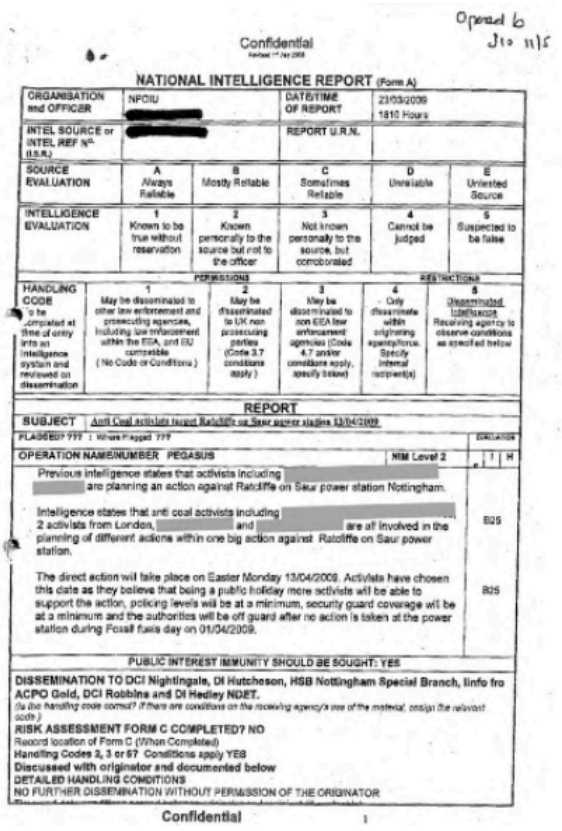
REGULATORY FRAMEWORKS

Rules of engagement for undercover police units in the 2000s



Confidential

NATIONAL INTELLIGENCE REPORT (Form A)

ORGANISATION and OFFICER	NPOIU [redacted]		DATE/TIME OF REPORT	21/03/2009 1810 Hours	
INTEL SOURCE or INTEL REF No (URN)	[redacted]		REPORT U.R.N.		
SOURCE EVALUATION	A Always Reliable	B Mostly Reliable	C Sometimes Reliable	D Unreliable	E Untested Source
INTELLIGENCE EVALUATION	1 Known to be true without reservation	2 Known personally to the source but not to the officer	3 Not known personally to the source, but corroborated	4 Cannot be judged	5 Suspected to be false

HANDLING CODE	PERMISSIONS 1	2	3	RESTRICTIONS 4	5
To be completed at time of entry into an intelligence system and reviewed on dissemination	May be disseminated to other law enforcement and prosecuting agencies, including law enforcement within the EEA, and EU compatible (No Code or Conditions)	May be disseminated to UK non prosecuting parties (Code 3,7 conditions apply)	May be disseminated to non EEA law enforcement agencies (Code 4,7 and/or conditions apply, specify below)	Only disseminate within originating agency/force. Specify internal recipient(s)	Disseminated Intelligence Receiving agency to observe conditions as specified below

REPORT

SUBJECT: Anti Coal activists target Ratcliffe on Saur power station 13/04/2009

FLAGGED ??? : Where Flagged ???

DATE/TIME | I | H

OPERATION NAME/NUMBER PEGASUS — NIM Level 2

Previous intelligence states that activists including [redacted] are planning an action against Ratcliffe on Saur power station Nottingham.

Intelligence states that anti coal activists including [redacted] 2 activists from London, [redacted] and [redacted] are all involved in the planning of different actions within one big action against Ratcliffe on Saur power station. — B25

The direct action will take place on Easter Monday 13/04/2009. Activists have chosen this date as they believe that being a public holiday more activists will be able to support the action, policing levels will be at a minimum, security guard coverage will be at a minimum and the authorities will be off guard after no action is taken at the power station during Fossil fuels day on 01/04/2009. — B25

PUBLIC INTEREST IMMUNITY SHOULD BE SOUGHT: YES

DISSEMINATION TO DCI Nightingale, DI Hutchoson, HSB Nottingham Special Branch, Info fro ACPO Gold, DCI Robbins and DI Hedley NDET.

(Is the handling code correct? If there are conditions on the receiving agency's use of the material, assign the relevant code.)

RISK ASSESSMENT FORM C COMPLETED? NO

Record location of Form C (When Completed)

Handling Codes 2, 3 or 5? Conditions apply YES

Discussed with originator and documented below

DETAILED HANDLING CONDITIONS

NO FURTHER DISSEMINATION WITHOUT PERMISSION OF THE ORIGINATOR

Confidential

a report by the
undercover research group
April 2025

List of key documents cited

- Association of Police Chief Officers / National Centre for Policing Excellence: Guidance on the National Intelligence Model, 2005 ('Guidance 2005')

- Centrex / National Centre for Policing Excellence, National Intelligence Model – Code of Practice, January 2005, ('Centrex 2005')

- National Criminal Intelligence Service, National Intelligence Model, 2000, ('NCIS 2000')

- Home Office, Code of Practice on the Management of Police Information, July 2005, ('HO CP-MoPI 2005')

- How to Complete a 5x5x5 Form and Relevant Supplements, archived via College of Policing

A. Introduction

1. In the 1990s, UK policing saw a strong push to adopt an intelligence-led policing model, which was thought would offer greater efficiency and better results. The end of the 1990s saw significant legislative changes, taking into account the increased focus on information and intelligence. These changes came in parallel with a focus on procedures for gathering information, including processing and storing it and turning it into an intelligence product of use to others. This required an overhaul of the regulation system.

2. The Regulation of Investigatory Powers Act 2000 (RIPA) covers the legal authorisation of deployment of Covert Human Intelligence Sources (CHIS), including undercover police. However, a swathe of policing policies was created alongside to give these new and greater powers a legal framework. Some policies took existing practice and

updated it; others created entire new regimes, the most important of which, for undercover policing units, was the National Intelligence Model (NIM).

3. While it appears to play little role in the day-to-day life of undercovers, this wider framework set out the protocols for police intelligence work in the 2000s. In particular, it established criteria on both how to set priorities for intelligence gathering, and also the authorisation of undercover deployments. This latter process also required a structured intelligence gathering case to support the authorisation.

4. Many of the intelligence structures that appeared from the late 1990s started to parallel the NIM, which was being developed at that time. For instance, at the senior management level, RIPA required that authorising officers signed off undercover deployments as being necessary to achieve objectives. Part of the role of the NIM was supposedly to ensure oversight that those authorising had the policing objectives set out to be able to decide objectively whether or not to deploy an undercover officer (UCO). This included aspects such as risk to the undercover officers and collateral intrusion, among other factors.

5. At the level of undercover deployments, we see the introduction of particular types of intelligence forms used to pass information on. In particular a new set of criteria was introduced to grade information, to determine whether it could be considered as intelligence. Indeed, information was not considered intelligence until it had passed through that process. The most important of these is known as the 5x5x5 form, so called because it was based on three sets of criteria, each with five options, to rate the information, such as reliability, etc. In some forms these three sets are explicitly spelled out and marked. Others make references to code such as Bx2x5, which is shorthand for the NIM criteria.

6. Between the high-end authorisation process and the ground level 5x5x5 forms, is a less visible pair of intertwined processes that set out the objectives to be achieved. This was handled by the managers of the units involved, depending on their role and seniority within the structure, and turned the high-level objectives into concrete action.

The Control Strategy which determined what intelligence was needed, was known as the Intelligence Requirement. Once that requirement was established, the processes to focus on its collection, and the resources (technical or human) were tasked to gather it. Thus, when the 5x5x5 forms or other documents refer to Control Strategy, this is a reference to the documentation that makes the case for the intelligence gathering in the first place.

7. As these processes are the most opaque, but of fundamental importance to the deployment of undercovers, their authorisation and the processing of their information gathering, it is the aspect most focused on in this briefing. This will be followed by a discussion on interpreting a generic 5x5x5 form and how the information in it relates to these higher level processes. Other issues, such as to whom intelligence should be disseminated, its retention and disposal of information, are outlined as well, being important both to the regulatory regime and the handling of intelligence gathered by the undercover officers.

B. Regulatory Regime

1. The undercover units were bound by legislation. The two main statutes are the
   a) Regulation of Investigatory Powers Act 2000
   b) Data Protection Act 1998

   The 2004 Home Office Guidelines for a Special Branch are explicit about this:[1]

   > *Moreover, the covert activities of law enforcement agencies have seen radical legislative reform with the passing of the Regulation of Investigatory Powers Act 2000 and the Regulation of Investigatory Powers (Scotland) Act 2000. Special Branch staff, like other members of the police service, must comply with these pieces of legislation. In particular, and in support of the overriding principle of protecting human rights, the use of the powers and authorities provided to the*

[1] Home Office, Guidelines on Special Branch Work in the United Kingdom, 2004, page 3, https://www.documentcloud.org/documents/6792176-2004-Special-Branch-Guidelines/ ('SB Guidelines 2004')

Police Service by virtue of these Acts are regulated subject to inspection and oversight by two independent commissions. Special Branch, as with all other areas of policing, is subject to the provisions contained within the Data Protection Act 1998 and, more recently, the Freedom of Information Act 2000.

