONTENTS

2.1 SYSTEM ASSETS

System assets create the infrastructure which supports NIM. These assets must provide or supply access arrangements to systems and facilities for the secure capture, recording, reception, storage, linkage, analysis and use of information. They provide:

- Information storage, retrieval and comparison during the research process;
- A capability and process for the acquisition of new information and intelligence;
- Security systems.

SYSTEM ASSETS INCLUDE:

- Physical security;
- Security policies;
- Sterile corridor;
- Authorities management;
- Effective briefing and debriefing;
- Information exchange protocols.

The rules and policies which control the use of those assets are included within the definition of system assets. Examples of these include:

- Physical security policies and procedures, including secure access to buildings;
- Technical security policies and procedures, such as computer firewalls and passwords;
- A process for managing information including, for example, the management of intrusive surveillance authorities – Regulation of Investigatory Powers Act 2000 (RIPA);
- A process to brief and debrief staff;
- A process by which the Police Service works with partner agencies, eg, with regard to information access and exchange.

2.2 'NEED TO KNOW'

'Need to know' is a security principle which states that the dissemination of classified information should be no wider than is required for the efficient conduct of business, and should be restricted to those who have authorised access. A balance must be struck between making information as widely available as necessary to maximise potential benefits, and restricting availability to protect the security of sources, techniques and information. The development of systems helps to support the integrity and effectiveness of the intelligence environment.

2.3 SECURITY SYSTEMS

It is extremely difficult to protect all organisational information from attack by a determined assailant because of the increased portability of computer hardware and the sophistication and spread of telecommunications networks. The risk of loss of information through staff incompetence or dishonesty should also not be overlooked. To ensure integrity and confidentiality, police forces must develop and establish measures that include computer firewalls, physical security policies and staff vetting.

Information held by the police is frequently open source, but some information is confidential. Confidentiality usually relates to the origin of the material. For example, information obtained from covert human intelligence sources (CHIS) or from technical deployments would usually attract a general protection in law from disclosure. This is known as Public Interest Immunity (PII). Such information is protected because disclosure would destroy or endanger the source, or would be against the public interest in future law enforcement activity.

Sterile corridors must be implemented to protect the source of covertly obtained material and to establish confidentiality when sharing and disseminating intelligence, both internally and externally.

Sterile corridors are created by ensuring that covertly obtained information cannot be passed directly to others without prior sanitisation and appropriate authorisation. This ensures that the source of the information is protected. Document management systems must be in place so that authorisations for all covert and intelligence processes can be audited. For further information see the *ACPO and HMCE (2004) Manual of Standards for Covert Human Intelligence Sources.*

Document management file tracking systems for auditing paper records and authorities (eg, a system to show input and access history, dates, owners and authority) must be established.

Security issues are considered in greater depth later in this section.

2.4 BRIEFING AND DEBRIEFING

System assets include the effective briefing and debriefing of staff. Briefing enables police staff, in particular patrol officers, to understand daily tasking, be aware of personal and organisational threats and familiar with their specific responsibility to secure information in line with force and/or local intelligence requirements. The quality of a briefing can have a significant impact on operational outcomes.

Supporting the development of staff through training can enhance their briefing skills. Systems, policies and training are core elements of the NBM (adopted by all forces in England and Wales as of April 2004) and these principles are set out in *ACPO (forthcoming) Guidance on the National Briefing Model.*

Briefing and debriefing staff requires:

- Information feedback to the intelligence unit;
- Dedicated briefing facilities;
- That structures and processes for briefing and debriefing are installed at all areas of activity;
- That the patrol function briefing is driven by T&CG actions and results in individual tasking;
- Adherence to the NBM principles.

2.5 IMPORTANCE OF DEBRIEFING

Failure to gather information from operational staff through debriefing can create significant gaps in the intelligence infrastructure. The debriefing principles set out in the NBM enable the Police Service to learn from tactical operations and deployments, to populate and enhance organisational memory and to deploy resources efficiently. Successful police operations often result in offenders changing their tactics. Debriefings also enable officers to maintain a current understanding of criminal methods and behaviour.

Intelligence debriefings should concentrate on the quality of information collected, rather than quantity. The information gathered should primarily relate to identified knowledge gaps in order to meet force and/or local intelligence requirements. Performance regimes that focus on the quality of information (which is submitted in a timely fashion) enables the input of intelligence to be prioritised, thereby reducing debriefing time and the need for subsequent assessment.

2.6 SECURITY

The support of chief officers, staff associations and other key staff members is essential to obtaining maximum benefit from a police security management programme. In addition, such programmes must be seen by staff as an enabling process to achieve force and service objectives. Appropriate security should not inhibit the efficient provision and exchange of information and intelligence but, rather, should be designed to generate a climate of trust and integrity. At the same time, the programme must send a clear message to dishonest or disloyal staff that any corrupt actions will be exposed and dealt with through the criminal courts, internal discipline or both.

A police security management programme policy statement (see NIM Minimum Standard 13, Appendix 2) must emphasise the need to safeguard the interests of both the public and the Police Service when dealing with privileged information. The policy statement should set out the requirement for a process of risk assessments and systems audits, the need for appropriate security policies and procedures, and a senior management commitment to the centrality of the security programme. While no security programme can be perfect, the effectiveness of this system lies in the provision of a series of overlapping countermeasures which, when taken together, meet the level of security required.

2.7 THE NEED FOR SECURITY

As a consequence of the move to intelligence-led policing through NIM, there is an increased risk that intelligence products will be compromised through unauthorised disclosure of information. Failure to counter this risk will affect forces' ability to combat criminal behaviour and sustain crime reduction. It could also jeopardise the personal safety of police staff and members of the public, as well as result in adverse media coverage and an increase in civil claims.

Police forces are now reliant on computerised systems for the storage, transmission and analysis of information and intelligence. Data quality is critical. It is equally important to prevent unauthorised disclosure of material. Clear and concise policies on information system security need to be established and understood by all staff. These policies must address access rights, audit trails and analysis of access, virus protection and the use of email, intranet, internet and portable computing equipment. The impact and implications of the Freedom of Information Act 2000 should also be taken into account within police force policies. Consideration must also be given to preserving security with respect to contractors who maintain and support intelligence databases. Data security, disclosure, authorised access and accuracy are essential to NIM. Security must be addressed at the design stage of any new information technology (IT) system; adding security to existing systems is expensive and much less effective.

A police security management programme must achieve a balance between a level of trust where staff are valued and empowered, and a level of security where appropriate supervision and safeguards provide a degree of assurance. An unquestioning trust culture can constrain supervisors from exercising appropriate management intervention.

2.8 THE SECURITY MANAGEMENT PROCESS

The security management process involves identifying police system assets, evaluating them in terms of key policing objectives, and identifying threats to them and any risks. This process also includes reviewing existing security measures, implementing any necessary changes and conducting continuous assessment. Details on each of the elements of the process and their relevance to the key objectives are outlined in the following sub-sections.

Equipment such as modems, scanners, CD-Roms, writeable CDs, electronic organisers and electronic organiser connectors can be used to gain unauthorised access to, and allow the unauthorised disclosure of, information. Although computers are relatively cheap to replace, the consequences of the loss of the intelligence contained within their databases may be significant. Information can be removed by direct theft, copying, faxing or downloading through the use of electronic equipment. This includes records in all forms such as electronic databases, paper and microfiche.

Criminals have as much interest in intelligence as the police. Information which can assist criminals may be exposed through corruption or by carelessness. For example, a document which appears to be innocuous may, in fact, suggest targeting procedures which would be beneficial to criminals. All information and technologies that support information handling within the intelligence process should be subject to risk assessment and security policy.

2.9 STAFF VETTING

Vetting enquiries must be conducted for all members of staff known to have specialist knowledge that could be used to circumvent the electronic countermeasures protecting the intelligence databases. Members of staff who have direct access to a wide range of IT applications must also be vetted. Staff members who disclose information to criminals, the press or private detectives for personal gain, under coercion or because of disaffection can cause significant harm to law enforcement operations.

2.10 DETERMINE ASSET VALUES

Asset values are determined by identifying information which, if disclosed, could seriously impede the Police Service's ability to reduce crime and arrest offenders. Information that falls into this category must be protectively marked using the Government Protective Marking Scheme (GPMS) and handled in accordance with the level of marking applied. Each asset is considered in terms of the likely consequence of breaches of confidentiality or availability. A number of pieces of information at one level of protective marking, when taken as a whole, may need a higher level of protection.

Information classified as secret or top secret is usually retained within Special Branch offices. The vast majority of intelligence which the Police Service relies on for crime reduction and arrests is, however, maintained outside the special branch security environment. Appropriate protection is, therefore, essential and can be achieved by using the GPMS marking policy. For further information on GPMS see *ACPO (2001) Adoption of the Government Protective Marking Scheme (GPMS).*

The quality of any information held determines its value in terms of achieving key policing objectives. It is, therefore, essential that databases and documents are maintained to the highest levels of integrity and accuracy, and that they are readily available to all members of staff who have a legitimate access to them. This process can be monitored through a series of audits and compliance checks. In order to maintain confidentiality, measures must be implemented to prevent unauthorised access and disclosure.

It is critical that all buildings and sites within a police force are protected to a level of security that is commensurate with the current threat assessment.

Employees are the most valuable asset, but they also present the highest security risk. In order to concentrate the security process efficiently, staff with specialist skills (particularly in IT) must be identified along with specific posts where the post holders have a ready access to a wide range of intelligence databases and documentation. Relevant personnel should be subject to security vetting procedures at the appropriate level for their job.

2.11 IDENTIFY THREATS AND VULNERABILITIES

Threats and vulnerabilities must be identified in the following five areas.

1. Intelligence

Most intelligence products will be electronically available to all police staff. Information on specific operations and intelligence-gathering activities must, however, remain restricted to a limited number of staff on a 'need to know' basis. Such control can be achieved by taking four steps. These are:

- Defining areas of the database for specified users only;
- Protectively marking documents and files;
- Ensuring appropriate handling, storage and disposal of records;
- Conducting audits and investigations.

In order to provide an appropriate level of security, police forces should consider conducting a security analysis review of their intelligence databases. The Central Computing Telecommunications Agency Risk Analysis Management Method (CRAMM) is the government's preferred method of risk assessment.

A CRAMM ANALYSIS WILL PROVIDE THE FOLLOWING:

- Identification and evaluation of a system and associated infrastructure assets;
- Identification of the level of threat and vulnerability to assets, leading to an assessment of risk;
- Proposals on how identified risks can be addressed, including cost implications.

Risks can then be identified by individual force security managers and committees who will consider the implications and take appropriate action to address these vulnerabilities by introducing appropriate countermeasures.

Other in-force databases (for example, Personnel, Firearms and Special Branch) should be risk assessed.

2. Buildings and Sites

Security measures to protect police buildings and sites to a level commensurate with the assessed risk should be implemented. This includes the physical security of buildings, ie, the installation of closed circuit television (CCTV), lighting, intruder alarms, access controls, identification (ID) systems and secure storage facilities. Personnel security in this context includes the reception and supervision of visitors and contractors, and technical security relates to the use of telephones, fax machines and photocopiers.

3. Key Personnel and Posts

As indicated in 2.10 Determine Asset Values, staff with a wider access to databases and those holding key intelligence posts within a force, must undertake a management vetting procedure.

4. Radio and Telephony

Voice communications frequently include information which the public should not hear. Scanners and lists of police frequencies are readily available from high street retailers and the specialist press. Unauthorised disclosure of subject information is more likely by this means than any other. Using mobile data terminals also includes an element of risk. The use of encryption and digital technology (such as Airwave) will, therefore, provide added security.

5. Existing Security Measures

A security review by CRAMM analysis or another method of evaluation will identify a number of vulnerabilities with regard to physical, personnel and IT security, and any security review should be addressed under these three headings. Actions to meet these vulnerabilities should be included within the resulting security management programme.

2.12 IMPLEMENTING NECESSARY CHANGES

Security policies must be approved and published under the security management programme.

The overriding objective of data protection management is to ensure that any information held on police computer systems is obtained, stored, used and disclosed in accordance with the Data Protection Act 1998 (DPA), other relevant legislation and ACPO and local force policy and procedures. The DPA does not prevent the lawful gathering, recording, dissemination, retention and disclosure of information for policing purposes. See *ACPO (2005) Code of Practice on the Management of Police Information.*

The Police National Computer (PNC) security policy is set out in the *ACPO (2000) PNC Compliance Strategy* and *ACPO (2002) Code of Practice for Data Protection* and *ACPO (forthcoming) Data Protection Manual of Guidance.* Under the *ACPO (2000) PNC Compliance Strategy* police forces are required, as information users, to comply with a number of legal and statutory obligations in relation to their access, and use of the PNC. Paragraph 23 of the *ACPO (2005) Code of Practice on the Police National Computer* includes a table listing documents which provide guidance on required actions, good practice and operating procedures for PNC. The requisite security roles and responsibilities, security policies and administration procedures are also set out in these documents.

A review of job descriptions for staff in key posts will be necessary so that an appropriate level of training and security awareness can be achieved. Training and guidance on compliance with security policies and procedures and the mandatory supervisory responsibilities of those in charge of staff in key posts will also be required. This will involve staff learning how to use technology and being trained in using appropriate processes, policies, audits, compliance checks and investigations.

2.13 CONTINUOUS REVIEW

Security management is an ongoing process. Threats and vulnerabilities vary over time according to changes in threat assessments which, in turn, require that changes are made to policies and procedures. The effectiveness of countermeasures introduced to meet threats will, therefore, have to be reviewed on a regular basis and new countermeasures developed as necessary.

Those in charge of key units, including supervisors, have a specific duty to carry out audits of the work of their staff and to deal with, as well as report on, any irregularities. Furthermore, all officers, police staff and their supervisors must report any security concerns.

Those tasked with taking forward the security management programme will be responsible for co-ordinating all physical, personnel and IT security matters, and for providing advice and guidance. The Security Manager must, therefore, maintain close business links with other key members of staff, including area/divisional commanders, heads of departments, and a wide range of internal and external departments and agencies.

2.14 MARKETING, TRAINING AND EDUCATION

Even the most comprehensive security management programme will have little effect if staff are not made aware of its content and the reason for its introduction. Policies, procedures and guidance provide the rules for staff compliance but these should only be introduced following consultation with key departments and staff associations. Police forces may wish to consider using a marketing or communication strategy. Such a strategy might include security presentations and seminars, force newsletter articles, a poster campaign, and the issue of security leaflets and booklets to all police staff, including members of the Special Constabulary and external contractors.

In addition to the requirements of the security management programme, staff should also receive guidance on integrity, corruption and police ethics. Efficient management and supervision is vital. Managers and supervisors must be made aware of the requirements placed on them, not only to implement the policies, procedures and guidance contained in the programme, but also to encourage a culture of security and to ensure compliance with this.

2.15 POLICE CORRUPTION

A constant emphasis on integrity and standards of behaviour is an essential countermeasure to corruption in the workplace. Research into police corruption in England and Wales has produced vulnerability profiles for a number of recurrent cases. There is evidence to suggest that there is a pattern of corruption where certain types of staff, ie, those with a specific length of service, age and personal circumstances, appear to be more susceptible to corruption than others. For more information on vulnerability profiling, see *Dr B W Caless (1999) Police Corruption: Vulnerability Profiling.*

> **Note:** The accuracy of a vulnerability profile is limited by the amount, detail and reliability of the information provided by forces.

Very few police staff are, however, corrupt. Nonetheless, research and information that helps supervisors and investigators to focus attention on the kind of staff and posts most at risk from corruption is useful.

2.16 OPSY AND CHIS HANDLING

The role of the Operational Security Officer (OPSY) has been established in national security management and has proved to be good practice for the Police Service, particularly in high risk areas such as CHIS, see 3.12 Covert Human Intelligence Sources. For further information see *ACPO (forthcoming) Practice Advice on Resources and the People Assets of NIM.*

The role of the OPSY is to look objectively at:

- The CHIS handling process;
- Intelligence gathering;
- The quality of intelligence;
- Analysis and assessment of intelligence;
- Relationship between the handler and CHIS;
- Security of the case;
- Security of file-keeping and documents.

All OPSYs must have recent service in a senior role within law enforcement and an extensive track record in all aspects of CHIS handling. They must also possess the credibility to gain handlers' trust, as well as the experience to be appointed to the role and acumen to spot corruption, the lack of dividend in a case and malpractice. An OPSY must have the right to intercede in any investigative or intelligence operation so that they can test the integrity of an operation without restraint.

Standing outside the chain of command and without direct involvement in the processes, the OPSY will regularly review cases and highlight any which appear to be insecure in any way. They will also identify handlers believed to be manufacturing intelligence or making inappropriate or unusual payments, and any CHIS not delivering. The OPSY also has a support function to help inexperienced staff undertake CHIS handling. Furthermore, they can help focus the direction of a case and encourage imaginative approaches to recruitment and targeting.

2.17 CHECKLIST OF MINIMUM STANDARDS

Checklist 2: Minimum Standards for System Assets

Standards 12 to 26 relate to system assets and must be implemented by November 2005. **For details on these requirements and how to meet them, see Appendix 2.**

12. Physical security.
13. Security policies re: integrity, confidentiality and vetting standards within intelligence work.
14. Disclosure.
15. Sterile corridor.
16. Real-time research capability.
17. Standard analytical tools.
18. Effective briefings and debriefings.
19. Inter-agency information sharing protocols.
20. Standardised and integrated intelligence database.
21. High-speed search capability.
22. Authorities processes and document management systems in place.
23. Human resources system.
24. System development.
25. IT critical incident recovery procedures/process (force disaster recovery strategy).
26. Use of PNN2 and CJX (standard levels of access).

Section 3
SOURCE ASSETS

NIM requires a wide range of source assets in order to work efficiently. CHIS are just one source of information available to the Police Service. There are many others which should also be considered and an overview of some of them is given here.

CONTENTS

3.1 SOURCES OF INFORMATION

NIM requires access to information in order to fill intelligence gaps which are known as the intelligence requirement. The intelligence requirement can be obtained from numerous, varied sources (see 5 Information Sources) and will enable the Police Service to assess the full picture of policing needs and set their priorities accordingly.

The term, sources, is often taken to mean the use of CHIS, previously known as informants. Efficiently managed and controlled CHIS – recruited specifically for that purpose and operating to control strategy objectives and intelligence requirements – are a highly effective tool. CHIS are discussed in greater detail in 3.12 Covert Human Intelligence Sources. Other sources are discussed throughout this section.

3.2 SOURCE ASSETS

SOURCE ASSETS INCLUDE:

- Victims and witnesses;
- Communities and members of the public;
- Crimestoppers;
- Prisoners;
- Forensic information;
- Undercover operatives;
- Surveillance product;
- CHIS.

A list of source assets available to the Police Service, as a minimum standard, is in Appendix 2, entries 27 to 40. Appendix 3 contains a Directory of Information Sources.

3.3 ASSETS USED TO DEFINE BUSINESS PRIORITIES

A strategic assessment (see 8 Intelligence Products) based on all the information available, will define the business priorities for the police force or BCU. All of the information assets available which may assist in further profiling of the problems identified should, therefore, be determined. In order to exploit these assets, investment in IT connectivity, staff training and the development of information-sharing policies and protocols may be required.

3.4 THE INTELLIGENCE REQUIREMENT

The intelligence process is concerned with identifying and understanding critical links and associations. Gathering intelligence to fill the intelligence requirement (see 9 Tasking and Co-ordination) requires a proactive deployment of resources. This may include human sources, undercover officers, police community support officers (PCSO), patrol officers, open data source or the deployment of human or technical surveillance resources. At higher levels of operation there will be a requirement to access sophisticated covert entry techniques or to intercept communications. Investment in the intelligence function will, therefore, depend on the degree of difficulty or complexity in accessing the information required.

Intelligence units will require access to proactive resources to an extent which is appropriate to the activity or operation involved. More intrusive techniques are only available in the investigation of serious crime, and the requirement to protect the secrecy of such methods makes it undesirable to use them where they cannot be securely deployed. Mobile surveillance resources are expensive and a compelling intelligence case must be made before their deployment. Following a review of a case, however, such means may turn out to be the only effective method of securing the intelligence required.

3.5 CONTROL STRATEGIES

The control strategy sets out and communicates the current strategic operational priorities for the force or area. Police commanders will usually align source opportunities to control strategy priorities (see 9 Tasking and Co-ordination). The construction of an intelligence requirement written in accordance with the control strategy and also taking into account the emerging threats, trends and national, and/or force intelligence requirements, will determine the information needed to fill gaps in the Police Service's organisational memory. This will greatly assist staff when assessing the available information sources, and particularly when considering the recruitment of CHIS.

3.6 THE RECORDING PROCESS

The Police Service uses victims, witnesses and prisoners as information sources on a daily basis. Relevant intelligence may be found in witness statements or in comments made to officers during formal interview. This information can be used during problem profiling. There may be issues relating to confidentiality or the likelihood of identification of a source. Security considerations such as these must be taken into account on a case-by-case basis when determining procedures and policies.

Any information received by the police will be recorded through the 5x5x5 procedure or through other business areas such as crime, incident and custody records. The use of the National Information/Intelligence Report Form (5x5x5) is approved ACPO policy and a NIM minimum standard. The recording process is covered further in 6 Intelligence/Information Recording and in *ACPO (forthcoming) Guidance on the Management of Police Information.*

3.7 VICTIMS AND WITNESSES

Victims of crime and witnesses to crime and incidents are important sources of information. Victim and witness information can be accessed from a number of locations, including:

- Crime and incident reporting systems;
- Missing person reports;
- Child abuse case files;
- Domestic violence reports;
- Hate crime cases.

All police forces should establish processes to ensure that victim and witness information is captured for intelligence evaluation as appropriate.

3.8 COMMUNITY INFORMATION

Community information can come to the police from members of the public and through partner agencies. Where it is given directly to police staff by members of the public, it must be submitted for evaluation through the 5x5x5 procedure. Information originating from Crimestoppers will be submitted for evaluation through nationally agreed processes.

The Police Service should take full advantage of external source opportunities, particularly partner agencies. Such opportunities help to determine, both strategically and tactically, the best methods to adopt to reassure the public, improve quality of life, reduce crime and the fear of crime and enforce the law.

Signal crime – Any criminal incident that causes a change in the public's behaviour and/or beliefs about their security.

The identification of signal crimes and the development of neighbourhood policing has led the Police Service to gather information held by partner agencies. For more information on neighbourhood policing, see *ACPO (2005) Practice Advice on Professionalising the Business of Neighbourhood Policing (Draft).* For more information on signal crimes research see *Dr M Innes and MR C Roberts (2005) i-NSI Trial & Evaluation Report.*

3.9 FORENSIC INFORMATION

Information obtained from scenes of crime examination is another source asset. Crime scene investigators should take an active role in intelligence and T&CG processes to ensure that forensic information held at a local or force level is captured for intelligence analysis. Forensic evidence such as paint transfer, DNA, fingerprints, fibre transfer and tool marks are increasingly used to link scenes to each other as well as to suspects. These links are essential in identifying a crime series. To ensure the capture and management of intelligence, forensic information held at a national level should be subject to agreed protocols.

3.10 PRISON AND PRISONER INTELLIGENCE

The capture of information from prisoners held in custody including those serving a prison sentence will also provide a source of potential intelligence. Police forces can employ a prison intelligence capability and use intelligence approaches to obtain information on criminal networks, criminal business profiles and target profiles. This will provide new information that cannot be gathered by any other means and will also help to confirm existing intelligence. Intelligence gathering of this type requires the police to work in partnership with the prison authorities in order to access information within prison systems.

Police forces should ensure that processes are in place to obtain information from prisoners through agreed policies and protocols. For further information see *ACPO and HMCE (2004) Manual of Standards for Covert Human Intelligence Sources* and *ACPO (forthcoming) Practice Advice on Prison Intelligence and Related Matters.*

3.11 COVERT OPERATIONS

Covert operations always generate large amounts of information which must be recorded on to force intelligence systems. Making such information available on police force systems can expose the tactics used and the people involved. Systems must be in place to minimise this risk, while ensuring that the information remains accessible.

Covert operational teams are regularly deployed within communities and in the investigation of serious crimes. In addition to gathering operation-specific information, unrelated information will also be generated. This must also be recorded and evaluated following the principles for managing and sanitising confidential information. For further information see 6 Intelligence/Information Recording and *ACPO (forthcoming) Guidance on the Management of Police Information.*

Covert operational teams can provide beneficial intelligence to BCU/local areas. In order to do so, they must be aware of the key intelligence requirements and needs for that location. Systems should be in place to enable briefing of central support services when officers are operating in a locality they are unfamiliar with.

3.12 COVERT HUMAN INTELLIGENCE SOURCES

The use of CHIS is a valuable source of information but carries inherent risks which must be managed. The *ACPO and HMCE (2004) Manual of Standards for Covert Human Intelligence Sources* is retained by the force Director of Intelligence and, locally, by CHIS controllers. It provides the standards to be adhered to and guidance for all police and customs staff engaged with CHIS, and is designed to significantly reduce the risks associated with such work. The principles of this policy include that:

- CHIS handling must be recorded and follow authorisation and professional regimes;
- CHIS are handled by staff who are properly trained and dedicated to that task, operating within the intelligence function.

The CHIS system must be within the continual oversight of designated controllers, supervisors and other defined managers, eg, the Force Director of Intelligence. The system must also be subject to analysis (to indicate both strengths and weaknesses), security checking (OPSY) and review. The CHIS system must be flexible enough to allow for the tasking of covert sources in line with T&CG requirements.

HMIC encourages the continued use of CHIS as a cost effective means of developing operations against crime.

3.13 DEDICATED SOURCE UNITS

Dedicated source units (DSU) have been established to manage CHIS. These have provided a greater ability to manage risk and, through the use of highly trained staff, concentrate on the recruitment of CHIS in line with intelligence priorities. This is very different to recruiting CHIS who wish to provide information for the significant self-benefit it provides, such as trading charges or sentence reductions. CHIS should be recruited according to need and only authorised when they are able to make a contribution to control strategy priorities, or when managing high risk issues.

3.14 PRIORITISED INTELLIGENCE WORK

As discussed in 3.12 Covert Human Intelligence Sources, tasking will fulfil force and/or local intelligence requirements. Individual operational intelligence requirements specific to a target, criminal organisation or location are also necessary. Such tasking will usually be engineered to aid a tactical operation.

Intelligence requirements drive key issues and must be widely communicated to police staff. Identifying sources of intelligence is a service-wide responsibility and can be generated through briefing or tasking staff, in particular those operating in patrol teams and others dealing with victims and prisoners. Law enforcement relies on intelligence from local officers and the identification of problems through community engagement. This is then reinforced through the neighbourhood policing agenda.

3.15 INTRUSIVE REVIEW

The intelligence function has a primary responsibility for the active identification, research and development of source opportunities. A regular intrusive review of the various source assets available should be conducted by command teams and OPSY. This will reinvigorate drive and lead to innovation in the identification of new and emerging source opportunities.

An obvious example of an intrusive review is the examination of CHIS assets to ascertain whether they are:

- Informing on control strategy priorities;
- Living in, or able to inform on, priority locations;
- Providing information that meets the intelligence requirement;

Or, following an assessment of the force and national intelligence requirements, they are;

- Of benefit to another discipline within the force, for example, Special Branch, or another agency such as SOCA.

The enhanced profiling database at the National Source Management Unit (at NCIS) may assist when attempting to infiltrate groups or locations that are hard to reach.

3.16 TALENT SPOTTING

Many police forces or BCUs now provide induction and briefing material to staff prior to their first operational duties. This material should cover local and national force intelligence requirements, along with intelligence, CHIS and control strategy priorities. CHIS strategies should reinforce the concept that dedicated specialists are not solely responsible for the identification of intelligence sources. The Police Service as a whole must continually look for such opportunities, often referred to as talent spotting.

3.17 CHECKLIST OF MINIMUM STANDARDS

Checklist 3: Minimum Standards for Source Assets

Standards 27 to 40 relate to source assets and must be implemented by November 2005. **For details on these requirements and how to meet them, see Appendix 2.**

27. Victims and witnesses.
28. Repeat victims.
29. Priority and prolific offenders.
30. Access to community intelligence.
31. Crimestoppers.
32. Prisoners/prison visits.
33. Prison intelligence.
34. Covert human intelligence sources (CHIS).
35. Use of enhanced CHIS profiling.
36. Undercover/test purchase operatives.
37. Access to interception product.
38. Surveillance product.
39. Forensic data and forensic intelligence policy.
40. Other service/agency tasking.

Section 4
PEOPLE ASSETS

NIM cannot operate without key personnel, roles and functions, all of which are referred to as people assets. It is essential that police forces invest in skilled staff and ensure that accredited training programmes are established.

CONTENTS

4.1 ESSENTIAL FACTORS

There are a number of essential factors in prioritising intelligence work and embedding NIM as the core business model for policing. These are:

- An ACPO lead driving the implementation of minimum standards;
- Investment in appropriate people for specific roles, ensuring full capacity and succession planning;
- Ensuring continual professional development of the intelligence discipline through key heads of profession and the identification of the National Intelligence Learning Requirement;
- Appointing highly skilled intelligence managers as the catalyst for bringing together the business of the command unit with intelligence collection and analysis;
- Providing appropriate resources for
  - Information and intelligence management
  - Analysis
  - Tasked intelligence collection, including source handling;
- Dynamic command of tasking and co-ordination;
- Sufficient tactical capability to deliver resolutions.

4.2 ROLES AND FUNCTIONS

The minimum standard requirements for the policies, roles and functions that enable an effective intelligence-led capability and which reinforce the above essential factors, are described in Appendix 2, entries 41 to 62. The development of each force or BCU intelligence capability is dependent on organisational size, structure, finance, priorities and available human resources. Each force or BCU, however, will always maintain a capability that includes these roles and responsibilities. All staff, including intelligence professionals, must understand their roles within NIM and recognise how their job contributes to the overall intelligence function.

4.3 STAFF DEVELOPMENT

Staff development not only depends on the role performed by an individual, but also on the responsibilities and skills necessary to fulfil that role. Using *ACPO (forthcoming) Practice Advice on Resources and the People Assets of NIM,* managers can correlate roles, competencies and development, to ensure a professional and efficient service delivery. This process complies with the Skills for Justice National Occupational Standards and competency framework.

In addition to local training in force computer systems, information exchange protocols and priorities, further training will be required on the broader aspects and opportunities of intelligence collection. Details of nationally accredited courses are available through Centrex and are referred to in the *ACPO (forthcoming) Practice Advice on Resources and the People Assets of NIM.* These are designed for BCU commanders, intelligence specialists, intelligence managers and for the incremental development of analysts from initial training through to enabling them to conduct strategic analysis. Work has been commissioned to identify the National Learning Requirement for the intelligence discipline and to establish an accredited process for professional development.

4.4 KEY ROLE – ACPO LEAD

The appointment of an ACPO lead to ensure that the police force remains focused on its requirement to fully establish NIM to the required minimum standards is an essential factor in determining force performance. This officer should maintain an up-to-date knowledge of key and current developments regarding NIM.

4.5 KEY ROLE – HEADS OF PROFESSION

A senior member of the force, normally of superintendent rank with a credible track record in the field of intelligence and/or proactive investigations, should be appointed. These heads of profession, also known as Directors of Intelligence, provide a professional focus for the force, for the efficient management of the intelligence process.

Heads of profession have ownership of the intelligence function, its development, strategic direction, production of the intelligence products, control strategy and intelligence requirements for the force T&CG. They are also responsible for ensuring that standards within the intelligence profession on BCUs are maintained.

The force Principal Analyst acts as the head of profession for the analyst function and the development of the analyst profession within force. These highly qualified individuals are required to carry responsibility for the strategic development and quality assurance of intelligence products, maintenance of technical skill levels, training the workforce and managing the analytical discipline.

4.6 KEY ROLE – INTELLIGENCE MANAGER

The Intelligence Manager is responsible for the strategic direction and development of the intelligence function (the intelligence strategy), and for the production and submission of the four intelligence products to the force/BCU T&CG.

The Intelligence Manager's responsibilities are:

- Strategic and tactical assessment – reporting and advising on what is important to the BCU, including issues of risk to the public and policing;
- Understanding intelligence gaps – reporting and advising on setting intelligence requirements;
- Identifying criminal profiles – understanding how criminals operate in order to identify weaknesses in their systems, who is involved in their criminal networks and who their associates are;
- Infiltration and penetration – establishing tactical opportunities from collected intelligence and analytical products to secure infiltration or understanding of the criminal/organisation;
- Operational review – determining what worked or did not work and why;
- Management representation – ensuring that intelligence as a discipline is adequately represented in management discussions on resources;
- Tactical direction – engaging with managers of the command unit/force on behalf of the T&CG to ensure that specialists are consulted to provide options under the tactical menu which are realistic and clear;
- Understanding covert tactics – ensuring that the intelligence unit is equipped to handle information that is already known or acquired during reactive investigation, and gathering information through proactive or covert means.

An intelligence manager of appropriate status should be appointed to ensure that meaning and significance are added to the analytical techniques and products before they are presented as completed intelligence products to the T&CG. The officer, usually of inspector rank at the BCU level or superintendent at force level, will have successfully attended the nationally accredited intelligence manager's training course.

4.7 KEY FUNCTION – INFORMATION AND INTELLIGENCE MANAGEMENT

The requirements of a professional intelligence capability are timely recording, evaluation, dissemination and management of information. Information management includes the input of information and providing access to it for those with authorisation (see 5 Information Sources). It also has a research capability to support the work of analysts.

There must be sufficient capability to evaluate, input and manage information from a wide range of sources. There should also be sufficient capability to sustain IT systems, ensuring compliance with legislative requirements and maintaining effective information exchange with partners in support of policing purposes. For further information see *ACPO (forthcoming) Guidance on the Management of Police Information.*

4.8 KEY FUNCTION – ANALYSIS

Information analysed from a number of different sources can provide an informed, intelligent picture of policing issues. In order to produce quality intelligence products, forces must appoint sufficient numbers of trained analysts at every level of policing. Each force should consider minimum staffing levels based on its own individual crime and incident profile. Analysts must be given dedicated time to undertake quality analysis and should not be side-tracked into performing basic information management tasks.

4.9 KEY FUNCTION – INTELLIGENCE COLLECTION

Field support in line with the intelligence collection strategy must be provided to enable the development of an accurate tactical menu for consideration by the TT&CG. The intelligence collection function consists of the following capabilities.

Research and Development – Field Intelligence Capability

Field intelligence officers (see also 7 Research, Development and Analysis) are responsible for liaising with all staff, including specialist staff within prevention, intelligence and enforcement functions, ie, crime reduction units and investigative groups. They report qualified recommendations in both profiles and assessments (see 8 Intelligence Products). At a force level (level 2) the research and development field officers may include prison liaison (see below), sex and dangerous offenders resources, financial investigators, Crimestoppers, telecommunications single point of contact (SPOC), authorities' management, technical support unit (TSU), surveillance and covert operations teams.

Research and development of intelligence products on authorised nominated targets should also be conducted to assist the designated plan owner and to ensure that all authorised targets are the subject of appropriate flagging to comply with national/force policy. Research and development staff will be responsible for providing staff with an accurate product which will engage in operational review. This should be done through briefings. They will also have responsibility for ensuring that the requirements of the Criminal Procedure and Investigations Act 1996 (CPIA) are complied with, and that intelligence products are appropriately managed.

Security within the intelligence function is essential and all staff must adopt and adhere to the security policy. This will include the use of secure filing systems, a clear desk policy and ensuring that a high level of security is maintained at all times (see 2 System Assets).

Post holders should successfully complete an appropriate national research and development training course at the earliest opportunity following their appointment at BCU level, or prior to appointment when operating at level 2 or 3.

The primary function of the intelligence unit is to collect and receive information based on an identified intelligence requirement within prioritised or high risk areas determined by the T&CG control strategy. Rigorous management is required in order to avoid collecting intelligence on issues of secondary importance.

The law enforcement environment is fast moving and one in which matters requiring urgent attention are frequently likely to come to notice. While it is essential that a sense of direction is maintained, a fast-track procedure for acting on urgent intelligence which may relate to issues outside of the control strategy, is necessary.

Technical Field Officers

The responsibilities of this role are:

- Deploying technical equipment in line with T&CG actions;
- Purchasing equipment in accordance with Home Office Scientific Development Branch (HOSDB)/force TSU rules;
- Introducing an effective audit trail for BCU equipment;
- Identifying opportunities to use force TSU equipment or services;
- Ensuring compliance with health and safety legislation and technical standards.

Technical field officers should undertake an accredited programme of training. For further information see *ACPO (forthcoming) Practice Advice on Resources and the People Assets of NIM, ACPO and HMCE (2004) National Standards in Covert Investigations Manual of Standards for Surveillance* and *ACPO (2004) Deployment Standards for Technical Support in Tackling Volume Crime.*

CHIS Control

The intelligence development unit requires access to proactive field intelligence for the recruitment and deployment of sources as well as covert technical resources. Collectively the components of this process provide the intelligence products for both tasking and co-ordination, and operational support.

In line with RIPA, the controller of human sources should be an officer of substantive inspector rank. The *ACPO and HMCE (2004) Manual of Standards for Covert Human Intelligence Sources* determines that, where practicable, the officer should be solely dedicated to dealing with such human source issues. The Police Service, however, has found it considerably difficult to meet this requirement and frequently intelligence managers, in particular at BCU level, are given joint responsibility for both the strategic direction of the intelligence function and the management of human sources. This is an issue for each force to address and should be subject to a risk assessment and recorded and retained by the nominated chief officer responsible for RIPA issues. The CHIS controller is responsible for the management of all authorised sources, the recruitment of potential sources and compliance with force policy, national guidelines and RIPA legislation. Authorisation for all CHIS is given by the Director of Intelligence.

CHIS Handling

Source handlers are responsible to the CHIS controller and operate in a high-risk sphere. They will recruit, handle and co-handle human sources in accordance with the specified requirement of the T&CG to ensure intelligence is collated and gaps in knowledge are filled.

The use of source handlers for intelligence approaches to persons in custody will be determined by the intelligence manager, taking into account the profiles of both the source handler and the suspect.

Source handlers are not allowed to actively recruit sources outside the defined parameters. They are responsible on behalf of the T&CG for recruiting CHIS to infiltrate hard to reach groups, communities and locations in order to assess the levels of threat, and opportunities to reduce crime and improve the quality of life in communities.

They must be trained to national standards and operate in accordance with *ACPO and HMCE (2004) Manual of Standards for Covert Human Intelligence Sources.*

Prison Intelligence

Substantial intelligence benefits can be derived from the employment of prison intelligence officers. The intelligence officer provides the Police Service with an interface with the Prison Service for the mutual benefit of both organisations.