There are no special powers or privileges attached to individuals simply by virtue of the fact that they work within Special Branch. Police officers with executive powers within Special Branch are accountable in exactly the same way as other members of the police service: under the relevant legislation and to the relevant misconduct procedures and ethical standards set down by both the Association of Chief Police Officers (ACPO) and Association of Chief Police Officers Scotland (ACPOS).

2. Following the introduction of these laws, police bodies and the Home Office developed a number of practice guidelines to ensure compliance with the law and set national standards. Not all have been made public, but are referred to in those that have been. A number of these were produced under statutory authority, giving them important weight.[2]

3. In 2000, the Association of Chief Police Officers (ACPO) developed and then adopted the National Intelligence Model as policy. The National Minimum Standards for the NIM was published in April 2003, and all police forces in England and Wales were expected to adhere to them from April 2004.[3] [4]

---

[2] Centrex / National Centre for Policing Excellence, *National Intelligence Model – Code of Practice*, January 2005, ('Centrex 2005') http://library.college.police.uk/docs/npia/NIM-Code-of-Practice.pdf This Code of Practice was issued by Centrex, but done under the aegis of the Secretary of State for the Home Office, giving it statutory basis, particularly under the Police Act 1996, the Police Act 1997 as amended by Police Reform Act 2002. See para. 1.2.2 of document (page 3) for further detail. The HMIC 2014 (*ibid.*) report also stated that the Code of Practice was issued in January 2005 by the Home Secretary under sections 39 and 39A, Police Act 1996, sections 28 and 73, Police Act 1997, and sections 28A and 73A, Police Act 1997 – see Note 63, page 53.

[3] Association of Police Chief Officers / National Centre for Policing Excellence: *Guidance on the National Intelligence Model*, 2005 ('Guidance 2005'), https://www.spycopsresearch.info/sites/default/files/2025-03/centrex%20-%20guidance-on-the-national-intelligence-model-2005.pdf, page 8. Additional minimal standards were developed for implementation by November 2005 also, and incorporated into the 2005 Guidance.

[4] The NIM Minimum Standards can be found as Appendix 2 to the Guidance 2005 document, *ibid*.

Key documents

4. This brief focuses on the following available documents:
   a) National Intelligence Model, 2000[5]
   b) National Intelligence Model Code of Practice, 2005,[6] with the National Minimum Standards appended
   c) ACPO/Centrex: Guidance on the National Intelligence Model, 2005[7]
   d) Home Office Code of Practice on Management of Police Information, 2005[8]

   Practice and guidelines have evolved since these were created, however the basic practices have essentially remained the same; the National Intelligence Model is still current policing practice. Nevertheless, we have used the documents for the era which the Undercover Policing Inquiry will be concerned with.

5. As mentioned, a number of other documents have been referenced in the guidance cited here. Many have not been made public, but are important to understand the wider regime under which undercovers worked and/or have been cited as relevant in the documents that have been examined. These are:
   a) ACPO & HMCE (1999), Code of Practice on the Recording and Dissemination of Intelligence Material
   b) ACPO & HMCE (1999), Standards for the Recording and Dissemination of Intelligence Material
   c) ACPO (2003), Manual of Standards for the Deployment of Undercover Officers
   d) ACPO and HMCE (2004), Manual of Standards for [the Use of] Covert Human Intelligence Sources

---

5 National Criminal Intelligence Service, *National Intelligence Model*, 2000, ('NCIS 2000') https://www.spycopsresearch.info/sites/default/files/2025-03/NCIS%20-%20National-Intelligence-Model%20-%202000.pdf

6 Centrex 2005, *ibid*.

7 Guidance 2005, *ibid*.

8 Home Office Code of Practice on the Management of Police Information, July 2005, ('HO CP-MoPI 2005') https://library.college.police.uk/docs/APPref/Management-of-Police-Information.pdf

e) ACPO & HMCE, (2004) National Standards in Covert Investigations Manual of Standards for Surveillance
f) ACPO (2005), Code of Practice on the Management of Police Information
g) ACPO Practice Advice on Resources and People Assets of NIM
h) ACPO, Guidance on the Management of Police Information
i) ACPO Manual of Standards on the Recording and Dissemination of Intelligence Material
j) ACPO, Practice Advice on Tasking and Co-ordination
k) Home Office Code on Covert Surveillance
l) Home Office Code on Covert Human Intelligence Sources.

2005 NIM Code of Practice

6. The 2005 Centrex/Home Office National Intelligence Model Code of Practice is one of the documents issued under statutory powers.[9] This was done under the Police Reform Act 2002.[10] It makes the following important statements:[11]

> *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.*

---

9 This Code of Practice was issued by Centrex, but done under the aegis of the Secretary of State for the Home Office who gave it statutory basis under the Police Act 1996 and the Police Act 1997 as amended by Police Reform Act 2002. See Centrex 2005, para. 1.2.2 (page 3) for further detail.

10 Guidance 2005, page 8.

11 Centrex 2005, pages 6-7. Some irrelevant material omitted.

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 of relevance to the application of the National Intelligence Model are:

2.2.4.1 ACPO Manual of Standards for the Deployment of Undercover Officers

2.2.4.3 ACPO Manual of Standards on Surveillance

2.2.4.4 ACPO Manual of Professional Standards in Policing

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:

2.2.5.1 Covert Surveillance

2.2.5.2 Interception of Communications

2.2.5.3 Covert Human Intelligence Sources

7. Officers and staff working within the National Intelligence Model were required to have the appropriate training.[12]

Data management

8. The 2005 NIM Code of Practice notes the need to abide by the legislative data-protection regime, then the Data Protection Act 1998:[13]

Chief officers are responsible for the development and implementation of appropriate procedures and systems to ensure that personal information on

[12] Centrex 2005, p.12, section 6.1.
[13] Centrex 2005, p. 9, section 3.8.1.

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.

The NIM Code of Practicce also required:[14]

> *Chief officers will ensure that where these intelligence products impinge on an individual that the actions comply with the requirements of the Human Rights Act 1998, the Articles contained therein, and that the actions of the police force comply with the principle of 'proportionality'.*

9. The NIM Minimum Standards went further:[15]

> *Compliance with legal provisions such as the [Data Protection Act], [Police National Computer] 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.*
>
> *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.*

It added in a later section:[16]

> *All data systems should be subject to intrusive and proactive management supervision and quality assurance protocols.*

---

14 Centrex 2005, p.12, section 5.5.
15 NIM Minimal Standards, Element 4, section 57 – Guidance 2005, page 130.
16 NIM Minimal Standards, Element 6, section 80 – Guidance 2005, page 140.

10. In practice, this meant forces and units developed data review, retention and deletion (RRD) protocols to guide those maintaining intelligence databases. These were guided by protocols on the Management of Police Information (MoPI), which were codified in 2005. The 2005 Guidance noted that:[17]

> *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.*

It added

> *It will also ensure that the information management function of the intelligence unit is compliant with human rights, data protection legislation and regulatory codes.*

2005 Management of Police Information (MoPI)

11. A related document of relevance, also with statutory powers,[18] was the July 2005 Home Office Code of Practice on Management of Police Information, prepared by Centrex. It focused on information collected for policing purposes, including 'intelligence and personal data'. Such policing purposes were:[19]

> *a) Protecting life and property*
>
> *b) Preserving order*
>
> *c) Preventing the commission of offences*
>
> *d) Bringing offenders to justice, and*
>
> *e) Any duty or responsibility of the police arising from common or statute law.*

12. The significant section for our purposes is on the key principles for management of police information, which included

---

[17] Guidance 2005, section 6.3, page 50.

[18] HO CP-MoPI 2005, *ibid*. According to its prefix, it was made by the Secretary of State for the Home Department under sections 39 and 39A of the Police Act 1996 and sections 28, 28A, 73 and 73A of the Police Act 1997.

[19] 2005 MoPI Code of Practice section 2.2.

4.2 Requirement for police information

4.2.1 Chief officers must ensure that arrangements to gather police information ***comply with the principles of the National Intelligence Model.*** [emphasis added]

4.3 Grading and recording of police information

4.3.1 Information should be recorded where it is considered that it is necessary for a police purpose. Chief Officers must establish recording procedures in accordance with guidance issued under this Code.

4.3.2 Where appropriate and in accordance with guidance to be issued under this Code, the source of the information, the nature of the source, any assessment of the reliability of the source, and any necessary restrictions on the use to be made of the information should be recorded to permit later review, reassessment and audit.

4.3.3 Information should be assessed for reliability in accordance with guidance to be issued under this Code.

4.3.4 The format in which the information is recorded should comply with standards agreed and applied across the police service by means of guidance issued under this Code, to facilitate exchange of information and processing within standard police IT systems.

13. Sections 4.5 and 4.6 also spelled out that there should be policies to guide review, retention and deletion (RRD).

14. The relevance of this document is that it shows that police management of information was a statutory requirement, requiring this to be done within the framework that the National Intelligence Model set out.

2004 Guidelines for a Special Branch

15. In its 2004 update to the Guidelines for a Special Branch,[20] the Home Office set out the responsibilities of Special Branches in individual police forces, and how they should operate together. It notes the importance of national and regional bodies in co-ordinating this and mentions, in passing, the role of the NIM in facilitating this. It is probably more significant for the National Public Order Intelligence Unit, but it should be noted that the Metropolitan Police Special Branch – or Counter Terrorism Command, as it became in 2006 – was large enough to be considered a Regional Intelligence Cell in its own right. It had a responsibility to work with other Special Branches, not least through the Association of Chief Police Officers (Terrorism and Allied Matters (ACPO TAM) and its National Co-ordinator of Special Branch.

16. Relevant extracts are:

> *9. The Association of Chief Police Officers (ACPO/ACPOS) brings together police officers with senior officials from the Home Office, Ministry of Defence and intelligence agencies within a forum known as ACPO Terrorism and Allied Matters (TAM). This body is responsible for the development of national strategy and policy in relation to Special Branches, advising ministers and responding to consultation on issues of legislation and guidance. It is also responsible for the preparedness of the police service to investigate and respond to terrorist activity. Members of ACPO (TAM) represent the police service in a number of Government fora and provide a central point of strategic co-ordination for the police service.*
>
> *16. Special Branch Regional Intelligence Cells support the co-ordination of activity on a regional basis in accordance with the principles of the National Intelligence Model, which supports the identification and prioritisation of business. Working through Regional Special Branch tasking and co-ordination groups and other fora they provide regional strategic assessments of terrorism and other threats and develop regional responses to these issues in conjunction with police colleagues*

[20] SB Guidelines 2004, *ibid*.

and partner agencies. Special Branches require the support of other police specialists to perform their role. This will mean an on-going requirement for the assistance of local, regional and national police units.

27. Special Branches in most Forces will also have responsibility for gathering intelligence on those threats to public order and community safety from individuals motivated by racial hatred or political conviction where their specialist skills are able to support the wider investigation. In this regard, Special Branches will liaise with, and are supported by the National Public Order Intelligence Unit (NPOIU). The NPOIU provides critical support to Forces across the United Kingdom in maintaining a strategic overview of public order issues (other than issues such as organised football violence, which is the responsibility of the National Criminal Intelligence Service, Football Intelligence Unit). In addition, ***Special Branch will also gather intelligence on political and animal rights extremist activity, anti-globalisation and environmental extremism and seek to prevent criminal acts on persons or property targeted by such extremists.*** *Special Branches maintain links with all sections of the community and complement overall police responsibility to the public on relevant community safety issues. This relationship is parallel to the priorities of colleagues in other police service units.* [emphasis added]

C. National Intelligence Model (NIM)

1. The HM Inspectorate of Constabulary described the National Intelligence Model as:[21]

   a business model to ensure that policing is provided in a targeted manner through the development of information and intelligence. It facilitates the prioritisation of police activity…

2. In the following we draw on documents produced by police organisations that explain the NIM and how it was to be implemeted. The focus is on issues of governance and

[21] HMIC 2014, Annex C - Glossary, page 185.

tasking, and the structures/outcomes expected of a unit following the NIM. The model brought into statutory code in 2005 remains in force to today, although it has evolved.[22]

3. The NIM sets out a 'Tasking and Co-ordination Process', whose object is to lead to the 'production of intelligence products' and 'prioritised intelligence work'. As such the NIM is a top-down model; policy and strategy is set at a high level by senior police managers. Policy and strategy in turn inform the priorities and objectives required of the intelligence work delivered by the middle and lower level managers, whose job it is to organise collecting the intelligence. For the purposes of understanding the role of the NIM in the world of undercover policing, the precise nature of the intelligence produced is less significant than the processes that deliver it, and/or whether the processes were followed in line with NIM requirements. The NIM sets out what to put in place to measure the value of the information gathered.

4. The NIM 2005 views intelligence collection as a key function of policing which, in many cases, will be managed by a dedicated unit or cell. Management of intelligence then becomes a central issue, ensuring that it is both timely and useful, meeting requirements as tasked by the Control Strategy, see below, but also avoids information-gathering for its own sake. The deployment of intelligence-gathering resources has to be proportionate to the matter being investigated, well-managed and focused. Many tools of the NIM are designed to focus on meeting objectives while allowing teams to respond to emerging events.

5. Both the SDS and the NPOIU would have been defined as intelligence units, with a focus on 'domestic extremism'. The 2005 Guidance notes:[23]

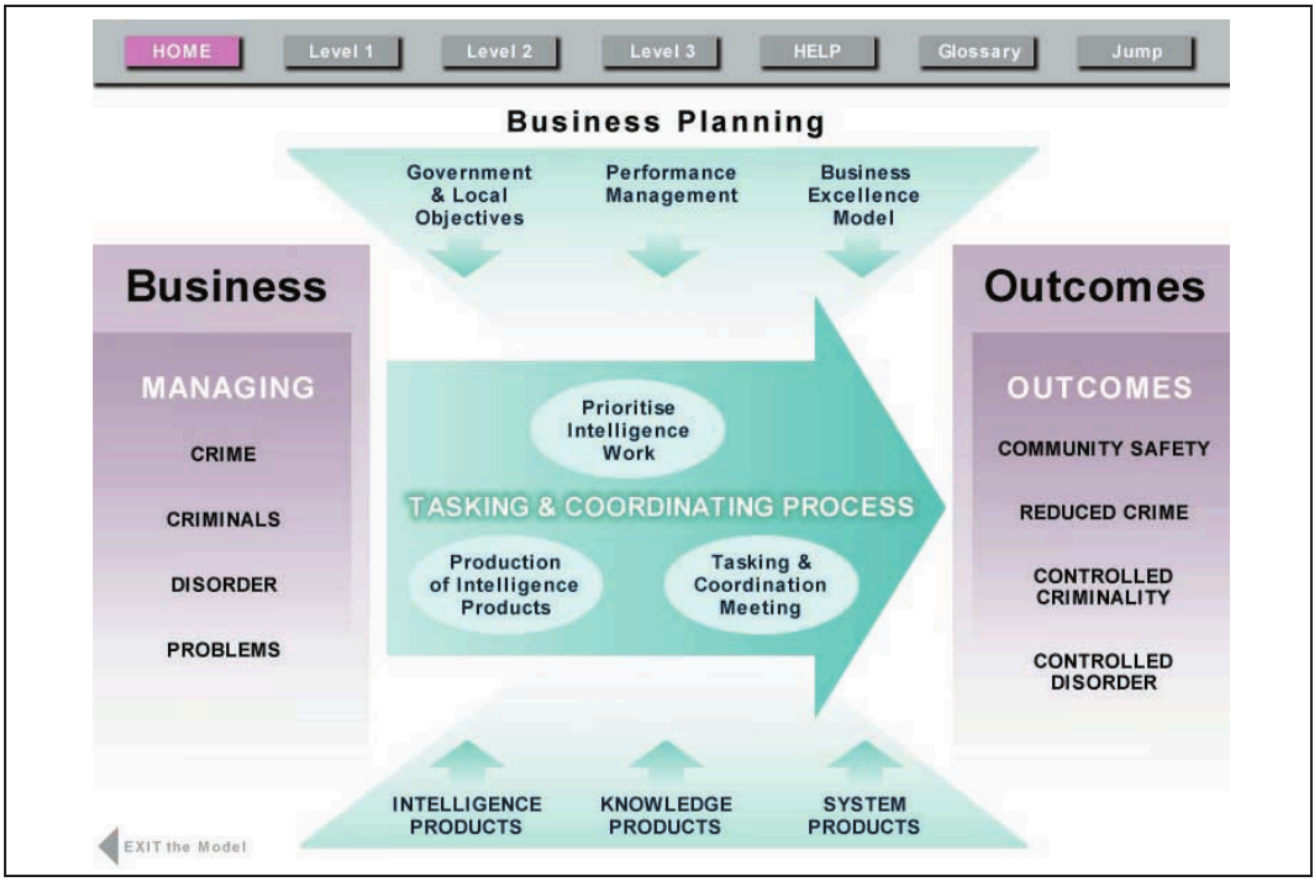
> *The primary function of the intelligence unit is to collect and receive information based on an identified intelligence requirement within prioritised or high risk areas determined by the T&CG control strategy. Rigorous management is required in order to avoid collecting intelligence on issues of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

[22] See Home Office, *National Intelligence Model Refresh* (presentation slide), 11 November, 2024. https://www.npcc.police.uk/SysSiteAssets/media/downloads/publications/disclosure-logs/npcc-central-office/2024/419-2024-session-05-intelligence-cb-nim-slide-29012025.pdf

[23] Guidance 2005, section 4.9, page 40.

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.

Tasking and Co-ordinating Process



6. According to the National Criminal Intelligence Service's guide to the NIM:[24]

The Tasking and Co-ordinating Process takes account of the business planning needs in the context of governmental and local objectives, performance management issues and business excellent [sic.]. It achieves its purpose by three activities:

[24] NCIS 2000, page 9.