The prison intelligence officer's primary function is to obtain criminal intelligence through the various prison sources, and to develop an in-depth knowledge of prisons and prison procedures that can provide practical support to the investigator. Prison intelligence officers should operate within the Force Intelligence Bureau (FIB) under the command of the Director of Intelligence as the focal point for prison-related issues.

4.10 KEY FUNCTION – INTELLIGENCE SUPPORT FUNCTIONS

A centrally located Authorities Bureau, linked through dedicated IT systems to local intelligence units, enables forces to manage the processes and administration concerned with covert operations and CHIS.

Similarly, management of all authorities and issues requiring access to evidence or intelligence through defined communications systems must be centrally sited in support of the intelligence function. A telecommunications SPOC with accredited, highly trained personnel provides a professional interface internally, with other agencies and externally to the Police Service.

For further information see *ACPO/ACPOS/HMCE (2003) Manual of Standards for Accessing Communications Data.*

4.11 KEY FUNCTION – COMMAND OF TASKING AND CO-ORDINATION GROUPS

NIM minimum standards (see Appendix 2) allow local determination on the chairing of force T&CG meetings. As the model has matured, so forces have recognised the significant benefits to be gained from the Chief Officer chairing the force strategic T&CG (ST&CG). The force strategic assessment (see 8 Intelligence Products) is an essential document in that it not only informs the force ST&CG but is also a core document for use during the business planning process.

Partner engagement during the development of strategic assessments at force and BCU level, has resulted in joint strategic tasking and co-ordination processes, with local authority chief executives and leaders from other key partnerships present.

Such a strategic interface enables the development of jointly defined strategies and clear direction in meeting objectives when operating tactically with crime and disorder partners. It also provides forces with a greater understanding of the intelligence opportunities that may be derived from information exchange protocols and the development of agreements to facilitate this.

4.12 KEY ROLE – TASKING AND CO-ORDINATION ACTIONS MANAGER

Police forces and BCUs should appoint a T&CG Actions Manager to co-ordinate actions resulting from the T&CG. Staff in this role will be empowered to enforce the delivery of actions, arrange and appoint resources where appropriate, monitor progress and report the results to the T&CG in conjunction with the intelligence unit. They may also be responsible for the general running and administration of the T&CG and briefing processes. The appointment of a T&CG Actions Manager prevents intelligence professionals becoming too involved in operational planning and tasking, thereby preserving their objectivity.

4.13 KEY FUNCTION – TACTICAL CAPABILITY

Performance delivery through NIM cannot be achieved if those actions approved by the T&CG are not acted on in a timely manner. Every BCU needs a dedicated, tactically deployable capability that is flexible to respond to the demands of the T&CG. This may include:

- Dogs;
- Public order units;
- Tactical units;
- Patrol officers;
- Neighbourhood units;
- Traffic patrol;
- Air and river support.

In some cases the BCU or force will require resources outside of their own capability which they can access at a higher level.

For suggested configurations of intelligence units and details of the role requirements of NIM, see *ACPO (forthcoming) Practice Advice on Resources and the People Assets of NIM.*

4.14 CHECKLIST OF MINIMUM STANDARDS

Checklist 4: Minimum Standards for People Assets

Standards 41 to 62 relate to people assets and must be implemented by November 2005. **For details on these requirements and how to meet them, see Appendix 2.**

41. Minimum establishment policy.
42. Succession planning.
43. ACPO lead for NIM implementation and development.
44. T&CG chairs.
45. Director of intelligence/head of profession (intelligence).
46. Authorities management.
47. Telecommunications SPOC.
48. Intelligence manager.
49. CHIS controller and designated deputy CHIS controller.
50. Source handler.
51. Analytical capability.
52. Head of profession – intelligence analysis.
53. Analysts accreditation.
54. Field and research capability.
55. Technical support unit capability.
56. Information and intelligence management.
57. Data protection.
58. Dedicated IT support.
59. Briefing capability.
60. Tactical T&CG actions manager.
61. High visibility/strike teams.
62. Joint agency and specialist operations intelligence cells.

Section 5
INFORMATION SOURCES

There are a number of ways in which information is captured on to information management systems. The term, information sources, refers to the different collection processes for source assets.

This section should be read in conjunction with *ACPO (forthcoming) Guidance on the Management of Police Information.*

CONTENTS

5.1 INFORMATION SOURCES

NIM is reliant on access to information, including that which is stored on retrievable systems and often referred to as data. This information may be obtained from a diverse range of sources (see 3 Source Assets) and enables the Police Service to produce a comprehensive picture of policing business and to determine its priorities.

CONSIDERATION OF INFORMATION SOURCES SHOULD INCLUDE:

- Open and closed source information, ie, public access information and structured police systems;
- Information management;
- Sanitisation and risk assessment processes;
- Compliance with DPA and Human Rights Act 1998 (HRA).

The application of information management policies and procedures ensures that the appropriate information is recorded and developed as intelligence, and that this intelligence is maintained and accessible to assist decision making and risk management through the tasking and co-ordination process. All processes concerned with information management must be conducted in compliance with *ACPO (forthcoming) Guidance on the Management of Police Information.*

INFORMATION ENTERS THE ORGANISATION IN ONE OF THREE WAYS:

- It is deliberately sought out and collected – **tasked collection;**
- It is collected as a result of another policing activity – **routine collection;**
- It is given to the police – **volunteered information.**

5.2 TASKED COLLECTION

Tasked collection refers to prioritised information collection on problems and target issues (including offenders and victims) identified within intelligence requirements. This information is usually submitted as an information/intelligence report (5x5x5) from:

- Intelligence collection plans;
- Proactive activity, including the use of surveillance;
- Tasking of CCTV and Automatic Number Plate Recognition (ANPR) systems;
- Tasking of sources (CHIS);
- Searching of internal and external databases, including commercial and partners' databases.

5.3 ROUTINE COLLECTION

Routine collection refers to the collection of information as part of routine operational and policing activity. It focuses on the known intelligence requirement or other issues of policing significance.

Information collected in this way is usually submitted as an information/intelligence report (5x5x5), but it may also be recorded elsewhere such as information within or from:

- Command and control systems;
- Crime recording;
- Criminal investigations, including stand-alone proactive or reactive operational databases/ case management systems, eg, Clue, HOLMES2;
- Fixed penalty and other traffic enforcement;
- Firearms licensing;
- Patrol – reactive attendance and proactive patrolling and stop checks, eg, HORT1's;
- Community and partnership activities and meetings;
- Custody records;
- Case files, criminal justice/case building units;
- Disclosure and vetting checks.

5.4 VOLUNTEERED INFORMATION

Volunteered information is offered to the Police Service by the general public, community contacts and partners. Its collection is focused (but not exclusively based) on the intelligence requirement. Information obtained is usually recorded and submitted on an information/intelligence report (5x5x5) from:

- Any public contact (this may include routine collection through command and control or crime systems);
- Neighbourhood Watch (NHW);
- Crimestoppers.

5.5 ACCESS TO INFORMATION AS AN INTELLIGENCE SOURCE

As can be seen in 3 Source Assets and Appendix 3, many information sources are readily available to the Police Service. Full advantage must be taken of external source opportunities, in particular, partner-agency information. Access to these information sources will enable the Police Service to understand more fully the difficulties faced and to determine (both strategically and tactically) the appropriate methods to adopt to enforce the law, reduce crime and the fear of crime and to improve quality of life.

5.6 COMMUNITY INFORMATION AS AN INTELLIGENCE SOURCE

Community intelligence is local information which, when assessed, provides intelligence on issues that affect neighbourhoods. It also informs the strategic and tactical operational policing of local communities. Information may be direct or indirect and can come from a diverse range of sources including community and partner agencies. It may include issues ranging from the general quality of life in the community to serious crime and terrorism.

5.7 INFORMATION

Not all information will be recorded as intelligence on to intelligence systems through the 5x5x5 process. The required information must, however, be collected, recorded and stored where it can be easily accessed by intelligence officers and analysts in response to the intelligence requirement. For further information see 7 Research, Development and Analysis and 9 Tasking and Co-ordination.

Information will be routinely collected and input on to force systems. This information may or may not be immediately identifiable as being of intelligence value. Where it is immediately recognised as being of value it should be submitted with an initial evaluation on to an information/intelligence report (5x5x5) to the intelligence unit where it will be further evaluated and assessed.

Based on accurate current and historic (in the case of trend analysis) data, a strategic assessment (see 8 Intelligence Products) will define business priorities at both the BCU and force level. Information assets assist in further profiling the problems identified. Exploitation of these assets may require investment in IT, staff training and development of data sharing protocols and policy, as described in 2 System Assets.

Poor data quality, in addition to potentially breaching human rights and data protection legislation, may lead to the use of tactics that are inappropriate, costly and ineffective. Access to timely and high quality internal and external information sources provides police forces with an enhanced picture of crime which assists them in deploying resources efficiently. This, in turn, can impact positively on results and performance.

5.8 INFORMATION EXCHANGE PROTOCOLS

Information exchange protocols and memoranda of understanding (MOU) provide a formalised basis for managing the sharing and exchange of information on a regular basis between forces and agencies. They can cover law enforcement and prosecuting agency information exchange, and Crime and Disorder Act 1998 (CDA) partnership activity which may include non-law enforcement agencies. The protocol agreements provide a formal framework which, although not legally binding, clarify the categories of information that can be exchanged and the process for doing this. The protocols also include the roles and responsibilities of those involved with the management of information.

Detailed guidance, a formatted template and specimens of information exchange protocols under section 115 of the CDA, can be found on the Home Office Crime Reduction tool kit website: http://www.crimereduction.gov.uk/infosharing_guide

5.9 CHECKLIST OF MINIMUM STANDARDS

Checklist 5: Minimum Standards for Information Sources

Standards 63 to 70 relate to information sources and must be implemented by November 2005. **For details on these requirements and how to meet them, see Appendix 2.**

63. Open and closed source data.
64. Intelligence, crime, custody and command and control records available in searchable form.
65. Access to HOLMES2/SCAS/NCF profiling data.
66. Access to live data exchange.
67. Full data integration model.
68. Access to human resources data.
69. Access to external information sources.
70. Cross-border information sharing.

Section 6
INTELLIGENCE/ INFORMATION RECORDING

NIM requires accurate and relevant information to be uniformly recorded onto standardised IT systems so that information can be efficiently retrieved and exchanged with key partners.

This section should be read in conjunction with *ACPO (forthcoming) Guidance on the Management of Police Information.*

CONTENTS

6.1 INTELLIGENCE/INFORMATION RECORDING

Information, once obtained, goes through a recording and evaluation process known as information/intelligence recording. This involves constructing an information management process using skills, people and information technology which results in further intelligence development, research, analysis and the accurate deployment of resources.

INFORMATION AND INTELLIGENCE RECORDING INCLUDES:

- The use of 5x5x5 as a standard evaluation method;
- Standardised systems which are centrally audited and compliant with the Community Security Policy;
- Uniform standards for information input onto IT systems;
- Protocols for the use of intelligence codes and flags to speed collation and retrieval, and to identify links between records;
- Information management and supervision protocols.

Efficient and effective tactical deployment can be achieved by investing in the intelligence/information recording process.

6.2 STANDARDS AND PROCESSES

The minimum standards for intelligence and information recording qualify the need for standards and processes to support NIM. These include the use of standard forms for intelligence reporting and evaluation, common standards for information input, the use of standard IT platforms to enable efficient research, and the use of codes and flags to speed the collation and retrieval of intelligence and to avoid compromise. Data quality assurance protocols are of particular importance to enable effective information management and supervision.

6.3 INFORMATION MANAGEMENT

By communicating the intelligence requirement staff will be aware of the information that needs to be collected. All staff involved in the collection, recording, evaluation, sharing, review, retention and deletion of information must consider the value of that information and any associated risks. Information that falls outside of the intelligence requirement will occasionally be collected and subject to the same considerations.

Information falling into one of the following categories and which is not recorded in another business area, eg, crime report or custody record, should be submitted on a information/intelligence report (5x5x5).

- Police force/BCU/ agency control strategy priorities and intelligence requirements.
- Operational intelligence requirements which relate to current operations.
- Information relating to a control strategy/information requirement of another police force/BCU/ agency, or regional/national issues.
- Information that is relevant to an identified emerging trend or problem.

- High risk issues which may not be included in any of the above, such as
  - Information relating to any risk or threat to the life or personal safety of any known individual or identifiable group against which action may be taken/is possible (*R v Osman*)
  - Information identifying a persistent or problematic offender who creates a threat to the community, including dangerous and sex offenders (eg, offending of minor nature which predicts more serious offending)
  - Information relating to a crime or disorder incident or involving vulnerable people, hate crime and disorder, football-related disorder, negative role models whose minor criminality encourage others to commit crime or create a localised fear of crime, and animal rights activists
  - Information that may preclude employment with access to children
  - Information relevant to an officer safety issue.
- Information relating to any other issues or problems of local significance or which indicates a problematic neighbourhood, tensions or problems within a community group or a signal crime.

The purpose of the Intelligence Unit at all levels of NIM is the management of information and intelligence. This includes accessing and searching other internal and external databases and making appropriate intelligence links to events and people.

Four themes must be considered to manage information.

- **Collecting and recording information for evaluation.** The recognised methods for collection and recording information are a structured information/intelligence report, either as a hard copy 5x5x5 or direct input on to an intelligence database, or information entered on to other business areas.
- **Evaluating information and authorisation of intelligence into the intelligence system.** The use of evaluation codes ensures the appropriate authorisation and evaluation of all information/intelligence received, either by 5x5x5 or by accessing other business areas.
- **Accessing and disseminating intelligence.** A risk assessment must be conducted before intelligence is disseminated to ensure that it is handled appropriately. This will also include the management and handling of search requests.
- **Retaining or deleting intelligence.** A review of intelligence held within the intelligence system must be regularly conducted to ensure that all information is relevant and accurate and fulfils the original, legitimate aims authorising its recording and retention. This includes managing data conflict issues and linking records.

Completing these processes will ensure that relevant intelligence is available for the development of intelligence products which provide information for the tasking and co-ordination process. It will also ensure that the information management function of the intelligence unit is compliant with human rights, data protection legislation and regulatory codes.

Sufficient resources must be made available to carry out the key responsibilities listed above without detriment to operational effectiveness.

6.4 EFFICIENT INFORMATION RECORDING

Efficiency can be achieved through prioritising information recording. A control mechanism ensures that the most important information is recorded first thereby providing a scale of priorities which should be imposed in line with the control strategy and current tactical plans. This will drive the prioritisation of information recording in line with strategic and tactical aims or high risk issues. Secondary issues for information recording may, for example, include information relevant to emerging trends that are not high priority but still require intelligence research.

The use of trained staff and investment in information technology, in particular within input and research functions, is critical to success. Regular proactive sampling of information awaiting recording onto an intelligence system will provide significant benefits. This can be conducted through inspection protocols, data protection or security review.

Research staff and analysts require timely input of accurate information in order to provide meaningful contributions to intelligence products. Inaccurate information such as incorrect postcodes, non adherence to national crime recording standards and limited or incorrect detail regarding stolen property will lead to the development of imprecise intelligence products.

6.5 TACTICAL LEVEL PROTOCOLS

The transfer of intelligence between agencies and the three levels of NIM activity (see National Intelligence Model – Levels of Operation) has been significantly improved by the implementation of NIM. Common language structures, standards, evaluation, assessment and intelligence dissemination are key factors to this success.

Information exchange protocols may be developed at a tactical level and tailored to a particular operation or person. The dissemination of personal and confidential information may be necessary because of the serious nature of the criminal offence or act. The advice of data protection officers and legal services departments should be sought prior to and during the development of protocols.

6.6 THE IMPACT PROGRAMME

Currently, the Police Information Technology Organisation (PITO) is evaluating technological solutions to create a national information exchange capability (IMPACT Programme). This will allow information from existing systems to be stored on a regional basis in a standard format. Access to force legacy systems will assist in the collection of intelligence, research and planning, particularly when operating on regional and national levels.

6.7 PRINCIPLES FOR INFORMATION MANAGEMENT

Police force policies and local procedures should reinforce the following principles.

- Information collected or recorded by the Police Service must be submitted using the approved 5x5x5 form or entered on to another business area.

- The decision to create an information/intelligence report should be based on whether policing purpose grounds have been met regarding the obtaining, recording, reviewing, deletion and dissemination of information. This is defined in *ACPO (2005) Code of Practice on the Management of Police Information* and *ACPO (forthcoming) Guidance on the Management of Police Information.* The main areas that fall within policing grounds include protecting life and property, preserving order, preventing the commission of offences and bringing offenders to justice.

- All information/intelligence reports must be correctly evaluated using the 5x5x5 evaluation method and completed in accordance with guidelines for the submission of national information/intelligence reports. Where appropriate, risk assessments should be completed by the officer submitting the information/intelligence report.

- Information/intelligence reports must be rigorously monitored by a supervisor whose principal responsibility is to quality assure the product, and ensure that it is correctly sanitised, evaluated and subject to a risk assessment. Where improvements in the quality of information/intelligence reports are required, the matter should be raised with the officer concerned and, if appropriate, the officer's line manager.

- Advice regarding the compilation and submission of information/intelligence reports to the required standards must be included in all probationer and supervisor training delivered locally.

- A fast-track procedure for acting on urgent intelligence must be established. Where practicable, this will be passed to the intelligence unit for assessment and a decision on the action to be taken. Where it is necessary to act without delay, staff must be identified to respond to the intelligence following consultation with the duty manager. The daily management meeting may also be a forum for allocating resources to respond to urgent intelligence.

- An electronic or manual action management system must be established to enable intelligence received by the intelligence unit to be acted on and recorded. The system should incorporate an audit trail which allows the assessment of progress and results.

- A system for identifying specific targets that are subject to operational tasking or intelligence collection should be used at all levels of policing. This is commonly known as flagging.

- Targets identified at level 2/3 are subject to policy held by NCIS. The FIB will be the central point of contact for all NCIS flags in line with policy held by the Director of Intelligence.

- A local flagging policy, level 1/2, should be determined to allow speedy collation and retrieval of relevant data for research purposes. This must observe NCIS policy and be developed in association with data protection or security staff.

- The use and subsequent removal of flags on local information systems is managed by the BCU authorising the use of the flag.

6.8 CHECKLIST OF MINIMUM STANDARDS

Checklist 6: Minimum Standards for Intelligence/Information Recording

Standards 71 to 81 relate to intelligence/information recording and must be implemented by November 2005. **For details on these requirements and how to meet them, see Appendix 2.**

71. Sanitisation and risk assessment protocols.
72. Data Protection Act compliance.
73. Agreed dissemination policy.
74. Prioritisation of data input and research.
75. Use of 5x5x5 as standard evaluation.
76. Electronic input of information/intelligence reports (5x5x5).
77. Common standards for data input on to force IT systems.
78. Standardised systems for authorising target selection.
79. Protocols concerning the use of intelligence codes/flags to speed collation and retrieval.
80. Data management and supervision protocols.
81. Performance measurement.

Section 7
RESEARCH, DEVELOPMENT AND ANALYSIS

In-depth research, professional development and skilled analysis all assist in creating quality intelligence products. This section discusses what is essential for conducting quality research, development and analysis.

CONTENTS

7.1 THE VALUE OF INTELLIGENCE

All intelligence should be actionable.

Intelligence is of no value if it does not result in defined intelligence products.

NIM is like any other business model in that it requires products to have a practical application. A useful intelligence product contributes to decision making and helps to guide investigations and/or resource deployment. Intelligence products are at the heart of the tasking and co-ordination process (see 9 Tasking and Co-ordination) and also have great value at all levels of NIM. Intelligence products are used to implement intelligence-led policing as well as to measure its impact on crime reduction, arrests, disruptions and enhanced community security and safety. Research, development and analysis leads to the creation of intelligence products.

Intelligence products are discussed in more detail in 8 Intelligence Products.

7.2 INTELLIGENCE UNIT REQUIREMENTS

The research and development (R&D) capability, which includes the analysis section, is at the heart of the intelligence function. This facility has the responsibility for developing intelligence products and the structured research that informs them.

A successful intelligence function creates qualified and accurate products by using the skills of trained investigators, analysts and researchers working with agreed priorities (commissioned by the T&CGs) and supported by high quality information and IT.

In order for research, development and analysis to take place, the following is required:

- An intelligence collection process based on the intelligence requirement;
- An intelligence collection process focused on the control strategy;
- Access to technical support and surveillance;
- Corporate standard products;
- Information exchange protocols.

In addition, police staff within local and force intelligence units require access to force IT systems which should include as a minimum:

- Local intelligence system;
- Licensing/firearms/domestic violence/stop checks information (if not included in the intelligence system);
- Crime management system;
- Command and control system (operational information);
- Custody system;
- PNC;
- Business information such as performance statistics and public satisfaction;
- National and local ANPR information.

Access to external sources of information through partnership arrangements can provide:

- Community intelligence;
- Non police ANPR sources;
- Neighbourhood Statistics Service and other open source information;
- Health and ambulance service data;
- Fire and rescue service data;
- Social services information.

The development of intelligence products is only possible when knowledge, analysis and systems are established. The quality of intelligence products depends, therefore, on management creating and maintaining the right conditions for intelligence activity.

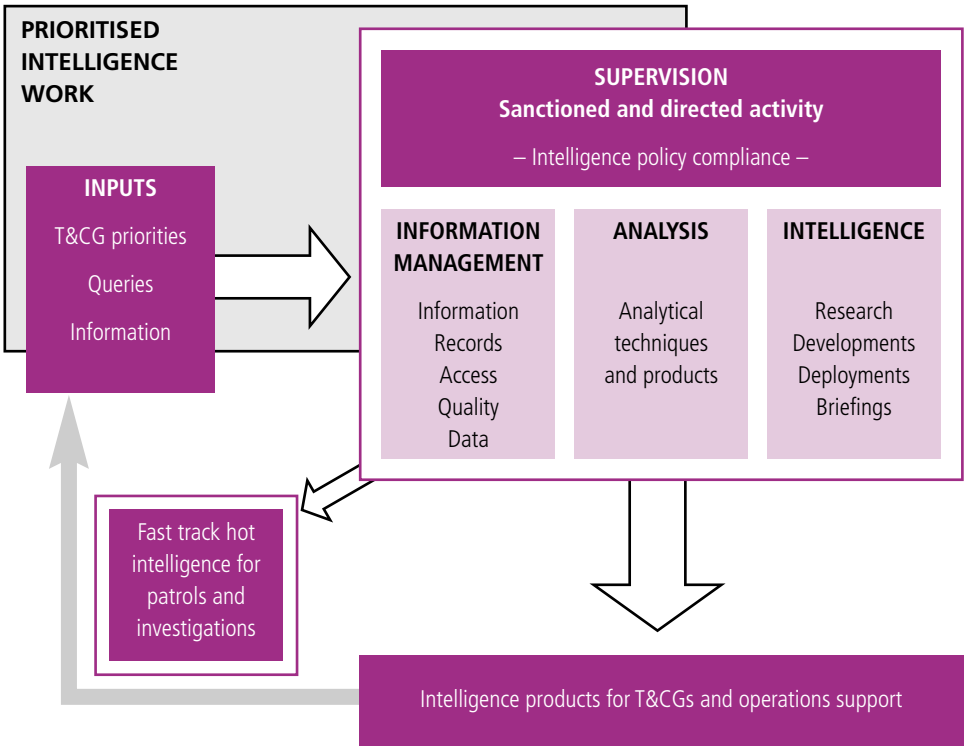
7.3 INTELLIGENCE UNIT STRUCTURES

A typical intelligence unit at a BCU level will include all of the components described in the minimum standards for people assets, see Appendix 2, entries 82 to 95. Resource levels will be determined by need and as a result of a local force resource policy decision. A force level intelligence capability may include covert resources or, in some cases, may be partially amalgamated with departments such as Special Branch. Provided that NIM minimum standards are met, resources will be dictated by force priorities.

A number of factors have to be considered when determining resource levels. Whether within a FIB or BCU intelligence unit, factors such as the size of the organisation, the resources available and the problems being faced will determine how these levels are set.

Information management and research, development and analysis are core functions within the intelligence unit. CHIS handling is closely aligned to an intelligence unit but separated by sterile corridor procedures. Each of these business areas focus on prioritised intelligence work as established by command and defined by the control strategy and intelligence requirements. The intelligence manager is in charge of the intelligence unit and responsible for co-ordinating all intelligence activity in the BCU or force. For further information see 6 People Assets and *ACPO (forthcoming) Practice Advice on Resources and the People Assets of NIM.*

FIGURE 2 Intelligence – Internal Process



The intelligence manager and CHIS controller should be separated when structuring the intelligence function. This arrangement may, however, be difficult to achieve in some forces. In such cases, the intelligence manager sits centrally above all the other intelligence capabilities and breaches the sterile corridor. This is not an ideal solution, although this approach does have significant benefits when complying with the CPIA, and when reviewing intelligence material for revelation and disclosure. It is unusual to find dedicated intelligence disclosure officers within the intelligence function and this responsibility often falls to the Intelligence Manager. Mechanisms must be established to ensure that any intelligence material (including that provided by sources) can be researched and submitted to the disclosure officer, particularly where such information could undermine the prosecution or assist the defence.

For further information see *ACPO and HMCE (2004) Manual of Standards for Covert Human Intelligence Sources* and *ACPO (forthcoming) Practice Advice on Resources and the People Assets of NIM.*

7.4 TASKING

The Intelligence Manager is responsible for tasking the research and development function in line with T&CG actions. These actions should be recorded in electronic form and provide precise detail of the T&CG requirements. This is in accordance with national good practice for major crime investigations which recommends the use of such policy files. Recording tasking decisions in a policy file is of particular benefit when tasking and reviewing staff according to priority needs.

7.5 REGULAR MEETINGS

Tasked actions within the research and development function form the basis of regular intelligence unit meetings chaired by the intelligence manager. These meetings, which are distinct from the T&CG meetings, are usually held on a weekly basis following the T&CG meeting. Intelligence managers may also conduct short daily reviews as these allow revision of actions, provide focus and the opportunity to rapidly change direction if an issue of high risk comes to note which requires fast action. The purpose of these meetings is to remain on track with prioritised intelligence work in accordance with control strategy priorities, and not to become diverted from these unless it is essential to do so.

7.6 INTELLIGENCE COLLECTION PLANNING

The primary responsibility of the intelligence capability is to develop intelligence products. This requires intelligence collection planning to take place. Research and development officers are responsible for the development of intelligence collection plans and these should make use of all the available information sources.

Intelligence collection planning relies heavily on the use of analytical products and focuses on the intelligence requirement. Due consideration must also be given to the cost of employing covert or intrusive surveillance to gather the required intelligence, and such methods should only be used where absolutely necessary.

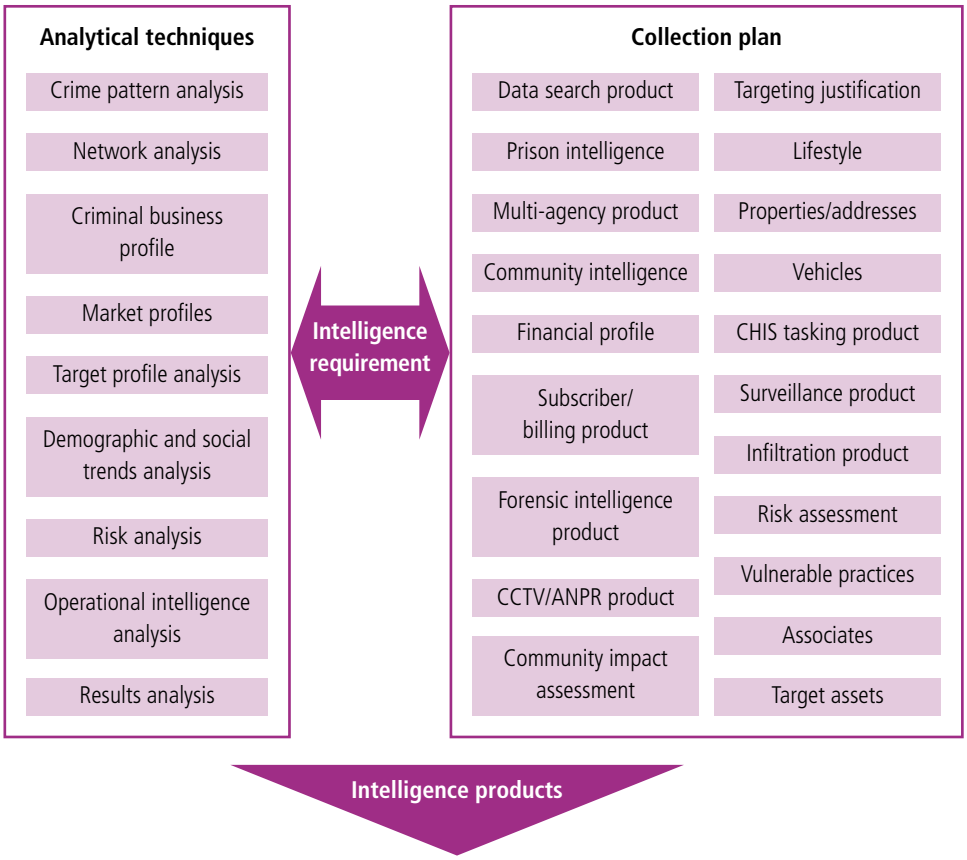
The research function must have access to a range of tactical options, including covert tactics and these may be found either centrally or locally. This requires a clear tasking protocol for level 2 resources which may not necessarily require the sanction of the level 2 T&CG. Such resource allocation protocols must be agreed between BCU command and the person responsible in force for intelligence or covert operations.

The range of capabilities available for intelligence collection include:

- Undercover officers, test purchase operatives and decoys;
- Covert surveillance, both mobile and static;
- Telecommunications SPOC;
- Financial investigation unit;
- Forensic computer expertise;
- Level 2 DSU;
- Force TSU;
- Road safety/traffic department;
- ANPR (fixed site, CCTV linked, in car);
- Force operational support services.

It may be appropriate to make use of CHIS during intelligence collection. Risk, both personal and organisational, must be taken into account and measured against the likely benefits of CHIS use. Decisions to make use of CHIS may require access to other specialist tactical services, particularly surveillance, to enable speedy resolution in the case of time-critical intelligence.

FIGURE 3 Intelligence Collection Planning



7.7 STANDARDISATION

NIM derives much of its strength from standardisation and a corporate approach, being particularly prescriptive when developing intelligence products. Standardising recording and other processes is clearly beneficial, particularly when information is being assessed for intelligence opportunities during the research phase. The use of standard formats is also highly desirable in the following processes:

- DSU tasking and response;
- Surveillance tasking and response;
- Prison intelligence tasking and response;
- Other partner agency tasking and response (such as securing CCTV footage or obtaining access to stored information).

For further information see *ACPO and HMCE (2004) Manuals of Standards for Covert Human Intelligence Sources* and *ACPO and HMCE (2004) National Standards in Covert Investigations Manual of Standards for Surveillance.*

The use of the 5x5x5 information/intelligence report is not appropriate for such tasking. A risk evaluation and grading system, particularly when accessing external information sources is, however, warranted.

7.8 THE TECHNICAL INTELLIGENCE GATHERING FUNCTION

The use of a technical intelligence and evidence gathering capability has significant benefits for BCUs, enabling greater tactical flexibility in meeting the requirements of the intelligence manager and T&CG actions. The TSU Manager and Procurement Officer will manage this role ensuring that high technical standards are maintained and that health and safety regulations are complied with.

Standardisation must extend to the purchase of technical equipment to support the BCU intelligence function. NIM minimum standards reinforce the need to engage with the local force technical support unit procurement officers prior to purchasing any such equipment. This is to ensure value for money and the procurement of equipment approved by the HOSDB.

For further information see 4 People Assets, *ACPO (forthcoming) Practice Advice on Resources and the People Assets of NIM, ACPO and HMCE (2004) National Standards in Covert Investigations Manual of Standards for Surveillance* and *ACPO (2004) Deployment Standards for Technical Support in Tackling Volume Crime.*

7.9 SENIOR INVESTIGATING OFFICERS AND THE INTELLIGENCE FUNCTION

Intelligence unit staff, including a research and development capability, should be appointed to support senior investigating officers (SIO) when investigating a major or serious crime. Where such a need arises, negotiation and agreement will be required to enable the intelligence unit to function effectively in support of T&CG processes and to support the SIO. A local force protocol and agreed structure for murder investigation intelligence cells should be developed, and this may drive a joint training programme for intelligence staff and murder investigators.

Actions allocated to the intelligence function should be prescriptive and recorded. This will enable the accurate development of a target/problem profile when required by the SIO. Non-prescriptive requests lead to an interpretation of needs and, often, wasted staff time.

For further information see *ACPO (2000) Murder Investigation Manual (MIM)* and *ACPO (2000) MIRSAP Guidance on Major Incident Room Standardised Administrative Procedures Manual (forthcoming November 2005).*

7.10 THE ANALYST

The role of the analyst is pivotal within the research and development capability. When supported by a research assistant or assistant analyst, the intelligence analyst can focus on analysing the information, assisting in the compilation of intelligence products and determining the key intelligence requirements. Using the analyst in this way will enable further effective profiling. Analysts should play a key role in compiling intelligence products together with other intelligence officers and investigators. Managers often make the fundamental mistake of using analysts' skills inappropriately. It is the manager's responsibility, however, to take ownership of the production of the intelligence products by the efficient use of analysts.

For further information on the role of the analyst, see 4 People Assets, *ACPO (forthcoming) Practice Advice on Resources and the People Assets of NIM* and *ACPO (forthcoming) Practice Advice on Tasking and Co-ordination.*

7.11 ANALYTICAL TECHNIQUES AND PRODUCTS

The use of defined analytical techniques and products created using recognised analytical tools and methods is fundamental to the development of intelligence products. The specifics of the situation will determine the number and combination of analytical techniques and products that should be drawn on to inform intelligence product requirements. A multi-dimensional view of the problem can be acquired by overlaying the results of analytical work. Analytical options include the following.

- **Crime pattern analysis** – a generic term for a number of related disciplines such as crime or incident series identification, crime trend analysis, hot spot analysis and general profile analysis.
- **Demographic/social trends analysis** – is centred on demographic changes and their impact on criminality. It also analyses social factors such as unemployment and homelessness, and considers the significance of population shifts, attitudes and activities.
- **Network analysis** – not only describes the links between people who form criminal networks, but also the significance of these links, the roles played by individuals and the strengths and weaknesses of a criminal organisation.
- **Market profiles** – are continually reviewed and updated assessments that survey the criminal market around a particular commodity, such as drugs or stolen vehicles, or of a service, such as prostitution, in an area.
- **Criminal business profiles** – contain detailed analysis of how criminal operations or techniques work, in the same way that a legitimate business might be explained.
- **Risk analysis** – assesses the scale of risks posed by individual offenders or organisations to individual potential victims, the general public, and also to law enforcement agencies.
- **Target profile analysis** – embraces a range of analytical techniques to describe the criminal, their criminal activity, lifestyle, associations, the risk they pose and their strengths and weaknesses in order to give focus to the investigation targeting them. Profiles may also focus on victims and vulnerable persons.
- **Operational intelligence assessment** – involves evaluating incoming intelligence to maintain the focus of an operation on previously agreed objectives, particularly in the case of a sizeable intelligence collection plan or other large-scale operation.
- **Results analysis** – evaluates the effectiveness of law enforcement activities, for example, the effectiveness of patrol strategies, crime reduction initiatives or a particular method of investigation.

For more information on analytical options contact the National Analyst Working Group (details in Appendix 6) and see *ACPO (forthcoming) Practice Advice on Tasking and Co-ordination.*

7.12 CHECKLIST OF MINIMUM STANDARDS

Checklist 7: Minimum Standards for Research and Development

Standards 82 to 95 relate to research and development and must be implemented by November 2005. **For details on these requirements and how to meet them, see Appendix 2.**

82. Access to technical support/surveillance equipment.
83. National technical support unit guidance used as a minimum standard (Yellow Book).
84. Other standard products.
85. Standards for delivery of product/services.
86. MOU/information exchange protocols.
87. Intelligence specialists/researchers trained to national standards.
88. System for development and review of intelligence collection plans.
89. Data collection directed and focused on control strategy.
90. Development and review of intelligence trigger plans.
91. Access to other agencies' technical resources and expertise.
92. Align joint intelligence cells to force intelligence process.
93. Tasking capability of wider intelligence assets.
94. Impact and benefit assessment.
95. Development of enhanced target and problem profiles.

Section 8
INTELLIGENCE PRODUCTS

NIM uses four intelligence products and these provide the information on which strategic and tactical decisions are made.

This section should be read in conjunction with *ACPO (forthcoming) Practice Advice on Tasking and Co-ordination.*

CONTENTS

8.1 CREATION OF INTELLIGENCE PRODUCTS

Intelligence officers develop intelligence collection plans detailing specific requirements to obtain information from many different sources. Analysts interpret the raw information collected to assist in the compilation of intelligence products which then enable the Police Service to accurately profile crime and disorder problems. The T&CG use intelligence products to make decisions and approve actions.

A quality intelligence product depends on:

- An intelligence requirement set by the T&CG in accordance with force and local priorities;
- A well developed intelligence collection plan, to direct the gathering of information;
- The use of analytical techniques and products.

8.2 THE FOUR INTELLIGENCE PRODUCTS

- **Strategic assessments** – drive the business of the ST&CG. The assessment gives an accurate overview of the current and long-term issues affecting the police force, BCU or region. The T&CG use the assessment to set the control strategy and intelligence requirement.
- **Tactical assessments** – drive the business of the TT&CG. The assessment identifies the shorter-term issues in a police force, BCU or region in accordance with the control strategy. The T&CG use the assessment to amend the intelligence requirement where necessary.
- **Target profiles** – the T&CG commission target profiles to secure a greater understanding of either a person (suspect or victim) or group of people, in line with the control strategy priorities or high risk issues.
- **Problem profiles** – the T&CG commission problem profiles to secure a greater understanding of established and emerging crime or incident series, priority locations and other identified high risk issues. It also recommends opportunities for tactical resolution in line with the control strategy priorities or high risk issues.

These products are discussed further in *ACPO (forthcoming) Practice Advice on Tasking and Co-ordination.*

The control strategy and intelligence requirement are discussed in 9 Tasking and Co-ordination and in *ACPO (forthcoming) Practice Advice on Tasking and Co-ordination.*

8.3 DEVELOPMENT OF ASSESSMENTS

Analysts need evaluated and accurate data to develop strategic and tactical assessments. They also need sufficient time to carry out the research and write a report. The development of a strategic assessment requires long-term analysis. It is a dynamic process of information collation and research that should **not** be reviewed every six months, but should be **continually** reviewed.