- *Tasking and co-ordination group meetings – they are chaired by a senior manager of the command unit who has the authority to deploy the necessary resources and comprise of people with key functional responsibility for the planning and execution of the law enforcement effort.*
- *Production of the intelligence products – the creation of the intelligence products requires the same commitment to resources and direction from the tasking and co-ordination group as the drive for intelligence capability. Whilst there are only four key intelligence products – strategic assessments, tactical assessments, target profiles and problem profiles – their breadth is very extensive.*
- *Prioritisation of intelligence work – a major responsibility of the tasking and co-ordination group is to resource, direct and sustain intelligence capability. For intelligence work to be fully effective, it needs adequate assets and disciplines which ensure that intelligence activity follows the identified strategic and tactical priorities.*

To enable the tasking and co-ordinating process, knowledge products and system products underpin the work. Knowledge products are a range of products, either national or local which define the rules for the conduct of the business or the best practice by which skilled processes are completed. They contribute to the corpus of professional knowledge on how components within the model operate. System products are enabling facilities for the collection, reception, recording, storage and use of information. They provide the means by which data is held, retrieved and analysed.

7. The NIM emphases the role of management in setting the agenda for intelligence work. The Tasking and Co-ordination Meeting is central to this. By reference to the Strategic Assessment, see below, it creates and amends what is known as the Control Strategy. The meetings work on two levels. Infrequent meetings set the overall strategy, and more frequent ones focus on tactical issues required to deliver the outcomes required by the Control Strategy. Subsequent intelligence-gathering tasking is expected to be in

line with the priorities set out by the Control Strategy. Both strategy and tactics meetings are informed by their own specific intelligence assessments, with control strategy also taking on board wider/national priorities.

8. The Strategy Tasking and Co-ordinating Meeting was to meet at least every six months[25] and not less than yearly,[26] while the Tactical Tasking and Co-ordination Meeting would meet more regularly as it also had a reactive role, responding to new issues.[27] [28] According to the NIM Minimal Standards, the strategy meeting was to be chaired by the chair of the relevant police body and the tactical meeting could be chaired by the associated deputy chair.[29]

9. The Code of Practice also required an officer of sufficient rank to take part in the Strategic and Tactical Tasking Co-ordinating Group Meetings, and for that rank to be at least at seniority of an assistant chief constable or commander. Likewise, each force was to select an officer holding at least this rank to be responsible for implementing NIM policy and practice and ensuring appropriate procedures were in place that complied with NIM Minimum Standards.[30] Importantly, since 2003, this was also the rank that could authorise deploying undercover officers, following a decision made by ACPO.[31]

10. The NCIS guidelines note a number of roles for the Tactical Tasking and Co-ordination Meeting:

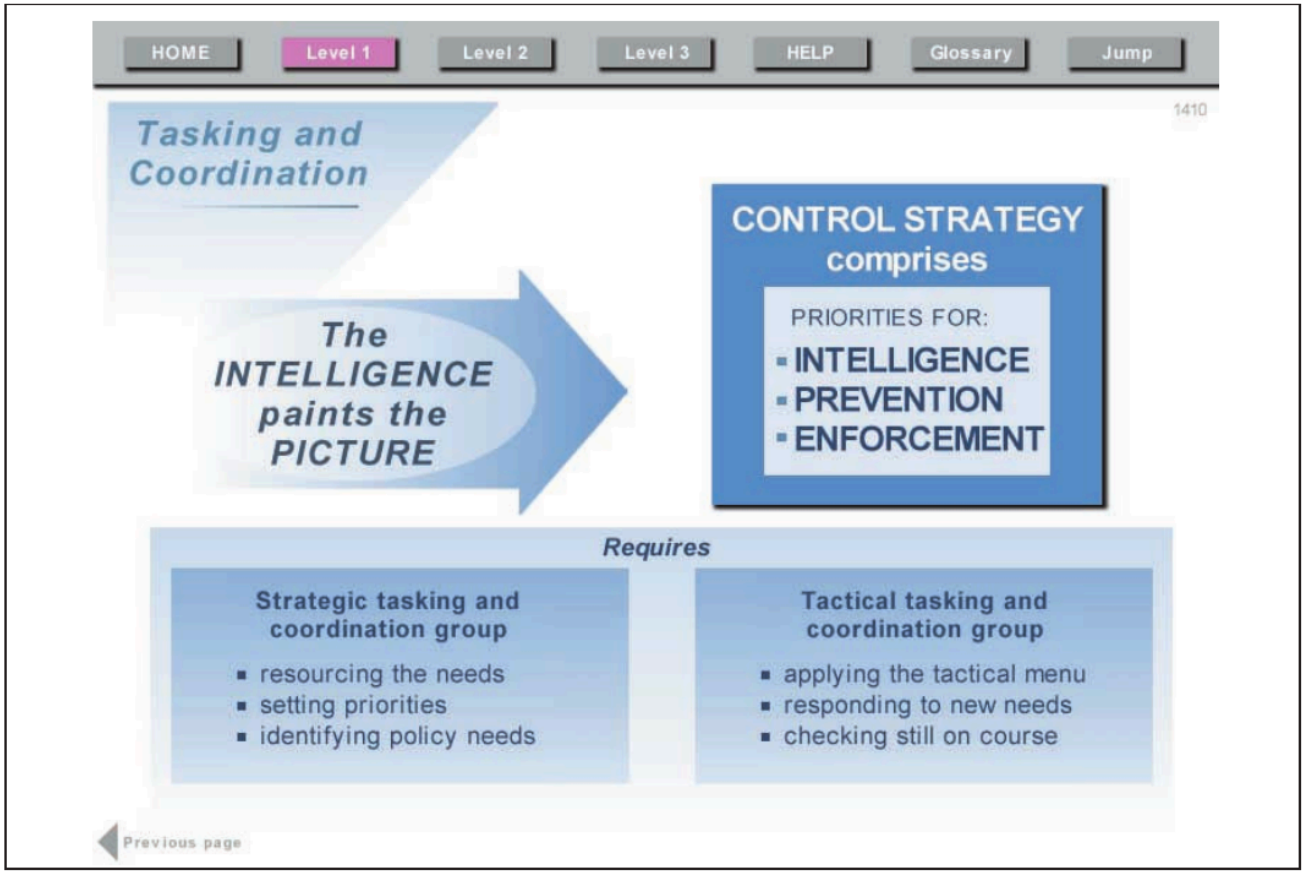
    a) '*demand accountability from those charged with investigating targets*'[32]

---

25 NIM Minimal Standards, Element 9, section 122 – Guidance 2005, page 154.
26 NCIS 2000, page 13.
27 Centrex 2005, page 10, section 4.2.
28 Daily management meetings, etc. were not to be considered at Tasking and Co-ordination Meeting as they are not driven by intelligence product review. NIM Minimal Standards, Element 9, section 123 – Guidance 2005, page 155.
29 NIM Minimal Standards, Element 4, section 44 – Guidance 2005, page 126.
30 Centrex 2005, page 7, section 3.2; page 10, section 4.1.2.
31 It was not until 2006, that the NPOIU came under the aegis of the National Co-ordinator for Domestic Extremism, a position held at Assistant Chief Constable rank by Anton Setchell. However, it appears that the NPOIU relied on authorisation for undercover deployments from senior officers of relevant rank from regional police forces or the MPS in any case.
32 NCIS 2000, page 14.

b) '*monitor the volume and quality of intelligence to and from operational staff and that is supplied to the tasking and co-ordination group*'.[33]

Control Strategy



11. The NIM guidance documents state that the Control Strategy is:[34]

a document that sets the agenda for intelligence, prevention and enforcement priorities

and provides a 'focus for policing activities', such that:[35]

---

33 NCIS 2000, page 15.
34 Centrex 2005, page 10, section. 4.1.1.
35 NIM Minimal Standards, Element 6, section 89 – Guidance 2005, page 143.

Police forces and BCUs should be able to demonstrate that the tasking for information and data collection is focused on their respective control strategies.

This included impact/benefit assessments:[36]

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.

12. Related to the Control Strategy is the 'Intelligence Requirement' – 'the identified gap between what is known and what is not known'.[37] Both Control Strategy and Intelligence Requirement had to be sanctioned by either the Strategic Tasking and Co-ordination Group (ST&CG*)* or the Tactical Tasking and Co-ordination Group (TT&CG) meetings.[38] Often, in the guidance, these are considered jointly and referred to as just the Tactical & Co-ordination Group (T&CG).

13. Management of these followed a top-down process:[39]

The meeting is 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.

14. For more immediate implementation, and to allow reaction to events, the NIM set out Tactical Plans and Trigger Plans:

    a) Tactical plans: [40]

[36] NIM Minimal Standards, Element 6, section 94 – Guidance 2005, page 144.
[37] NIM Minimal Standards, Appendix 4: Glossary – Guidance 2005, page 196.
[38] NIM Minimal Standards, Element 9, section 119-120 – Guidance 2005, page 154.
[39] NIM Minimal Standards, Appendix 4: Glossary – Guidance 2005, page 201.
[40] NIM Minimal Standards, Element 9, section 128 – Guidance 2005, page 157.

Tactical plans must be developed by owners appointed and tasked by the TT&CG.

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.

b) Trigger Plans:[41]

Trigger plans allow for instant, controlled and co-ordinated response to particular events, incidents or crime types.

Trigger plans must be in place to direct response capability to undertake certain tasks on the occasion of a particular event or circumstance occurring.

15. The NIM also required a number of review processes:

a) Results analysis and review. This was used to 'assess success of actions endorsed' by a Tactical and Co-ordination Group, and:[42]

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.

b) Monitor and review of Regulation of Investigatory Powers Act (RIPA) authority. According to the NIM Minimal Standards the 'usefulness of information gained as a result of RIPA authorities' requires review, with policies needed 'to guide this process'. As such:[43]

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

---

41 NIM Minimal Standards, Element 10, section 129 – Guidance 2005, page 158.
42 NIM Minimal Standards, Element 11, section 130 – Guidance 2005, page 159.
43 NIM Minimal Standards, Element 11, section 131 – Guidance 2005, page 159.

c) Audit trail:[44]

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.

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.

Intelligence products in the NIM

16. The NIM states:[45]

Its design reflects the principle that intelligence work is of no value if it does not result in intelligence products for managers and others; products which help decision making and guide investigations or deployments in the law enforcement effort. At the heart of the tasking and co-ordination process at all levels of the model are the key intelligence products. These are the 'deliverables' by which intelligence led policing can be implemented and its impact measured in terms of crime reduction, arrests, disruptions and enhanced community safety.

17. On intelligence itself, the 2005 guidelines emphasise that: [46]

All intelligence should be actionable. Intelligence is of no value if it does not result in defined intelligence products.

18. Management ownership of intelligence products is allocated to the chief officers, relevant unit commanders and senior intelligence managers. Directors of intelligence

[44] NIM Minimal Standards, Element 11, section 134 – Guidance 2005, page 160.
[45] NCIS 2000, page 16.
[46] Guidance 2005, section 7.1, page 56.

and intelligence managers are responsible for delivery of intelligence products and must not rely on junior officers and/or analysts to compile them.[47]

19. There are four intelligence products identified in the NIM:

    i. Strategic Assessments

    ii. Tactical Assessments

    iii. Target Profiles

    iv. Problem Profiles.

20. The **Strategic Assessment** informs the Control Strategy and high-level meetings, and has a longer-term view that takes into account wider objectives set by the force or by the government. It sets control strategies, business planning and resource allocation and identifies long-term issues in an area, and projections for 'growth in criminality'.[48] Strategic Assessments were to be produced on a bi-annual basis, with three-monthly reviews to ensure they were current.[49]

21. The **Tactical Assessment** informs the tactical tasking and co-ordination meeting. It does this by identifying short-term issues that require prompt action to resolve, and monitoring how the objectives set by the control strategy are being met. It has more of a focus on the current situation.[50] According to the Code of Practice, Tactical Assessments were required and:[51]

    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 will include appropriate interventions for intelligence gathering, enforcement and prevention activities; the

---

47 NIM Minimal Standards, Element 6, section 103 – Guidance 2005, p. 149. See also Guidance 2000, section 8.17, page 72.

48 Centrex 2005, page 11, section 5.1.2; NCIS 2000, page 17.

49 Centrex 2005, page 11, section 5.1.1.

50 NCIS 2000, page 17.

51 Centrex 2005, page 11, section 5.1.2.

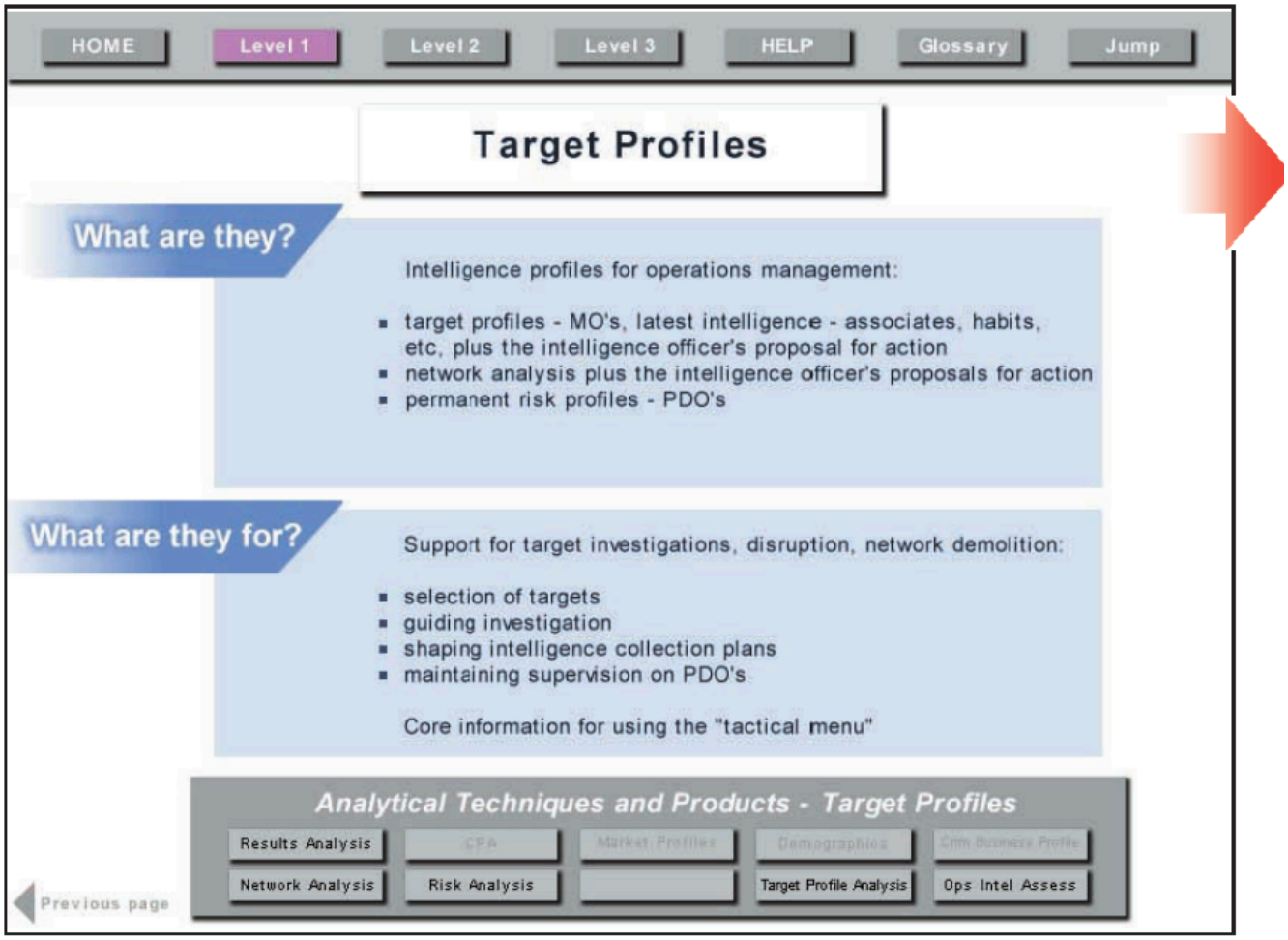
identification of emerging patterns of crime and incidents; and a performance assessment.

22. The **Target Profile** is:[52]

[person/s-specific] and contains sufficient detail to initiate a target operation or support an ongoing operation against an individual or networked group of individuals. It comprises as complete an information package as possible in the light of the available intelligence.[…] On the basis of the intelligence revealed, the target profile includes an interpretation of the best course of action and proposals to fill the gaps in the intelligence picture.

23. The following graphic comes from the NCIS 2000 guide to the NIM and sets out the content of the Target Profile. This includes information such as habits of the 'target'. Further information on the objectives and content of a Target Profile is set out in the 2005 Guidance, which notes that it should contain a personal record, intelligence-collection plan, justification and ratification by the Tactical Tasking and Co-ordination Group.[53]

[52] NCIS 2000, page 18.
[53] Guidance 2005, section 8.13, page 69.



Product	Aim	Purpose	Content
Target Profile	To provide a detailed picture of the (potential) offender and his associates for subsequent action.	To assist operational management in selecting targets, guiding investigations, shaping plans and maintaining supervision	Personal record[1] Criminal record[2] Financial profile Network/associations report Communications report[3] Transport report Surveillance appraisal[4] Intelligence gaps

24. **The Problem Profile**:[54]

> *A problem profile identified established and emerging crime or incident series. It also identifies established and emerging crime and incident 'hotspots' together with the opportunities for preventive work revealed by the intelligence.*

25. The NIM Minimum Standards placed restriction on the nature of the profiles:[55]

> *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.*
>
> *[...]*
>
> *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.*
>
> *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.*

26. Further information on the objectives and content of a Problem Profile is set out in the 2005 guidance, which notes that it should contain reasons for targeting the problem, operational objectives, intelligence-collection plan, justification and ratification by the Tasking & Co-ordination Group.[56]

27. The 2005 guidance also sets out the selection criteria for creating Target or Problem Profiles:

---

54 NCIS 2000, page 18.
55 NIM Minimal Standards, Element 6, section 101 – Guidance 2005, page 148.
56 Guidance 2005, section 8.15, pages 70-71.