8.4 STRATEGIC ASSESSMENTS

The strategic assessment drives the business of the ST&CG giving an accurate overview of the current and long-term issues affecting the BCU, force or region. It also makes recommendations for prevention, intelligence and enforcement priorities for the crime and disorder problems identified within it. The ST&CG members use the assessment to set a control strategy and decide on the intelligence requirement.

The strategic assessment is based on the research and analysis of a wide range of information sources. Information should not be restricted to police information on criminal activity and criminals. It should also include, where available, material from a range of sources including external information on public perception, public satisfaction surveys and health, welfare and education data. Local arrangements made to capture the effect of crime and disorder on the lives of residents in a neighbourhood can provide a valuable insight to the strategic assessment, and can also assist police officers to understand the fear of crime and the impact that localised crime and disorder can have on communities.

For more information on the use of community information, see *ACPO (2005) Practice Advice on Professionalising the Business of Neighbourhood Policing (Draft).*

8.5 LINKS TO POLICING PLANS

Strategic assessments should be considered alongside the priorities detailed within the *National Policing Plan, Force Policing Plan, Community Safety Strategy,* existing local police performance and CDRP objectives. The strategic assessment is not a performance review, but performance should also be considered by evaluating progress against previously set control strategy priorities.

The assessment should also consider the political, economic, social, technological, environmental, legal and organisational issues (PESTELO) that may present a risk to the process. These issues should be summarised in the assessment rather than provided in detail. The T&CG can commission further profiling as a result of any specific identified risks.

The strategic assessment must be linked to the policing plan. There is room within the strategic assessment, however, for hypothesis testing and speculative thinking about future policing problems.

8.6 SETTING THE CONTROL STRATEGY AND INTELLIGENCE REQUIREMENT

The strategic assessment highlights the gaps in intelligence which need to be filled and this forms the basis of the intelligence requirement. When the ST&CG have agreed the control strategy they will sanction the intelligence requirement, which the intelligence manager is then responsible for producing.

The intelligence requirement is a dynamic document that focuses not only on priorities but also on other key threats identified in the strategic assessment. The purpose of the intelligence requirement is to gain more information on crime and disorder problems. Gaining that knowledge will result in identifying new intelligence gaps. The intelligence requirement should remain under continual review and any amendments to it can be sanctioned by the TT&CG.

The control strategy is set as a direct result of the strategic assessment and will only ever be amended by the ST&CG.

The strategic assessment is a long term, high level analysis of policing problems and should be compiled to reflect the minimum content set out in recognised templates. For further information see *ACPO (forthcoming) Practice Advice on Tasking and Co-ordination.* Additional elements may be included in the assessment, provided that the minimum content is still met.

8.7 FEATURES OF THE STRATEGIC ASSESSMENT

There are several principles which should be taken into account when developing the strategic assessment. These include the strategic assessment being a document which:

- Drives the ST&CG;
- Is compiled in collaboration with all policing functions, and not solely produced by an analyst;
- Is informative and relevant to managers;
- Coincides with the commencement of planning for the Policing Plan;
- Examines longer term issues affecting BCUs, police force or region;
- Considers issues that may impact on neighbouring command areas;
- Looks forward, not just taking account of current priorities but also evaluating and reporting on emerging threats;
- Examines and comments on whether the current control strategy is working;
- Makes recommendations for setting a new control strategy and intelligence requirement, or amending the existing documents;
- Remains focused on recommendations for prevention, intelligence and enforcement;
- When performance information is used, includes an explanation of reasons for any changes that have occurred;
- Shows evidence of data analysis;
- Takes account of the storage and retention of assessments.

The strategic assessment should include as a minimum:

- Period of time covered, author, document unique reference number (URN) and date for deletion;
- Sensitivity of the contents (GPMS);
- Aim and scope of the report;
- Methods used, including information sources;
- External priorities to be considered when setting the control strategy, ie, government or local police force priorities;
- General picture since the last assessment period, ie, levels of all crime/incidents;
- Major areas of concern including the current control strategy and emerging issues.

The current and future picture of any identified crime and/or disorder problem should be summarised. Any changes since the last assessment should be identified and the known or suggested reasons for these changes highlighted. The assessment should also include factors that may cause changes in the future and identify any intelligence gaps.

PESTELO issues should be examined within each crime and disorder problem.

The report should end with the following information:

- A summary of the PESTELO issues as they impact on each crime and disorder problem and on the BCU, force or region as a whole;
- Recommendations for the new control strategy;
- An outline of the intelligence requirement;
- A summary of the most appropriate prevention, intelligence and enforcement priorities.

8.8 TACTICAL ASSESSMENTS

The tactical assessment drives the business of the TT&CG. The assessment identifies the short term issues in a BCU, force, or region, in accordance with the control strategy. The tactical assessment should be informed by information from a wide range of sources, in particular, records held on police databases or received through Local Action Group (LAG) forums.

The tactical assessment is a review of recent performance and actions set at previous TT&CG meetings. It also identifies emerging patterns and trends. The analyst preparing the assessment uses the tactical menu to recommend subjects that should be targeted, geographic locations regarded as priority locations, and series of crime and disorder that are emerging or which need greater examination. The TT&CG chairperson will commission the production of target and problem profiles with which to inform and support further operational activity. High risk issues which may fall outside of the control strategy or intelligence requirement will also be considered for action, eg, a vulnerable missing person, identified signal crime or intelligence about a high risk offender.

Further information on tactical assessments can be found in *ACPO (forthcoming) Practice Advice on Tasking and Co-ordination.*

8.9 FEATURES OF THE TACTICAL ASSESSMENT

Several principles should be taken into account when the tactical assessment is developed. These include the tactical assessment being a document which:

- Drives the TT&CG;
- Is compiled in collaboration with, rather than solely by an analyst;
- Assists in the management of current and new target and problem profiles;
- Considers short term issues affecting the BCU/force/region;
- Will be structured around control strategy priorities or matters of high risk;
- Reflects the tactical menu;
- Examines current tactical activity;
- Is forward-looking and identifies new problems and targets;
- When performance information is used, includes an explanation of why changes have occurred;
- Shows evidence of data analysis;
- Takes account of the storage and retention of assessments.

The tactical assessment should include as a minimum:

- Period of time covered, author, document URN and date for deletion;
- Sensitivity of contents (GPMS);
- Purpose and scope of the report;
- Methods used, including information sources;
- Progress on the current target and problem profiles;
- Results of previous TT&CG actions and an assessment of impact and further recommendations;
- Overview of the crime/incident picture since the last tactical assessment, and predictions for the next reporting period;
- Progress on the control strategy priorities since the last tactical assessment and predictions for the next reporting period;
- New problems and targets for TT&CG consideration;
- Significant events and operations likely to impact in the area in the short to mid-term;
- Predicted priorities and recommendations for prevention, intelligence and enforcement based on the contents of the assessment.

8.10 PRE-READ OF ASSESSMENT PRODUCTS

The strategic and tactical assessment should be circulated to all members of the respective ST&CG or TT&CG so that it can be read before a meeting. In order to improve the quality and efficiency of decision making all members must have an in-depth knowledge of the content of the strategic or tactical assessment prior to the meeting.

8.11 TARGET PROFILES

The chairperson of the T&CG commissions a target profile to secure a greater understanding of a person (suspect or victim) or group of people who require targeting, in line with the control strategy priorities or high risk issues. The target profile should contain sufficient detail to initiate or support ongoing, target operations but should only include directly relevant information. It should also recommend the best course of action to take and outline the specific intelligence requirement for suggested activity.

Operational commanders use target profiles to assist them in making decisions about the deployment of resources to targeting activity, as well as the tactics to apply. The content of a target profile will vary depending on the nature and significance of subjects. For example, the profile may contain a detailed investigation of a subject and their activity, or simply a brief review of the subjects' recent activities and current associates. The activity undertaken must be proportionate to the crime and disorder problem identified.

8.12 TARGETING AND PROLIFIC AND PRIORITY OFFENDERS

Targeting offenders is included under the heading subjects as one of the four components of the tactical menu. Target profiles should be commissioned by the TT&CG and allocated a specific owner responsible for the execution of any activity in relation to that subject. Target profiles can also be commissioned by the SIO in a major enquiry. This control over the commissioning process will ensure that the correct product is provided, thereby reducing wasted analytical effort.

When identifying subjects to target, the T&CG should take account of the current national Prolific and Other Priority Offenders Strategy. This strategy directs local police and their multi-agency partners to reduce the offending behaviour of certain individuals who are selected by using the following criteria:

- The nature and volume of the crimes they are committing;
- The nature and volume of other harm they are causing, eg, by virtue of their gang leadership or anti-social behaviour;
- Other local criteria based on the impact of the individuals concerned on their local communities.

This identifies individuals who are the most prolific offenders, the most persistently anti-social in their behaviour and those who pose the greatest threat to the safety and security of their local communities. Invariably, such issues will directly relate to the control strategy. See *Home Office (2005) Prolific and Other Priority Offenders Strategy* at: http://www.crimereduction.gov.uk/ppo.htm

8.13 FEATURES OF THE TARGET PROFILE

There are several principles that should be taken into account when developing a target profile. These include the profile being a document which:

- Provides a clear picture of the intelligence assembled on a target;
- Is compiled in collaboration with, and not solely by, an analyst;
- Identifies intelligence gaps;
- Makes recommendations for the prevention of crime, intelligence collection and law enforcement plans;
- Enables managers to make resource decisions and to determine tactics;
- Enables managers to prioritise targets;
- Provides justification for actions;
- Ensures legislative requirements are fulfilled;
- Must be authorised by the T&CG or intelligence manager and referred to the TT&CG for information and review at the next meeting;
- Must show evidence of information analysis;
- Considers the storage and retention of profiles.

The target profile should include as a minimum:

- File location, author and date for deletion;
- Sensitivity of the document;
- Reasons for targeting an individual;
- Operational objectives;
- Justification;
- Authorisation of initial development;
- Ratification by the TT&CG;
- Personal record;
- Summary of criminal record (where appropriate);
- Target profile analysis;
- Intelligence collection plan;
- Target/enforcement plan;
- Prevention plan;
- Risk assessment.

Additional elements can also be included in the target profile where relevant, including, for example:

- Surveillance information;
- Communications information;
- Financial information.

During the target operation it may be beneficial to carry out an operational intelligence assessment. It may also be beneficial to carry out a results analysis at the end of the operation. The use of each of these assessments depends on the objectives set at the start. The target profile should include those objectives and the likely need for any further assessments. Where the assessments are carried out they should be used to inform the target profile. The target profile should then include the predicted priorities and recommendations for prevention, intelligence and enforcement.

Further information on target profiles can be found in *ACPO (forthcoming) Practice Advice on Tasking and Co-ordination.*

8.14 PROBLEM PROFILES

A problem profile is a report produced after a detailed investigation of a problem faced. The T&CG chairperson commissions a problem profile to obtain a greater understanding of an established or emerging crime or incident series and problem locations in line with the control strategy priorities or other high risk issues. The problem profile should contain sufficient detail to initiate or support an ongoing operation but only include information that is directly relevant to it. It should also recommend the most appropriate course of action to take and outline the specific intelligence requirement for recommended activity.

Operational commanders use problem profiles to assist them in making decisions about resource deployment to resolve problems, as well as the tactics to apply. The content of a problem profile will vary according to the nature and significance of the problem. The activity undertaken must be in proportion to the identified crime and disorder problem.

Problem profiles should be commissioned by the T&CG at either the strategic or tactical level, and allocated a specific owner responsible for resolving that problem. Such control over commissioning will ensure that the appropriate product is provided, thereby reducing wasted analytical effort. It will also ensure efficient policing of problems that are having a significant impact on a community.

Problem profiles may result in the identification of specific individuals for whom it is appropriate to compile a target profile. For example, a problem profile about an area might identify a drug dealer who has customers that commit a significant proportion of crime in that location. A problem profile in this instance would lead to a target profile, but this will not always be the case.

Some problem profiles may relate to neighbourhood policing issues. Those that originate from the TT&CG process will be in relation to high risk, short term issues. Long term problem profiles, however, may be developed and maintained by local teams. These profiles provide information to the BCU tactical and strategic assessments and form an integral part of the T&CG process. A timely free-flow of information between neighbourhood policing teams and the intelligence unit is essential for this.

8.15 FEATURES OF A PROBLEM PROFILE

Several principles should be taken into account when developing a problem profile. These include the profile being a document which:

- Provides a clear picture of the intelligence assembled on a problem;
- Is compiled in collaboration with, and not solely by, an analyst;
- Identifies intelligence gaps;
- Makes recommendations for prevention, intelligence collection and enforcement plans;
- Enables managers to make resource decisions and determine tactics;
- Enables managers to prioritise problems;
- Provides justification for actions;
- Ensures legislative requirements are fulfilled;
- Must be authorised and co-ordinated by the T&CG or intelligence manager and referred to the TT&CG for information and review at the next meeting;
- Shows evidence of information analysis;
- Considers the storage and retention of profiles.

As a minimum, the problem profile should include:

- File location, author and date for deletion;
- Sensitivity of document;
- Reasons for targeting the problem;
- Operational objectives;
- Justification;
- Authorisation of initial development;
- Ratification by T&CG;
- Analysis of the problem;
- Intelligence collection plan;
- Prevention plan;
- Investigation/enforcement plan;
- Risk assessment.

A problem profile may also include a trigger plan if it is relevant and useful. During the period of activity to resolve a problem it may be beneficial to carry out an operational intelligence assessment. It may also be beneficial to carry out a results analysis at the end of the activity. The use of each of these assessments depends on the objectives set at the start. The problem profile should include those objectives and the likely need for any further assessments. Where the assessments are carried out they should inform the problem profile which should then include the predicted priorities and recommendations for prevention, intelligence and enforcement.

Further information on problem profiles can be found in *ACPO (forthcoming) Practice Advice on Tasking and Co-ordination.*

8.16 SELECTION CRITERIA

The T&CG commission the development of target and problem profiles and allocate specific owners to them. Problem profiles originate from either the strategic or tactical assessment, with authorisation and ongoing action co-ordinated from either group. Target profiles can only originate from the tactical assessment and will be authorised and co-ordinated by the TT&CG. Targets and problems should be approved for action based on the intelligence available in the strategic or tactical assessment.

Target profiles can be approved for action when they relate to one of the following:

- A serious/high risk offender
- An offender responsible for a crime series
- A prolific or priority offender
- A repeat or vulnerable victim identified as being at high risk

And they are in line with the control strategy and/or

- When current intelligence concerning their vulnerability, criminal activity or intent justifies targeting
- Targeted police activity is likely to disrupt the target in the short to mid term
- When they identify new targets.

Problem profiles should be approved for action when they are one of the following:

- In line with the control strategy;
- Of a serious/high risk nature;
- Concerned with a crime or incident series;
- Commissioned as a neighbourhood policing problem profile.

The production of a target profile may have implications for the person targeted in respect of their right to privacy under the HRA, Schedule 1, Article 8. Justification for the selection of targets and the tactics deployed must comply with the principles contained within the Act and associated case law.

A target or problem profile is a living document and should always be kept up to date while the individual is under investigation or a problem is being worked on. Further information on target and problem profiles can be found in *ACPO (forthcoming) Practice Advice on Tasking and Co-ordination.*

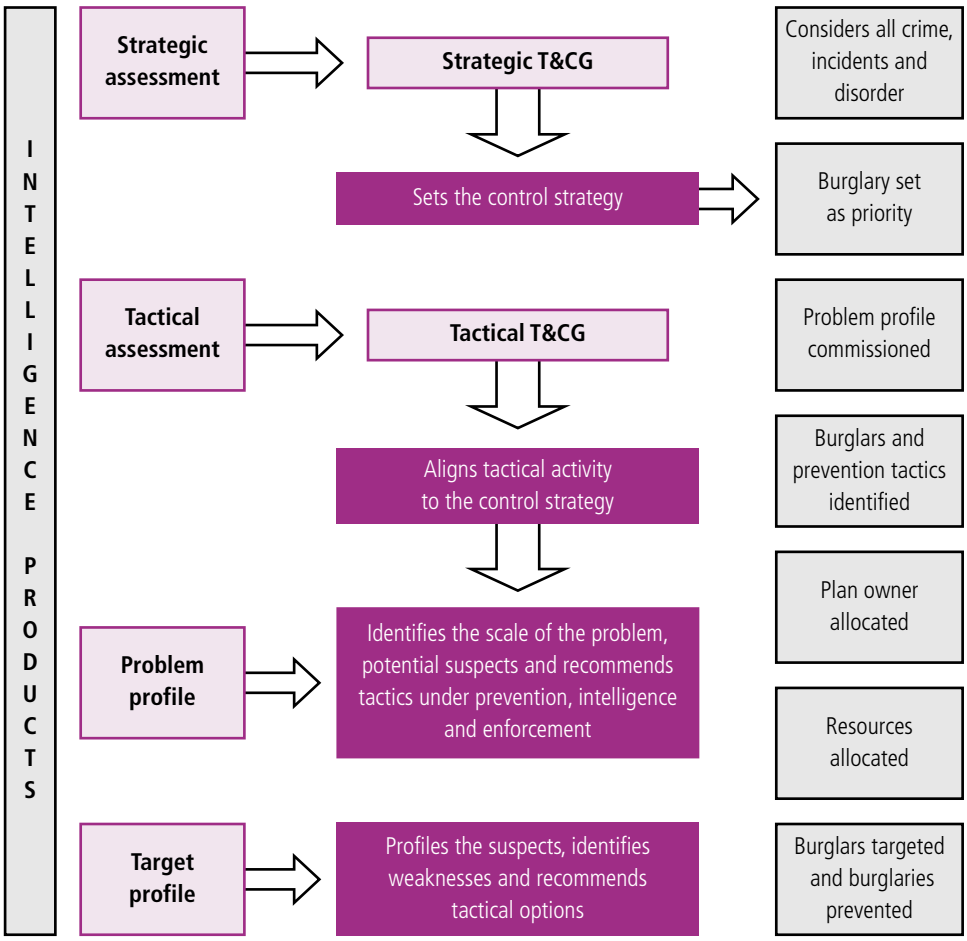
8.17 OWNERSHIP OF INTELLIGENCE PRODUCTS

Commanders own the intelligence products. The intelligence manager is responsible for the creation of the products and will ensure that analysts and intelligence officers work together to develop them. Further collaboration with enforcement and prevention specialists will be required to develop recommendations within the products in order to aid decision making at T&CG meetings.

8.18 RELATIONSHIP OF THE PRODUCTS

Figure 4 shows how the intelligence products may interrelate when tackling an identified problem (in this example, burglary).

FIGURE 4 How the Intelligence Products Interrelate



For further information see *ACPO (forthcoming) Practice Advice on Tasking and Co-ordination.*

8.19 CHECKLIST OF MINIMUM STANDARDS

Checklist 8: Minimum Standards for Intelligence Products

Standards 96 to 109 relate to intelligence products and must be implemented by November 2005. **For details on these requirements and how to meet them, see Appendix 2.**

96. Force policy dictating corporate standards of products.
97. Force policy dictating timing and circulation of products.
98. Force policing/business plan informed by intelligence products.
99. Strategic assessments.
100. Tactical assessments.
101. Target/problem profiles only commissioned by T&CG, intelligence manager or SIO in major enquiry.
102. Applying the analytical products and techniques.
103. Management ownership.
104. Pre-circulation and reading of products pre-T&CG.
105. Analyst as a standing member at T&CG.
106. Intelligence assessment flows.
107. Intelligence exchange.
108. Operational intelligence assessment.
109. Command training/appreciation programme relative to intelligence products and analysis.

Section 9
TASKING AND CO-ORDINATION

The strategic and tactical T&CG process is pivotal to the delivery of NIM. A T&CG is a decision-making and resource management body. NIM tasking and co-ordination processes link with community partnership structures.

This section should be read in conjunction with *ACPO (forthcoming) Practice Advice on Tasking and Co-ordination* and *ACPO (2005) Practice Advice on Professionalising the Business of Neighbourhood Policing (Draft).*

CONTENTS

9.1 TASKING AND CO-ORDINATION

The T&CG process provides managers with a decision-making mechanism with which to manage their business both strategically and tactically. Proactive leadership is an essential requirement in the T&CG process. Management decisions must be based on a full understanding of the problems faced and enable managers to prioritise the deployment of resources at their disposal.

Tasking and co-ordination is vital to the NIM process. Police forces must, therefore, be compliant with minimum standards 110 to 124, see Appendix 2.

The T&CG process is explained in *ACPO (forthcoming) Practice Advice on Tasking and Co-ordination.*

9.2 LEVELS OF OPERATION

T&CGs sit in their strategic and tactical formats at level 1 (local BCU), level 2 (force and regional) and level 3 (national). Care must be taken not to confine work to these levels in isolation. Issues at the next level must be taken into account to ensure that opportunities are not missed, and that appropriate resources are applied.

There is no recognised T&CG process below that of level 1. Police forces operating to sector and geographic policing methods retain the requirement to deliver tasking and co-ordination at BCU as the lowest level. This forum tasks geographically deployed staff with actions determined by BCU strategic priorities and emerging issues.

9.3 STRATEGIC TASKING AND CO-ORDINATION

The purpose of the ST&CG is to:

- Consider the strategic assessment;
- Set and amend the control strategy, where necessary;
- Sanction the intelligence requirement;
- Set the prioritisation of resources.

The group consists of senior managers in the local force or BCUs including those from operations, roads policing, business and administration, training, technology, forensics, intelligence management and analysis.

Some police forces have introduced partner agencies to the ST&CG. Senior representatives from police authorities, CDRP, the Crown Prosecution Service (CPS) and other key agencies are important contributors to this process and should be appointed by mutual consent.

The ST&CG should be chaired by the owner of all police resources at the appropriate level. This would be the chief or deputy chief constable at force level, or the commander or designated deputy at BCU level.

9.4 FREQUENCY OF ST&CG MEETINGS

The ST&CG may sit as often as once every three months. Minimum standards, however, advocate sitting every six months with a three-monthly interim review. A strategic assessment is usually necessary every six months, with a shorter update report produced for the quarterly review. Any need to engage in a full strategic assessment at the quarterly review stage will be established and delegated to the intelligence manager for action.

9.5 STRATEGIC PRIORITIES

NIM is concerned with the proactive deployment of resources to reduce the crime and disorder problems that are detrimental to the quality of life of communities. The need to secure intelligence in line with policing priorities is fundamental to NIM. This will ensure that both strategically and tactically, all information that may impact on decision making is clearly outlined.

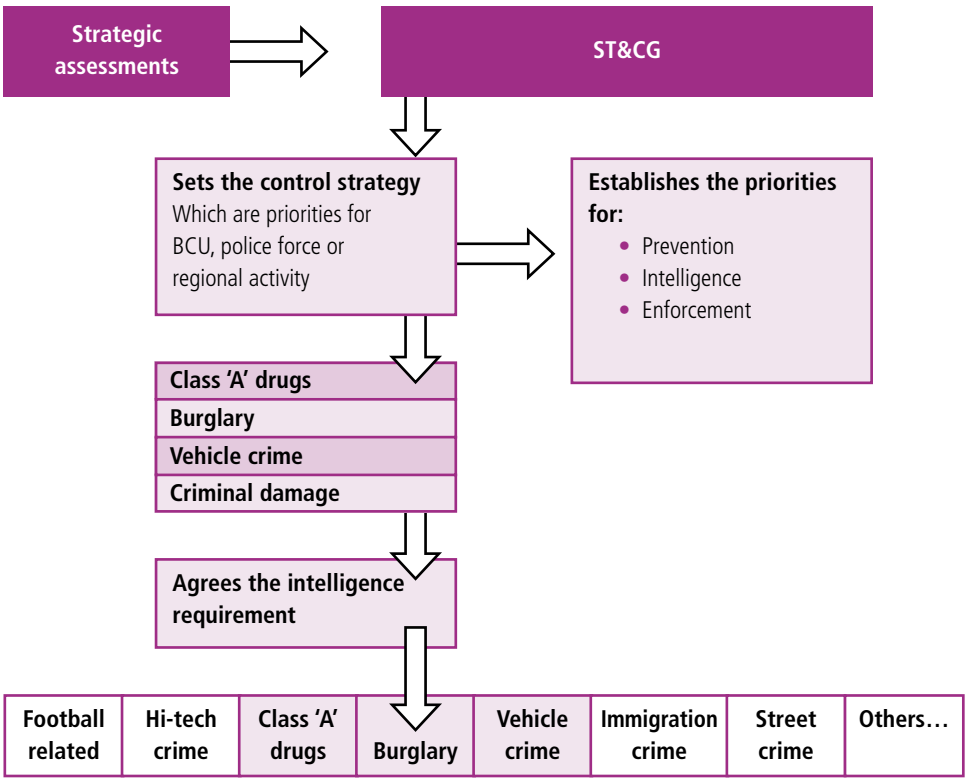
The business of the ST&CG is driven by the strategic assessment. The ST&CG will decide policing priorities based on the recommendations made in the strategic assessment. These will become the force or BCU priorities and shape business plan objectives that are likely to attract performance measurement and review.

Priorities set against crime types will be developed as strategies. The ST&CG will nominate owners for each strategy and they will be published and distributed to staff by means of the control strategy.

9.6 USING THE STRATEGIC ASSESSMENT

Figure 5 illustrates how the ST&CG uses the strategic assessment to set the control strategy and to establish priorities for prevention, intelligence and enforcement opportunities. It also demonstrates how the ST&CG agrees the intelligence requirement.

FIGURE 5 How the ST&CG Uses the Strategic Assessment



9.7 THE CONTROL STRATEGY

The control strategy sets the long term priorities for crime prevention, intelligence and enforcement opportunities. It is developed following a critical examination of the broad areas of criminality, public disorder and other unlawful acts affecting a BCU, local force or region as set out in the strategic assessment. It provides senior management with a framework in which decisions can be made about the issues that should take precedence when allocating resources.

9.8 THE INTELLIGENCE REQUIREMENT

In addition to making recommendations for crime prevention, intelligence and enforcement priorities, the strategic assessment also identifies gaps in intelligence that need to be filled. When the control strategy is agreed, the ST&CG will sanction the intelligence requirement in order to fill the intelligence gaps. Other issues identified as potential threats within the strategic assessment should also be examined for intelligence requirements. The intelligence requirement will be published with, but separate to, the control strategy. The group should then set the resource priorities for both the reactive and proactive capability, but not the tactical activity, as this is determined by the TT&CG.

The intelligence requirement may involve changes being made to the community policing or patrol strategy because it is based on a geographical understanding of crime and disorder problems. In the same way, the identification of trends in criminality may lead to a new forensic strategy being developed in which, for example, offences of a particular type receive a higher level of forensic examination.

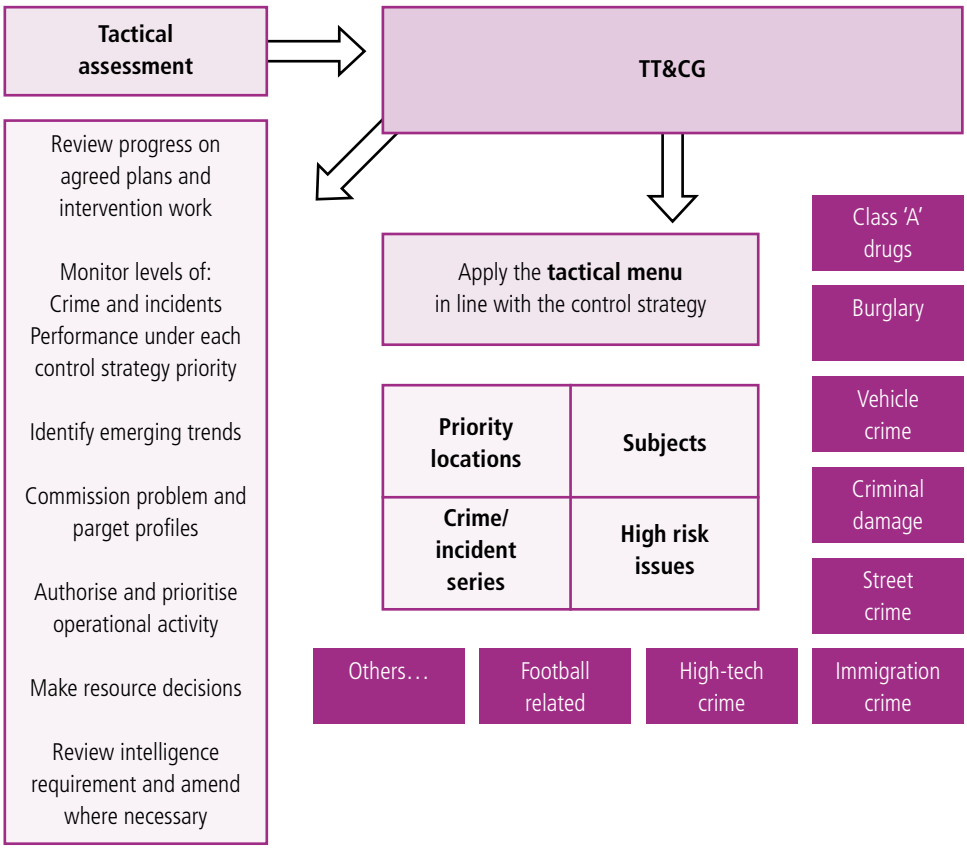
The intelligence requirement will also require a clear CHIS strategy. This should focus the activity of the DSU on the use and recruitment of informants who can provide information about identified crime and disorder problems. The control strategy may require CHIS handlers to recruit from hard to reach groups or geographical locations in order to secure community intelligence and to establish underlying catalysts for anti-social behaviour, in addition to traditional offences such as drugs and acquisitive crime.

Strategies should be designed to achieve the aims of the intelligence requirement.

9.9 TACTICAL TASKING AND CO-ORDINATION

The TT&CG has several functions. The tactical assessment identifies problems through the use of the tactical menu (see 9.10 The Tactical Menu). The TT&CG should use this and the control strategy to prioritise intervention activity. The group should also check that previously agreed plans and intervention work are still on course to meet objectives and ensure that the business plan focus is maintained. This will enable the workforce to be fully informed about performance, intervention priorities and command unit responses. The use of the tactical menu and control strategy by the TT&CG is illustrated in figure 6.

FIGURE 6 How the TT&CG Uses the Tactical Assessment



The TT&CG should sanction the deployment of resources and avoid excessive responses to random events. A purely reactive approach to policing without proper assessment and analysis – however brief – results in a loss of focus. By remaining focused, an organisation can be more effective at tackling the issues affecting it. Monitoring, rather than responding to, random events will enable an organisation to react appropriately should such events develop into issues which fall within the scope of the tactical menu.

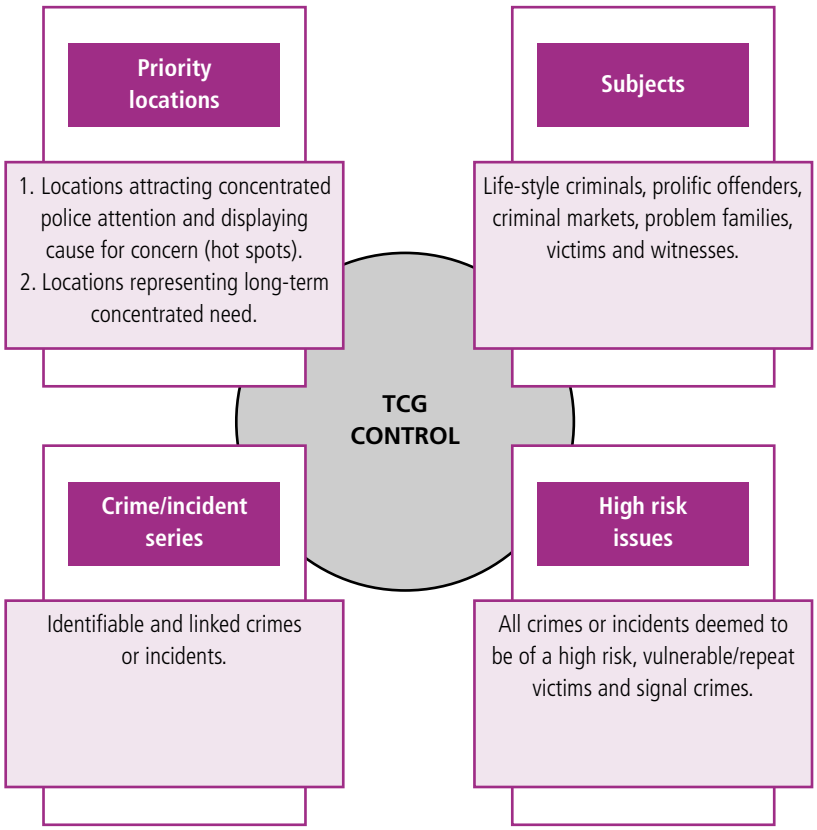
The TT&CG should identify the plan and problem owners who will take responsibility for the tactical resolution of issues raised in the tactical assessment. This will ensure that plan and problem owners are accountable to managers, and allow the TT&CG to be informed of progress until the matter is resolved and signed off by the chair of the group.

The TT&CG should also review the published intelligence requirement, ensuring that it remains up to date and making any amendments as necessary.

9.10 THE TACTICAL MENU

The TT&CG applies the tactical menu to authorise tactical activity around four elements: crime or incident series, subjects, priority locations and other high risk issues. In this way, the tactical menu is used as a problem identification matrix. The four main elements of the tactical menu should be considered by the intelligence unit in the development of the tactical assessment. This will ensure that a wide range of information is used to identify crime and disorder problems, and that effective responses to problems are implemented.

FIGURE 7 Tactical Menu



Crime/Incident Series

A crime or incident series can be defined as a number of similar crimes or incidents which are linked by modus operandi (MO), intelligence or forensic evidence, and where the link suggests they have been committed by one offender or group of offenders.

Identification and investigation of a series of offences can be aided by crime pattern analysis (CPA) and comparative case analysis (CCA) techniques to establish similarities and discrepancies between offences, see *ACPO (forthcoming) Practice Advice on Tasking and Co-ordination.*

Police forces should establish a process to manage series identification and ongoing series investigation. NIM does not detail what this process should be but a suitable management process would include the discussion of crime and incident series at a separate meeting, or as part of the weekly intelligence meeting (see 9.13 Intelligence Unit Meetings).

Subjects

Subjects are usually offenders or suspected offenders. They can also be repeat or vulnerable victims or witnesses, or an individual or group of individuals being considered for enforcement action such as Anti-Social Behaviour Orders (ASBO). The selection of subjects must be managed by the force or BCU intelligence unit under the control of the intelligence manager. The authorisation and sanction of activity in relation to subjects will ultimately rest with the TT&CG.

The TT&CG must ensure that target selection of offenders is prioritised, based on a current intelligence profile (see 8.11 Target Profiles). The group must also consider the impact and risk an offender is presenting to society. The decision to target a person or group of persons should not be driven by CHIS information alone. Rather, high yield targets should be identified in line with control strategy objectives. For example, a prolific and priority offender committing serious or control strategy offences would almost certainly be suitable for a targeting regime.

Priority Locations

Crime and disorder priority locations can be identified through the assessment of geographic and temporal trends apparent in the strategic and tactical assessment and routine crime pattern analysis. There are two types of priority locations:

- Those displaying significantly higher than average levels of crime or incidents requiring short or medium term police and partner agency action, referred to as hot spots;
- Those suffering from severe deprivation and endemic criminal activity requiring long term police and partner agency action. Reducing crime in these locations may significantly decrease reported crime in a geographic area as a whole.

Once a problem location has been identified, analytical techniques and products can be used to illustrate the unique characteristics of that area, eg, crime levels and types. The information resulting from this should be used to plan prevention, intelligence and enforcement activities in that area. When the problems of a priority location have been resolved, a results analysis should be used to assess the impact of the intervention activity, which can then assist in future intervention planning.

High Risk Issues

Police officers involved in the tactical assessment and TT&CGs must always be mindful of other high risk issues that often fall outside of the control strategy but which must be resourced as a matter of priority.

Daily management meetings should be held after high risks have been identified and responded to. High risk issues include:

- Missing persons;
- Domestic violence;
- Vulnerable/repeat victims;
- Spontaneous or planned public disorder;
- Terrorism;
- Serious road traffic incidents or disruption;
- Signal crimes;
- Prison releases;
- All issues dealt with under the Multi-Agency Public Protection Arrangements (MAPPA) process, including
  - Child protection incidents
  - Serious sexual offences
  - Serious sex offenders.

Should any of these incidents require more than an immediate short term response or investigation, then resource implications, the requirement for intelligence or analytical products and allocation of ownership should form part of the tactical assessment and TT&CG process.

9.11 FREQUENCY OF TT&CG MEETINGS

The TT&CG should meet once a fortnight. The timing, content, attendees and action-setting process should be set within a local force and BCU policy, complying with the minimum standards.

A standard approach should be reinforced throughout and this should have particular regard to the production of the tactical assessment. It should not constrain the expertise of any specialist, including the analyst, in their hypothesis; nor should it restrict commanders from requesting further information. The T&CG must be a business-like process and not stray into overly long meetings which delve into every recorded event.

Only those managers required for decision making should attend the TT&CG meeting to sanction action. Actions should then be delivered by plan owners and through briefings to all other police staff members.

9.12 T&CG POLICY FOR LEVEL 2 RESOURCE ALLOCATION

There are levels of activity beyond the reach of an individual BCU. These include criminal gangs operating over a wider territory, professional criminals involved in highly organised crimes and enquiries of national or international significance all which should be addressed at local force level.

Each police force must also support a local BCU by providing facilities and resources that a BCU does not hold, eg, surveillance teams and complex technical intrusion. Each police force's T&CG policy should detail the mechanisms required for access to such facilities and resources. This may involve personal BCU representation at local force level TT&CG, or a corporate tasking application process.

9.13 INTELLIGENCE UNIT MEETINGS

Intelligence unit meetings are designed to keep the intelligence unit activity in focus. It also enables the unit to review progress in relation to established priorities and any newly emerging issues.

Staff working in the intelligence unit should meet on a daily basis. They should consider the tactical menu and T&CG plans in the light of changing crime patterns, fresh intelligence, results from tasking and demands for intelligence support. These meetings will enable the intelligence manager to provide the relevant information to the daily management meetings (see 9.14 Daily Management Meeting). Intelligence unit meetings should, therefore, be held prior to the daily management meeting.

A formal weekly meeting should be held as a minimum, to discuss and agree the content of the new tactical assessment. The meeting must use the tactical menu as a problem identification tool to decide the content of the assessment. It should also examine the results of previous actions set by the TT&CG, emerging or developing issues, key dates for planning, ie, impending prison releases, public order events and seasonal trends relevant to the forthcoming period.

There are no standard attendance criteria for the intelligence unit meeting but it is recommended that the following should attend:

- **Crime manager (DCI) or intelligence manager** – chairs the meeting and determines what decisions are made about the work to be done, and ensures that there is clear ownership and understanding. Also establishes effective communication about both of these priorities within the intelligence unit and with other departments.
- **Analyst** – provides a preliminary report as a basis for the meeting and the next tactical assessment. Recommendations made by the analysts should be discussed and agreed or revised.
- **Crime scene investigators/crime management unit representative** – add valuable insight into potential crime and disorder series, enhancing the intelligence collection process and sharing information in relation to forensic intelligence.
- **Crime reduction unit representative** – applies expertise to recommendations regarding tactical options for crime reduction contained within the tactical assessment.
- **Representatives from investigative, patrol and neighbourhood policing units** – provide input into the assessment and updates in respect of ongoing operations.

9.14 DAILY MANAGEMENT MEETING

This meeting is not a T&CG. The purpose of a daily management meeting is to ensure that the conduct of each day's business is linked to the priorities and objectives set by the TT&CG. This should be done by:

- Looking ahead at the next twenty-four hours' business to
  - Reassess existing priorities for tactical resources against new demands
  - Deal with operational disruptions to plans currently being executed
  - Ensure balanced workloads;

- Looking back at the previous twenty-four hours' business to
  - Check tasks have been completed
  - Assess the significant changes in the operational and intelligence picture that may have implications for resources
  - Consider any performance issues;

- Examining
  - Crime levels
  - Response times and reasons for any that were missed
  - The volume and quality of arrests, ensuring they are consistent with objectives
  - The management of incidents
  - Any issues that require a media strategy.

The following people must attend the daily management meeting:

- BCU commander or deputy;
- Detective chief inspector or head of crime management;
- Chief inspector operations;
- Intelligence co-ordinator;
- Duty officer/manager.

The management team may permit anyone else to attend whose presence will contribute to the meeting. Members of the team should nominate someone to deputise for them in the event of their being absent from a meeting. The daily management meeting should be chaired by the commander or deputy.

9.15 LOCAL ACTION GROUPS

Neighbourhood policing uses NIM to manage activity. As the process begins with a local focus, it is primarily conducted within level 1 (BCU).

The development of neighbourhood policing models across the country has led to the introduction of Local Action Groups (LAGs). LAG, a multi-agency management group, is often known by other locally agreed names. Whichever name is used, this group ensures the delivery of local neighbourhood operations. It is also responsible for overseeing the development of an engagement plan to support the NIM process in three areas:

- Community involvement in setting local policing priorities;
- Problem solving activity to use against local policing priorities;
- Review of action.

Resource allocation and parameters within which local staff should operate must be agreed by the T&CG, and be subject to review. Following agreement, effective tactical resolution of local priorities will be within the domain of local neighbourhood management.

LAG is an extension of the BCU T&CG at level 1. The LAG meeting must take place before the BCU T&CG meeting, and should have suitable representation present to update the BCU manager.

All community information obtained from meetings must be forwarded through the local intelligence system for evaluation at BCU level. This is in order to inform the tactical and strategic assessment and T&CG process.

The link between NIM and partnership tasking is illustrated in *ACPO (2005) Practice Advice on Professionalising the Business of Neighbourhood Policing (Draft).*

9.16 CHECKLIST OF MINIMUM STANDARDS

Checklist 9: Minimum Standards for Tasking and Co-ordination

Standards 110 to 124 relate to tasking and co-ordination and must be implemented by November 2005. **For details on these requirements and how to meet them, see Appendix 2.**

110. T&CG policy.
111. Consistency in T&CG meetings throughout the force.
112. Chairpersons.
113. Engagement of stakeholders in the strategic T&CG process.
114. Inspection.
115. Strategic assessment.
116. Tactical assessment.
117. Regional ST&CG and TT&CG.
118. Attendees at ST&CG and TT&CG.
119. Sanction of the control strategy.
120. Sanction of the intelligence requirement.
121. Minimum 6-monthly review.
122. Briefing policy.
123. Daily management meeting/briefing – BCU.
124. Level 2 resource allocation criteria.

Section 10
TACTICAL RESOLUTION

In order to meet the needs of the TT&CG and to resolve identified and prioritised problems and targets, sufficient intelligence, enforcement and tactical resources to support it are required.

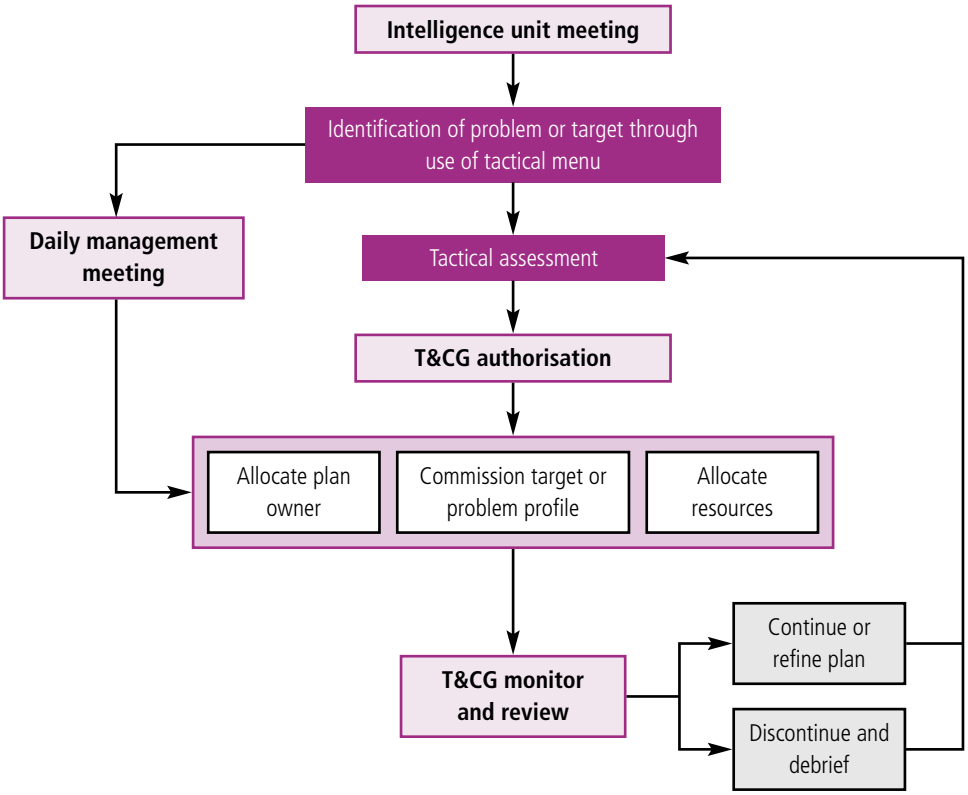
This section should be read in conjunction with *ACPO (forthcoming) Practice Advice on Tasking and Co-ordination* and *ACPO (2005) Practice Advice on Professionalising the Business of Neighbourhood Policing (Draft).*

CONTENTS

10.1 TACTICAL RESOLUTION

The TT&CG manage and control the tactical resolution of identified crime and disorder problems defined by the tactical menu. This resolution is achieved through various tactical options. The nominated plan or problem owner must use these options to create a plan to resolve the problem, and to ensure that the individual activities in the plan are carried out. The plan or problem owner will also report the results back to the TT&CG for review at the next meeting. This process is shown in figure 8.

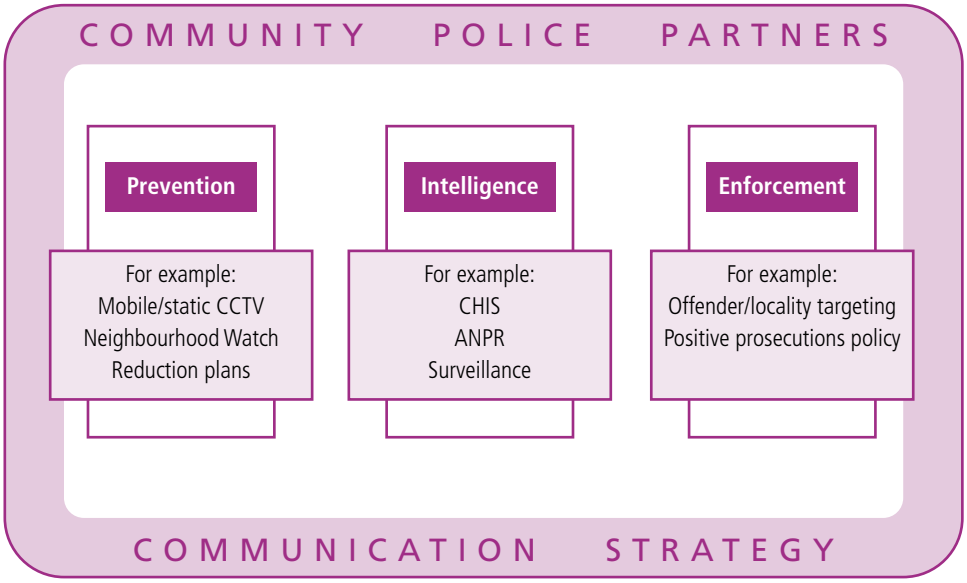
FIGURE 8 Applying the Tactical Menu



10.2 USING THE TACTICAL OPTIONS MENU

The tactical options menu has three elements: prevention, intelligence and enforcement. These elements are the framework for any intervention on TT&CG authorised crime and disorder problems. Figure 9 illustrates the tactical options available.

FIGURE 9 Tactical Options Menu



10.3 PREVENTION

Prevention of crime is a primary function of the police. Intelligence specialists and plan owners must liaise with prevention specialists to ensure that appropriate prevention tactics are employed for each crime and disorder problem that the TT&CG authorises for intervention.

Problem oriented policing (POP) provides a preventative response to policing problems. There are a number of styles of POP, but all have the same core principals.

These are:

- Scanning – for information on the problem;
- Analysing – the information obtained to understand the problem;
- Responding – to the problem to reduce it;
- Assessing – the impact of activity and determining whether the problem has been solved.

Within POP the selected response should counteract the factors that are causing the problem. The response should be to use theory-based approaches that are known to work, and take into account how other agencies, partnerships or communities have dealt with a similar problem. Preventive measures within this framework can often provide the most sustainable solution.

These are the same principles that are at the heart of NIM. There should, therefore, be no difficulty in using NIM and POP together to determine prevention tactics.

Situational Crime Prevention

Situational crime prevention (SCP) reinforces and informs the problem solving processes. SCP focuses crime prevention toward situation-specific methods of preventing offenders from committing crime and disorder by convincing them that committing a particular crime in a particular place at a particular time is not worthwhile. It is based on the premise that specific crime problems need to be analysed and the results of the analysis used to guide the development of solutions. SCP also emphasises the role of opportunity. It suggests that as the number of criminal opportunities rise, so crime and disorder rises and, conversely, as the numbers of criminal opportunities are reduced, crime and disorder is reduced. A range of situational techniques have been developed to reduce the opportunity for crime to be committed. These include the management and manipulation of the environment.

Problem Profiles and Prevention

Problem profiles can be used as a basis for determining crime prevention tactics, especially in relation to priority locations. Once a priority location has been identified and profiled, the factors that might allow criminality to exist and prosper should be identified. This can be done by establishing the rationale or motive behind particular crime categories, patterns and trends. The identification of situational, economic and environmental factors that may increase the opportunity for crime, for example, abandoned vehicles, poor lighting and multi-occupancy dwellings, should be prioritised. A rigorous assessment of these factors will inform crime reduction initiatives and highlight the most appropriate agencies or departments to address the issue.

Preventive Analysis

Analysis of concentrated crime patterns can lead not only to an increased understanding of how particular offences are committed, but also to an assessment of whether offences are being committed by random multiple offenders or particular offender groups. This information can then be used to create appropriate prevention tactics.

10.4 INTELLIGENCE

When the TT&CG authorises a crime and disorder problem for intervention, there may still be gaps in the intelligence. This will form part of a revised intelligence requirement, but the actions required to gain that intelligence may also form part of the tactical plan. It is possible that the tactical option chosen may only relate to further intelligence development, prior to enforcement or preventative measures being considered.

In all cases considered for action by the TT&CG, continued intelligence gathering will be a core requirement and should persist throughout any prevention or enforcement activity. All methods of intelligence development should be considered, including data research, telecommunications analysis, CHIS tasking, covert deployments and other analytical techniques.

10.5 ENFORCEMENT

A reduction in crime and improvement in the quality of life of residents in given locations should be at the forefront of policing activity. The arrest and prosecution of those responsible is an essential part of the crime reduction process, and one which underpins the requirement to improve the levels of sanctioned detections.

Plan and problem owners should obtain early identification of people suspected to be criminally active or responsible for anti-social behaviour within a priority location, crime or incident series, or high risk issue. This could be achieved through a number of methods including source intelligence, crime reports, NHW, Crimestoppers, pupils from local schools, youth club attendees and customers leaving licensed premises. Once these subjects have been identified, enforcement activities can be focused on them.

Enforcement tactics can include:

- Arrest and interview of suspects;
- Execution of search warrants;
- Covert operational deployments;
- Overt disruption and targeted patrol;
- ANPR intercept operations and in-car ANPR;
- Multi-agency operations.

Police action to disrupt criminal activity through targeted patrol should be seen not only as a preventative measure but also as an investigative and enforcement tool. Disruption tactics also provide the opportunity to gather intelligence.

10.6 POLICE, PARTNERS, COMMUNITY AND COMMUNICATION STRATEGY

Effective working relations between the police, partner agencies and the community are essential to the successful tactical resolution of crime and disorder problems. The police should work together with partner agencies and the community to ensure that prevention, intelligence and enforcement actions are carried out. For example, the police would be responsible for collecting intelligence on a crime series suspect, but the local council may be responsible for improving street lighting as a prevention measure.

Communication is the major factor in all elements of business and is fundamental to the success of NIM and policing. An efficient community strategy must be established in all police forces. This must address both internal and external communication needs, ensure that briefings are delivered effectively, that decisions of the T&CG are properly disseminated and that information is shared between partner agencies through appropriate information exchange protocols. Police forces should also have a clear communication strategy in relation to NIM which gives consideration to using media releases or public appeals to disseminate crime prevention messages or to gain more information about a crime and disorder problem. Positive use of the media to highlight the results of high profile police operations and arrests will help to reduce the fear of crime and reassure the public.

10.7 TACTICAL PLANS

The TT&CG must allocate a plan owner to organise the response to an identified crime and disorder problem authorised for intervention. The problem may be in the form of a priority location, subject, crime or incident series, or high risk issue and will have been analysed within the tactical assessment and subject to problem and target profiling as appropriate. The plan or problem owner will normally be an inspector who has the majority of tactical resources at their disposal with which to resolve the problem, or who has geographical responsibility for the area where the problem is occurring.

Tactical plans must be aligned with the control strategy priorities and relate to each element of the tactical menu as appropriate. Tactical planning may take a number of options into account, including:

- The use of directed patrol;
- Tasking activity such as bail checks or traffic speed monitoring;
- Working with partners, for example, to control unruly tenants or install CCTV;
- Proactive media releases;
- Offender targeting;
- Positive prosecutions activity;
- Deployment of ANPR technology.

An extensive range of the prevention, intelligence and enforcement activities that can be used to resolve crime and disorder problems and further information on tactical plans can be found in *ACPO (forthcoming) Practice Advice on Tasking and Co-ordination.*

10.8 TRIGGER PLANS – SECOND LEVEL TACTICAL PLAN

A trigger plan is a simple and effective action plan. It can improve performance by stopping a crime series through the earliest possible action. It ensures a proactive, appropriate response to an identified crime or incident series and requires the cooperation of a number of teams in order to work effectively. This activity initiates early investigation and control of further series offences, thereby minimising evidential loss and co-ordinating a predetermined police response based on intelligence already identified.

The purpose of such a plan is to respond immediately to the notification of a crime that forms part of an identified crime series. A trigger plan is identified by staff attending crime scenes, planned by investigators with the assistance of intelligence units, monitored by crime recording and call management units and results in fast-time actions being taken by patrol officers. This then gives officers the best opportunity to arrest offenders, identify suspects and witnesses, capture forensic evidence and reduce crime. Specific actions might include:

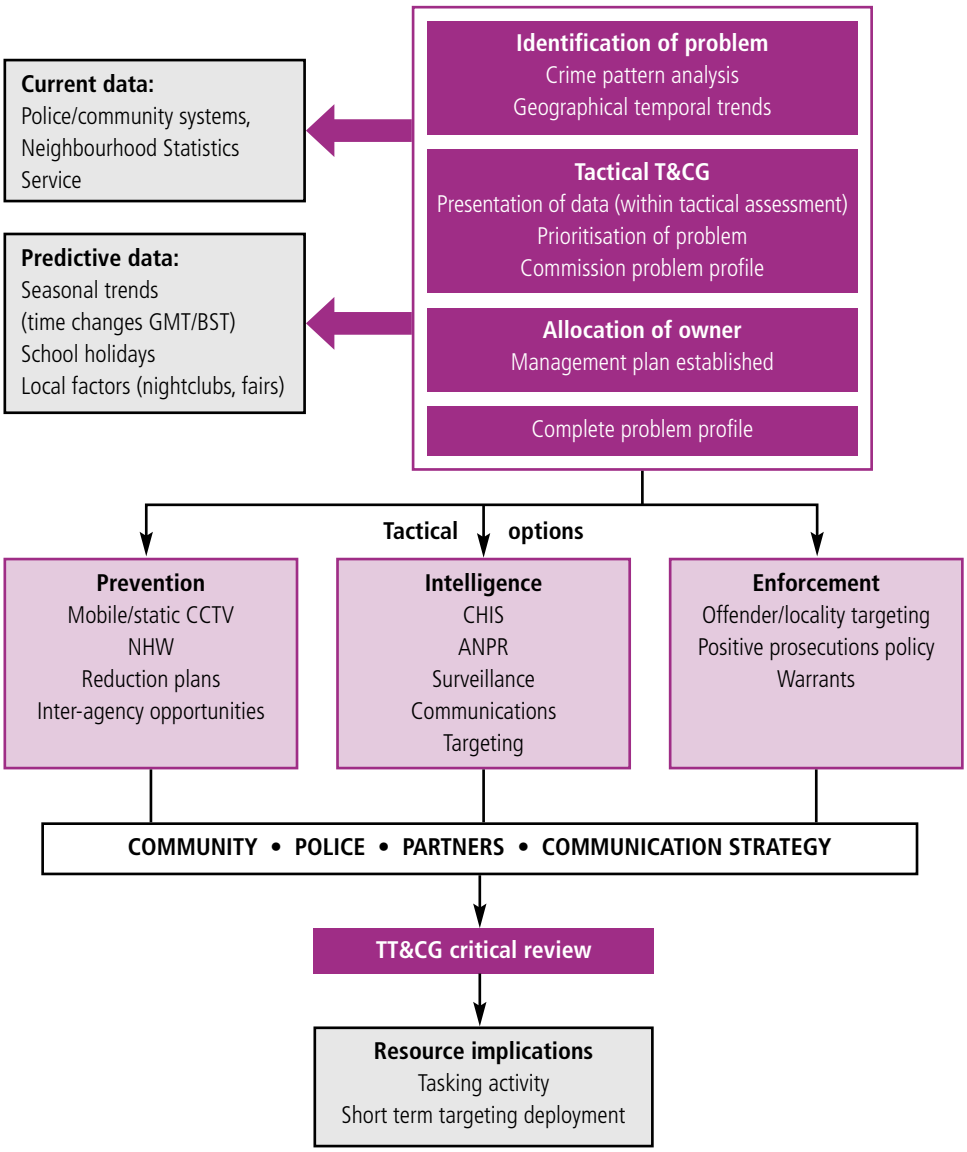
- Scene attendance criteria (specific route, silent approach, property search);
- Bail checks on suspects;
- Linked premises checks;
- Call out protocols;
- Forensic examination instructions;
- Hot witness interviews;
- CCTV retrieval.

The number of trigger plans must be restricted and ownership of each one clearly identified. Each plan must be focused, meaningful and subject to monitoring and review.

10.9 TACTICAL RESOLUTION, CAPABILITY AND THE TT&CG PROCESS

The overall purpose of the TT&CG is to achieve a successful tactical resolution to crime and disorder problems. The TT&CG attempts to achieve this by co-ordinating activity, beginning with the collection of information by the intelligence unit through to the review of tactical operations and resolution. Figure 10 illustrates the process of problem management.

FIGURE 10 Problem Management



The TT&CG must apply the tactical menu to ensure that a focused resolution to problems is achieved. The T&CG must also be fully aware of the local force or BCU capability. This will prevent the unnecessary production of problem and target profiles and will ensure crime prevention, intelligence and enforcement priorities can be managed with the available resources.

Sufficient tactical capability must be available to deal with prioritised problems and targets. This will involve staff working with partner agencies and police personnel in intelligence, enforcement and investigative roles.

Police forces or BCUs should determine the numbers of staff to employ in each unit. Intelligence and tactical teams must be sufficiently resourced so that the decisions of the T&CG can be carried out. With quality intelligence but no tactical capability, nothing meaningful can be accomplished. Conversely, with a heavily resourced tactical capability but inadequate intelligence resources, there will be a lack of informed direction and the results are unlikely to be in line with control strategy priorities.

The high cost of training required for some key roles will make it necessary to impose a red circle policy for such posts to enable the organisation to obtain a return on the investment made. Sufficient tactical resources must be available at all policing levels to ensure that plan owners are able to draw on the required expertise, whether this is a locally provided search team or specialist officers such as surveillance operatives.

10.10 CHECKLIST OF MINIMUM STANDARDS

Checklist 10: Minimum Standards for Tactical Resolution

Standards 125 to 129 relate to tactical resolution and must be implemented by November 2005. **For details on these requirements and how to meet them, see Appendix 2.**

125. Investigative capability.
126. Red circle policy.
127. Tactical capability.
128. Tactical plans.
129. Trigger plans.

Section 11
OPERATIONAL REVIEW, PERFORMANCE MEASURES AND ORGANISATIONAL MEMORY

Operational reviews and the use of results analysis ensures that lessons are learned and retained in the organisational memory. This then allows performance issues to be identified and measured.

This section should be read in conjunction with Section 5 Information Sources, *ACPO (forthcoming) Practice Advice on Tasking and Co-ordination* and *ACPO (forthcoming) Guidance on the National Briefing Model.*

CONTENTS

11.1 OPERATIONAL REVIEW

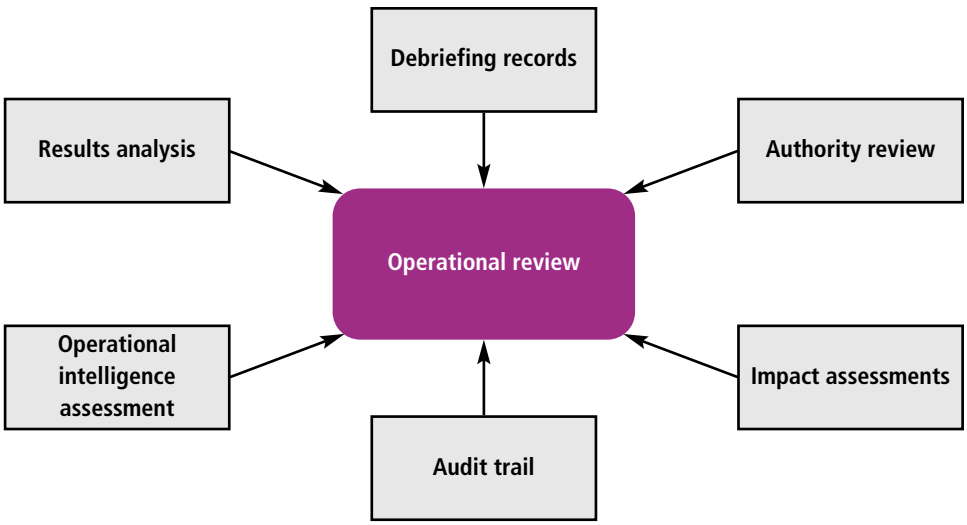
Operational review is not the same as an operational debriefing. An operational review is commissioned by the TT&CG. It may involve a number of processes which, when combined, ensure that the information gained from incidents, tactical plans or investigations, as well as any impacts and lessons learned, are fed back into the organisational memory. This activity must be conducted whether an operation has been successful or not. It can be a particularly informative exercise when using new technology or after a failed operation.

Ideally the objectives of the review should be stated before the operation begins. The TT&CG must decide whether the review is designed to cover all aspects of the operation or just specifics such as tactical performance or the impact on crime levels or partnership capability. The TT&CG direction provides police staff with guidance on the information to collect to assist the subsequent analysis.

The operational review should establish what intelligence was acquired and if any new gaps have emerged. It should ask such questions as follows.

- Was the intelligence accurate?
- What did we learn from victims, witnesses, offenders and locations?
- Was there useable intelligence from any technical or surveillance activity?
- What do we now know and what are the gaps in our knowledge now?
- Did the problem change after activity? If so, why was this?
- Did the activity cause displacement?
- What tactics were used and is/are the offender/s vulnerable to the same approach in the future?
- Did new offenders move in?
- Did we involve any partner agencies in the plan?
  - What were the benefits of this?
  - What feedback have they provided?
  - What feedback have they received?
- Did the risk assessment appropriately raise awareness of police staff to potential hazards linked to the operation?
- What measures have been put in place to minimise the possibility of the problem arising again?

FIGURE 11 Potential Components of an Operational Review



11.2 OPERATIONAL INTELLIGENCE ASSESSMENT

The analyst will conduct an assessment and evaluation of incoming intelligence throughout an operation or the intelligence collection process. This assessment can form part of the overall operational review, identifying stages of an operation that may have been delayed through the inability to fill intelligence gaps. This is one of the nine key analytical techniques and products, see 7 Research, Development and Analysis. For further information contact the National Analyst Working Group (details in Appendix 6) and see *ACPO (forthcoming) Practice Advice on Tasking and Co-ordination.*

11.3 DEBRIEFING RECORDS

The NBM provides a standardised and structured briefing and debriefing process. When implemented, it ensures efficient tasking and briefing of the patrol function and enables an assessment to be made of the meaning of an intelligence product and its timeliness. It also allows for a gap analysis to improve the product.

Debriefings by team leaders, operational commanders and SIOs may be used to assess the operational effectiveness of a particular team, the tactics used or investigative techniques employed. The results of all debriefs must be recorded.

11.4 AUDIT TRAIL

All forces must have a standard system for recording tactical decisions, operational plans and results. Such systems will provide an easily accessible audit trail. This audit trail is essential to the operational review process and can be a beneficial source of organisational learning. It will also remind decision-makers of the reasons why they took certain courses of action in case of future scrutiny by inspectorates and the courts.

11.5 AUTHORITY REVIEW

Where an operation involves the use of covert tactics the mandatory reviews of authorities (granted under relevant legislation) may form part of the operational review. Reviewing mechanisms will have been established as part of the legislative requirements under RIPA, the Police Act 1997 or other appropriate legislation, and as a minimum standard of NIM. For further information see standard 130 in Appendix 2.

11.6 RESULTS ANALYSIS

Results analysis evaluates the effectiveness of intervention activity. It is commissioned by the TT&CG and prevents analysis being conducted unnecessarily. It also ensures that intelligence and operational staff are fully aware of the need to review an operation or action. This is also one of the nine key analytical techniques and products of NIM. See 7 Research, Development and Analysis and *ACPO (forthcoming) Practice Advice on Tasking and Co-ordination.*

11.7 IMPACT ASSESSMENTS

Assessing the impact of interventions is difficult but essential as they can reveal whether interventions have been properly implemented, and whether or not they work. There are two evaluation initiatives.

- **Process evaluation** – is concerned with how the initiative was implemented.
- **Outcome evaluation** – identifies the impact on crime and determines whether the outcome is attributable to the interventions.

There are numerous texts available on how to evaluate initiatives used by the Police Service and their partners. For example, *Home Office (2002) Passport to Evaluation: An Introduction to Evaluating Crime Reduction Initiatives and Projects* is available from the Crime Reduction College. R Clarke and J Eck have published a guide that includes sections on evaluation called *(2003) Becoming a Problem-Solving Analyst.*

Some of the main issues that must be considered in impact assessments are summarised below.

TABLE 1 Considerations for Impact Assessments

EVALUATION STAGE	QUESTIONS TO BE ADDRESSED
Process Evaluation	
Identifying whether the project was implemented and, if so, how	Was the activity implemented when it was supposed to be? Was it implemented in the right place? Was the response appropriate to the problem? Was it targeted at the right group? Was it implemented as planned?
Identifying whether sufficient action was taken	Were there enough resources available to fully implement the activity? Was it implemented for an appropriate length of time? Was it sufficiently intense?
Outcome Evaluation	
Measuring the impact	What type of evaluation design is appropriate? Is a control group required and, if so, what type? How often can the problem be measured?
Attribution of impact	What are the main process evaluation results? What are the impact results? Did the problem decline after the response? (Did it decline at a faster rate? What other explanations could have caused the decline? Are you confident that the response caused the decline?)

11.8 PERFORMANCE MEASURES

Early indications from HMIC inspections show that where NIM is fully implemented, that police force also performs well against key performance targets.

NIM should be subject to rigorous performance management, including clear monitoring processes set against local and force business plans. High performance can be achieved by remaining focused on priority issues (identified through quality strategic and tactical assessments and other intelligence products) provided by appropriately resourced and rigorous intelligence processes.

When this is supported by targeting processes, focused tasking regimes and succinct and explicit tactical plans delivered through force policy and minimum standards, many key performance measures can be targeted. These include:

- Reductions in anti-social behaviour and disorder;
- Reductions in key crime categories;
- Improvement in quality of life and reductions in the fear of crime;
- Improved criminal justice performance, with higher levels of sanctioned detections and convictions of priority and prolific offenders.

Chief officers should have due regard to the Race Relations Act 1976, as amended, and the Disability Discrimination Act 2005 when considering performance measures for targeted activity in the community.

Internal performance regimes should be established in local forces to improve the quality of information recording and dissemination and the tasking of specific intelligence collection plans. Such regimes will improve the level and integrity of information and intelligence held on existing and any future databases, and will also assist in meeting the requirements set out in the *ACPO (2005) Code of Practice on the Management of Police Information.*

11.9 ORGANISATIONAL MEMORY

Organisational memories are a significant information source which will inform future strategic assessments. All BCUs and local police forces must establish policies and systems for capturing the outcome of an operational review so that the results can be used. Impact assessments, results analysis, debriefing records and performance outcomes are some of the main elements of an organisational memory. Organisational memories should be searchable and integrated to enable research, development and analysis. Organisational memory systems should be created within intelligence IT systems to capture, manage and make available knowledge of the BCU and local forces' processes and previous operational activity. In addition to evaluated intelligence, such systems may include information regarding:

- Previously mounted operations in response to seasonal trends;
- The results of previous public satisfaction surveys;
- The level of resources that were necessary to conduct previous operations of a similar nature;
- The identity of key officers involved in previous high-profile operations.

A police force without an organisational memory is likely to repeat mistakes and has little scope for answering the question – has this been done before?

11.10 CHECKLIST OF MINIMUM STANDARDS

Checklist 11: Minimum Standards for Intelligence/Operational Review

Standards 130 to 135 relate to operational review and must be implemented by November 2005. **For details on these requirements and how to meet them, see Appendix 2.**

130. Results analysis and review.
131. Monitor and review of RIPA authorities.
132. National Briefing Model.
133. Organisational memory.
134. Audit trail.
135. Community impact assessment review.

APPENDIX 1
CODE OF PRACTICE ON THE NATIONAL INTELLIGENCE MODEL

CONTENTS

1 INTRODUCTION

1.1 PURPOSE OF THE CODE

1.1.1 The purpose of this code is:

- To set out to chief officers of police the basic principles and minimum common standards for the National Intelligence Model;
- To promote compatibility of procedures and terminology for the National Intelligence Model;
- To clarify the responsibilities of chief officers and police authorities in relation to the application of the National Intelligence Model;
- To ensure that observance of these principles and the standards for implementation results in a systematic programme of continuous development of police policy, practice and capability;
- To identify and promulgate good practice.

1.2 STATUTORY BASIS OF THE CODE

1.2.1 This code of practice comes into effect on 12 January 2005.

1.2.2 This code of practice is made under:

- Section 39 of the Police Act 1996 which permits the Secretary of State to issue codes of practice relating to the discharge by police authorities of any of their functions;
- Section 39A of the same Act, as inserted by Section 2 of the Police Reform Act 2002, which permits the Secretary of State to issue codes of practice relating to the discharge of their functions by chief officers for the purpose of promoting the efficiency and effectiveness of police forces in England and Wales;
- Sections 28 and 73 of the Police Act 1997 which permits the Secretary of State to issue codes of practice relating to the discharge by the National Criminal Intelligence Service and the Director General of the National Crime Squad of any of their functions.

1.2.3 It applies directly to the police forces maintained for the police areas of England and Wales defined in section 1 of the Police Act 1996 (or as defined in any subsequent legislation), and to the National Crime Squad and the National Criminal Intelligence Service.

1.2.4 The code of practice is issued by the Secretary of State in relation to the discharge of the functions of chief officers of police. A chief officer of police shall have regard to this code, as will the members of the police force for whom the chief officer of police is responsible.

1.2.5 In the case of the National Crime Squad and the National Criminal Intelligence Service, references in this code to chief officers of police apply to the Directors General of those organisations, and references to forces shall include the National Crime Squad and the National Criminal Intelligence Service.

1.2.6 Should the definition of police forces under section 1 of the Police Act 1996 change, and should there be changes to the present constitution of the National Crime Squad or the National Criminal Intelligence Service, the Secretary of State may revise this code to ensure the application of the code to the chief officers of those forces.

1.2.7 It is available for adoption by other police forces in England and Wales, and by other jurisdictions within the United Kingdom.

1.3 DIVERSITY ISSUES UNDER THIS CODE

1.3.1 In the application of the National Intelligence Model issues relevant to all areas of diversity and culture such as race, religion, gender, disability, sexual orientation, gender identity and age, will be taken into account. This principle applies to equipment and personnel selection procedures, and in the application of the business model.

1.4 PROCEDURES COVERED BY THIS CODE

1.4.1 This code applies to intelligence and information used to direct police activity through a planned and systematic business process.

1.4.2 Guidance on the use of covert human intelligence sources and dedicated source units is set out in the ACPO Manual of Standards for the Use of Covert Human Intelligence Sources and is not otherwise dealt with in this code.

1.5 CONFIDENTIALITY

1.5.1 In laying this code of practice before Parliament, the Secretary of State declares that nothing in this code is of a confidential nature.

2 SCOPE AND STATUS OF THIS CODE

2.1 LEGAL CONSIDERATIONS

2.1.1 This code applies within the framework of the domestic law of England and Wales and has been written in accordance with the principles of the Human Rights Act 1998, which incorporates the European Convention on Human Rights.

2.1.2 Statutes of direct relevance to the code include:

- Police and Criminal Evidence Act 1984;
- Criminal Procedure and Investigations Act 1996;
- Police Act 1997;
- Crime and Disorder Act 1998;
- Data Protection Act 1998;
- Regulation of Investigatory Powers Act 2000;
- Terrorism Act 2000;
- Anti-Terrorism, Crime and Security Act 2001;
- Police Reform Act 2002.

2.1.3 Nothing in this code alters the existing legal powers or responsibilities of any chief officer of police, or any other police officer.

2.2 RELATIONSHIP OF THE CODE TO OTHER GUIDANCE

2.2.1 The National Intelligence Model Minimum Standards document of April 2003 (and any successor document) sets out the criteria by which the model should be applied. Chief officers will ensure that the arrangements for applying the model within their force comply with that document (and with any successor document as directed by the Association of Chief Police Officers).

2.2.2 Chief officers of police will make arrangements under this code for the authorisation, registration, deployment and usage of covert human intelligence sources, taking account of relevant legislation and the operational guidance set out in the ACPO Manual of Standards for the Use of Covert Human Intelligence Sources.

2.2.3 The Code of Practice on Management of Police Information (once published) as recommended by the Bichard Inquiry and associated guidance including the ACPO Manual of Standards on the Recording and Dissemination of Intelligence Material, set out national standards for the management of police information, including intelligence material, its physical security and security of sensitive material. They are the authority on all questions of integrity of intelligence material and must be included as part of the operating protocols of the National Intelligence Model.

2.2.4 Other manuals of guidance that are relevant to the application of the National Intelligence Model are:

- ACPO and HMCE Manual of Standards for the Deployment of Undercover Officers;
- ACPO and HMCE Manual of Standards for the Deployment of Test Purchase and Decoy Officers;
- ACPO and HMCE Manual of Standards for Surveillance;
- ACPO Manual of Professional Standards in Policing;
- ACPO Kidnap Manual of Guidance;
- ACPO Murder Investigation Manual.

2.2.5 The Home Office has also issued codes of practice that should be taken into account along with the above manuals. Those codes are for:

- Covert Surveillance;
- Interception of Communications;
- Covert Human Intelligence Sources.

2.2.6 The National Intelligence Model will impact on force policies and it will be necessary for forces to review their policies to ensure standardisation and compatibility. In particular, chief officers will ensure that there is a corporate approach to the timing, content and circulation of National Intelligence Model products and that there are established and consistent links between those products and the force planning cycle.

2.2.7 The code is not a policy document for forces or intended to prevent or constrain forces from developing new operational tactics.

2.3 ROLE OF HM INSPECTORATE OF CONSTABULARY

2.3.1 HM Inspectorate of Constabulary will inspect police forces in England and Wales to ensure compliance with this code and with the Minimum Standards document of April 2003 (and any successor document).

2.4 ROLE OF POLICE AUTHORITIES

2.4.1 Police authorities should ensure that police forces are adequately resourced to deliver the National Intelligence Model.

2.5 ROLE OF THE NATIONAL CENTRE FOR POLICING EXCELLENCE

2.5.1 The National Centre for Policing Excellence, or any successor body designated by the Secretary of State, has responsibility on behalf of the police forces of England and Wales for the management and development of the intelligence doctrine and, in that respect, will have responsibility in collaboration with the Association of Chief Police Officers (ACPO) and the National Criminal Intelligence Service for the continuing development of the National Intelligence Model.