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.

Prioritised intelligence work – the intelligence units

28. An intelligence unit provides the information used to form the four intelligence products. Its work is determined by the Control Strategy, which sets 'operational intelligence priorities'.[57] This can include use of Confidential Human Intelligence Sources (CHIS – both undercover officers or informants) or other covert means to fill in the knowledge gap. The NCIS notes:[58]

    The prime function of the intelligence unit is the collection and reception of data, against the background of the priorities set by the tasking and co-ordination group in the control strategy. The unit will only deliver the intelligence products that lead to the greatest impact if its work is kept on course, and strong management is required to prevent its wandering,and collecting intelligence on issues of secondary importance. The law enforcement environment is, however, a fast moving one in which matters requiring urgent attention are frequently likely to come to notice.

29. However:[59]

    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.

    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

[57] NCIS 2000, page 20.
[58] NCIS 2000, page 22.
[59] Guidance 2005, section 7.3, page 57.

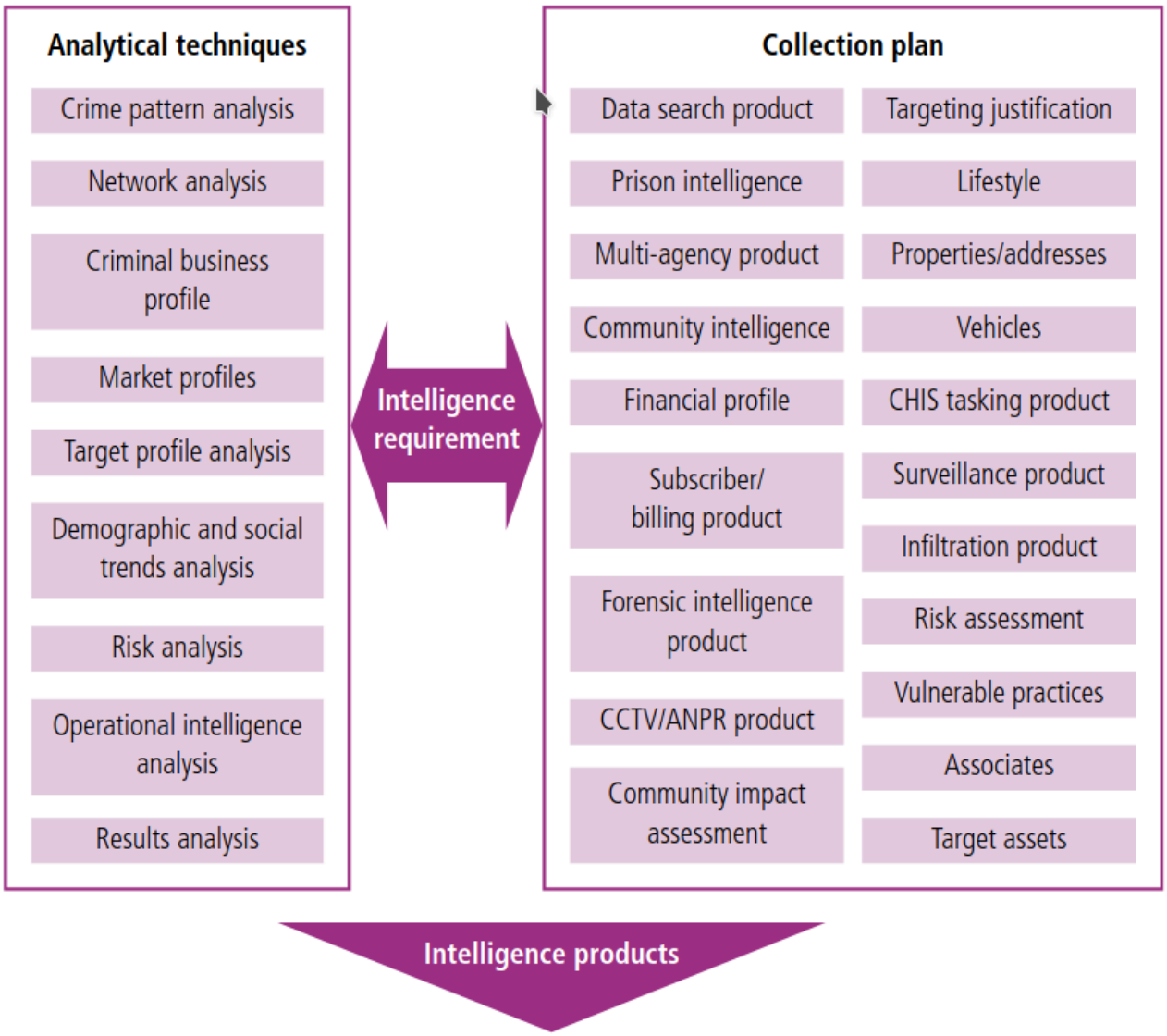
the intelligence function and this responsibility often falls to the Intelligence Manager. ***Mechanisms must be established to ensure that any intelligence material (including that provided by sources) can be researched and submitted to the disclosure officer, particularly where such information could undermine the prosecution or assist the defence.*** [emphasis added]

30. In order to fulfil the intelligence products required under the NIM, intelligence collection needs to take place, drawing on a variety of sources. This includes material gathered through covert tactics such as undercovers, which may be resourced on a national level, such as the NPOIU. This requires clear tasking protocols between the intelligence cells and the units delivering the covert tactics, including resource allocation protocols.[60]

31. The NCIS guidance notes that, among other issues, the following needed to be taken into account when training staff:[61]
    a) Current legislation
    b) The ACPO Crime Committee Intelligence Strategy
    c) The national codes of practice for covert law-enforcement techniques and related manuals of 'tradecraft' standards and similar issues
    d) The role of the national working groups on standards in covert techniques
    e) Local protocols governing exchanges of information and joint working with other agencies
    f) Current national training requirements, for example for informant handlers and analysts.

[60] Guidance 2005, section 7.6, pages 58-59
[61] NCIS 2000, page 24.

FIGURE 3 Intelligence Collection Planning



Analysis reports

32. The NIM notes a variety of analyses that can be built from processed intelligence, which then inform strategy and action. Key ones are listed below:

33. **Network Analysis**:[62]

> *Network Analysis describes not just the linkages between people who form criminal networks, but also the significance of the links, the roles played by individuals and the strengths and weaknesses of a criminal organisation. Network analysis needs therefore to examine the key attributes and functions of individuals within the network together with financial and communications arrangements. This type of analysis closely complements target profiling. At the strategic level, network analysis provides a detailed understanding of the scale and seriousness of the threat posed by criminal groups, enabling the appropriate priority to be attached to dealing with them. At the tactical level it will distinguish the most important networks to tackle* ***as well as how best to go about undermining them****. The analyst's assessment of the continuing resilience of the network will be an important consideration in measuring the success of the law enforcement attack.* [emphasis added]

34. **Target Profile Analysis**:[63]

> *Target profile analysis embraces a range of analytical techniques which aim to describe the criminal, his criminal activity, lifestyle, associations, the risk he poses, his strengths and weaknesses in order to give focus to the investigation targeting him. As with all analytical techniques, the profile will also enable the analyst to indicate where the gaps in knowledge exist. This enables the intelligence requirement to be identified and sources, human and technical, to be deployed to meet the requirement. In some cases the profile analysis will require access to a very wide range of source data including publicly available records,police and law*

[62] NCIS 2000, page 34.
[63] NCIS 2000, page 36.

enforcement records, information from public authorities and utilities,information from commercial organisations, from open sources and informants in order to provide the fullest possible picture. The analysis will include appropriately detailed relevant information about associates and lifestyle. The profile should also reveal techniques which have worked against the target in the past and an assessment of the target's capability in protecting himself from investigation and countering covert techniques.

35. **Operational Intelligence Assessment**[64]

The purpose of this form of evaluation of incoming intelligence is to maintain the focus of an operation on the previously agreed objectives, particularly in the case of a sizeable intelligence collection plan or other large scale operation. A plan initially directed against a particular group or individual will invariably lead to other groups and individuals which, in turn, have further connections. As a result the original plan risks being diverted to pursuing leads and linkages which do not follow the set objective. The operational intelligence assessment tries to provide real time evaluation of, and research into, all incoming data connected with an operation, together with an analysis of other events and discoveries connected with the targets. The result should continually be compared with the objectives of the original collection plan. This will help identify gaps in and priorities for the operation's intelligence effort and ensure the continuing alignment of the work.

36. Further information on Operational Intelligence Assessments appears in the ACPO Practice Advice on Tasking and Co-ordination. The NIM Minimum Standards noted they sought to focus investigations to:[65]

Prevent mission creep;
Identify priorities for the operation's intelligence effort;
Focus intelligence gathering;
Inform resource decisions;

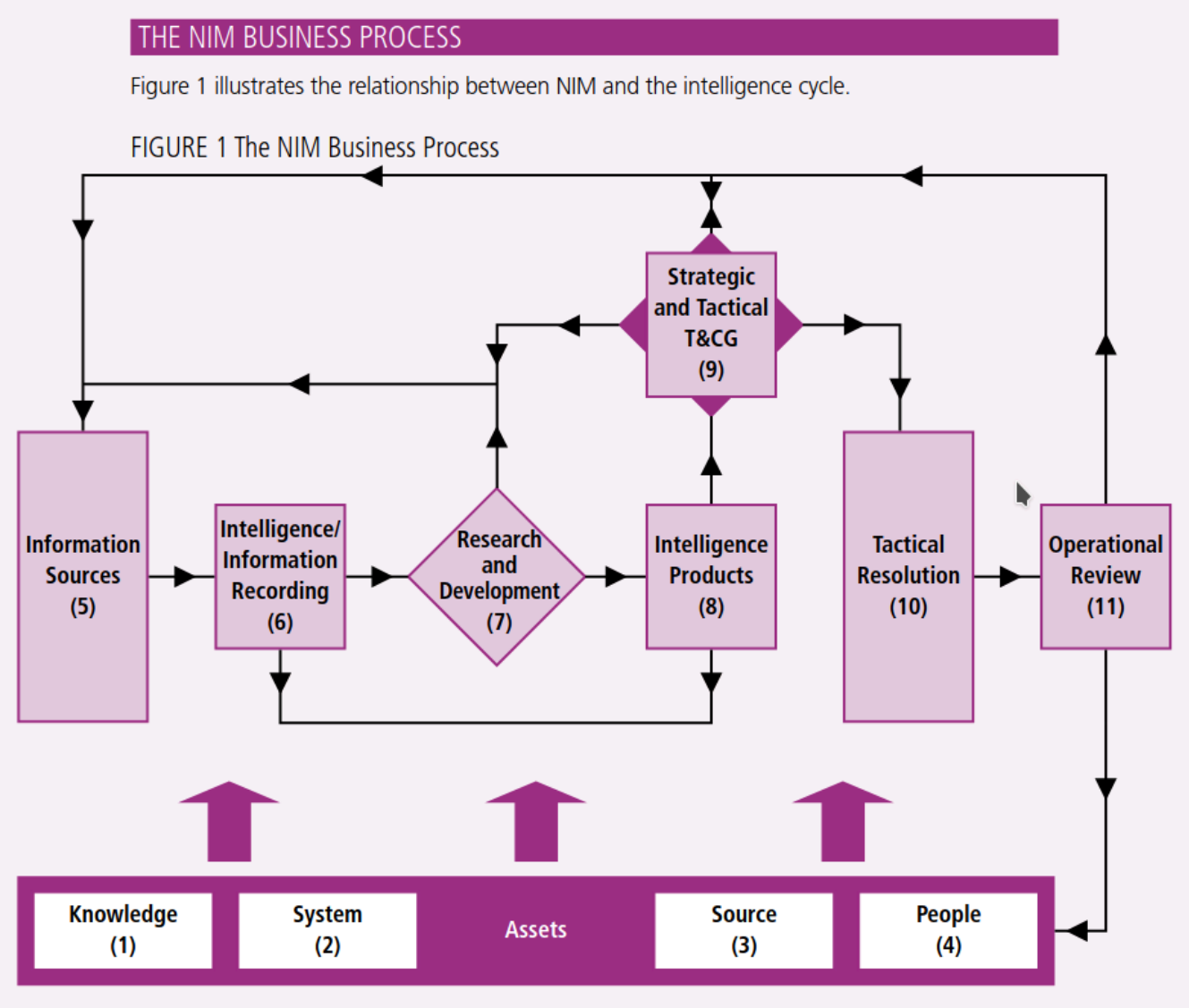
64 NCIS 2000, page 36.
65 NIM Minimal Standards, Element 8, section 108 – Guidance 2005, page 150.

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.

Tactical management and review

37. Further elements for the practical working of the NIM are noted in the 2005 Guidance Notes, the Tactical Resolution and Operational Review. In line with the Strategic and Tactical Tasking and Co-ordination (ST&CG) meeting, the tactical manager decides on tactics to be used. The Operational Review provides feedback to the ST&CG meeting on the task and what outcomes there were, including 'anything else of intelligence value gained'. [66]

[66] Guidance 2005, page 18.



Knowledge Assets

38. The NIM is clear that police applying the model need to ensure they have access to 'knowledge assets' and up-to-date information relating to relevant codes of practice/manuals of guidance, policy and procedure and legislation. All staff and officers must have access to such knowledge repositories. This is for all relevant

material, not just NIM, and involves communicating control strategy and intelligence requirements.[67]

39. It also required that the following sets of policy were in place and being adhered to:[68]
    - Intelligence strategy
    - CHIS policy
    - Tasking and co-ordination policy.

CHIS / covert assets within the NIM

40. To fill the intelligence gaps in the Intelligence requirement, sources of information are used, including surveillance, CHIS and undercover officers.[69] As these carry cost implications, their use must meet the objectives of the Control Strategy. Likewise, their use must be proportional.[70] The 2005 guidance sets out how the Control Strategy sets the terms for such use:[71]

    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. 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.

41. The NIM Minimum Standards noted: [72]

---

67 NIM Minimal Standards, Element 1, sections 1-6, 9-10 – Guidance 2005, pages 111-113, 114.
68 NIM Minimal Standards, Element 1, section 5 – Guidance 2005, page 113.
69 Guidance 2005, section 3.1, page 32.
70 Guidance 2005, section 3.4, page 32.
71 Guidance 2005, section 3.5, page 33.
72 NIM Minimal Standards, Element 3, section 34 – Guidance 2005, page122.

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.

It added later:[73]

The integrity of any intelligence system relies on ethical processes and legislative compliance.

There must be a policy and resources in place to enable hot intelligence assessments, human rights compliance, officer safety and duty of care considerations.

42. When it came to undercover and/or test purchase operatives, the unit deploying them needed to rely on the standards set out in the following documents:[74]

    a) ACPO and HMCE (2003). Manual of Standards for the Deployment of Test Purchase and Decoy Officers; and

    b) ACPO and HMCE (2003). Manual of Standards for the Deployment of Undercover Officers.

43. The NIM Minimum Standards noted that there was a duty of care and protection towards covert assets. In the same section, it also noted:[75]

    Sterile Corridor
    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.*** [emphasis added]

44. It also subsequently noted in relation to covert deployments, including surveillance:[76]

---

73 NIM Minimal Standards, Element 6, section 71 – Guidance 2005, page 138.
74 NIM Minimal Standards, Element 3, section 36 – Guidance 2005, page 123.
75 NIM Minimal Standards, Element 2, section 12 – Guidance 2005, page 117.
76 NIM Minimal Standards, Element 3, section 38 – Guidance 2005, page 123.

Information or intelligence obtained from covert deployments [...] 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.* [emphasis added]

45. The NIM Minimum Standards specifically addressed the management of authorities for Covert Human Intelligence Sources such as undercover officers:[77]

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.*

[77] NIM Minimal Standards, Element 4, section 46 – Guidance 2005, page 126.

46. The 2005 guidance is somewhat inconsistent in its use of the term Covert Human Intelligence Source (CHIS); it can refer solely to informers, to undercover police officers, or to both.[78] The relevant legislation, the Regulation of Investigatory Powers Act 2000 (RIPA) does not distinguish between the two types of 'sources'. The following material from the 2005 guidance relates to CHIS' generally.[79]

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.

3.13 DEDICATED SOURCE UNITS

---

78 For example Section 4.9 (page 41) of the 2005 Guidance discusses the role of CHIS Control and CHIS Handlers, however appear to focus entirely on informants rather than undercovers, so have not at this stage, been included here

79 Guidance 2005, sections 3.12-3.13, page 35.

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. […] 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.

47. The 2005 Guidance also calls for 'intrusive review' of CHIS assets, including to ascertain 'whether they are… providing information that meets the intelligence requirement'.[80]

Management Specialists

48. The National Intelligence Model viewed its work as leadership-driven, and dependent on senior management having sufficient knowledge and specialisms:[81]

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.

---

80 Guidance 2005, section 3.15, page 35.

81 NIM Minimal Standards, Element 4, section 62 – Guidance 2005, page 132.

A number of specialist management roles are identified, including intelligence managers and CHIS controllers. Another role is the tasking and co-ordination action manager, whose job is to co-ordinate actions resulting from the Tasking and Co-ordination Group meetings.[82]

49. **Intelligence manager.** From the NIM Minimal Standards:[83]

> *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.*

50. The intelligence manager will be of appropriate rank,[84] will have attended a nationally accredited intelligence manager's training course and their responsibilities will include:

- *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*

---

82 Guidance 2005, section 4.12, page 42.
83 NIM Minimal Standards, Element 4, section 48 – Guidance 2005, page 127.
84 Usually inspector at BCU level or superintendent at force Level. See Guidance 2005, section 4.6, page 39.