3 BASIC REQUIREMENTS OF THIS CODE

3.1 A NATIONAL MODEL FOR POLICING

3.1.1 The National Intelligence Model is a business process. The intention behind it is to provide focus to operational policing and to achieve a disproportionately greater impact from the resources applied to any problem. It is dependent on a clear framework of analysis of information and intelligence allowing a problem solving approach to law enforcement and crime prevention techniques. The expected outcomes are improved community safety, reduced crime and the control of criminality and disorder leading to greater public reassurance and confidence.

3.1.2 At the heart of the business process is the Strategic and Tactical Tasking and Co-ordination Group meetings. The process is conducted at three levels to correspond with the specified levels of incidents: Level 1 represents local crime capable of being managed by local resources (which may include the most serious crime) and anti-social behaviour; Level 2 represents force, inter-force and regional criminal activity usually requiring additional resources; and Level 3 represents the most serious and organised crime. The purpose of the Strategic Tasking and Co-ordination Group meetings is to agree a control strategy which establishes the intelligence requirement and sets the agenda for prevention, intelligence and enforcement priorities. The purpose of the Tactical Tasking and Co-ordination Group meetings is to apply a planned response to the control strategy.

3.1.3 The National Intelligence Model is not confined to or restricted for specialist usage. It is relevant to all areas of law enforcement: crime and its investigation, disorder and community safety. Overall, it is a model for operating policing.

3.1.4 As such, effective application of the National Intelligence Model should enable police forces to trace the continuum between anti-social behaviour and the most serious crime, and then to identify those local issues in most urgent need of attention. The model is compatible with other operational policing methodologies, in particular those which focus on problem solving by using analytical techniques.

3.1.5 The National Intelligence Model is a tool that Crime and Disorder Reduction Partnerships should use to develop and deliver the strategic priorities in their three year crime and disorder and misuse of drugs strategies. The National Intelligence Model should also be used to inform the strategic priorities of Drug Action Teams.

3.2 OWNERSHIP

3.2.1 For the purpose of maintaining standards within each force, chief officers will ensure that an officer of at least the rank of assistant chief constable, or equivalent, is appointed to take the lead within the force in relation to policy and practice for the National Intelligence Model.

3.2.2 Chief officers of police will ensure that an appropriate officer of ACPO rank will chair Strategic and Tactical Tasking and Co-ordination Group (T&CG) meetings held at force level, and that there is appropriate ACPO level representation at Strategic and Tactical T&CG meetings held on a regional basis.

3.2.3 At BCU level, the responsibility for delivery of the National Intelligence Model will rest with the local BCU commander. The exercise of that responsibility should include the chairing of the BCU Strategic T&CG meeting and overseeing of the Tactical T&CG meetings. Chief officers will ensure consistency of operation of the National Intelligence Model within the BCUs for which they are responsible.

3.3 ASSETS

3.3.1 Assets are those resources available to forces that underpin the business process of the National Intelligence Model. There are four key asset areas:

- Knowledge Assets – the professional knowledge, procedural documents, policies, databases and codes of practice held by forces and by partner agencies that enable the delivery of core business within those organisations;
- System Assets – those products that provide for the secure collection, recording, reception, storage, linkage, analysis and use of information;
- Source Assets – information from a wide variety of sources relevant to policing, from community intelligence at neighbourhood level to intelligence on serious and organised crime and terrorism at a national and international level;
- People Assets – the specific functions and posts required to enable the National Intelligence Model to function.

Detailed descriptions of the above assets are set out in the National Intelligence Model Minimum Standards document of April 2003 (and any successor document) and chief officers will ensure that their force arrangements comply with that document (and with any successor document as directed by the Association of Chief Police Officers).

3.4 BRIEFING

3.4.1 Chief officers will ensure that an appropriately resilient briefing model, based on the principles of the National Briefing Model, is in place throughout their force to ensure the communication of intelligence that informs and directs operational policing activity at both levels 1 and 2.

3.5 INFORMATION TECHNOLOGY

3.5.1 A standardised, consistent and secure electronic information management system is essential to the success of the National Intelligence Model. To meet their responsibilities for delivering the National Intelligence Model, chief officers and police authorities will be required to adopt a national IT system to support police intelligence in line with recommendations from the Bichard Inquiry.

3.5.2 Chief officers should ensure that geographic crime and incident mapping technology is used to aid decision making, problem solving, communication and performance management within the National Intelligence Model business process.

3.6 CONSISTENCY AND COMPATIBILITY

3.6.1 In order for the National Intelligence Model to function effectively at all levels, chief officers must ensure that there is consistency and compatibility of records and data sets. Forces will have in place the National Crime Recording Standard, and a standardised intelligence recording system as recommended by the Association of Chief Police Officers.

3.6.2 To enable the efficient transfer of information forces will ensure that secure data transference capabilities are established with other forces and partner agencies, and that appropriate data sharing protocols are in operation in accordance with the provisions of the Data Protection Act 1998.

3.7 SECURITY

3.7.1 The integrity of the National Intelligence Model requires adequate standards of physical, environmental, technical and personnel security. The Government Protective Marking Scheme (GPMS) sets out common standards for the protection of sensitive documents and other material. Its principles also extend to data held on computer and electronic recording systems. The ACPO Manual of Standards for the Recording and Dissemination of Intelligence Material sets out the GPMS in detail and gives guidance on the key features of a secure intelligence environment.

3.7.2 The management of security issues in Information Technology is complex and usually requires specialist advice at design, installation and implementation stages. The government has published a Manual of Protective Security as a guide to this subject.

3.7.3 Chief officers will ensure that appropriate security procedures are maintained for the National Intelligence Model.

3.8 DATA PROTECTION

3.8.1 Chief officers are responsible for the development and implementation of appropriate procedures and systems to ensure that personal information on individuals is held in accordance with the requirements of the Data Protection Act 1998 and any other relevant legislation. The management of information must be in accordance with the Code of Practice on Management of Police Information (once published) as recommended by the Bichard Inquiry. This could include the retention of the information for purposes other than that for which it was collected where retention of that information could be shown to be necessary for policing purposes or is in the wider public interest.

3.9 HEALTH & SAFETY

3.9.1 Chief officers of police should ensure that in applying the National Intelligence Model within their force, the identification and assessment of any health and safety risks has been conducted and that suitable preventative or remedial action has been taken.

4 TASKING AND CO-ORDINATION GROUPS

4.1 STRATEGIC TASKING AND CO-ORDINATION GROUP (ST&CG)

4.1.1 The purpose of a Strategic Tasking and Co-ordination Group operating at Levels 1, 2 or 3 is to consider the Strategic Assessment in order to set a control strategy and establish an intelligence requirement for the level at which it is operating. The **control strategy** is a document that sets the agenda for prevention, intelligence and enforcement priorities. As well as setting the control strategy for that level the Strategic T&CG will ensure it contains relevant links to other levels.

4.1.2 Chief officers will ensure that appropriate procedures, compliant with the National Intelligence Model Minimum Standards document of April 2003 (and with any successor document as directed by the Association of Chief Police Officers), are in place for the effective operation of a Strategic T&CG. The Strategic T&CG will meet to set the **control strategy** and, thereafter, every six months to review and monitor progress, to adjust the control strategy and to maintain links with other levels of activity. In addition, chief officers will have regard to the protocols of the regional T&CG meetings.

4.2 TACTICAL TASKING AND CO-ORDINATION GROUP (TT&CG)

4.2.1 The purpose of the Tactical Tasking and Co-ordination Group is to implement the control strategy through a menu of tactical options and to manage any subsequent priorities that may arise. The Tactical T&CG has three main roles:

- To apply the tactical menu to the control strategy;
- To respond to new problems; and
- To monitor plans agreed from earlier T&CG meetings.

4.2.2 The principal document that informs the Tactical Tasking and Co-ordination Group is the Tactical Assessment.

4.2.3 The Tactical T&CG will meet as frequently as is necessary in accordance with force policy.

4.2.4 Chief officers will ensure that appropriate procedures compliant with the National Intelligence Model Minimum Standards document as of April 2003 (and with any successor document as directed by the Association of Chief Police Officers), are in place for the effective operation of a Tactical T&CG and for the management and auditing of tasks and operational activity emanating from the Tasking and Co-ordination process.

4.3 REVIEWS

4.3.1 Reviews of the National Intelligence Model business process and in particular, intelligence analysis and the use of standardised products and operational plans, are essential if the model is to operate efficiently and effectively. Chief officers will ensure such reviews are conducted on a regular basis.

4.3.2 Further reviews of operations should be conducted to inform future resource deployments and tactics employed.

5 INTELLIGENCE PRODUCTS

5.1 STRATEGIC ASSESSMENTS

5.1.1 Strategic Assessments must be produced on a biannual basis and should be reviewed every three months to ensure they are current. Chief officers will ensure that they are developed against the national minimum standard template to ensure standardisation of procedures and products between forces in order to enable priorities to be set at regional, force and local levels.

5.1.2 The aim of the Strategic Assessment is to identify the medium to long term issues that are apparent or emerging, and to determine resource, funding and communication requirements. In this respect, force strategic assessments should be considered in the business planning process and available for consultation between chief officers and police authorities. A further aim is to ensure there are links covering Level 1, 2 and 3 criminal activities between local, regional and national agencies.

5.1.3 While BCUs and forces will produce strategic assessments covering Level 1 and Level 2 issues, and in certain police areas a Level 3 strategic assessment will be produced, the UK Level 3 threat assessment shall be the responsibility of the National Criminal Intelligence Service.

5.2 TACTICAL ASSESSMENTS

5.2.1 Chief officers will ensure that Tactical Assessments are produced to inform Tactical Tasking and Co-ordination Group meetings, specifically with regard to decision making and the allocation of resources.

5.2.2 The aim of the Tactical Assessment is to identify the short-term issues which require attention and to monitor progress on current business in line with the control strategy. The areas the Tactical Assessment will cover include appropriate interventions for prevention, intelligence gathering and enforcement activities, the identification of emerging patterns of crime and incidents and a performance assessment.

5.3 TARGET PROFILES

5.3.1 A target profile is a detailed analysis of an individual or network, and should contain sufficient detail to enable a targeted operation or intervention against that person or network. It will also recommend operational intelligence requirements in order to secure the information required to implement a tactical response.

5.4 PROBLEM PROFILES

5.4.1 The purpose of a problem profile is to provide an assessment of a specific problem or series of problems which may be criminal, may pose a threat to public safety or which may be anti-social in context. The profile will include an analysis of the problem with recommendations for prevention, intelligence gathering or enforcement. Problem profiles are ideally suited for existing problem-oriented policing methods.

5.5 PROPORTIONALITY

5.5.1 Chief officers will ensure that where intelligence products impinge on an individual that the actions comply with the requirements of the European Convention on Human Rights Articles as enacted in English law via the Human Rights Act 1998, and that the actions of the police force comply with the principle of 'proportionality'.

6 TRAINING: STANDARDS AND ACCREDITATION

6.1 SELECTION, TRAINING AND MAINTAINING COMPETENCE

6.1.1 Staff roles within the National Intelligence Model will have competencies required for the posts. These will be profiled by the Integrated Competency Framework and underpinned by National Occupational Standards. The Skills for Justice Organisation will determine those requirements. Chief officers of police will ensure that personnel in such posts are trained to those standards. There should be an annual assessment of personnel against the standards.

6.1.2 Where applicable, those attaining the required standards of competence will be entered on the relevant professional register as determined by the Skills for Justice Organisation. They will remain on the register in accordance with any provisions for reassessment and requalification which may be required under the conditions for registration.

6.2 INDEPENDENT ACCREDITATION OF TRAINING

6.2.1 The body responsible for the approval and accreditation of training courses and of trainers for these purposes will be the Police Licensing and Accreditation Board or any successor body designated by the Secretary of State.

6.2.2 The National Centre for Policing Excellence or any successor body designated by the Secretary of State, will accredit all training courses for intelligence analysts to a common recognised standard.

7 MONITORING, EVALUATION AND PROMULGATION OF GOOD PRACTICE

7.1 MONITORING AND EVALUATION

7.1.1 Chief officers will ensure that there are procedures in place throughout their force to monitor compliance with this code of practice and the National Intelligence Model Minimum Standards document of April 2003 (and with any successor document as directed by the Association of Chief Police Officers). Her Majesty's Inspectorate of Constabulary will inspect and report on those procedures.

7.1.2 For that purpose chief officers will ensure that regular reviews of the National Intelligence Model take place within their force, together with an evaluation of its effectiveness and efficiency.

7.2 PROMULGATION OF GOOD PRACTICE

7.2.1 Notwithstanding that this code and the Minimum Standards are specific, part of the purpose of the code is to encourage continuous development of police practices relating to the National Intelligence Model and to ensure that such developments are made available throughout the police service. Where there is reason to believe that improvements have been identified in procedures, these should be reported to the National Centre for Policing Excellence or any successor body designated by the Secretary of State.

7.2.2 It will be the responsibility of the National Centre for Policing Excellence to ensure that any necessary action is taken as soon as practicable on such reports passed to them.

7.2.3 While recognising that police forces will seek to improve the operation of the National Intelligence Model, in order to secure a corporate approach chief officers will ensure that any departures from established practice are only implemented, subject to the agreement of the National Centre for Policing Excellence (or any successor body), and where it can be shown that the change is an innovation that has resulted in an improvement to the operation of the model.

7.2.4 It will be the responsibility of the Association of Chief Police Officers and the National Centre for Policing Excellence to ensure that any such changes are not a diversion from the overall aim of achieving national corporacy in the application of the National Intelligence Model.

8 COMMUNICATION AND INFORMATION STRATEGY

8.1 COMMUNICATION AND INFORMATION STRATEGY

8.1.1 The Association of Chief Police Officers and the National Centre for Policing Excellence should have in place a procedure by which police forces, other law enforcement agencies and relevant partner agencies may be informed of changes and developments to the National Intelligence Model.

8.1.2 Chief officers will have in place a communication and information strategy to support the National Intelligence Model. The purpose of such a strategy is to ensure that all members of a police force, practitioners and specialists and other agencies with whom there is a partnership agreement are informed of relevant developments in the application of the National Intelligence Model.

8.1.3 The strategy should also be applied to assist forces to bring the National Intelligence Model into the mainstream of police activity in seeking to enforce the law and protect the public.

APPENDIX 2 NATIONAL INTELLIGENCE MODEL MINIMUM STANDARDS

The features that enable the intelligence unit and other staff to operate effectively and to the minimum standard prescribed by ACPO are covered here. Police forces must take appropriate action to ensure that they comply with all 135 standards listed by November 2005. HMIC will inspect the application of NIM in forces against the national minimum standards.

CONTENTS

ELEMENT 1 – KNOWLEDGE ASSETS

1. CURRENT LEGISLATION AND CASE LAW

A professional Police Service will ensure that its staff remain fully informed of legislation and case law developments, and that they have ready access to up-to-date information sources on a round the clock basis.

Meeting the Criteria

There must be continual access to a knowledge repository (locally, centrally, or electronically) and it must cover all areas of policing activity, for example:

- Crime;
- Traffic;
- Community;
- Special Branch;
- Firearms;
- Domestic violence;
- Child protection;
- Genesis;
- National Centre for Applied Learning Technologies (NCALT);
- Various private legal databases, details of which can be found in Appendix 3 or through the Office of Public Sector Information: http://www.opsi.gov.uk

Global Force access is considered highly beneficial.

2. CODES OF PRACTICE AND SECONDARY LEGISLATION

A code of practice under the Police Act 1996 is a statutory document which provides a high level strategic framework and principles enabling the development of detailed guidance and practice advice. Some codes of practice are in the form of secondary legislation, providing mandatory compliance, eg, the Police and Criminal Evidence Act 1984 (PACE).

Meeting the Criteria

Ensure access to, and an understanding of, codes of practice relating to:

- NIM;
- RIPA;
- CPIA;
- PACE;
- DPA;
- Criminal Records Bureau (CRB);
- Serious Crime Analysis Section (SCAS);
- PNC;
- Police use of firearms and less lethal weapons;
- Any future or proposed associated codes of practice and secondary legislation.

3. MANUALS OF GUIDANCE

Manuals of guidance describe the minimum level of standards and subsequent compliance required by forces or law enforcement agencies in respect of various policing activities, for example the investigation of missing persons or the police use of information. This enables effective deployment within a legal framework, and provides a basis for a national learning requirement.

Meeting the Criteria

Ensure access to, and an understanding of, standards in respect of relevant subjects, for example: NIM, data communications SPOC, dangerous offenders, priority and prolific offenders, prison intelligence, covert operations and the ANPR system.

4. PRACTICE ADVICE

Practice advice documents provide details of good practice, suggest operational methods and structures and provide a further basis for the delivery of training.

Meeting the Criteria

Ensure access to, and an understanding of, practice advice where relevant. For example, practice advice on NIM, murder investigation and anti-corruption. Access can be locally or centrally available, or made available electronically through the use of systems such as the ACPO Intranet or Genesis.

5. FORCE POLICY RELEVANT TO INTELLIGENCE

Individual force policies on intelligence must complement minimum standards and practice advice, while further establishing NIM into everyday policing.

Meeting the Criteria

The following must be in place and adhered to:

- Intelligence strategy;
- CHIS policy;
- Forensic policy;
- T&CG policy.

6. ACCESS TO KNOWLEDGE ASSETS

Providing ready access to knowledge assets is vital to the success and universal understanding of NIM and the intelligence-led policing process.

Meeting the Criteria

Ensure access to NIM guidance and practice advice documents through NCALT, Genesis, force intranet sites and hard copy documents. Ensure access to the periodic *NCPE Covert Intelligence Journal* (see Appendix 6 for contact details) and the Genesis NIM website, both of which provide a forum for frequently asked questions (FAQ) and promote good practice, data sharing protocols, marketing materials and briefing products.

7. FORCE NIM COMMUNICATIONS STRATEGY

The development of a marketing and communications strategy designed to promulgate the benefits of NIM both internally and externally to the Police Service, is fundamental to the successful implementation and further development of NIM.

Meeting the Criteria

There must be a method in place such as Genesis, for communicating a standard message to all staff and partner agencies, including the capture and dissemination of case study examples of local and/or national good practice.

8. FORCE IT STRATEGY (FORCE INFORMATION STRATEGY)

All police forces' IT strategies must include issues relating to the support and maintenance of intelligence IT structures. This will ensure the continual employment of intelligence-led policing.

Meeting the Criteria

There must be a force IT strategy in place that is consistent with intelligence-led policing. This includes a priority service for the maintenance of technology used by intelligence analysts, and the regular review and upgrading of analytical tools in line with individual force needs. Police forces must ensure the security vetting of a limited number of IT staff, and make certain that those staff have access to secure information for maintenance purposes.

9. IT DISSEMINATION OF FORCE/LOCAL CONTROL STRATEGY AND INTELLIGENCE REQUIREMENTS

In order to maintain the Police Service's focus of direction, all staff members must be aware of BCU, force and/or national priorities for law enforcement, together with the information required to support those priorities, including the *National Policing Plan, Force Policing Plan, Community Safety Strategy* and local Best Value Performance Indicators (BVPI).

Meeting the Criteria

A force intranet should be used to communicate force/local priorities and intelligence needs to all staff. This may include IT access to force/local control strategic assessments, although security, ie, GPMS, must be taken into account. See 2.10 Determine Asset Values for more information on protectively marked material using the GPMS.

10. IT DISSEMINATION OF T&CG ACTIONS

Effective management of the T&CG process includes providing an appropriate means of ensuring tasks are carried out and monitored.

Meeting the Criteria

An IT system should be in place to disseminate force/local strategic and tactical T&CG actions to staff and to confirm that all the necessary actions have been carried out and recorded. Dissemination must take security into account and the content may be reduced, particularly at level 2. Access must be restricted to nominated staff only, and good practice identified.

11. FORCE TRAINING STRATEGY

A project is currently underway designed to identify the National Learning Requirement for the intelligence discipline. Many forces provide specialist intelligence training, for example, in research and development and source handling. Only intelligence manager and analyst training courses are, however, delivered as nationally accredited products. It is, therefore, incumbent on forces to provide a training strategy which ensures that all staff members are fully aware of their roles and responsibilities under NIM, until such time as national training products are fully developed. For further information see *ACPO (forthcoming) Practice Advice on Resources and the People Assets of NIM.*

Meeting the Criteria

A force training strategy must be in place covering explanations of NIM and the processes involved in gathering and submitting intelligence. It should emphasise the importance of intelligence submissions, and the fact that such submissions are especially important from staff in specialist roles outside of the intelligence function.

IMPACTS AND BENEFITS

The impacts and benefits of meeting all of the minimum standards related to the knowledge assets element of NIM are outlined below.

Increasing Professional Knowledge and Understanding

Having readily accessible products that allow staff to increase their professional knowledge and understanding, benefits the individual and the organisation.

Central repositories of knowledge reduce the duplication of research to locate good practice and legal advice. This repository should be available to operational officers at all times.

Effective IT Strategies and Structures to Deliver Corporate Standards

Providing an effective IT strategy which encompasses the intelligence processes and sets a direction for standard IT systems, will improve accessibility to local force and BCU published priorities.

Using a standard format for delivering knowledge assets allows for a corporate localised message, greater sharing of standardised information and a more timely access to information.

Improved Communications

A communications strategy aimed at marketing the benefits of NIM, both internally and externally, will promote easier implementation and understanding of NIM and ultimately reduce communication costs.

Training

A published NIM and intelligence training strategy ensures that focus is maintained on improving the knowledge and skills profile of staff.

ELEMENT 2 – SYSTEM ASSETS

12. PHYSICAL SECURITY

Access to and from vulnerable areas must be monitored and controlled, and intelligence material must be managed in a secure manner.

Meeting the Criteria

Clear desk policies and secure file storage systems must be in place, located within secure intelligence accommodation. Local police forces must ensure that access policies are in place that enable staff to gain entry to secure environments.

13. SECURITY POLICIES RE: INTEGRITY, CONFIDENTIALITY AND VETTING STANDARDS WITHIN INTELLIGENCE WORK

Those individuals working within secure environments must be subject to clearance themselves. The manner in which material is recorded, disseminated and retained must also be the subject of security policy.

Meeting the Criteria

The use of the GPMS must be apparent. Documents and products must be appropriately GPMS coded. IT access and access to data must be restricted and auditable. Vetting protocols for intelligence staff must accord with ACPO Anti-Corruption Advisory Group (ACAG) policy.

14. DISCLOSURE

Compliance with the rules relating to disclosure under the CPIA is vital to maintaining the integrity of intelligence-led policing.

Meeting the Criteria

A system must be in place to provide an assessment of intelligence products which enables the release of intelligence material to the disclosure officer.

15. STERILE CORRIDOR

Duty of care and the protection of covert assets are principles that must be adhered to in the targeting of criminals and criminality.

Meeting the Criteria

Police forces must ensure source protection and confidentiality both internally and externally in information sharing and the dissemination of intelligence. A firewall must be installed between the employment of covert resources and all other elements of business outside the authorisation process.

16. REAL-TIME SEARCH CAPABILITY

Being able to make an early risk assessment on the nature of any incident being attended, through the use of sound intelligence, is vital to ensuring effective police response.

Meeting the Criteria

This capability particularly applies to the patrol function. Police forces should consider providing a service for staff attending incidents (usually located within command and control) which enables informed decisions and risk assessments to be made by relaying pertinent intelligence. This service should be located within command and control. Data integrity and quality is essential for it.

17. STANDARD ANALYTICAL TOOLS

Nationally recognised analytical tools are essential to effective analysis.

Meeting the Criteria

Local force standards must be set and implemented. They will include a wide search capability for all intelligence analysts and also the provision of IT and training. For further information contact the National Analyst Working Group (details in Appendix 6) and see *ACPO (forthcoming) Practice Advice on Tasking and Co-ordination.*

18. EFFECTIVE BRIEFINGS AND DEBRIEFINGS

All staff should be fully briefed and continually informed of all tasking and intelligence requirements. Debriefing is also vitally important in maintaining the cycle of information.

Meeting the Criteria

Intelligence must be fed back to the Intelligence Unit and dedicated briefing facilities, structures and processes must be established in all areas of activity. The patrol function briefing must correlate with the tactical menu and drive tasking. The NBM must also be adhered to. For further information see *ACPO (forthcoming) Guidance on the National Briefing Model.*

19. INTER-AGENCY INFORMATION SHARING PROTOCOLS

Information management and the provision of protocols, standard operating procedures and MOUs between agencies, are essential to the efficiency of NIM. The *ACPO (2005) Code of Practice on the Management of Police Information* and *ACPO (forthcoming) Guidance on the Management of Police Information* provides information on such protocols at a national and international level.

Meeting the Criteria

Examples of inter-agency information sharing protocols include:

- *ACPO (2002) HM Customs and Excise Memorandum of Understanding Disclosure of Information;*
- CDRP;
- Wider crime reduction partnership community protocols at both local (level 1 and 2) and regional (level 2 and 3) levels;
- Section 115 of the CDA, which provides a statutory gateway for information sharing for crime and disorder purposes.

Prison intelligence protocols must be established to enable profiling of dangerous/sex or priority and prolific offender releases.

20. STANDARDISED AND INTEGRATED INTELLIGENCE DATABASE

Integrated information and intelligence systems provide a reliable framework for quality data management and analysis and such systems are the forerunners of a nationally integrated network.

Meeting the Criteria

Forces will have an integrated custody/case/nominal, forensic, crime and incident reporting database in place to aid in the search and retrieval of data to assist analysis. Partner agency information/data will be included in accordance with agreed protocols, thereby assisting local prevention and enforcement planning. Being a member of a data warehousing consortia together with other regional forces enables the search and retrieval of information across organisational boundaries.

21. HIGH-SPEED SEARCH CAPABILITY

Rapid information searching and retrieval is vital.

Meeting the Criteria

There must be direct single key access/input and search capability across integrated databases.

22. AUTHORITIES PROCESSES AND DOCUMENT MANAGEMENT SYSTEMS IN PLACE

Compliance with legislation such as HRA, CPIA and RIPA requires an auditable and secure authority and management system.

Meeting the Criteria

Police forces must have document management and file tracking systems that facilitate the auditing of paper systems and authorities (electronic or paper system to show history of input and access, dates, owners, authority). Police Informant Management Systems (PIMS) is an example of such a system.

23. HUMAN RESOURCES SYSTEM

Personnel management is a key factor in delivering NIM successfully. See standards 41 Minimum Establishment Policy and 42 Succession Planning.

Meeting the Criteria

Police forces must have a human resources system in place to monitor the skills profile and availability of key personnel.

24. SYSTEM DEVELOPMENT

Ensuring the availability of up to date IT solutions and systems development for the purposes of information and intelligence management will provide credible NIM products.

Meeting the Criteria

An Intelligence Steering Group must be established which has responsibility for continual systems development, including IT. This group should identify the requirements and report on or investigate solutions. Connectivity of information systems and analytical tools is a priority to ensure the quality and timeliness of intelligence product delivery.

25. IT CRITICAL INCIDENT RECOVERY PROCEDURES/PROCESS (FORCE DISASTER RECOVERY STRATEGY)

The ability to provide access to, and the use of, information sources must be maintained in the intelligence process.

Meeting the Criteria

Protocols must be established to facilitate priority IT service, maintenance and recovery to allow the continuity of business in the event of a crash to the intelligence function and, in particular, the analytical capability.

26. USE OF PNN2 AND CJX (STANDARD LEVELS OF ACCESS)

National IT standards must be maintained including the security standards essential for the use of the second generation Police National Network (PNN) telecommunications infrastructure, PNN2, which supplies forces with telephony, internet access and secure extranet. The use of the Criminal Justice Extranet (CJX) allows secure information sharing with other agencies connected to the network, including the CPS, CRB and Forensic Science Service.

Meeting the Criteria

Forces must comply with the national standards set by PITO and install inspection measures to confirm adherence to these.

IMPACTS AND BENEFITS

The impacts and benefits of meeting all of the minimum standards related to the system assets element of NIM are outlined below.

Local Force Policy and Procedure for System Assets

The establishment of policies and procedures in line with minimum standards allows police forces to undertake internal checks against agreed national and local standards, and to give better value for money including reducing cost and bureaucracy.

Security and Integrity

Implementing the minimum standards regarding security and integrity will provide improved protection of intelligence assets. Personnel vetting and the establishment of sterile corridors and clear desk policies will embed a 'need to know' culture.

Research and Analysis

An efficient and timely research capability giving immediate and direct access to information enables informed operational risk assessments and appropriate action to be taken. It also provides reassurance to front line staff.

Improved access to data through the use of standard products for intelligence and analytical functions leads to greater efficiency and effective use of resources.

Information Management

Adherence to both NIM and information management standards (in terms of intelligence databases and authorities processes) creates a more competent platform when accessing and sharing data with partners. This, in turn, improves the flow of information and data sharing. It also improves cross-border search ability and enables remote access to systems.

Compliance with the NBM will assist in providing an efficient, intelligence-led, response service.

Information Technology Policy

An information systems strategy to underpin police force and local core business processes is at the heart of NIM. Essential data must be safeguarded. In the event of a system failure, this strategy will clearly demonstrate the measures to be taken to ensure the continuity of information management during any recovery period.

ELEMENT 3 – SOURCE ASSETS

27. VICTIMS AND WITNESSES

Victims of crime and witnesses to crime are vital sources of intelligence. The ability to identify repeat victims; vulnerable persons, areas of criminal activity and categories of crime provide important sources of information for the NIM process.

Meeting the Criteria

Intelligence should be secured from victims/witnesses who have been the subject of offences that fall within the control strategy or who have witnessed such offences. The details obtained from them must be reported to the intelligence function. This will include data input in to the SCAS from such sources. For further information see *Home Office (forthcoming) Codes of Practice for the Use of the Serious Crime Analysis Section.*

A force policy must be implemented locally to engage in intelligence interviews with repeat victims. These interviews must be subject to risk assessment and conducted with the knowledge and sanction of the senior investigator.

28. REPEAT VICTIMS

See standard 27 Victims and Witnesses

29. PRIORITY AND PROLIFIC OFFENDERS

Collecting as much information as possible about the activities of priority and prolific offenders enables offender profiling, improves tasking and enhances the effectiveness of analytical products.

Meeting the Criteria

A force policy must be in place, and implemented locally to engage in intelligence interviews with priority and prolific offenders. These interviews will be subject to risk assessment and conducted with the knowledge and sanction of the senior investigator.

30. ACCESS TO COMMUNITY INTELLIGENCE

Access to community intelligence is an important aspect of integrating NIM with neighbourhood policing. Information gained from local communities should be used to inform the strategic and tactical assessments at level 1 and 2 which will assist in the deployment of resources in response to problems of crime and disorder. See *ACPO (2005) Practice Advice on Professionalising the Business of Neighbourhood Policing (Draft).*

Meeting the Criteria

There must be force/local management of knowledge around community information such as local demographic profiles, community contacts and resources, community profiles and multi-agency information.

31. CRIMESTOPPERS

The Crimestoppers process provides vital sources of information which, in response, require research, analysis and appropriate action.

Meeting the Criteria

There must be access to corroborative evidence or the capability to receive, evaluate and seek corroboration, to enable assessment and tactical resolution to be conducted where appropriate.

32. PRISONERS/PRISON VISITS

Intelligence approaches to persons in police custody, conducted within guidelines, and early visits to convicted prisoners have been shown to provide high quality information and intelligence which can be used effectively in the NIM processes. See *ACPO and HMCE (2004) Manual of Standards for Covert Human Intelligence Sources* and *ACPO (forthcoming) Practice Advice on Prison Intelligence and Related Matters.*

Meeting the Criteria

An intelligence approach policy must be established in accordance with identified priorities. Active use should be made of prison visits to assist the capture of intelligence. Risk assessments must be carried out.

33. PRISON INTELLIGENCE

Intelligence approaches to persons detained in police custody, conducted within guidelines, and early visits to convicted prisoners can provide high quality information and intelligence which can be highly beneficial in the NIM processes. See *ACPO (forthcoming) Practice Advice on Prison Intelligence and Related Matters.*

Meeting the Criteria

At a force level, there must be the capability to develop meaningful profiles of criminals who are to be released from Her Majesty's Prison (HMP) or future equivalent or a National Offender Management process. This is likely to include certain recidivists and defined priority and prolific offenders who fall within control strategy priorities, together with dangerous offenders and sex offenders that pose a high risk. Target profiles should be developed to national standards using police, probation and prison intelligence to enable a threat assessment to be conducted and tactical plans to be developed, thereby reducing risk to the public.

Protocols and authority levels for data exchange must also be in place (see 2 System Assets).

34. COVERT HUMAN INTELLIGENCE SOURCES (CHIS)

The lawful, ethical and efficient use, conduct and tasking of CHIS in accordance with identified priorities, is seen as one of the most powerful and cost effective intelligence tools available to law enforcement.

Meeting the Criteria

There should be active use of CHIS in line with legislation, ACPO minimum standards and control strategy priorities.

35. USE OF ENHANCED CHIS PROFILING

The use of enhanced CHIS profiling can be particularly beneficial when used as part of an intelligence collection plan on an organised criminal group or a location difficult to infiltrate.

Meeting the Criteria

Police force and/or local enhanced profiling of all CHIS assets and searches of the National Source Database (at NCIS) should be considered, where necessary, in order to optimise intelligence opportunities.

36. UNDERCOVER/TEST PURCHASE OPERATIVES

For further information see *ACPO and HMCE (2003) Manual of Standards for the Deployment of Test Purchase and Decoy Officers* and *ACPO and HMCE (2003) Manual of Standards for the Deployment of Undercover Officers.*

37. ACCESS TO INTERCEPTION PRODUCT

For further information see *ACPO/ACPOS/HMCE (2003) Manual of Standards for Accessing Communications Data.*

38. SURVEILLANCE PRODUCT

Covert deployments, while often evidential in nature, provide a large volume of intelligence concerning the subject of an operation as well as their associates and other related issues.

Further information can be found in *ACPO and HMCE (2004) National Standards in Covert Investigations Manual of Standards for Surveillance.*

Meeting the Criteria

Information or intelligence obtained from covert deployments (identified in 3 Source Assets) should be recorded onto the intelligence function and organisational memory. Sterile corridor processes should be considered at the time of the exchange of material between covert units and the intelligence function, including the sanitisation of information reports. Access to covert units will be through defined gateways. Covert deployments will be in line with control strategy priorities, but may also be used on other high profile crime issues.

Policy logs must be maintained and full risk assessments evident for all stages of the information exchange. Policies must be in place to allow direct submission of intelligence to operational command where immediate personal and/or operational risk is identified.

39. FORENSIC DATA AND FORENSIC INTELLIGENCE POLICY

The incorporation of forensic sources of information or intelligence enhances the NIM processes by giving a fuller picture of criminal behaviour and patterns.

Meeting the Criteria

Forensic data, in particular from linked crime scenes, should be used as source material and introduced into the intelligence function in line with control strategy objectives. Force level management of forensic hits will be in place to ensure inclusion within the T&CG process and ensure that information is acted on in a timely fashion. Forensic intelligence and data should be included in the crime series and target management forums along with access to SCAS data.

Forensic and intelligence strategies and policies will enforce these standards.

40. OTHER SERVICE/AGENCY TASKING

Sources of information are available from a wide variety of other agencies and law enforcement bodies and must be used where appropriate.

Meeting the Criteria

Measures must be in place to identify and use external source opportunities to enable tasking and access to products through agreed gateways. Tasking another law enforcement agency's CHIS via the National Source Management Unit at NCIS, which is in line with control strategy priorities or an approved major enquiry, will be subject to an auditable and justifiable request and authority process.

IMPACTS AND BENEFITS

The impacts and benefits of meeting all of the minimum standards related to the source assets element of NIM are outlined below.

Multiple Sources of Information

Adopting the stated minimum standards will ensure that information is obtained from multiple sources. Engagement with partner agencies can provide a vast source of information and data relating to community issues which have previously been under-used.

Assets outside the scope of the Police Service can be realised and used to assist both force and local objectives. This will lead to an improved information base with regard to community priorities including crime and disorder issues.

Ownership of Intelligence

The minimum standards will create a culture of understanding that intelligence is everywhere and it is every police person's job to find it and report it. Creating a minimum standard for gathering intelligence from other internal sources (for example, crime records, child protection records and incident records), and issues such as a focused CHIS strategy communicated to all police staff, will encourage the flow of information and assist the efficiency of the NIM processes.

Profiling

An increased access to victims, witnesses and prisoners for the purpose of intelligence interviewing will lead to enhanced profiling and the development of a victimology. This will provide opportunities to realise the causes of crime and who might have committed them.

Community sourced information will assist in the ability to identify local tension hot spots and disorder and behaviour effecting the quality of life in a community.

Targeting and Tasking

These standards will also lead to visible targeting of particularly disruptive elements in a community. Where the standards reflecting source assets are focused on control strategy priorities and intelligence requirements, a more structured and consistent intelligence-led approach at BCU (level 1) and service level (level 2) can be achieved. This will lead to precision tactical deployments, a more cost effective use of resources and better informed decision making – from constable to chief officer.

ELEMENT 4 – PEOPLE ASSETS

41. MINIMUM ESTABLISHMENT POLICY

The successful implementation of NIM and its subsequent operation as a model is dependant on ensuring that minimum levels of resources are in place in key roles.

Meeting the Criteria

A local force policy relating to intelligence functions must be in place and adopted at all levels. Key roles and the number of staff required to meet the expectation of a T&CG must be outlined, in accordance with the minimum standards established for those roles.

This includes:

- Analysts;
- Data input;
- Evaluation and management;
- Research and development;
- Briefing and source management.

Skills for Justice competency levels must also be met.

42. SUCCESSION PLANNING

The success of an intelligence structure is reliant on building a professional body of knowledge. Succession planning for the key roles identified in NIM is vital.

Meeting the Criteria

A succession planning policy must be in place and adhered to. It is likely to include initiatives such as job share and buddy systems for specific critical roles within the specialist intelligence function.

43. ACPO LEAD FOR NIM IMPLEMENTATION AND DEVELOPMENT

The appointment of an ACPO lead to ensure that respective forces remain focused on their requirements to meet the national minimum standards is an important factor in determining force performance.

Meeting the Criteria

An officer of ACPO rank must be appointed as a lead in each police force to ensure the implementation and development of NIM and the maintenance of minimum standards.

44. T&CG CHAIRS

The minimum standards allow local determination of the chairing of local force T&CG meetings. Significant benefits can be obtained from the chief officer chairing the force strategic T&CG. The roles are:

- ACPO Chair of force strategic T&CG;
- ACPO/Designated Deputy Chair of force tactical T&CG;
- ACPO Chair of regional strategic and tactical T&CG;
- BCU Commander Chair of BCU strategic T&CG;
- BCU Commander/Designated Deputy Chair of BCU tactical T&CG.

Meeting the Criteria

All police forces must ensure that the relevant T&CG chairs are appointed and have executive authority empowering them to make resource decisions. T&CG chairs should develop the necessary skills and knowledge of their role in line with *ACPO (forthcoming) Practice Advice on Tasking and Co-ordination.*

45. DIRECTOR OF INTELLIGENCE/HEAD OF PROFESSION (INTELLIGENCE)

A senior member of the force with appropriate experience in the field of intelligence and/or proactive investigation can provide a focus for the efficient management of the intelligence process.

Meeting the Criteria

The staff member in the role must have ownership of the intelligence function, its development and strategic direction. The head of profession also has responsibility for the production and submission of the four intelligence products, the force control strategy and the intelligence requirement to the force T&CG.

46. AUTHORITIES MANAGEMENT

The establishment of a centrally located police authorities bureau enables forces to manage the processes and administration concerned with covert operations and CHIS competently. Dedicated police staff can build a body of knowledge relating to NIM and intelligence processes through this.

Meeting the Criteria

Police forces must have all of the following in place:

- RIPA authorising officer(s) in compliance with the Act, ie, an ACPO and Detective Superintendent at force level and a BCU commander locally;
- Infrastructure and systems to ensure appropriate tasking of CHIS, surveillance, undercover and intrusion;
- Records management for compliance with relevant legislation, manuals of standards and codes of practice;
- Evidence of security and sterile corridors.

47. TELECOMMUNICATIONS SINGLE POINT OF CONTACT (SPOC)

The code of practice and manual of standards for accessing communications data dictates that each force will have a SPOC department to manage all authorities and issues around accessing evidence or intelligence through defined communication systems. Accredited, highly trained personnel provide a point of contact for all police staff and other external agencies.

Meeting the Criteria

A telecommunications SPOC must be in place. SPOC departments are usually located centrally as a resource to individual forces through agreed gateways.

All staff operating in a telecommunications SPOC department must have completed the required accredited course. Post-holders must operate according to force policy (see *ACPO/ACPOS/HMCE (2003) Manual of Standards for Accessing Communications Data*) with regard to accepting requests and disseminating intelligence.

48. INTELLIGENCE MANAGER

An intelligence manager must be of appropriate status to be appointed. This is to ensure that experience is added to the analytical techniques and products before they are presented to the T&CG.

Meeting the Criteria

Intelligence managers are usually of inspector rank at the BCU level of operation. They must have successfully attended an intelligence management training course. As with the role of director of intelligence as described above, an intelligence manager is responsible for the intelligence function and intelligence product delivery locally.

49. CHIS CONTROLLER AND DESIGNATED DEPUTY CHIS CONTROLLER

These roles maintain the integrity of systems and processes and manage the risk involved in the day-to-day engagement with members of the criminal fraternity. These roles are mandated by the *ACPO and HMCE (2004) Manual of Standards for Covert Human Intelligence Sources,* Part 3 – Roles and Responsibilities.

Meeting the Criteria

The CHIS controller and designated deputy CHIS controller must have successfully completed suitable, accredited, CHIS training. They are responsible for:

- Team supervision of field capability;
- Supervising meetings with sources;
- Ensuring day-to-day alignment with the T&CG control strategy and tactical priorities.

They must also ensure staff compliance with:

- RIPA;
- Dissemination of intelligence policy;
- DPA;
- Internal auditing.

The CHIS controller should be of inspector rank. For further information see *ACPO and HMCE (2004) Manual of Standards for Covert Human Intelligence Sources.*

50. SOURCE HANDLER

Forces must establish DSUs staffed by highly trained and accredited source handlers. For further information see the *ACPO and HMCE (2004) Manual of Standards for Covert Human Intelligence Sources.* NIM supports this principle and recognises source handling as a core function in intelligence-led policing.

Meeting the Criteria

Source handlers must be a dedicated resource and appropriately trained to a minimum of Training Level 2 on a nationally accredited course. They are responsible for the effective, ethical and lawful recruitment, handling and co-handling of covert human intelligence sources in accordance with the requirements of the T&CG.

51. ANALYTICAL CAPABILITY

NIM analyses information and data from numerous sources, thereby providing an intelligent picture of policing issues. The delivery of proven analytical products and key assessments is fundamental to the success of this model. For further information contact the National Analyst Working Group (details in Appendix 6) and see *ACPO (forthcoming) Practice Advice on Tasking and Co-ordination.*

Meeting the Criteria

Sufficient accredited intelligence analysts must be in place to support tasking processes at both strategic and tactical levels, and in order to support the investigation of major crime. In addition to local analysts, it is highly beneficial to have centrally based analysts so that they can profile force control strategy priorities. There must also be an analytical capability to identify series offences both locally and centrally. A process of series identification should be established to enable reporting to the TT&CG and to aid crime series forums. Minimum staff numbers should take into account force crime/incident profiles and not be prescribed.

52. HEAD OF PROFESSION – INTELLIGENCE ANALYSIS

This position is usually filled by a principal analyst with the post-holder being head of profession for all the intelligence analysts. This role carries responsibility for the strategic development and quality assurance of intelligence products, technical skill levels and training the workforce and will include joint training with partner agencies

Meeting the Criteria

Police forces must ensure that a fully qualified and trained force principal analyst is appointed and authorised to provide a professional management focus for the analytical discipline.

53. ANALYSTS ACCREDITATION

The deployment of analysts across all levels of policing is a vital component of NIM. Resource strategies for analysts should be linked to the national training strategy for the discipline. Analysts must gain accreditation through training and workplace assessment in order to support prosecutions on the basis of standardised, high quality, intelligence products.

Meeting the Criteria

Police forces must ensure that they appoint sufficient analysts who are trained to appropriate national standards, to meet the needs of the entire scope of policing from the community and partnership level to serious and organised crime, working at all three levels of law enforcement.

54. FIELD AND RESEARCH CAPABILITY

Field and/or research intelligence officers (see 7 Research, Development and Analysis) are responsible for the provision of field and research support in accordance with the intelligence collection strategy. They provide the vital link between covert intelligence collection and analysis, and appointed investigators.

Meeting the Criteria

The deployment of field and/or research officers is aligned to control strategy priorities, unless otherwise sanctioned. Their role consists of the research and development of packages for action (usually to assist the investigative process), a sterile access to source handlers and proactive intelligence collection. They must successfully complete accredited Research and Development training at the earliest opportunity and prior to appointment to level 2/3 resources.

A specialist intelligence research capability should be provided where necessary. Such resources are usually based centrally and may consist of:

- Prison liaison;
- Sex offender and dangerous offender resources;
- Financial investigators;
- Crimestopper capability.

All of these resources should be available to police forces through agreed gateways.

55. TECHNICAL SUPPORT UNIT CAPABILITY

Intelligence units will usually have their own technical field capability which will be able to deploy technical equipment against level 1 criminality, based on criteria set by the T&CG and in line with the area control strategy. Although line-managed at BCU level, professional development and procurement of technical equipment should be governed by the head of police force dedicated TSUs. For further information see 4 People Assets and also *ACPO (forthcoming) Practice Advice on Resources and the People Assets of NIM.*

Meeting the Criteria

There must be access to the TSU, which is usually located centrally. In smaller forces there must be access to a regional unit. TSU officers must be trained to relevant technical standards. See *ACPO (2004) Deployment Standards for Technical Support in Tackling Volume Crime* and CD published by the former PSDB known as *The Yellow Book.*

56. INFORMATION AND INTELLIGENCE MANAGEMENT

The timely recording, dissemination and subsequent management of information and data sources are crucial to the provision of a competent intelligence structure.

Meeting the Criteria

There must be sufficient capability to evaluate, input and manage information from a wide range of sources. Data quality, consistency, timeliness of input and compliance with relevant legislation and inputting standards must be ensured. The *ACPO (2005) Code of Practice on the Management of Police Information* and *ACPO (forthcoming) Guidance on the Management of Police Information* must be adhered to.

57. DATA PROTECTION

Compliance with legal provisions such as the DPA, PNC Codes and the *ACPO (2005) Code of Practice on the Management of Police Information* must be stringently adhered to in order to maintain the integrity and security of the intelligence process. This must not, however, prevent the exchange of information with partners in support of policing purposes.

Meeting the Criteria

Intrusive inspections must take place to ensure compliance. This must include the security of IT and information and intelligence assets. Data protection must be seen as part of the process of information management, rather than as a separate process to NIM.

58. DEDICATED IT SUPPORT

In the continually changing world of information technology, intelligence IT systems must be sufficiently robust, efficient and subject to future proofing to ensure that the necessary capacity and quality of product is achieved.

Meeting the Criteria

A post holder must be in place centrally and accessible locally, in order to meet the critical incident recovery policy and to develop IT in accordance with needs. They must also ensure linkage between local systems and national information systems developments, for example, Impact. Service level agreements (SLA) are signed off by the intelligence director and the head of IT.

59. BRIEFING CAPABILITY

See *ACPO (forthcoming) Guidance on the National Briefing Model.*

Meeting the Criteria

A briefing capability is the responsibility of the intelligence unit. This can be a dedicated role although it does not have to be. Briefing packages, particularly for the patrol function, must be prepared in accordance with T&CG tactical menu actions. The results emanating from briefings must be fed back into the organisational memory.

60. TT&CG ACTIONS MANAGER

This standard should be read in conjunction with *ACPO (forthcoming) Guidance on the National Briefing Model* and *ACPO (forthcoming) Practice Advice on Tasking and Co-ordination.* The TT&CG actions manager role is that of an enforcer. It carries responsibility for arranging the execution of TT&CG actions, including follow-up actions allocated to other managers. It may also include responsibility for managing the briefing process. This role may be found on BCU and centrally at level 2.

Meeting the Criteria

Police forces must ensure that there is a capability responsible for co-ordinating actions emanating from the T&CG meetings, enforcing the delivery of those actions, monitoring progress and feeding back results to the T&CG and organisational memory.

61. HIGH VISIBILITY/STRIKE TEAMS

This standard should be read in conjunction with *ACPO (forthcoming) Practice Advice on Tasking and Co-ordination.*

Meeting the Criteria

Resources must be available for tactical T&CG tasking. The numbers are not prescribed, but may include:

- Dogs;
- Public order units;
- Tactical Support Groups;
- The patrol function;
- Cycle patrol;
- Traffic, air and river support.

If no dedicated capability is in place, a logistics capability to use neighbouring BCU or police force resources, necessary to meet T&CG requirements, should be evident.

62. JOINT AGENCY AND SPECIALIST OPERATIONS INTELLIGENCE CELLS

The formation of joint agency intelligence cells or cells set up specifically for major operations requires careful management and adherence to strict protocols. The following are common examples of joint agency and specialist intelligence cells:

- CDRP;
- Prisons, through adequate investment in prison intelligence officers;
- Immigration investigations;
- Serious crime investigations;
- National security investigations and operations.

Meeting the Criteria

A policy must be in place in police forces to enable the use of multi-agency staff in a joint intelligence cell and should include agreed data sharing protocols, governance issues and security policies. Joint agency intelligence cells usually operate from a single site, with one common purpose dictated by a control strategy.

IMPACTS AND BENEFITS

The impacts and benefits of meeting all of the minimum standards related to NIM people assets are outlined below.

Professionalising the Workforce

Compliance with the minimum standards in respect of establishment policy and succession planning will create resilience within intelligence structures and enable business continuity. In addition, a standardisation of roles throughout the service will promote and enable cross-border cooperation and rationalisation of investigative activities.

The minimum standards give rise to a focused training strategy by training personnel to specific skill requirements. Training costs will be reduced through training key staff on the basis of need, while specialising has the effect of increasing professionalism in a particular area and thereby reducing personal and organisational risk.

Corporate Standards and Ownership

The appointment of an ACPO lead will ensure that NIM implementation and the development of NIM as a business model remains at the centre of the strategic processes of each police force. ACPO driving forward implementation provides a level of responsibility commensurate with the mandatory requirement to firmly establish NIM in day-to-day policing concepts.

Appointing a head of profession (director of intelligence) along with maintaining the continual professional development of intelligence roles defined in NIM, and ensure maintenance of standards.

The appointment of T&CG chairs (with the appropriate level of responsibility and authority) will provide sustainable resource and deployment decisions and specific ownership of each level of the T&CG process.

Legislative Compliance

The provision of specialist SPOC advice and authority units is necessary in ensuring common standards of compliance with legislation and the police authorities processes applicable to NIM and associated policing disciplines. Central Authorities Bureaux and communications SPOC offices provide a protected knowledge base and streamlined compliance capability, which enables the intelligence and covert business community to more readily use and obtain intelligence from specialist sources such as covert surveillance and interception of communications.

Management Specialists

Senior management specialists (with an in-depth understanding of the management of intelligence operations, NIM and related issues such as covert policing tactics) are essential to a professional intelligence structure and the development of NIM.

Compliance with the minimum standards in respect of directors of intelligence, intelligence managers, CHIS controllers and heads of analysis will give forces a strong leadership focus in respect of NIM.

Analysis

A highly trained analytical capability with career structures, appropriate grading and professional accreditation, is a core element in the implementation and continual development of NIM.

Implementation of the standards relating to analysis will result in the acquisition of a corporate analysis knowledge base, and improve the assessment of policing activity, thereby allowing informed decision making and promoting better quality data for higher quality intelligence products.

Field and Research Capability

An ability to build efficient intelligence packages on a foundation of comprehensive research and field operations will lead to improved investigations into targets, crime problems and identified hot spots.

Professionally managed and trained technical human resources will provide a tactical capability necessary for the development of intelligence tasking and tactical resolutions.

Specialist resources can be more effectively deployed through improved target file development.

Information Management

The importance and value of providing an efficient information and data management resource with systems maintained by dedicated IT support cannot be overemphasised.

Implementation of standards in respect of information management resources will reduce the risk of compromised sources, data and information. It also has the effect of increasing information flows.

High quality information management leads to improved intelligence communication and creates an audit trail to indicate why (justification) issues were, or were not, acted on. It also enables police forces to maintain a consistent flow of information and ensures that police staff have an up-to-date knowledge and understanding of business problems.

Effective Briefing and Debriefing

Ensuring that the minimum standards are met will result in improved tasking and direction of patrol officers and that intelligence collection opportunities are optimised.

T&CG action managers driving forward the BCU or force business will ensure that the necessary resources are available and actions and tasks are acted on and completed.

Tactical Response

Implementation of this standard will deliver an increased focus on proactive policing in accordance with control strategy priorities and enable evaluated information to be quickly acted on, thereby encouraging police staff to support NIM. It will also promote public reassurance, help to resolve problems and disrupt targets, resulting in reduced crime.

ELEMENT 5 – INFORMATION SOURCES

63. OPEN AND CLOSED SOURCE DATA

Staff should be sufficiently trained and IT must be in place to fully exploit all available sources of data.

Meeting the Criteria

Both training and IT should be available to enable local or central access to open/closed source data such as:

Forensic information

- Shoe Mark Index;
- Forensic medical training;
- DNA database;
- Weapons and injuries database;

Behavioural/offender profiling information

- Catchem;
- Murder Method Index;
- Badman;
- Fire investigation unit;
- Rape and sexual offences;
- V1 Class (behavioural CPA);

Crime/offender profiling

- PNC/VODS;
- Quest;
- Nimrod;
- National prisoner tracing;

Public access and consumer credit agencies

- Internet;
- Media;
- Lexis-Nexis;
- Equifax;
- Experian;
- National Voters;
- CDA.

For more information on these sources and others available to the Police Service, see the Directory of Information Sources in Appendix 3 of this guidance.

64. INTELLIGENCE, CRIME, CUSTODY AND COMMAND AND CONTROL RECORDS AVAILABLE IN SEARCHABLE FORM

All internal data sources must be developed to allow ready access, ease of search and analysis.

Meeting the Criteria

The intelligence function should have IT access to data in a form that is capable of search and analysis through data IT applications.

65. ACCESS TO HOLMES2/SCAS/NCF PROFILING DATA

All major crime enquiries require the ability to interrogate national profiling data.

Meeting the Criteria

Following a risk assessment, there must be a capability for authorised access to national profiling intelligence databases through agreed policy gateways. A policy log should be in place of decisions made. This type of access usually assists a major enquiry SIO. See *ACPO (2000) MIRSAP Major Incident Room Standardised Administrative Procedures Manual (forthcoming November 2005).*

66. ACCESS TO LIVE DATA EXCHANGE

The ability to research and exchange information on national intelligence data enhances intelligence collection.

Meeting the Criteria

Links must be in place to enable access to national intelligence assets, ie, ANPR, Livescan, Alert database, Antiques database, NCIS Desks and DNA. MOU, data sharing protocols and nominated staff to aid collection are highly recommended at both force and local levels in accordance with force data protection policies.

67. FULL DATA INTEGRATION MODEL

The compilation of efficient strategic assessments requires access to, and research of, many diverse sources of data in order to form a comprehensive picture of issues affecting policing.

Meeting the Criteria

IT access to the following types of data, possibly achieved through central data warehousing with local links to BCUs must be in place:

- Stop and search;
- Forensic data;
- Human resources (HR) data;
- Crime statistics;
- Custody;
- Domestic violence;
- Firearms;
- Budget and finance;
- Business information;
- Public/victim survey data.

See also 2 System Assets.

68. ACCESS TO HUMAN RESOURCES DATA

While access to human resources data will inform strategic assessments, it is also necessary for day-to-day decision making.

Meeting the Criteria

Police forces must ensure that human resources data provides skills profiles, staffing levels and abstraction and sickness levels to assist operational decision making. Human resources data must enable fast time deployment in accordance with assessed risk and enhanced command/control. See also 2 System Assets.

69. ACCESS TO EXTERNAL INFORMATION SOURCES

The many sources of data now available through partnership approaches to policing provide sources of information that have previously remained unused. Intelligence requirements should be set to examine external information sources.

Meeting the Criteria

Local forces and BCUs must ensure access to other law enforcement agencies, government regulated organisations, business and company data. This should be achieved centrally through agreed gateways and authority protocols. Locally, access to external data can be achieved through CDRP agreements, particularly in planning preventative measures.

Examples of external information sources include:

- Public safety/road safety data – local authority;
- Community intelligence – police/CDRP;
- Quality of life data – census/survey;
- Taxi/hackney carriage data – licensing departments;
- Health and education data – local relevant authorities;
- Local authority housing data.

70. CROSS-BORDER INFORMATION SHARING

Sharing information between neighbouring police forces and within police regions will enable a fuller picture of strategic policing issues to be developed. Similar structures at BCU level will give clearer insight into local issues.

Meeting the Criteria

There must be access to neighbouring force and BCU strategic and tactical assessments to provide a comprehensive picture of strategic and local policing issues.

IMPACTS AND BENEFITS

The impacts and benefits of meeting all of the minimum standards related to the information sources element of NIM are outlined below.

Improved Access to Information

Establishing protocols which ensure access to all available information sources will enable greater research capability for analysts and others to enhance decision-making and justification processes. This will improve knowledge and awareness of external factors effecting policy and lead to high quality strategic assessments and well qualified intelligence products.

Integrated IT Processes

Application of the stated standards will lead to more robust and applicable IT policies with better security in place. IT functions will develop in line with need and this will assist in creating a national integration of force intelligence systems. Improved connectivity of data across all systems will provide more accurate, timely and efficient research and use of data.

Improved Operational Effectiveness

The establishment of minimum standards with respect to information sources will increase staff knowledge of the intelligence and investigative tools available for qualitative research. There will be better informed command and control of operational matters with officer profiling to specific requirement and an improved intelligence assessment. This will also enable more effective management, risk assessments and improved officer safety.

Intelligence products enhanced by a wider access to information sources and national intelligence databases will greatly improve local, force, regional and national intelligence-led processes.

ELEMENT 6 – INTELLIGENCE/INFORMATION RECORDING

71. SANITISATION AND RISK ASSESSMENT PROTOCOLS IN PLACE

The integrity of any intelligence system relies on ethical processes and legislative compliance.

Meeting the Criteria

There must be a policy and resources in place to enable hot intelligence assessments, human rights compliance, officer safety and duty of care considerations.

72. COMPLIANCE WITH DATA PROTECTION ACT

The DPA, *ACPO (2000) PNC Compliance Strategy, ACPO (2002) Code of Practice for Data Protection* and the *ACPO (forthcoming) Guidance on the Management of Police Information* provide minimum requirements for access to, and the retention and deletion of, information. All storage of information must be subject to the appropriate security measures.

Meeting the Criteria

There must be an information access, retention, review and security policy in place. Data Protection Officers will proactively and intrusively supervise compliance through thematic testing.

73. AGREED DISSEMINATION POLICY

In addition to data access agreements covered in Element 5 – Information Sources, protocols between law enforcement agencies and partners must be established with respect to the dissemination of information and intelligence material.

Meeting the Criteria

Police forces should ensure that protocols are in place, both at a force and local level, governing the transfer of information and its subsequent dissemination. Agreements with CDRP and Criminal Justice Boards are examples of this process.

74. PRIORITISATION OF DATA INPUT AND RESEARCH

Published control strategies (see 9 Tasking and Co-ordination) should be used as a basis for prioritising data input and research. Other issues may take precedence, providing their tasking is subject to control mechanisms.

Meeting the Criteria

BCU and force publication of control strategies should be evident and be seen to drive prioritised input and research.

75. USE OF 5X5X5 AS STANDARD EVALUATION

The National Information/Intelligence Report Form 5x5x5 is the only system recognised nationwide for the recording, evaluation and dissemination of information into the intelligence system. The ability of staff to have ready access to data input systems, in order to record information, will enhance intelligence collection.

The Impact Programme proposes the design of a national data warehouse system allowing all forces to exchange information and intelligence. This system is reliant on forces having common processes for information data inputting and 5x5x5 information/intelligence reports.

Meeting the Criteria

All forces must show evidence of the 5x5x5 system being used in line with the *ACPO (forthcoming) Guidance on the Management of Police Information.* There must also be evidence of staff training in respect of the 5x5x5 process, including evaluation and risk assessment (by the intelligence function) of submitted information. All forces must be compliant with the guidance mentioned above in respect of the data input of 5x5x5 information/intelligence reports. Direct input of information on to the intelligence process by electronic means must be available to staff.

76. ELECTRONIC INPUT OF INFORMATION/INTELLIGENCE REPORTS (5X5X5)

See standard 75 Use of 5x5x5 as Standard Evaluation.

Meeting the Criteria

See standard 75 Use of 5x5x5 as Standard Evaluation.

77. COMMON STANDARDS FOR DATA INPUT ON TO FORCE IT SYSTEMS

See standard 75 Use of 5x5x5 as Standard Evaluation.

Meeting the Criteria

See standard 75 Use of 5x5x5 as Standard Evaluation.

78. STANDARDISED SYSTEMS FOR AUTHORISING TARGET SELECTION

Standard systems for target selection, managed through the relevant intelligence manager, provide auditable processes which allow decisions to be recorded in compliance with the principles of proportionality, justification and risk assessment. These processes are particularly important when target research and target profiles are authorised prior to T&CG sanction.

Meeting the Criteria

Police forces and BCUs must implement standard target selection systems. Processes are authorised by intelligence managers and will evidence due account of such issues as community impact assessments and human rights principles.

79. PROTOCOLS CONCERNING THE USE OF INTELLIGENCE CODES/FLAGS TO SPEED COLLATION AND RETRIEVAL

The *ACPO (forthcoming) Guidance on the Management of Police Information* and NCIS policy govern the use of codes and target flagging.

Meeting the Criteria

Police forces must demonstrate compliance with the relevant guidance and policy and have internal standard operating procedures in place. Practical application of such protocols must be evident.

80. DATA MANAGEMENT AND SUPERVISION PROTOCOLS

All data systems should be subject to intrusive and proactive management supervision and quality assurance protocols.

Meeting the Criteria

Police forces should have data quality assurance protocols in place to ensure high data standards. These protocols should include defined review processes with respect to the maintenance of up-to-date intelligence records, file tracking and audit trails. Due consideration must be given to other related NIM standards and practice advice, for example, Data Protection Officers (see 4 People Assets) and OPSY (see 2 System Assets).

81. PERFORMANCE MEASUREMENT

Setting performance targets against specified control strategies and intelligence collection requirements will assist in maintaining the business focus of a force or BCU and encourage the need for good quality intelligence recording.

Meeting the Criteria

There must be evidence of the development of performance measures around the collection of actionable intelligence. This should be in accordance with force and/or local priorities as set in the control strategy and intelligence requirement and sanctioned by the T&CG process. CHIS recruitment in hard to reach groups/locations is an example for DSU staff.

IMPACTS AND BENEFITS

The impacts and benefits of meeting all of the minimum standards related to the information and intelligence recording element of NIM are outlined below.

Recording, Dissemination and Retention Standards

Compliance with the stated standards will provide consistent and timely inputting of information. Consistency of data standards brings effective communication, increases professionalism and reduces the likelihood of misunderstanding. This, in turn, will lead to increased confidence in the quality of intelligence.

Accessible IT Systems

Provision of intelligence forms (5x5x5) in electronic format enables easier access to information sources. Users of intelligence databases will also have faster access to information. Intelligence managers, operational heads and T&CG chairs will be given the ability to assess risks and threats more accurately. IT data standards through reduced bureaucracy will result in time and cost savings and create an increased security of information and intelligence.

Performance Measures

Establishing a performance regime synchronised with identified priorities will drive the corporate alignment of NIM across forces and BCU.

Performance measures can be tailored to fit with priorities when proactive resources are deployed.

Data quality assurance will help to remove the possibility of substandard intelligence products being developed on the basis of poor information collection and recording.

ELEMENT 7 – RESEARCH AND DEVELOPMENT

82. ACCESS TO TECHNICAL SUPPORT/SURVEILLANCE EQUIPMENT

The means with which to support the intelligence-led policing process through technical support and surveillance must be available at all levels of policing.

Meeting the Criteria

There must be access to technical support and surveillance equipment at all levels of policing. BCUs may hold and deploy equipment through their own dedicated technical field capability or force TSU. Level 2 and 3 deployments will invariably be through dedicated covert resources or TSU departments. Access to specialist resources and equipment for all levels will be through agreed authorisation and tasking processes.

83. NATIONAL TECHNICAL SUPPORT UNIT GUIDANCE USED AS A MINIMUM STANDARD (YELLOW BOOK)

National standards for the procurement, deployment, training and authority processes for technical support are defined in a CD published by the former PSDB known as *The Yellow Book* and in *ACPO (2004) Deployment Standards for Technical Support in Tackling Volume Crime.*

Meeting the Criteria

Evidence of compliance with the above standards in the purchase of HOSDB approved equipment, training of operatives and adherence to deployment protocols must be evident. Force TSU managers should ensure that there is access to the appropriate standards manual and that procurement rules are in place to prevent the local purchasing of inappropriate equipment.

84. OTHER STANDARD PRODUCTS

In addition to the defined standard intelligence products, a corporate approach should be taken in the development of processes and documentation for all other intelligence functions.

Meeting the Criteria

Standard processes and documentation for the intelligence function should be corporately agreed and recorded with regard to such issues as the intelligence unit, terms of reference, source tasking, data search, surveillance, prison intelligence, other covert operations, multi/other agency product, CCTV/ANPR and risk assessments, together with the four intelligence products.

85. STANDARDS FOR DELIVERY OF PRODUCT/SERVICES

SLA provide expected standards of service delivery between departments, organisations or for individual operations, for example, between an intelligence manager and an SIO when the intelligence function is in operation during a major crime investigation.

Meeting the Criteria

A policy must be established to convey force minimum SLA requirements.

86. MOU/INFORMATION EXCHANGE PROTOCOLS

Similarly, an MOU should be developed to set out protocols between departments, agencies and organisations enabling effective joint working or partnership arrangements.

Meeting the Criteria

Protocols should be established to determine parameters within which research may be conducted or data secured to enable competent research to be undertaken for recommendations for resolutions to be made. Adherence to such protocols must be evidenced.

See *ACPO (forthcoming) Guidance on the Management of Police Information.*

87. INTELLIGENCE SPECIALIST, RESEARCH AND ANALYTICAL CAPABILITY TRAINED TO NATIONAL STANDARDS

Sufficient numbers of well trained intelligence specialists are necessary to carry forward the business of a BCU or force.

Meeting the Criteria

BCU and forces, however limited their establishment of staff, must have access to sufficient numbers of trained intelligence specialists capable of meeting T&CG demands. National Specialist Law Enforcement Centre (NSLEC) training products or any products identified through National Learning Requirement research should be used. Staff must meet the levels of competency required by the Skills for Justice National Occupational Standards, see 4 People Assets.

88. SYSTEM FOR DEVELOPMENT AND REVIEW OF INTELLIGENCE COLLECTION PLANS

Processes should be in place which allow for the development and review of intelligence collection plans in line with the requirements of the T&CG and a method of reporting such actions.

Meeting the Criteria

Reviewing the progress of intelligence collection plans against tactical T&CG actions, refinement and recommendations are to be reported in the tactical assessment. Local systems enabling this standard to be achieved will be evident and reported in T&CG policy.

89. DATA COLLECTION DIRECTED AND FOCUSED ON CONTROL STRATEGY

The control strategy provides a focus for policing activity.

Meeting the Criteria

Police forces and BCUs should be able to demonstrate that the tasking for information and data collection is focused on their respective control strategies. Exceptions to this standard can be considered where directed by the T&CG or SIO with authority during a major reactive enquiry. A policy determining the intelligence research and development capability for a murder enquiry is highly recommended.

See also 6 Intelligence/Information Recording and *ACPO (2000) MIRSAP Major Incident Room Standardised Administrative Procedures Manual (forthcoming November 2005).*

90. DEVELOPMENT AND REVIEW OF INTELLIGENCE TRIGGER PLANS

The production of trigger plans used to alert tactical resources to notifiable incidents and to specify response actions, is recognised as good practice.

Meeting the Criteria

A system must be in place to alert tactical resources to respond to a specified set of circumstances using tried and tested methods. Methods adopted should be available from good practice which has been committed to an organisational memory process.

91. ACCESS TO OTHER AGENCIES' TECHNICAL RESOURCES AND EXPERTISE

Access to technical resources and expertise held by other agencies will provide a valuable additional capability to gather intelligence and evidence.

Meeting the Criteria

This may include databases, CCTV systems and specialist highways, environmental health and licensing officers (see also 2 System Assets).

92. ALIGN JOINT INTELLIGENCE CELLS TO FORCE INTELLIGENCE PROCESS

Joint Intelligence Cells, as described in 4 People Assets, must follow all of the same principles and practices as defined for the force intelligence process.

Meeting the Criteria

Policies and protocols must be in place which define common and corporate processes for Joint Intelligence Cells aligned to the force intelligence model.

93. TASKING CAPABILITY OF WIDER INTELLIGENCE ASSETS

All available resources, both internally and externally, should be used to gather intelligence and be subject to the tasking process.

Meeting the Criteria

Tasking processes should be in place for the wider policing community including PCSOs, Special Constabulary, local authority park rangers, street wardens, NHW, shop watch and river watch. A directory of assets should be recorded and available to staff during intelligence research.

94. IMPACT AND BENEFIT ASSESSMENT

Any authorised intelligence collection and tasking will need to be assessed for its impact and benefits against the overall tactical and strategic direction of the BCU and/or force.

Meeting the Criteria

Local forces and BCUs should consider the use of community impact assessments within the risk assessment process. Operational costs and effective communication and briefing and similar processes need to be subject to analysis and not just identified through a tactical review.

95. DEVELOPMENT OF ENHANCED TARGET AND PROBLEM PROFILES

Intelligence products, such as target and problem profiles must be subject to continual enhancement and development.

Meeting the Criteria

Police forces and BCUs must evidence the use and development of corporate target and problem profile templates. Systems capable of being scanned for crime and incident problems should be in place. Analysis is to include hypothesis on causation and recommendations for resolution.

IMPACTS AND BENEFITS

The impacts and benefits of meeting all of the minimum standards for research and development are outlined below.

Effective Research and Development

An efficient intelligence unit will be able to provide detailed research into authorised targets and problems using the suggested intelligence collection model. This will lead to the development of high quality intelligence products.

Access to all available intelligence collection techniques, including surveillance, technical observation, telecommunications analysis and forensic computer expertise will aid this research and may reduce time spent on target file development.

First class intelligence products will inform decision making and reduce both risk and investigation costs.

The creation of systems and processes which allow for the review of collection plans and which ensure data collection remains focused on control strategy priorities, will permit a more comprehensive and detailed level of analysis and product delivery according to need.

Corporate Standards

Ensuring that intelligence unit functions and documentation are conducted to a corporate standard will enable effective communication between command and analysis and with neighbouring BCUs and forces. This process can be supported by the existence of SLAs and MOUs, particularly when exchanging information between agencies.

A corporate response to specific circumstances through the development of intelligence trigger plans will assist the T&CG function. When linked to an organisational memory process, there will be improvements in harnessing and promulgating best practice. This, in turn, will inform policy review.

Co-ordination of the procurement of technical equipment and technology through Force TSU Managers, with adherence to national standards, will prevent unnecessary cost, duplication of purchases and potential health and safety issues. Equipment can also be more effectively assessed and evaluated.

Skills and Training

The benefits of having skilled and trained staff within the intelligence unit structure will be borne out by the delivery of high quality, well researched products, in which command teams can have confidence.

National training products, while still under development, are available through Centrex, NSLEC and various forces and should be adopted by all intelligence units.

A resource formula ensuring establishment levels are maintained will enable more effective planning to meet priority research needs.

For further information see 4 People Assets and *ACPO (forthcoming) Practice Advice on Resources and the People Assets of NIM.*

The Wider Intelligence Community

Closer links between the Police Service and external partners will provide a wider variety of information and intelligence sources.

Many external agencies have access to technical resources, data and expertise which are of value in intelligence collection.

The extended police family of PCSOs, wardens, rangers, traffic wardens, parish special constables, together with volunteer organisations, such as neighbourhood and farm watch are an invaluable source of information. When included in tasking and collection planning the intelligence capability is greatly enhanced.

Permanent Joint Intelligence Units, combining police, customs, immigration and other agencies are established in many forces. Experience has shown that where processes which are common to NIM standards are developed, such units function without difficulty.

ELEMENT 8 – INTELLIGENCE PRODUCTS

96. FORCE POLICY DICTATING CORPORATE STANDARDS OF PRODUCTS

The defined intelligence products must follow nationally recognised templates.

Meeting the Criteria

The standards adopted must reflect NIM operational standard templates for the four intelligence products. For further information see *ACPO (forthcoming) Practice Advice on Tasking and Co-ordination.*

97. FORCE POLICY DICTATING TIMING AND CIRCULATION OF PRODUCTS

The content and timing of the delivery of strategic and tactical assessments must be synchronised at local, force, regional and national level. A corporate circulation policy is necessary to ensure the appropriate audience for the respective product is reached.

Meeting the Criteria

Police force and BCU policies setting out the corporate standards for content reflecting national guidance, timescales and circulation of the intelligence products must be developed in line with ACPO NIM minimum standards. Timing must reflect local, force and regional needs. Business planning cycles will be a significant driver of delivery timings. Confidentiality must be considered and compliance with GPMS must be evident.

98. FORCE POLICING/BUSINESS PLAN INFORMED BY INTELLIGENCE PRODUCTS

Strategic assessments at all levels must inform the policing and business planning processes of a force and BCU.

Meeting the Criteria

Strategic assessments must be used in the business planning process and should be available for chief officer consultation with police authorities to enable issues of resource applications to be addressed, and for BCU commanders during CDRP consultation phases.

99. STRATEGIC ASSESSMENTS

Strategic assessments are vital to the functioning of NIM.

Meeting the Criteria

Strategic assessments must reflect NIM templates and be reported as a minimum at BCU, force and regional levels. Strategic assessments must be used by the strategic T&CG to agree control strategies and intelligence requirements.

100. TACTICAL ASSESSMENTS

Tactical assessments enable effective targeting, tasking and co-ordination based on information that has been provenanced through an analytical process.

Meeting the Criteria

Tactical assessments should reflect NIM templates and be reported as a minimum at BCU, force and regional levels. They should identify priority locations, subjects, crime and incident series and high risk issues in accordance with the control strategy and, in turn, recommend tactical options for prevention, intelligence and enforcement, and suggest potential communications strategies.

101. TARGET/PROBLEM PROFILES ONLY COMMISSIONED BY T&CG, INTELLIGENCE MANAGER OR SIO IN MAJOR ENQUIRY

Target and problem profiles create greater clarity and definition around the respective issues of priority, prolific and recidivist offenders or those suspected of more serious crime and priority locations or crime types. These profiles are as relevant to neighbourhood policing issues, such as problem families or locations, as they are to serious and organised crime groups.

Target and problem profiles should, in the main, relate to the control strategy and stated intelligence requirement. In some circumstances the commission of a serious crime, major crime investigation, issues of community concern or identified signal crimes, fall outside of the control strategy remit. In these cases a corporate line of authority for commissioning must be adopted. See *ACPO (2005) Practice Advice on Professionalising the Business of Neighbourhood Policing (Draft).*

Meeting the Criteria

These profiles must reflect NIM templates. They will be commissioned by tactical T&CGs to determine tactical resolutions; strategic T&CGs to assist with greater definition prior to setting the control strategy; an intelligence manager, in exceptional circumstances, for limited profiling to aid research in accordance with the control strategy, and a SIO in a major or serious crime enquiry to aid the investigation.

In all cases a common approach to commissioning must be undertaken. Profiles should be self-explanatory and evidenced by debate with the T&CG chair or SIO and analyst. Detailed documents are only necessary in order to delve in depth to a problem or people to aid resolution.

102. APPLYING THE ANALYTICAL PRODUCTS AND TECHNIQUES

All intelligence products must be subject to a wide range of analytical products and techniques. For further information contact the National Analyst Working Group (details in Appendix 6) and see *ACPO (forthcoming) Practice Advice on Tasking and Co-ordination.*

Meeting the Criteria

Analytical techniques and products (listed in 7 Research, Development and Analysis) must be used effectively to develop the intelligence products. An appropriate gateway must be established for tasking analysts via the T&CG and/or the intelligence manager. This will ensure the analyst's product is focused on the intelligence requirement and control strategy and is not used solely for administrative purposes such as performance management. A hypothesis on causation and recommendations for resolution will be included in the intelligence products.

103. MANAGEMENT OWNERSHIP

Chief officers, BCU commanders and senior intelligence managers are responsible for the ownership of intelligence products.

Meeting the Criteria

Directors of intelligence and BCU intelligence managers are responsible for the delivery of intelligence products and corporate publications. Final approval of the relevant strategic assessments must be given by chief officers and BCU commanders.

It must not be left to the analyst to compile intelligence products. Senior managers must be given responsibility for different aspects of the products and must ensure the delivery of the necessary information and data to the analyst as determined in policy standards. Available NIM Assets must be used to determine qualified recommendations.

104. PRE-CIRCULATION AND READING OF PRODUCTS PRE-T&CG

The speed and efficiency of the T&CG process is assisted by pre-reading of assessments by attendees.

Meeting the Criteria

Police forces and BCUs must make assessments available in a timely manner, allowing pre-meeting reading time for attendees.

105. ANALYST AS A STANDING MEMBER AT T&CG

The role of the analyst and analytical products are a fundamental part of NIM. An analyst is a key member of the T&CG process. Analysts will provide interpretation of the analysis within the intelligence products that drive the T&CG process.

Meeting the Criteria

Police forces and BCUs must ensure that an analyst is present at all T&CG meetings in order that a qualified interpretation of the analysis can be given and is used in the development of intelligence products.

106. INTELLIGENCE ASSESSMENT FLOWS

The two-way flow of an intelligence assessment between community level and national level via BCUs, force, regions and national organisations is critical to the success of intelligence-led policing.

Meeting the Criteria

BCU assessments must inform the force assessments which, in turn, will inform the regional assessments and United Kingdom Threat Analysis (UKTA) via NCIS. The process must also be reciprocal and operate at both strategic and tactical levels. This will not be simple aggregation but will be used, in association with other intelligence, to inform the process, in order to determine priorities. Timelines for reporting must be set in policy and met.

107. INTELLIGENCE EXCHANGE

The exchange of intelligence across all boundaries is particularly relevant to target profiles relating to the travelling criminal or in identifying noteworthy trends or themes.

Meeting the Criteria

IT systems must be in place for sharing intelligence products and T&CG outcomes with neighbouring BCUs, forces and regions. This should also include processes for receiving feedback.

108. OPERATIONAL INTELLIGENCE ASSESSMENT

Operational intelligence assessments are key to remaining focused during agreed T&CG tasking. For further information see *ACPO (forthcoming) Practice Advice on Tasking and Co-ordination.*

Meeting the Criteria

An operational intelligence assessment must take place to ensure that investigations remain focused in order to:

- Prevent mission creep;
- Identify priorities for the operation's intelligence effort;
- Focus intelligence gathering;
- Inform resource decisions;
- Guide investigative activities;
- Verify that protocols, such as the correct authorisations, are present;
- Highlight diversification from agreed objectives;
- Aid compliance with HRA, RIPA and other legislation.

109. COMMAND TRAINING/APPRECIATION PROGRAMME RELATIVE TO INTELLIGENCE PRODUCTS AND ANALYSTS

Commanders and intelligence managers must fully understand intelligence products and the analytical process.

Meeting the Criteria

A full understanding within command of the analytical role and intelligence products is essential. National, regional or local appreciation programmes relating to intelligence products and analysis are necessary and must be in place. Training packages must reflect the minimum standards listed in this manual.

IMPACTS AND BENEFITS

The impacts and benefits of meeting all of the minimum standards related to the intelligence products element of NIM are outlined below.

Intelligence Products – Standard Format and Delivery

The compilation of standard intelligence products and the appropriate use of archiving will allow the inclusion of standard formats to improve compliance with legislative requirements such as HRA, DPA, RIPA and Freedom of Information Act 2000.

The inclusion of human rights obligations in respect of proportionality and justification.

Corporate civil liability will be reduced by having justification in place for operational targeting.

Strategic and Tactical Assessments

Strategic assessment products create the ability to engage with policy makers regarding business priorities from a scientific, knowledge-based position. Resource and performance issues, when aligned with regional and national processes, can be tied to control strategy priorities.

New and emerging trends or threats outside the control strategy can be identified by the tactical assessment and then fed back into the strategic assessment.

Applying standard analytical products can provide more timely and accurate identification of priority locations and the ability to respond more effectively to emerging issues and series crime and incidents.

Target and Problem Profiles

High quality profiling can reduce the criminal justice attrition rate and reduce priority and prolific offending through targeting the correctly identified offenders and problems.

Sharing profiles with neighbouring BCUs and forces will lead to better targeting of travelling criminals that do not respect artificial BCU and force boundaries.

Operational Intelligence Review

Continual operational review and results analysis can be used by command to aid performance measurement and to develop an organisational memory capability.

Training

As with all areas of NIM, the provision of training products to ensure a full understanding of the available analytical techniques and intelligence product development, will enhance the force and BCU capability.

ELEMENT 9 – STRATEGIC AND TACTICAL TASKING & CO-ORDINATION

110. T&CG POLICY

Tasking and co-ordination is essential to the NIM process and requires policy to be developed by forces.

Meeting the Criteria

T&CG policy should detail the key attendees, products and timescales in line with national standards and good practice, reinforcing use of national minimum standards for strategic and tactical assessments and use as a core decision making document by command teams.

NIM is not purely focused on crime. Strategic and tactical assessments which have been created using community intelligence as an information source are likely to indicate issues of disorder and social decay as being important areas for local police to take action. This will clearly change the likely direction of decision making at the T&CG meeting.

111. CONSISTENCY IN T&CG MEETINGS THROUGHOUT THE FORCE

Co-ordination of T&CG processes to ensure consistent activity will improve intelligence flows and assessments.

Meeting the Criteria

Local tasking and co-ordination groups must be arranged consistently to time with the rest of the force and take account of the regional and national picture. Compliance will enable a greater use of intelligence products to inform others and to assist in the collaboration with, and tasking of, external resources.

112. CHAIRPERSONS

Meeting the Criteria

See standard 44 T&CG Chairs

113. ENGAGEMENT OF STAKEHOLDERS IN THE STRATEGIC T&CG PROCESS

Stakeholders and partner agencies play a key role in informing the strategic assessment and influencing strategic tasking and co-ordination processes.

Meeting the Criteria

Police forces and BCUs should evidence the involvement of stakeholders in the strategic process. This may include Police Service or Police Authority representatives at force level, and the chief executive and other key CDRP, Local Safety Partnership Team and/or Drugs Action Team (DAT) representatives at BCU level.

114. INSPECTION

NIM tasking and co-ordination processes require regulation and inspection, in order to maintain standards.

Meeting the Criteria

Police forces must develop a thematic inspection template to assess the effectiveness of T&CG action setting. This must centre on the use of the control strategy and outputs linked to operational performance and reporting at performance reviews.

115. STRATEGIC ASSESSMENT

Strategic assessments must be compiled in accordance with minimum standards.

Meeting the Criteria

Police forces and BCUs must evidence commission and use of strategic assessments as a core decision making document. The assessments will adhere to the national template. The assessment is to be used in business planning processes to enable the setting of force and local priorities as reported in the control strategy. This will also enable resource, funding and communication strategies to be set.

116. TACTICAL ASSESSMENT

Tactical assessments must be compiled in accordance with minimum standards.

Meeting the Criteria

Police forces and BCUs must evidence the commission and use of tactical assessments as a core decision making document. The assessments must adhere to the national template and recommend actions from the menu of tactical options. These options must be adopted in accordance with the control strategy. Target and problem profiles may also be commissioned to aid definition of a problem raised, see 8 Intelligence Products. The tactical assessment will review and amend intelligence requirements according to force needs. It must, however, take account of force control strategy priorities and report on them as necessary.

117. REGIONAL ST&CG AND TT&CG

Tasking and co-ordination must continue into the regional arena to ensure the effective targeting of criminality at levels 2 and 3.

Meeting the Criteria

Police forces must demonstrate active participation in regional ST&CG and TT&CG, in adherence to the ACPO approved protocols.

118. ATTENDEES AT ST&CG AND TT&CG

Key personnel and role functions must attend ST&CG and TT&CG.

Meeting the Criteria

ST&CG should include relevant representation from operations, traffic, crime management, community safety, intelligence analysts and partners. Attendance criteria must be set down in local T&CG policy.

TT&CG may include representation from all departments. Attendance need not be rank specific, however, and attendees should have the authority over task-able resources. Attendees may include partner agencies, CDRP representation and the Probation Service. Security of information and assets, however, must be taken into consideration.

119. SANCTION OF THE CONTROL STRATEGY

ST&CGs must sanction the control strategy.

Meeting the Criteria

Priority issues for prevention, intelligence and enforcement must be identified in the control strategy. The professional heads of the respective disciplines should be consulted and play an active role in ensuring accurate and informed strategies are set.

120. SANCTION OF THE INTELLIGENCE REQUIREMENT

ST&CGs must sanction the intelligence requirement.

Meeting the Criteria

ST&CG provides the principle sanction of a requirement on all staff to secure intelligence to fill intelligence and knowledge gaps in line with the control strategy. This requirement must be reviewed and amended according to need, by the TT&CG.

121. MINIMUM 6-MONTHLY REVIEW OF ST&CG

The setting of strategic direction requires review to ensure that the appropriate policing focus is maintained.

Meeting the Criteria

The ST&CG must sit every 6 months with the minimum of a paper review at 3 monthly intervals. The meetings must review the control strategy and amend this as necessary, taking into account performance, effectiveness of the strategies set, emerging threats, and trends and resource capability.

122. BRIEFING POLICY

The actions set in accordance with the tactical menu must be delivered to the patrol and investigative function through effective briefing.

Meeting the Criteria

Minimum standards for briefing must be adopted, including strategies and effective delivery mechanisms, see *ACPO (forthcoming) Guidance on the National Briefing Model.*

123. DAILY MANAGEMENT MEETING/BRIEFINGS AND LAG – BCU

Daily management meetings, briefings and LAG meetings **are not a T&CG meeting** as they are not driven by the intelligence products review. These informal tasking meetings may use remote conferencing facilities due to the geography of a BCU.

Meeting the Criteria

Daily meetings should be chaired by a local commander or their deputy and reinforce and maintain the focus of TT&CG decisions. Briefings should be conducted by the appropriate operational lead and inform designated teams of their tasking requirement while LAGs should be chaired in accordance with partnership arrangements and inform the T&CG process.

124. LEVEL 2 RESOURCE ALLOCATION CRITERIA

The allocation of finite level 2 resources should be governed by set protocols.

Meeting the Criteria

There should be a transparent policy and decision-making process in place for the application and allocation of level 2 resources primarily in support of priority issues reported in the force control strategy or in support of major investigations. BCU command representation at either level 2 T&CG or resource forum is highly recommended.

IMPACTS AND BENEFITS

The impacts and benefits of meeting all of the minimum standards related to both the strategic and tactical tasking and co-ordination elements of NIM are outlined below.

Strategic Direction

Effective ST&CG processes which use well-defined intelligence products will create a better informed Police Service with a greater understanding of the risks to performance and efficient service delivery. Informed strategic direction will lead to improved planning processes.

The adoption of minimum standards for ST&CG will focus operational strategies on key priorities, CHIS recruitment according to need, forensic resources to locations, and people and patrols to hot spots and priority locations.

The ST&CG maintains the currency of control strategies and allows flexibility to include emerging trends or issues. Well-informed strategic direction will enable and drive data sharing requirements for common and justifiable aims.

Tactical Delivery

Compliance with TT&CG minimum standards and disciplines will lead to more officers being focused on targeting the most active criminals, patrolling locations of the highest priority and collecting intelligence on key needs.

Maintaining focus through strong co-ordination will ensure operations are only commissioned where necessary. The consequential improvement in planning will lead to greater officer safety and more effective deployment of resources.

Tasking forums provide a platform for better organisational communication, briefing and feedback of information.

Partnership Integration

Tasking processes, particularly at the strategic level, should include full integration with partnership arrangements. Involvement of local politicians in ST&CG will ensure overview and understanding of operational and resource conflicts.

Improved integration in the tasking and co-ordination process with partner agencies, ie, DATs/drug reference groups, youth crime offender teams and other local authority bodies will enhance action setting linked to partnership development and joint ownership.

Partnership involvement will assist with the development of reassurance programmes by engaging partners through the application of the tactical menu.

The adoption of these minimum standards reinforces the principles of the CDA.

Performance

Effective tasking regimes, creating high quality targeting processes will lead to improved quality of prosecution case files and the reduction in, and increased conviction rates for, recidivist offenders.

Results analysis used by command to aid performance review and develop organisational memory will create greater understanding of resource capabilities. This will enable forces and BCUs to link T&CG decisions and outputs to performance.

Robust tasking and targeting sanction will provide auditable processes leading to improved legislative compliance, for example, HRA and greater public satisfaction. Inspection regimes will maintain standards.

National Perspective

Ensuring the full integration of tasking and co-ordination and delivery of strategic assessments at local, force, regional and national level, will enable government to produce informed priorities through the National Threat Assessment.

The implementation of level 2 tasking policies will also lead to greater effectiveness in managing cross-border criminality between BCUs and forces.

ELEMENT 10 – TACTICAL RESOLUTION

125. INVESTIGATIVE CAPABILITY

A dedicated tactical investigations team is necessary to ensure effective resolution of core priorities.

Meeting the Criteria

There must be evidence of a tactical investigative capability able to meet the tasking requirements of TT&CG, both at force and BCU level. Establishment numbers of such teams is not prescribed but staff must be trained to a high level of investigative skills.

126. RED CIRCLE POLICY

Intelligence staff members need to be dedicated to fulfilling T&CG actions and to retaining the profile of control strategy priorities. In addition specialist intelligence roles must retain a position of covertness.

Meeting the Criteria

Policy must be implemented which prevents the use of intelligence staff for other functions unless very exceptional circumstances dictate. This policy will include analysts, intelligence management, briefing and co-ordination and those in covert roles, ie, CHIS handling, surveillance and TSU.

127. TACTICAL CAPABILITY

T&CGs must be aware of available tactical capability to ensure there is a balance of work and tasking in accordance with the tactical menu.

Meeting the Criteria

Police forces and BCUs must evidence the following capabilities as being present:

- Sufficient tactical and operational capability to respond to fast time intelligence and tactical resolution through a fast track process;
- A high visibility patrol capability and general policing or sector options;
- Access to covert resources, ie, surveillance, test purchase and undercover;
- Tactical traffic management options;
- Mutual aid agreements with neighbouring BCUs and forces on a regional or national level through force and regional T&CG structures;
- Capability to provide operational response to ANPR operations;
- Crime reduction/prevention resources to assess and review reduction and prevention opportunities.

128. TACTICAL PLANS

Tactical plans must be developed by owners appointed and tasked by the TT&CG.

Meeting the Criteria

Tactical plans must accord with the tactical menu and control strategy priorities. Inspection will evidence compliance as recorded in TT&CG minutes and action setting. Copies of plans developed in a corporate style must be retained in force organisational memory systems.

129. TRIGGER PLANS

Trigger plans allow for instant, controlled and co-ordinated response to particular events, incidents or crime types.

Meeting the Criteria

Trigger plans must be in place to direct response capability to undertake certain tasks on the occasion of a particular event or circumstance occurring.

IMPACTS AND BENEFITS

The impacts and benefits of meeting all of the minimum standards related to the tactical resolution element of NIM are outlined below.

Response

The use of T&CG will create a co-ordinated response inclusive of all resources available within the organisation, as well as providing access to the resources of other agencies. The ability to make faster and more accurate decisions, guided by the control strategy and intelligence requirement, will mean that forces can make a more timely response to operational problems or targets at all levels of operation. This will also lead to the earlier arrest of offenders.

Professional Investigation

Implementation of the minimum standards for tactical resolution will lead to dedicated tactical investigation teams. These dedicated teams will lead to better performance in terms of improved evidential standards, reduced attrition rates and increases in the detection rate. The direction offered through T&CG will enable forces to focus on gaining the best evidence of worst offences to help secure more convictions. This should, in turn, have a qualitative impact throughout the criminal justice system.

ELEMENT 11 – INTELLIGENCE/OPERATIONAL REVIEW

130. RESULTS ANALYSIS AND REVIEW

Results analysis is an analytical technique which can be used to inform the NIM process. It should be used to assess the success of actions endorsed by the T&CG.

Meeting the Criteria

T&CG commissioning of results analysis and operational review must be evidenced. Recommendations must be reflected in tactical assessments and operational plans and the organisational memory updated. This is particularly necessary when using technology or after a failed operation.

131. MONITOR AND REVIEW OF RIPA AUTHORITIES

The usefulness of information gained as a result of RIPA authorities will also require review, and policies will need to be in place to guide this process.

Meeting the Criteria

Forces must undertake a proactive review of RIPA authorities and ensure that the retention policy is adhered to. This is usually a function of the person or team with responsibility for the management of authorities, see standard 46 Authorities Management. Intelligence gained under an authority is usually located elsewhere (see standard 38 Surveillance Product) but will be subject to assessment and input on to the intelligence function as required.

132. NATIONAL BRIEFING MODEL

The ability to brief and debrief effectively is critical to the success of intelligence-led policing. The essence of NIM is to tailor the response to the problem in hand. This is inherently difficult to achieve if officers are not briefed as to what and where the problem is. Conversely, it is difficult to identify and address problems with any degree of success if debriefing systems are ineffective. In order to maximise the usefulness of harvested intelligence, effective briefings and debriefings are essential. See also *ACPO (forthcoming) Guidance on the National Briefing Model.*

Meeting the Criteria

A standardised and structured briefing/debriefing process, using the National Briefing Model, must be implemented. This will ensure the effective tasking and briefing of the patrol function and enable assessment of intelligence product accuracy and timeliness and also allows gap analysis to improve the product.

133. ORGANISATIONAL MEMORY

The evaluation of the outcomes and processes of operations should be fed into corporate knowledge. This will improve the expertise of staff involved and lead to the improved effectiveness of future operations.

Meeting the Criteria

Operation logs, operational reviews and case histories should all be examined. The results and analysis of this examination must be added to the organisational memory through the NIM process and in line with control strategy objectives or emerging high risk issues.

134. AUDIT TRAIL

A system for monitoring and reviewing tactical decisions, operational plans and results ensures that operational and intelligence tasking is compliant with the HRA. It also provides an audit trail for subsequent scrutiny.

Meeting the Criteria

Police forces must have in place systems for recording, monitoring and reviewing tactical decisions, operational plans and results to ensure that operational and intelligence tasking is compliant with the HRA. The subsequent audit trail will then be suitable for later scrutiny by third parties.

135. COMMUNITY IMPACT ASSESSMENT REVIEW

In order to fully assess the impact and success of operations it is necessary to consult with partner agencies and the wider community. This is especially important where operations are in response to locally identified problems.

Meeting the Criteria

There should be evidence of the use of community impact assessments as part of the results analysis. This will include such questions as:

- Was activity implemented as planned?
- Did the problem change after activity?
- Why was this?
- Did activity cause displacement?
- Did new offenders move in?

This will evidence that forces have worked with partners to establish the impact on the community of actions implemented.

IMPACTS AND BENEFITS

The impacts and benefits of meeting all of the minimum standards related to the intelligence/operational review element of NIM are outlined below.

Better Learning and Development Opportunities

The evaluation aspects of operational review within NIM will mean that the relevant skills needed by police staff will be identified at an early stage. This knowledge will then inform the decision-making process for the distribution of human resources within NIM. Such evaluation will also allow for the identification of knowledge gaps for individual staff or groups of staff, allowing focused and relevant training programmes to be developed. The conduct of an operational review gives the opportunity to recognise good work. Positive feedback within the organisation will improve motivation and engender more thought and attention being given to the production of intelligence reports, and errors being corrected quickly and easily. Effective review also avoids the situation where the same mistakes are repeatedly made, improving the organisational memory, processes and performance.

Increased Availability of Good Practice

The implementation of an operational review process will lead to improved arrangements for harnessing, assisting and promulgating good practice. Appropriate and timely recording and dissemination of good practice will mean officers have ready access to corporate memory and a knowledge base. In this way the identification of good practice can be used to create better operational solutions and improve the formulation of operational policing policy. The increased availability of good practice increases learning ability, avoids duplication, reduces costs and subsequently improves operational effectiveness.

Improved Operational Effectiveness

The use of operational review creates an in-built audit trail of operational decision making and its results. It also leads to a more informed response to incidents. The learning that comes from the review process will lead to improved arrangements for exploiting scientific and technological advances to assist in reducing crime, and add further to improved operational effectiveness.

APPENDIX 3
DIRECTORY OF INFORMATION SOURCES

Numerous sources of information are available to the Police Service. This directory lists some of them.

Air Accident Investigation Branch (AAIB)
Part of the Department for Transport and responsible for the investigation of civil aircraft accidents and serious incidents within the UK.

Access
DPA (Data Protection Act 1998, primarily only necessary for the exchange of personnel information only)

Alarm/Security Companies
Commercial information regarding business, customers and incidents

Access
DPA
Common law – a general requirement to assist police with their enquiries

Antique Shops
Commercial information regarding business, customers and property

Access
DPA
Common law – a general requirement to assist police with their enquiries

Antiques Database
Commercial database of stolen antiques, intelligence exchange between insurance companies and loss adjuster investigators – see Art Loss Register.

Access
DPA
Common law – a general requirement to assist police with their enquiries

Area Child Protection Committees
Local authorities and Law Enforcement Agencies (LEA) inter-agency forums to deal with child protection issues, cases and referrals.

Access
DPA – protocol

Armed Forces
Intelligence exchange

Access
DPA – ACPO
MOU
Local points of contact

Arrest/Drug Referral Workers
Local authorities and LEA meeting may include charity or commercial partners – inter-agency forum or tactic for diversion of problematic drug users into treatment schemes. May come under Drugs Action Teams or CDRPs.

Access
DPA – protocol

Art Loss Register
Worldwide free service to police and law enforcement officers to assist with the identification and recovery of stolen arts, antiques and collectables (endorsed by the Home Office and ACPO).

Access
DPA
Common law – a general requirement to assist police with their enquiries

Anti-Social Behaviour Order (ASBO) Groups
Local authorities and LEA meeting, may include public and commercial, inter-agency forums to refer or deal with cases requiring an inter-agency response to deal with anti-social behaviour issues.

Access
DPA – CDRP protocol

Association of Foreign Banks and Securities Houses
Information exchange forum for foreign banks and securities houses with offices in London, operating in and out of the UK. Commercial interests of mutual benefit.

Access
DPA

Aviation Regulation Enforcement and Investigation Branch
Investigation of breaches of aviation legislation relating to UK aircraft anywhere in the world, and overseas aircraft operating within the UK.

Access
DPA

BADMAN (Behavioural Analysis Data Management Auto-indexing Network)
Rape database developed by Surrey Police of over 900 national (and some international) details of rape offences, coding offender behavioural patterns and crime characteristics. Developed as an offender profiling database, it represents a sample of all sexual offences dating back to 1973. Superseded by ViCLAS due to greater sample size. See ViCLAS and SCAS.

Access
Standard grounds and justification to search internal law enforcement database
NCPE Operations, contact SCAS on 01256 602305

Bail Hostels
Information regarding customers, may be provided by local authority or commercial enterprise

Access
DPA – local protocols

Banks
Commercial information regarding business and customers

Access
Authorised Financial Investigators – initial enquiries
DPA – production orders

BBC Security and Investigation Services
Liaison with Police Forces in respect of matters affecting BBC TV and Radio

Access
DPA
Common law – a general requirement to assist police with their enquiries

Breakdown Services (RAC/AA)
Commercial information regarding business and customers

Access
DPA
Common law – a general requirement to assist police with their enquiries

British Gas
Commercial information regarding business and customers

Access
DPA
Common law – a general requirement to assist police with their enquiries

British Transport Police
Non Home Office Civil Police Force – national police for the railways, policing the rail network, underground and Dockland light railway

Access
Home Office circular
DPA – ACPO protocols

British Vehicle Rental and Leasing Agency
Commercial information regarding business and customers

Access
DPA
Common law – a general requirement to assist police with their enquiries

BT Payphones Security Group
Responsible for dealing with or assisting with all aspects of payphone crime affecting BT (not for accessing telecommunications data – see Communication Providers).

Access
DPA
Common law – a general requirement to assist police with their enquiries

BT Security
Investigation of crime committed against BT and assisting police in respect of criminal matters affecting the company (not for accessing telecommunications data – see Communication Providers).

Access
DPA
Common law – a general requirement to assist police with their enquiries

Building Societies
Commercial information regarding business and customers

Access
Authorised Financial Investigators – initial enquiries
Production orders

Call Credit
Call Credit is a consumer credit reference agency (also see entries for Equifax, Experian and Dun & Bradstreet) that provides information on electoral roll, county court judgements, sequestration, decrees and trust deeds. It can share financial accounts supplied to them by lenders, utilities and debt collectors, and hold information on payments and status of accounts over the past six years. As well as information on previous searches conducted by all clients using the system to validate individuals over the past two years, there is also information on any linking addresses for the individual, and any names financially associated with that individual, ie, aliases.

Access
Commercial, searches recorded and may be disclosed to the subject. Confidential requests require DPA. Evidential requests may require production orders. Covert searches – surveillance authorities may be required – collection of personal data by covert means.

Car Dealers
Commercial information regarding business and customers

Access
DPA
Common law – a general requirement to assist police with their enquiries

Caravan Club
Commercial information regarding business and customers

Access
DPA
Common law – a general requirement to assist police with their enquiries

Cash in Transit Companies
Commercial information regarding business, customers and security incidents. Regional and national forums attended by Police Forces and primary cash carriers.

Access
DPA
Common law – a general requirement to assist police with their enquiries

CATCHEM (Centralised Analytical Team Collating Homicide Expertise and Management)
Database developed by Derbyshire Constabulary representing a distillation of facts from a comprehensive study of child sexually motivated murders and the persons who have committed them over the past 43 years. Contact SCAS for details on database custodian.

Access
Standard grounds and justification to search internal law enforcement database
NCPE Operations, contact SCAS on 01256 602305

Cautions
Force database

Access
Standard grounds and justification to search internal law enforcement database.

CCA (Comparative Case Analysis)
A PNC application developed in 1985 as a result of the Lawrence Byford report into the Yorkshire Ripper murders enquiry. Previously known as Crime Pattern Case Analysis (CPCA) and is used as a search tool into serious offences.

Access
Standard grounds and justification to search internal law enforcement database
PNC – national guidance

CCTV
Local authorities – maybe CDRP or joint police ventures

Access
DPA – protocol, Codes of Practice

Charity Commission Investigation Divisions
Investigation of charity abuse

Access
DPA

Chemists, Drug Registers
Force database – inspection of premises licensed for the storage of certain categories of controlled drugs and medicines.

Access
Standard grounds and justification to search internal law enforcement database

CIFAS
System for fraud prevention: member organisations to exchange details of applications believed to be fraudulent, usually where the applicant fails verification checks. Does not provide a credit reference database; only provides a fraud prevention service. Will assist in circulating personal suspect details to members for research purposes.

Access
DPA
Common law – a general requirement to assist police with their enquiries

Civil Nuclear Constabulary (CNC)
Formerly known as the UK Atomic Energy Authority Constabulary – non Home Office law enforcement agency intelligence exchange.

Access
ACPO – protocols
Home Office circular

Child Support Agency
Agency for administering estranged parents' payments.

Access
DPA – protocol

Child Welfare Forum
Local authorities and LEA meeting – inter-agency forum to share intelligence in cases of sexual exploitation of children.

Access
DPA – CDRP protocol

Civil Aviation Authority (CAA) Security Services
Responsible for information, personnel, physical security and counter terrorism, crime prevention and the investigation of criminal and security matters affecting the CAA.

Access
DPA

Communication Providers (telecommunications, postal and internet)
Commercial information regarding business and customers, including communication traffic.

Access
RIPA/ACPO Codes of Practice for SPOCs

Community Safety Partnerships – Crime and Disorder Partnerships, Local Responsible Authorities
Designated inter-agency forum identifying police and local authority, together with other key local and national organisations, for conducting local crime audits within their communities. Also co-ordinates activity to address community concerns and issues in respect of crime and disorder.

Access
DPA – CDRP protocol
See Home Office – Crime Reduction toolkits website:
http://www.crimereduction.gov.uk/infosharing_guide
Information sharing protocol templates

Companies House
Agency – national register of public limited companies and directorships:

- Current and former directorships etc of companies;
- Shareholders;
- Mortgages.

Access
DPA

Court Enforcement Officers
Court officers

Access
DPA – local arrangements

Covert Human Intelligence Sources (CHIS)
LEA – resource/tactic

Access
RIPA/ACPO Codes of Practice

Credit Reference Agencies
Commercial databases – see entries for Call Credit, Experian, Equifax and Dun & Bradstreet.

Access
DPA

Crime & Disorder Partnerships and Audits
See Community Safety Partnerships and Home Office – Crime Reduction toolkits website: http://www.crimereduction.gov.uk/infosharing_guide
Information sharing protocols guidance

Access
DPA – CDRP protocol

Crimestoppers
Charity supporting law enforcement

Access
DPA – CDRP protocol

Criminal Injuries Compensation Board
Agency

Access
DPA

Dedicated Cheque & Plastic Crime Unit
Investigation of cheque, ATM, identity theft, payment card fraud and counterfeiting of plastic cards where organised crime is involved.

Access
DPA – production orders
Authorised financial investigators – initial enquiries

DEFRA, Department for Environment, Food & Rural Affairs (MAFF, Ministry of Agriculture, Fisheries & Food)
Investigates fraud and irregularities affecting DEFRA.

Access
DPA

Department of Trade and Industry (DTI) – Legal Services Directorate
Criminal investigations and prosecution of offences of fraud, perjury, theft and breaches of Insolvency Act, Companies Act, Companies Directors Disqualification Act and Financial Services Act.

Access
DPA

Department for Transport – Security Division
Required to advise and inspect provisions for protection of airports, ports, British airlines worldwide and overseas airlines operating in UK, against terrorism and violence, under Aviation, Maritime and Channel Tunnel Security legislation. All incidents of violence against civil aviation, maritime and Channel Tunnel activities must be reported to DT – Transport Security Division.

Access
DPA

Dept for Work & Pensions (DWP)
Agency client records – date of birth, last known address, national insurance number and benefits received.

Access
DPA – ACPO MOU

Dept for Work & Pensions (Job Centre plus Counter Fraud Investigation Division)
Investigation of organised and systematic abuse of social security claims and payment systems.

Access
DPA – ACPO MOU

Divorce Court Welfare
Criminal Justice

Access
DPA

Domestic Violence Partnerships
Local authorities and LEA inter-agency forum to share intelligence and co-ordinate activity to deal with domestic violence – may be linked to local CDRP activity.

Access
DPA – CDRP protocol

Drugs Action Teams (DAT)
Inter-agency groups set up by the National Drugs Strategy to facilitate activity dealing with problematic drug use. In some areas now formally linked to or part of the CDRP networks.

Access
DPA – protocols for information sharing between members
See Home Office – Crime Reduction tool kit website:
http://www.crimereduction.gov.uk/infosharing_guide
Information sharing protocols guidance

Drug Related Incidents in Schools
Local authorities and LEA meeting which may include public and commercial

Access
DPA – CDRP protocol

Dun & Bradstreet
Commercial credit reference company – contains information regarding international registered companies and directors. See also Call Credit, Experian and Equifax.

Access
Commercial, searches recorded and may be disclosed to the subject. Confidential requests require DPA. Evidential requests may require production orders. Covert searches – surveillance authorities may be required – collection of personal data by covert means.

DVLA (Driver and Vehicle Licensing Agency)
Agency, vehicle registration and driver details and histories

Access
ACPO protocol and SPOC system

Electoral Register
Local authority database of registered voters – open source

Access
Open source

Elementary
NCIS intelligence database in respect of national targets of serious and organised crime.

Access
ACPO/NCIS
Intelligence search requests (DPA) – protocols

Embassies and High Commissions
Large embassies and High Commissions maintain police/law enforcement liaison capability

Access
DPA – possibly require Interpol

Environment Agency
National agency responsible for the protection of the environment (air, land and water) in England and Wales and is the enforcement and prosecuting agency in respect of:

- Discharges to controlled waters;
- Disposal and management of wastes;
- Major industrial processes;
- Management and disposal of radioactive substances.

Access
DPA – ACPO Environment Agency MOU

Europol/Interpol
Enquiries through NCIS, International Division

Access
DPA and other statutes, international protocols

EQUIFAX
Credit reference agency holding data relating to credit agreements, primarily provided by banks and other credit companies. Together with Experian and Call Credit, Equifax is recognised by the Data Protection Registrar for the purposes of collecting the electoral roll. A source for:

- Financial information and credit status;
- Names of financial associates;
- Address checking – list of every name linked to Equifax data for an address, current addresses and details of other addresses linked to an individual;
- Electoral roll data (for a given address dating back to 1983);
- County Court judgements;
- Telephone numbers and a list of all credit searches that have been carried out on a person, including identity verifications;
- Relevant information on fraud linked to a particular address and details on repossessions;
- Information on business proprietors (can cross-reference business registrations using address and telephone number data in addition to directors' names).

Also see Call Credit, Experian and Dun & Bradstreet.

Access
DPA. Forces can log on via the internet and submit an electronic declaration that the search is compliant with DPA. They can then search by individual or address. Evidential requests may require production orders.

EXPERIAN
Commercial database providing identification confirmation, credit reference and business information. Also insurance claims and HPI. Combined publicly held records with credit account details received from all major institutional lenders. Includes:

- Voters roll information;
- Information on individuals who have opted out of voters roll;
- Credit history checks (DPA request required);
- Related/previous addresses;
- HPI.

Also see Call Credit, Equifax and Dun & Bradstreet.

Access
Commercial, searches recorded and may be disclosed to the subject. Confidential requests require DPA. Evidential requests may require production orders. Covert searches – surveillance authorities may be required – collection of personal data by covert means.

Family Practitioners
NHS Agency – possibly CDRP or DAT involvement with LEA and crime and disorder audits.

Access
DPA – CDRP protocols

Federation against Copyright Theft Limited
Commercial – formed to combat illegal copying of films and TV product – will undertake private prosecutions under Copyright, Design & Patents Act and Video Recordings Act.

Access
DPA – ACPO/Industry MOU on Intellectual Property Right Offences
Common law – a general requirement to assist police with their enquiries

Financial Institutions
Commercial information regarding business and customers

Access
Authorised Financial Investigators – initial enquiries
Production orders

Financial Services Authority
Agency – central UK authority responsible for supervising financial service firms, banks and regulating investment business.

Access
DPA – protocols

Fingerprint Bureau
National Identification Service and Local Force databases, and unidentified crime scene lifts.

Access
Standard grounds and justification to search internal law enforcement database

Fire Brigade
Local authority agency

Access
DPA – CDRP protocols

Fire Investigation Unit
Local authority agency

Access
DPA – CDRP protocols

Firearms Dealers
Commercial information regarding business and customers

Access
DPA
Common law – a general requirement to assist police with their enquiries

Firearms Licensing
Force databases

Access
Standard grounds and justification to search internal law enforcement database

Firearms Registers
Force database. Currently being integrated into a National Firearms Licensing Management system – linked to PNC application national firearms register.

Access
Standard grounds and justification to search internal law enforcement database

Fixed Penalty Tickets
Force databases

Access
Standard grounds and justification to search internal law enforcement database

Food Standards Agency – Investigation Branch
Agency

Access
DPA

Forensic Medicine Database (previously at Guys Hospital)
See National Injuries Database

Access
NCPE Operations, Major Crime Helpdesk 01256 602443

Forensic Data
Forensic Science Service or other commercial provider

Access
Protocol/contract/MOU

Forensic Science Service (FSS)
Agency

Access
ACPO protocol/MOU

Gaming Board of Great Britain
Agency

Access
DPA – protocol

Gardia Siochana
Eire – police force

Access
DPA – protocol

General Dental Council
Professional body

Access
DPA

General Medical Council
Professional body

Access
DPA

Genesis – NCPE Operations Centre database of police publications
Secure repository for good practice and other operational policing information and manuals (not intelligence) available over the CJX.

Access
Genesis Help Desk 01256 602778
genesis@centrex.pnn.police.uk

Guernsey Police
Crown Dependency – LEA intelligence exchange

Access
DPA

Health & Safety Executive
Government agency (some LEA)

Access
National protocol – local agreements, procedures for dealing with work related deaths

Health Authorities
Agency – involvement with law enforcement as responsible authority in CDRPs and/or DATs.

Access
DPA – CDRP protocol

Hire Purchase Index
Commercial – now part of Experian. Details of hire purchase agreements involving motor vehicles.

Access
DPA – commercial access

Historic Data held by law enforcement agencies
Various force databases

Access
Standard grounds and justification to search internal law enforcement database

HM Coastguard
Agency

Access
DPA – local agreement
Maybe CDRP

HM Immigration Service
LEA exchange of intelligence

Access
ACPO Manual of Standards protocol/MOU
Immigration and Asylum Act 1999 (sect 20-21)

HMRC (Her Majesty's Revenue & Customs)
Amalgamation of HMCE (Customs & Excise) and Inland Revenue. LEA exchange of intelligence derived from enforcement activity – tax, duty and VAT collection. Including movement of people and vehicles at port. Register of VAT registered businesses. Also information relating to:

- Individual and companies, declared tax;
- PAYE details of employers and employees;
- Tax charges and payments;
- Third party information.

Personal information includes: name, address, date of birth, national insurance number, employment history, salary, trading profits and other taxable income sources.

Access
DPA – protocols
ACPO protocol (APOC)
ACPO MOU – SPOC arrangements

HOLMES2 (Home Office Large Major Enquiry System)
Force database – computer system for Major Incidents (SCAS document management system).

Access
Standard grounds and justification to search internal law enforcement database

HORT1 (Home Office Traffic Report 1)
Force database containing information resulting from traffic stops

Access
Standard grounds and justification to search internal law enforcement database

Hospitals
See Health Authorities

Access
DPA – national protocols, part of CDRP protocols

Hotels
Commercial information regarding business and customers

Access
DPA
Common law – a general requirement to assist police with their enquiries

Housing Associations
See the housing landlord – local authority or commercial

Access
DPA – CRDP protocols

Housing Departments
Local Authority

Access
National protocol
DPA – CDRP protocols
Local MOUs

Information Commissioners (Data Protection)
Notifications, assessments and investigation of alleged breaches of Data Protection legislation and Freedom of Information Act 2000.

Access
DPA

Intelligence Practitioners Liaison Group
Local authorities and LEA meeting – pre CDRP information exchange groups organised locally, regionally and nationally.

Access
Agencies to outline information held, how to access it and develop points of contact

Internet – open source
Security and compromise issues regarding the use of equipment identifiable as law enforcement, or from computers used to store other law enforcement data and material. World Wide Web addresses that provide details of crime, deprivation, population and similar in an area, for example:
http://www.homecheck.co.uk
http://www.upmystreet.co.uk
http://www.homeoffice.gov.uk

Access
Some cities are password protected
Other issues such as requiring RIPA authority if done covertly

Isle of Man Constabulary
Crown dependency – LEA intelligence exchange

Access
DPA

Jersey Police
Crown dependency – LEA intelligence exchange

Access
DPA

Key Holders
Force database

Access
Standard grounds and justification to search internal law enforcement database

Land Registry
Government registry:

- Property ownership and purchases;
- Mortgages taken out on the property with lender's details;
- Previous property purchases.

Access
DPA – payment, senior officer authorisation

Licensing Applications
Force database

Access
Standard grounds and justification to search internal law enforcement database

Licensing Office at Council
Local Authority

Access
DPA – protocol/MOU

Local Authorities, District, County, Unitary
Local Authority – see Crime & Disorder Partnerships

Access
DPA – CDRP protocols

Local Authority CCTV
Local Authority

Access
DPA – ACPO protocols
Information Commissioners Codes of Practice

Local Intelligence, Crime or Operational Systems
LEA

Access
Standard grounds and justification to search internal law enforcement database

Management of Dangerous and Sexual Offender Groups (MAPPS)
Multi-agency management group – possibly CDRP

Access
DPA – protocols

Media
Commercial information regarding business and potential sources of information

Access
DPA – production orders
PACE – special procedures material
ACPO Guidance release of photographs of named people to the media (ACPO Media Advisory Group)

Media – Lexis-Nexis
Commercial company – open source media – services provided over the internet

Access
Open source

Mediation Services
Local authority or multi-agency initiatives – sometimes charity status and LEA involvement in management, referrals and information exchange.

Access
DPA protocols (possibly CDRP)

Medicines & Health Care Products Regulatory Agency (formerly, Medicines Control Agency & Medical Devices Agency)
Enforcement of Medicines Legislation, European Medical Devices Directives Biological Standards Act, investigations include unlawful manufacture, counterfeited and diverted products, illegal sale, supply and importation of medicinal products and the unlawful manufacture and illegal counterfeiting, fraudulent and non-compliant medical devices.

Access
DPA protocols
(ACPO Guidance – Medical Devices Agency)

MIAFTR (Motor Insurance Anti-Fraud and Theft Register)
Commercial exchange of information and intelligence between insurance companies and loss adjusters, regarding insurance claims and fraudulent and suspicious claims.

Access
DPA

Ministry of Defence Police (MDP)
Non Home Office Civil Police Force – responsible for the security and policing of the MOD environment, providing a comprehensive police service to the MOD as a whole.

Access
ACPO – MOD protocol
Home Office circular

Missing Persons Bureau
LEA database

Access
Standard grounds and justification to search internal law enforcement database

Motor Manufacturers
Commercial information regarding business and customers

Access
DPA
Common law – a general requirement to assist police with their enquiries

Motor Trader Magazines
Commercial information regarding business and customers

Access
See Media

Motorfile CCN (Credit Control Nottingham)
Commercial credit reference company

Access
Commercial, searches recorded and may be disclosed to the subject. Confidential requests require DPA. Covert searches – surveillance authorities may be required – collection of personal data by covert means.

National Archive
Merger of Public Records Office and Historical Manuscripts Commission – holds archived court records including changes of name by deed poll.

Access
Open source
May require DPA – standard grounds

National Compromise Database
LEA database managed by NCIS containing information on law enforcement activities which have been undermined or exposed through awareness of the deployment of sensitive sources or the release of restricted information.

Access
ACPO protocol/MOU – NCIS Regional Offices – external search request

National Crime Squad (NCS)
LEA – lead for the prevention and detection of organised crime

Access
NCS protocols with ACPO, NCIS, HMRC etc.
ACPO Manual of Standards

National Criminal Intelligence Service (NCIS)
LEA intelligence exchange and co-ordination. Production of regional strategic assessments and UK threat assessment. National Flagging database, National Compromise database.

Access
ACPO/protocol/MOU – NCIS Regional Offices – external search request

National Firearms Forensic Intelligence Database
ACPO/FSS database of relevant data in respect of the criminal use of firearms. Comparison of forensic submissions nationally and development of strategic intelligence on firearms crime.

Access
Standard grounds and justification to search internal law enforcement database

National Firearms Register
PNC application updated through force inputs by the National Firearms Licensing Management system. See Firearms Registers.

Access
Standard grounds and justification to search internal law enforcement database

National Injuries Database (previously, Forensic Medicine Database at Guys Hospital)
Focused on analysis of victim, scene and wounds. Four thousand cases of suspicious deaths, homicides and clinical cases. Linked to the Serious and Sexual Assault and Attempted Murders Database correlation between live and dead victims. Under development – weapons and wounds index, catalogue of weapon images with images of the injuries caused.

Access
NCPE Operations Centre, Major Crime Helpdesk 01256 602443

National Lottery staff
Commercial information regarding business and customers

Access
DPA
Common law – a general requirement to assist police with their enquiries

National Method Index
CPA PNC application – in relation to all notified offences

Access
Standard grounds and justification to search internal law enforcement database

National Missing Persons Helpline (NMPH)
A charity dedicated to helping missing people, their families and those who care for them.

Access
NMPH Helpline
0500 700700

National Prisoner Tracing
HM Prison Service, LEA intelligence exchange

Access
Law enforcement liaison number

National Rivers Authority
Agency

Access
DPA

NCPE Operations Centre
Access to a range of law enforcement information, advice and support on good practice in operational policing.

Access (until 08/01/06)
Major Crime Helpdesk 01256 602 443
Covert Operational Support Team 0870 241 5641
Genesis Helpdesk 01256 602 778

Access (from 09/01/06)
NCPE Opsline 0870 241 5641

Neighbourhood Watch Scheme
Volunteer, community support to law enforcement

Access
Policing and Watch Schemes Guidance on Information Sharing, ACPO Crime and Disorder Reduction Partnership committee.
Common law – a general requirement to assist police with their enquiries

NHS – Counter Fraud Service
Investigatory body

Access
DPA

Nimrod
Possibly historical data only. West Midlands Police database of sex offenders and offences principally within the West Midlands Police area, including a register of offenders identified as high risk or potentially dangerous. See SCAS and ViSOR.

Access
Standard grounds and justification to search internal law enforcement database

Office for National Statistics
Government agency responsible for compiling national statistics and government research, access to grey literature on an open source basis, such as crime statistics and polling research papers. Including other national registers, such as records of all patients registered with a doctor – accessible under DPA (not medical record).

Access
DPA – standard grounds and justification

Open Source Research
Normally referred to in relation to searching on the internet, however, it also relates to any publicly accessible material. The fact that information is publicly available does not preclude it from being private information relating to a known individual.
Overt research – if using a computer and the internet consider that a traceable electronic footprint may be left behind which may divulge law enforcement interest and activity.
Covert research – will include measures intended to hide the fact that the search is being conducted by law enforcement, and where the likelihood that private information will be gathered.
Covert communication on-line – such as covertly entering a chat-room, establishment of communication with another user for the purpose of obtaining information. Conduct and use as CHIS required.

Access
Overt research – standard grounds and justification apply to the recording of any information regarding a known individual
Covert research – directed surveillance authority required
Covert communication on-line – RIPA authority conduct and use of CHIS required

Office of Fair Trading
Agency

Access
DPA

Passport Agency
Agency – applications received and passports issued, also stop list names associated with fraudulent applications and those banned from holding passports, eg, football banning orders.

Access
DPA – ACPO protocol

Pawn Brokers
Commercial information regarding business, customers and property held.

Access
DPA
Common law – a general requirement to assist police with their enquiries

Persons/Prisoners in Police Custody
Intelligence Approach Policy, Prison Intelligence Strategy.

Access
Standard grounds and justification to search internal law enforcement database

PHOENIX
PNC application containing modus operandi, offence history, personal habits and description etc.

Access
Standard grounds and justification to search internal law enforcement database
PNC – national guidance

Planning Department
Local Authority

Access
DPA – CDRP protocols

Plant & Equipment Register
Worldwide free service to police and law enforcement officers to assist with the identification and recovery of stolen construction, demolition and quarrying plant and equipment, tractors and agricultural machinery, trailers and caravans. Has investigators in UK and Eire (endorsed by the Home Office and ACPO).

Access
DPA
Common law – a general requirement to assist police with their enquiries

Police National Computer (PNC)
Mechanism to access DVLA records of vehicles, criminal convictions and arrests, national firearms registers and other applications. A source of intelligence and an aid to criminal investigations.
PHOENIX – includes modus operandi, offence history, personal habits and description
VODS (Vehicle Online Descriptive Search) – allows the searching of vehicle details by forces using a descriptive detail, even down to a postcode area
QUEST (Query Using Extended Search Technique) – allowing people to be searched using a variety of personal and descriptive details
Stolen property – trailers, boats, firearms
CCA – Comparative Case Analysis
TE – Transaction log query

Access
Standard grounds and justification to search internal law enforcement database
PNC – national guidance

Police Reports
LEA database

Access
Standard grounds and justification to search internal law enforcement database

Police Service of Northern Ireland
LEA intelligence exchange

Access
Standard grounds and justification to search internal law enforcement database
ACPO Manual of Standards

Policing and Watch Schemes
Volunteer community support to law enforcement

Access
DPA – national guidance

Port Authority
Commercial

Access
DPA – local arrangements

Postcomm: Postal Services Commission
Licenses and regulates postal services in UK, as a public authority investigates offences under the Postal Services Act and licence breaches.

Access
DPA

Premier Monitoring Services (Tagging)
Commercial – tagging orders and sentences – provides electronic monitoring for London, the Midlands and Wales. See also Securicor Justice Services.

Access
Formal agreement

Prison Service (HMP)
Agency – intelligence regarding prisoners and management of prisoners within the prison estate:

- Personal officer's report;
- Wing orderly officer's report;
- Home leave reports;
- Security information reports and adjudications;
- Major and minor incidents reports;
- Prison visit registers;
- Parole reports;
- Prison psychiatric/medical reports;
- Sex Offenders Treatment Programme reports;
- Category 'A' reviews;
- Prison correspondence/telephone calls (Target Monitoring);
- Details of private cash disturbance (disbursement).

Access
ACPO/Home Office MOU
HMP Police Advisor Section
Force/Prison Liaison Officers

Prisoner Carriers
Commercial – criminal justice, regarding court/prisoner escort and management

Access
DPA

Probation Service
Agency

Access
DPA – national protocol CDRP member

Product from Technical Surveillance including Visual, Audio and Tracking Data
LEA intelligence exchange

Access
Standard grounds and justification to search internal law enforcement database

Public
LEA intelligence obtained from contact with the public intelligence derived from witnesses, victims and others.

Access
Standard grounds and justification to search internal law enforcement database

QUEST
Query Using Extended Searching Techniques (PNC application) – allowing people to be searched on PNC using a variety of personal and descriptive details.

Access
Standard grounds and justification to search internal law enforcement database
PNC – national guidance

Racial Harassment Partnerships
Stand alone community forums or linked CDRP forums regarding specific community engagement or issues affecting them. May directly or indirectly involve commercial interests, community groups, local authority and law enforcement organisations. Source of intelligence for strategic products and risk assessments.

Access
DPA – possibly CDRP protocols

Radio Investigation Service (part of DTI Radio Communications Agency)
Enforcement of the Wireless Telegraphy Act and acts against illegal users of radio. Assists police in tracing illegal radio communications.

Access
DPA

Rape and Sexual Offences
See SCAS and CCA.

Access
Standard grounds and justification to search internal law enforcement database

REACT UK (European Anti-Counterfeiting Network)
Manages information system (Local Information Network Computer system – LINCs) developed by Trading Standards Services and Industry organisations, in consultation with NCIS. Funded by industries affected. Provides a network for the exchange and sharing of information regarding anti-counterfeiting and intellectual property right offences. British Phonographic Industry, Mechanical Copyright Protection Society, Federation Against Software Theft, Federation Against Copyright Theft, European Leisure Software Producers Associations, Anti Copyright in Design, The Business Software Alliance.

Access
DPA – ACPO/Industry MOU on Intellectual Property Right Offences
Common law – a general requirement to assist police with their enquiries

Regional Asset Recovery Teams
Law enforcement

Access
Standard grounds and justification to search internal law enforcement database

Regional Intelligence Cells (Special Branch)
Law enforcement

Access
Standard grounds and justification to search internal law enforcement database

Registry Office
Local Authority

Access
DPA

Retail Crime Partnerships
Commercial retail information exchange and forums, may directly involve law enforcement

Access
DPA – protocols

Royal Air Force Police
Responsible for criminal and security matters affecting the RAF under the functional control of the Air Officer Security and Provost Marshal (RAF)

Access
DPA – ACPO MOU
(Military)

Royal Mail Corporate Security
Security and criminal investigations affecting Royal Mail Group, including Royal Mail, Parcelforce Worldwide and Post Office Limited.

Access
DPA
Common law – a general requirement to assist police with their enquiries

Royal Mail Security and Investigation Services
Royal Mail security, risk management intelligence services, SPOC for accessing communications data, intercepts, retrievals and tracking.

Access
RIPA/ACPO Codes of Practice for SPOCs

Royal Marines Police
Supports the Royal Marines. Includes provision of garrison police facilities, law enforcement and crime prevention affecting Royal Marines interests.

Access
DPA – ACPO MOU
(Military)

Royal Military Police
Role of policing the army at home and overseas. Includes provision of garrison police facilities, law enforcement and crime prevention affecting army interests and close protection of serving MOD principals.

Access
DPA – ACPO MOU
(Military) (Army)
Central Criminal Records Office

Royal Naval Regulating Branch
The provision of Police Service facilities in major naval ports, law enforcement and crime prevention.

Access
DPA – ACPO MOU
(Military)

RSPCA
Charity and LEA

Access
DPA

Rural Payments Agency
Counter Fraud & Compliance Unit – investigation of fraud against the Common Agricultural Policy in the UK.

Access
DPA

Safer Estates Agreements
Local authorities and LEA meeting which may include public and commercial.

Access
DPA – CDRP protocol

SCAS (Serious Crime Analysis Section)
A part of NCPE Operations. Comparative Case Analysis (CCA) of all:

- Murder – sexual, unknown motive, undetected after 28 days, victim under 18;
- Rape – stranger, date rape, stalker rape;
- Abduction- – stranger, no demand, sexual nature.

Access
Contact SCAS on 01256 602305

Scenes of Crime Officers
LEA intelligence exchange

Access
Standard grounds and justification to search internal law enforcement database

School Welfare Officers
Local Authority

Access
DPA – CDRP protocol

Schools
Local Authority

Access
DPA – CDRP protocol

Scottish Drug Enforcement Agency
LEA intelligence exchange

Access
Standard grounds and justification to search internal law enforcement database

Scrap Yards
Commercial information regarding business, property and customers

Access
Legislative inspection powers
Common law – a general requirement to assist police with their enquiries

Sea Fisheries
Agency

Access
DPA

Securicor Justice Services (Tagging)
Commercial – tagging orders and sentences – provides electronic monitoring for the north of England. See also Premier Monitoring Services.

Access
Formal agreement

Security Services
Agency

Access
ACPO protocols and liaison through NCIS

Sex Offender Register
LEA database

Access
Standard grounds and justification to search internal law enforcement database

Shipping Companies
Commercial information regarding business and customers

Access
DPA
Common law – a general requirement to assist police with their enquiries

Shoe Mark Index
Local and National FSS (Forensic Science Service) database

Access
Standard grounds and justification to search internal law enforcement database

Sirene Bureau (UK)
UK access point to the Schengen Information system data, which is a European wide law enforcement data exchange system, in respect of:

- People wanted for extradition in another member state;
- Missing persons;
- Requests to locate witnesses and people for court appearances;
- Requests for information or checks on major criminal and linked vehicles;
- Stolen vehicles, trailers, firearms, identity documents and registered bank notes.

Co-ordination of responses to alerts and requests for assistance in gathering of information in other countries and tracing fugitives from justice.

Access
Accessed directly through PNC checks
National guidance – standard grounds and justification to search law enforcement database

Social Services
Local Authority

Access
DPA – CDRP protocols
ACPO guidance

Surveillance Product
LEA intelligence data

Access
Standard grounds and justification to search internal law enforcement database

Taxi Companies
Local authority licensing

Access
DPA
Common law – a general requirement to assist police with their enquiries

Thatcham Vehicle Identification System (TVIS)
Commercial database of locations of vehicle identification numbers

Access
CD-ROM annual update fee
TVIS contact no. 01635 294825
sales@thatcham.org

Tobacco Manufacturers Association
Liaison and co-ordination in the prevention and detection of crime affecting tobacco manufacturers, importers and their goods.

Access
DPA
Common law – a general requirement to assist police with their enquiries

Trading Standards
Local Authority/LEA

Access
DPA – CDRP protocols

Traffic Department
LEA intelligence exchange

Access
Standard grounds and justification to search internal law enforcement database

Travellers Office
Local Authority

Access
DPA – CDRP protocols

Utilities (gas, water, electricity, sewerage, satellite TV companies)
Commercial information about business and customers

Access
DPA

ViCLAS – Violent Crime Linkage Analysis System
See SCAS – principal SCAS database

Access
Contact SCAS on 01256 602305

ViSOR – Violent Sex Offender Register
Criminal justice agencies database for the registration and management of violent and sex offenders, including intelligence and information exchange regarding violent and dangerous offenders, over the CJX.

Access
DPA – national guidance
Standard grounds and justification to search internal law enforcement database

Victim Support
Charity and LEA

Access
DPA – national guidance

VODS (Vehicle Online Descriptive Search)
PNC application that allows the searching of vehicle details by forces using a descriptive detail, even down to a postcode area.

Access
Standard grounds and justification to search internal law enforcement database
PNC – national guidance

Warrants
Force database

Access
Standard grounds and justification to search internal law enforcement database

Weapons and Wounds Database (see National Injuries Database)
Under development – weapons and wounds index, catalogue of weapon images with images of the injuries caused (to be linked to the National Injuries Database).

Access
NCPE Operations Centre, Major Crime Helpdesk 01256 602443

Wine Standards Board
Enforcement authority responsible for the provisions of the EU wine regulations in the non-retail sector.

Access
DPA
Common law – a general requirement to assist police with their enquiries

Youth Offending Teams
Local Authority/LEA

Access
DPA – CDRP protocol
Joint working protocols

APPENDIX 4
GLOSSARY

5x5x5
An information/intelligence report in which the source, the intelligence and the way in which the material should be disseminated (known as the handling code) have all been evaluated and assigned a grading between 1 and 5.

AA
Automobile Association

ACAG
Anti-Corruption Advisory Group

ACPO
Association of Chief Police Officers – police bodies which provide a professional corporate view on policing in England, Wales and Northern Ireland (ACPO) and Scotland (ACPOS). Membership includes Chief Constables, Deputy Chief Constables and Assistant Chief Constables or their equivalent in England, Wales and Northern Ireland.

AFR
Automatic Fingerprint Recognition

Airwave
The first national digital communication service designed for the police forces of England, Wales and Scotland.

ANPR
Automatic Number Plate Recognition

ASBO
Anti-Social Behaviour Order

Assets
NIM uses four types of assets – knowledge, system, source and people assets. See individual entries for definition of each type of asset.

ATM
Automated Teller Machine

Authorities Management
The process adopted to ensure RIPA is ECHR compliant and meets the standards set by the Surveillance Commissioners.

BCU
Basic Command Unit – a geographical area within a police force (ie, Metropolitan Police) also known as Area, Division or Operational Command Unit.

Blue Book
The original NCIS publication describing the National Intelligence Model.

BST
British Summer Time

Business Excellence Model
A model for assessing organisational quality designed by the European Foundation of Quality Management.

BVPI
Best Value Performance Indicator

CasWeb
A web access version of the HOLMES2 Casualty Bureau that makes it easier for forces to co-operate in the even of a major incident.

CATCHEM
Centralised Analytical Team Collating Homicide Expertise and Management

CCA
Comparative Case Analysis

CCTV
Closed Circuit Television

CDA
Crime and Disorder Act 1998

CDRP
Crime and Disorder Reduction Partnership

Centrex
Centrex is the working name for the Central Police Training and Development Authority

CHIS
Covert Human Intelligence Source

CJU
Criminal Justice Unit

CJX
The Criminal Justice Extranet – all forces are connected to the CJX, allowing them to communicate and share information and documents with each other securely. Forces are also able to communicate securely with any other criminal justice partners who are connected (eg, Crown Prosecution Service and Criminal Records Bureau).

Community Intelligence
Local information which, when assessed, provides intelligence on issues that affect neighbourhoods and informs both strategic and operational perspectives in the policing of local communities. Information may be direct or indirect and come from a diverse range of sources including the community and partner agencies.

Comparative Case Analysis
PNC application used as a search tool into serious offences

Control Strategy
Sets out and communicates the current strategic operational priorities for the force or area

CPA
Crime Pattern Analysis

CPIA
Criminal Procedure and Investigations Act 1996

CPS
Crown Prosecution Service

CRAMM
Central Computing Telecommunications Agency Risk Analysis Management Method. This is a complete method for identifying and justifying all the necessary protective measures to ensure the security of both current and future information technology systems used for processing valuable or sensitive data (the Government's preferred risk assessment methodology).

CRB
Criminal Records Bureau

Crime and Incident Series
A crime or incident series can be defined as a number of similar crimes or incidents which are linked by M.O., intelligence, or forensic evidence, where the link suggests they have been committed by one offender or group of offenders.

Crime Pattern Analysis (CPA)
The aim of crime pattern analysis is to identify the nature and scale of emerging and current crime trends, patterns, linked crimes or incidents, and hot spots of activity. It is a generic term for a number of related disciplines such as crime or incident series identification, crime trend analysis, hot spot analysis and general profile analysis.

Crime Trend
The direction or pattern that specific types or general crimes are broadly following

Criminal Business Profiles
Criminal business profiles contain detailed analysis of how criminal operations or techniques work, in the same way that legitimate business may be explained.

Daily Management Meeting
Not a T&CG – this meeting ensures that the conduct of daily business is linked to the priorities and objectives set by the tactical T&CG.

DAT
Drugs Action Team

Demographic/Social Trends Analysis
Centred on demographic changes and their impact on criminality, as well as on the deeper analysis of social factors, this technique considers the significance of population shifts, attitudes and activities.

DNA
Deoxyribonucleic Acid

Doctrine
The principal purpose of doctrine is to provide a framework of guidance for policing activities and underpin police training and operational planning.

DPA
Data Protection Act 1998

DSU
Dedicated Source Unit

DVLA
Driver and Vehicle Licensing Agency

ECHR
European Convention on Human Rights

Enforcement Priorities
Actions required in order to impose the law in relation to crime and disorder problems that the TT&CG has authorised for intervention (in line with the control strategy). This may include such tactics as: arrest and interview of suspects, execution of search warrants and covert operational deployments (see Tactical Options Menu).

FAQ
Frequently Asked Questions

FIB
Force Intelligence Bureau

FSS
Forensic Science Service

General Profile
Common characteristics of offenders displaying particular offending behaviour.

Genesis
Online information service provided by Centrex to support operational policing (service within CJX).

GMT
Greenwich Mean Time

GPMS
Government Protective Marking Scheme – for the security of sensitive material

Grey Literature
Grey literature refers to publications issued by government agencies, professional organisations, research centres, universities, public institutions, special interest groups and associations and societies whose goal is to disseminate current information to a wide audience.

HMIC
Her Majesty's Inspectorate of Constabulary

HMIS
Her Majesty's Intelligence Services

HMP
Her Majesty's Prison

HMRC
Her Majesty's Revenue and Customs (responsible for the business of the former Inland Revenue and HM Customs and Excise).

HO
Home Office

HOLMES/HOLMES2
Home Office Large Major Enquiry System – computer system for major incidents (SCAS document management system).

HOSDB
Home Office Scientific Development Branch (formerly known as the Police Scientific Development Branch – PSDB).

Hot Spots
Locations attracting concentrated police attention and displaying cause for concern.

HR
Human Resources

HRA
Human Rights Act 1998

ID
Identification or identity

IIMARCH System
Information, Intention, Method, Administration, Risk assessment, Communication, Human rights – a nationally recognised formula for presenting briefings based on operational orders.

ILPM
Intelligence Led Policing Model

IMPACT
Intelligence Management, Prioritisation, Analysis, Co-ordination and Tasking – programme to deliver a national IT intelligence system.

Information
Information refers to all forms of information obtained, recorded or processed by the police, including personal data and intelligence.

Intelligence
Intelligence is defined as information that has been subject to a defined evaluation and risk assessment process in order to assist with police decision making.

Intelligence Priorities
When the TT&CG authorises a crime and disorder problem for intervention (in line with the control strategy), there may still be gaps in the intelligence. Actions required in order to gain the intelligence will form part of the tactical plan and may include activities such as: telecommunications analysis, CHIS tasking and surveillance (see Tactical Options Menu).

Intelligence Products
NIM includes four types of intelligence products – strategic assessments, tactical assessments, target profiles and problem profiles. They provide the information upon which strategic and tactical decisions are made. See individual entries for a definition of each type of intelligence product.

Intelligence Requirement
Within the intelligence process, the identified gap between what is known and what is not forms the intelligence requirement.

IT
Information Technology

J-Track
Web based system that allows police officers and the CPS to track repeat offenders' progress through the criminal justice system.

Knowledge Assets
A range of products, either national or local, which define the rules for the conduct of the business or best practice by which skilled processes are completed, and under what conditions work between agencies may take place. Examples include legislation, case law, force policies and procedures and codes of practice.

LAG
Local Action Group

Lawtel
Easy to use service for case law and legislation with separate sections on Human Rights, Personal Injury, Civil Procedure and Employment.

LEA
Law Enforcement Agency

Level 1
Local crime and disorder, including anti-social behaviour, capable of being managed by local resources, eg, crimes affecting a BCU or small force area.

Level 2
Cross border issues, affecting more than one BCU within a force or affecting another force or regional crime activity, usually requiring additional resources.

Level 3
Serious and organised crime usually operating on a national and international scale, requiring identification by proactive means and a response primarily through targeted operations by dedicated units and a preventative response on a national basis.

Lexis-Nexis
Comprehensive electronic information resource that includes UK and EU case law and legislation, full text UK journals, UK (national and regional) newspapers, US material and material from other jurisdictions.

LPU
Local Policing Unit – smaller geographical area within a BCU

MAPPA
Multi-Agency Public Protection Arrangements

Market Profiles
These are profiles, continually reviewed and updated, that survey the criminal market around a particular commodity, such as drugs or stolen vehicles, or of a service, such as prostitution, in a given area.

MIM
Murder Investigation Manual

Minimum Standards
Standards developed by the ACPO NIM Team in collaboration with practitioners from around the country and HMIC. Forces must be compliant with all of the minimum standards listed in this manual by November 2005.

MIRSAP
Major Incident Room Standardised Administrative Procedures

MO (Modus Operandi)
The particular way in which a person performs a task or action, or the way something operates. Latin phrase meaning, 'way of operating' (plural – modi operandi).

MOU (Memorandum of Understanding)
A protocol setting out agreed working arrangements and/or information sharing between partner organisations (plural – memoranda).

NAFIS
National Fingerprint System

National Policing Plan
Introduced as part of the Police Reform Act, it highlights anti-social behaviour, street crime, drug-related crime, burglary, and car crime as key areas for police forces to tackle locally to improve public reassurance and engage all sections of the community. It also reaffirms the key role the police play in encouraging vigilance about terrorist attack. As well as identifying national policing priorities, it sets national objectives to measure how police forces are performing.

NBM
National Briefing Model

NCALT
National Centre for Applied Learning Technologies (component of Centrex)

NCF
National Crime Faculty

NCIS
National Criminal Intelligence Service

NCPE
National Centre for Policing Excellence

NCS
National Crime Squad

Network Analysis
Network analysis describes the linkages between people who form criminal networks, and the significance of the links, the roles played by the individuals and the strengths and weaknesses of a criminal organisation.

NHW
Neighbourhood Watch

NIM
National Intelligence Model

NPP
Neighbourhood Policing Plan

NSLEC
National Specialist Law Enforcement Centre

NSMU
National Source Management Unit (at NCIS)

OCU
Operational Command Unit

Operational Intelligence Assessments
Operational intelligence assessments evaluate the development of an operation, based on previously agreed objectives, in order to maintain the focus.

OPSY
Operational Security Officer

OSU
Operational Support Unit

PACE
Police and Criminal Evidence Act 1984

PAYE
Pay-as-you-earn

PCSO
Police Community Support Officer

People Assets
The selection, recruitment and retention of the right people in the right roles. It is essential that certain roles are filled in sufficient numbers to provide a high level of resilience.

PESTELO
Political, Economic, Social, Technological, Environmental, Legal, Organisational

PII
Public Interest Immunity

PIMS
Police Informant Management System

PITO
Police Information Technology Organisation

PNC
Police National Computer

PNN2
The second generation Police National Network – telecommunications infrastructure used by the UK Police Service. It provides forces with telephony, internet access and a secure extranet – the Criminal Justice Extranet (CJX).

POP – Problem Oriented Policing
Described by Herman Goldstein as a model for enabling understanding of the root causes of problems in society through analysis.

Prevention Priorities
Actions required to keep crime and disorder from happening for each problem that the TT&CG has authorised for intervention (in line with the control strategy), and may include such tactics as: use of mobile/static CCTV, NHW and preventative analysis (see Tactical Options Menu).

Priority Locations
Hot spots and locations representing long-term concentrated need.

Problem Profiles
A problem profile is a detailed picture of an identified problem, established or emerging, in line with the control strategy priorities or high risk issues.

PSNI
Police Service of Northern Ireland

Public Interest Immunity (PII)
A principle of law which enables the courts to reconcile the conflict which sometimes arises between two public interests: the interest for courts to have the fullest possible access to all relevant material, and the need to maintain confidentiality of information that could be damaging to the public interest if disclosed. PII means that special care must be taken to decide where the balance lies between these two interests before any question of disclosure is decided.

R&D
Research and Analysis

RAC
Royal Automobile Club

Results Analysis
This analytical technique evaluates the effectiveness of law enforcement activities in order to inform future decision making.

RIPA
Regulation of Investigatory Powers Act 2000

Risk Analysis
Risk analysis assesses the scale of risks posed by offenders or organisations to potential victims, the public and law enforcement agencies.

Sanctioned Detections
Recordable offences charged or taken into consideration and subsequently confirmed by court processes and official cautions for such offences.

Sanitisation
The practice of removing or altering the content of a document with the aim of protecting sensitive sources and/or methodology to arrive at a form appropriate for dissemination.

SB
Special Branch

SCAS
Serious Crime Analysis Section (part of NCPE Operations)

SCP
Situational Crime Prevention

Signal Crimes
Any criminal incident that causes change in the public's behaviour and/or beliefs about their security.

SIO
Senior Investigating Officer

Skills for Justice – National Occupational Standards
Skills for Justice is the sector skills council covering all employers, employees and volunteers in the criminal justice sector throughout the United Kingdom, including the police. They are responsible for setting and reviewing the national occupational standards which outline the level of knowledge, skills and understanding somebody working in a particular role within the Police Service must have in order to be competent.

SLA
Service Level Agreement

SOCA
Serious and Organised Crime Agency

SPOC
Single Point of Contact

ST&CG
Strategic Tasking and Co-ordination Group

Strategic Assessments
The strategic assessment drives the business of the strategic tasking and co-ordination group (ST&CG) by providing it with an accurate overview of the current and long-term issues affecting the BCU, force or region.

Strategic Tasking and Co-ordination Meeting
The meeting where the ST&CG considers recommendations made in the strategic assessment in order to set a control strategy for the basic command unit or force. The ST&CG nominates owners for each strategy. Once the control strategy is agreed, the ST&CG sanctions the intelligence requirement and sets the prioritisation of resources. The control strategy will only ever be amended by the ST&CG; amendments to the intelligence requirement can be made at the TT&CG. The ST&CG also sets the resource priorities for reactive and proactive capabilities, but not for tactical activity, which is determined at the TT&CG meeting.

T&CG
Tasking and Co-ordination Group

Tactical Assessments
The tactical assessment drives the business of the tactical tasking and co-ordination group (TT&CG), identifying and monitoring the progression of the shorter-term issues in a BCU, force or region, in accordance with the control strategy.

Tactical Capability
The officers and support staff in a BCU, force or region, and/or partners, who are in a position to provide a quick and flexible tactical resolution for any problem or target profile produced by the intelligence unit.

Tactical Menu
The tactical menu is a problem identification matrix. It focuses attention on priority locations, subjects, crime/incident series and high risk issues so that the T&CG can prioritise the problem-solving work and direct the allocation of resources to those problems accordingly.

Tactical Options Menu
The tactical options menu is made up of three elements: prevention, intelligence and enforcement. It is the framework used for deciding and organising an appropriate tactical resolution for a crime and disorder problem that has been authorised for intervention action by the TT&CG.

Tactical Tasking and Co-ordination Meeting
The meeting where the TT&CG make decisions in relation to crime and disorder problems that are identified in the tactical assessment. The TT&CG should use the tactical assessment, along with the control strategy, to prioritise intervention activity. The group should also check that previously agreed plans and intervention work are still on course to meet objectives and ensure that the business plan focus is maintained. The TT&CG should sanction the deployment of resources and avoid excessive responses to merely random events. They should also identify plan and problem owners to take responsibility for the tactical resolution of issues raised in the tactical assessment. The TT&CG should also review the published intelligence requirement, ensuring it remains applicable and making any necessary amendments.

Target Profile Analysis
Target profile analysis uses a range of analytical techniques that aim to describe the criminal, their criminal activity, lifestyle, associations, the risk they pose and their strengths and weaknesses. This is in order to provide sufficient detailed analysis to initiate a target operation or support an ongoing operation against an individual or networked group of individuals.

Target Profiles
Target profiles provide a detailed picture of either a person or group of people who have been identified in line with the control strategy priorities or high risk issues.

TSU
Technical Support Unit

TT&CG
Tactical Tasking and Co-ordination Group

UK
United Kingdom

UKIS
United Kingdom Immigration Service

UKTA
United Kingdom Threat Analysis

URN
Unique Reference Number

VAT
Value Added Tax

Victimology
The study of the victims of crime and the psychological effects on them

VODS
Vehicle Online Descriptive Search

Westlaw
Electronic law library – comprehensive service – contains UK and EU case law and includes legislation, Legal Journals Index, full text UK journals and special practice areas.

Yellow Book, The
Name of CD published by the former PSDB which is used by TSUs alongside *ACPO (2004) Deployment Standards for Technical Support in Tackling Volume Crime.*

APPENDIX 5
REFERENCES

ACPO (2000) *MIRSAP Major Incident Room Standardised Administrative Procedures Manual (forthcoming November 2005)*

ACPO (2000) *Murder Investigation Manual*

ACPO (2000) *PNC Compliance Strategy*

ACPO (2001) *Adoption of the Government Protective Marking Scheme (GPMS)*

ACPO (2002) *Code of Practice for Data Protection*

ACPO (2002) *HM Customs and Excise Memorandum of Understanding Disclosure of Information*

ACPO (2004) *Deployment Standards for Technical Support in Tackling Volume Crime*

ACPO (2005) *Code of Practice on the Management of Police Information*

ACPO (2005) *Code of Practice on the National Intelligence Model*

ACPO (2005) *Code of Practice on the Police National Computer*

ACPO (2005) *Practice Advice on Core Investigative Doctrine*

ACPO (2005) *Practice Advice on Professionalising the Business of Neighbourhood Policing (Draft)*

ACPO (forthcoming) *Data Protection Manual of Guidance*

ACPO (forthcoming) *Guidance on the Management of Police Information*

ACPO (forthcoming) *Guidance on the National Briefing Model*

ACPO (forthcoming) *Practice Advice on Prison Intelligence and Related Matters*

ACPO (forthcoming) *Practice Advice on Resources and the People Assets of NIM*

ACPO (forthcoming) *Practice Advice on Tasking and Co-ordination*

ACPO/ACPOS (2002) *Information Systems Community Security Policy*

ACPO/ACPOS/HMCE (2003) *Manual of Standards for Accessing Communications Data*

ACPO/HMCE (2003) *Manual of Standards for the Deployment of Test Purchase and Decoy Officers*

ACPO/HMCE (2003) *Manual of Standards for the Deployment of Undercover Officers*

ACPO/HMCE (2004) *Manual of Standards for Covert Human Intelligence Sources*

ACPO/HMCE (2004) *National Standards in Covert Investigations Manual of Standards for Surveillance* Regulated by Part III, Police Act 1997 and Part II, Regulation of Investigatory Powers Act 2000

Caless, B.W., Kent County Constabulary (1999) *Police Corruption: Vulnerability Profiling*

Clarke, R.V. and Eck, J (2003) *Becoming a Problem-Solving Crime Analyst*

Home Office (2002) *Passport to Evaluation: An Introduction to Evaluating Crime Reduction Initiatives and Projects*

Home Office (2005) *Prolific and Other Priority Offenders Strategy*

Home Office (forthcoming) *Codes of Practice for the Use of the Serious Crime Analysis Section*

Innes, M. and Roberts, C., Signal Research (2005) *i-NSI Trial & Evaluation Report*

NCIS (2000) *The National Intelligence Model (Blue Book)*

Skills for Justice (2004) *Integrated Competency Framework v7 for the police sector*

APPENDIX 6
CONTACT DETAILS

NCPE NIM Doctrine Development
Wyboston Lakes,
Great North Road,
Bedford MK44 3BY
Telephone: 0870 351 0264

NCPE NIM Support Team
NCPE
PO BOX 8000
London SE11 5EN
Telephone: 0207 238 8620

NCPE Programme Implementation Team
Wyboston Lakes,
Great North Road,
Bedford MK44 3BY
Telephone: 0870 351 0418

National Analyst Working Group
Wyboston Lakes,
Great North Road,
Bedford MK44 3BY
Telephone: 0870 351 0326

NCPE Operations Helpdesk
Email: crimehelpdesk@centrex.pnn.police.uk
Telephone: 01256 602443

Genesis Helpdesk
Email: genesis@centrex.pnn.police.uk
Telephone: 01256 602778

Covert Law Enforcement Advice Line
The Covert Journal is available through:
Email: covert_adviceline@centrex.pnn.police.uk
Telephone: 0870 241 5641
or via Covert Operational Support Team site on Genesis