- *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.*

51. **CHIS controller and designated deputy CHIS controller.** These roles are designated within the NIM Minimal Standards:[85] [86]

> *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.*
> *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*

52. **Operational security officer (OPSY) and CHIS handling.** The OPSY is considered good practice for high-risk areas such as CHIS. It is noted that further information on

---

85 NIM Minimal Standards, Element 4, section 49 – Guidance 2005, page 127.
86 Non-undercover sources are handled a little differently. See for example, NIM Minimal Standards, Element 2, section 50 – Guidance 2005, page 128.

their role is given in the ACPO Practice Advice on Resources and People Assets of NIM, which URG has not obtained.[87]

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.

[87] Guidance 2005, section 2.16, page 28.

Other matters

53. ***Level 2.*** Sometimes the 5x5x5 forms make reference to NIM Level 2. The levels are defined as:[88]

> *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*
>
> *Level 3 represents the most serious and organised crime.*

Most NPOIU undercover work is at level 2 as it is targeting groups that are working on a regional level, not just within a specific policing force's district. The NPOIU is part of the 'additional resources', providing assistance to local police forces. This sits clearly within its remit.[89] The NCIS guidance about this emphasises the multi-agency approach as core to issues classified at a level 2 in the NIM:[90]

> *At Level 2 and three [sic], tasking and co-ordination are effected by multi-agency groups, regional or national. The same requirements arise about setting priorities and overseeing the application of the tactical menu which, at the higher level, predominantly concerns targeting criminal and criminal organisations. Level 2 tasking and co-ordination is concerned to identify the regional criminal activity which can only be tackled on a collaborative basis. The provision of a regional strategic overview is only possible when force and agency intelligence products are of such a standard that they can be aggregated into the bigger picture. NCIS plays a major role in bringing the strategic overview into being in partnership with force intelligence bureaux and agency intelligence units.*

---

[88] Centrex 2005, page 12
[89] See under the 2004 *Guidelines for a Special Branch*, above.
[90] NCIS 2000, page 15.

54. ***Authorising systems.*** The NIM Minimum Standards has a specific section for authorising target selection which requires a standardised system that met human-rights requirements:[91]

> *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.*
>
> *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*.

55. ***Emerging situations.*** The guiding documents make allowances to manage emerging or urgent situations at a tactical level. The 2005 Guidance notes:

> *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: [...]*
>
> - *Spontaneous or planned public disorder*
>
> *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.*

[91] NIM Minimal Standards, Element 6, section 78 – Guidance 2005, page 139.

D. Guide to 5x5x5 forms

TEMPLATE 1

NOT PROTECTIVELY MARKED UNTIL COMPLETED

GPMS	PROTECT ☐	RESTRICTED ☐	CONFIDENTIAL ☐	SECRET ☐

5x5x5 Information Intelligence Report Form A

ORGANISATION AND OFFICER				DATE/TIME OF REPORT	
INFORMATION/INTELLIGENCE SOURCE/INTELLIGENCE SOURCE REF NO. (ISR)				REPORT URN	
SOURCE AND INFORMATION/INTELLIGENCE EVALUATION TO BE COMPLETED BY SUBMITTING OFFICER					
SOURCE EVALUATION	A Always Reliable	B Mostly Reliable	C Sometimes Reliable	D Unreliable	E Untested Source
INFORMATION/ INTELLIGENCE EVALUATION	1 Known to be true without reservation	2 Known personally to the source but not to the person reporting	3 Not known personally to the source, but corroborated	4 Cannot be judged	5 Suspected to be false
REPORT					
PERSON RECORD:		DoB:		NIB CRO:	
OPERATION NAME/NUMBER:				S	I H

INTELLIGENCE UNIT ONLY					
HANDLING CODE To be completed by the evaluator on receipt and prior to entry onto the intelligence system. **To be reviewed on dissemination.** ☐	1 **Default:** Permits dissemination within the UK Police Service AND to other law enforcement agencies as specified ☐	2 Permits dissemination to UK non-prosecuting parties ☐	3 Permits dissemination to (non-EU) foreign law enforcement agencies ☐	4 Permits dissemination within originating service/agency only: specify reasons and internal recipient(s) Review period must be set ☐	5 Permits dissemination but receiving agency to observe conditions as specified ☐
5x5x5 REVIEWED BY: RE-EVALUATED: Yes ☐ No ☐		CROSS-REF URN:		TIME/DATE OF REVIEW:	
DISSEMINATED TO:			PERSON DISSEMINATING TIME/DATE:		
DETAILED HANDLING INSTRUCTIONS:			PUBLIC INTEREST IMMUNITY:		
INPUT ON TO AN INTELLIGENCE SYSTEM Yes ☐ No ☐					
SIGNATURE (PAPER COPY):					
GPMS	PROTECT ☐	RESTRICTED ☐	CONFIDENTIAL ☐	SECRET ☐	

1. As previously mentioned, information is filed via a document known as a 5x5x5 form, which evaluates it according to preset criteria to determine whether the report can be considered ‘intelligence’ and brought into the system. To facilitate this, the form sets out different fields and tables that had to be filled in by those managing the information. The form had a number of variations and clearly evolved over time, according to need,

but in general they were relatively consistent in content for the period under consideration. They were later replaced by the 3x5x2 intelligence system.[92]

2. It is important to note that these are filled in by the CHIS' handlers in the intelligence/undercover unit, rather than by the undercovers themselves.

3. To confuse matters, the SDS made use of 'Information Reports' that were not designated as 'intelligence', but recorded what the SDS undercovers had passed on to their handlers to turn into intelligence for onward dissemination. However, they would often have a note grading the intelligence Bx2x5, for more on this , see below.

4. Likewise, late-1990s forms that pre-date the formal establishment of the NIM, used a less developed grading system, but SDS undercover-police reports effectively reflect the same system, often being given Source Code: B and Information Code: 2, which corresponds to the schema described below.

5. A Centrex/National Policing Improvement Agency document provides a good guide to compiling such a form.[93] Here, we extract the information most relevant to the reports which are appearing in disclosure around undercover policing. The quotes in the following are taken from this document.

6. Guide to fields

    a) **GPMS**: Government Protective Marking Scheme. The cross-government scheme for classifying documents' security level.[94] The levels were Protect, Restricted, Confidential, Secret and Top Secret. From what we have seen to date, undercover reports appear to be classified between Restricted and Secret.[95] For example, to be

[92] See https://www.college.police.uk/app/intelligence-management/intelligence-report
[93] How to Complete a 5x5x5 Form and Relevant Supplements, https://www.spycopsresearch.info/sites/default/files/2024-10/how-to-complete-5x5x5-form.pdf Metadata show it was created in 2013, but it is believed to date from much earlier. See for example, the NPIA / ACPO Guidance on Management of Policing Information (Second Edition), 2010, https://www.spycopsresearch.info/sites/default/files/2025-03/management-of-police-information-mopi-guidance-2010.pdf
[94] This scheme has also evolved over time. For the period in question, the guidance for police would be found in *ACPO and ACPOS Handling of Protectively Marked Material − A Guide for Police Personnel*, October 2007.
[95] See Sections 5.9 to 5.16 of the Manual of Standards for the Deployment of Undercover Officers (2003), unpublished.

marked Secret would mean satisfying criteria that disclosure of the document would:[96]

- *... seriously prejudice public order or individual security or liberty.*
- *Cause serious damage to the operational effectiveness or security of UK or allied forces or the continuing effectiveness of highly valuable security or intelligence operations.*

Whereas Restricted could include:

- *Prejudice individual security or liberty*
- *Cause damage to the operational effectiveness or security of UK or allied forces or the effectiveness of valuable security or intelligence operations*
- *Work substantially against national finances or economic and commercial interests*
- *Impede the investigation or facilitate the commission of serious crime*
- *Seriously impede the development or operation of major government policies.*
- *Shut down or otherwise substantially disrupt significant national operations.*

b) **Intelligence / Information Source Reference (ISR)**: a code identifying the person providing the information, often the code name or number for the undercover. In Mark Kennedy's case, this was UCO133, for instance, but the reference could also be the two-letter code for the SDS undercovers.

c) **Unique Reference Number (URN)**: to be added to the submitted report to allow an audit trail of received information.

Should editing or sanitisation be required, the Intelligence Unit will create a second, sanitised version of the report, ensuring the removal of the source details and will allocate a further URN to this report. The second report will then

[96] See, for example: https://pdacounterfraud.co.uk/wp-content/uploads/2023/07/Nottinghamshire-Police-Government-Protective-Marking-Scheme-Guidance.pdf

be cross referenced to the original URN to continue the audit trail of received information. The original report must be retained and stored securely to ensure that source information is not revealed.

d) **Source Evaluation**:

> *the assessment given to the person, agency or technical equipment providing the information/intelligence. The source reliability is assessed initially by the person recording the information…*

These were graded A to E. A meant always reliable and usually referred to technical sources, e.g. listening devices, DNA, and so on. B was mostly reliable and appears to have been the rating given most commonly to information from the undercovers. A B rating meant:

> *Information has been received from this source in the past and in the majority of instances has proved to be reliable.*

e) Information/Intelligence Evaluation: this was the evaluation by the person making the report to rate how reliable the intelligence was. It was instructed that:

> *The evaluation will involve using objective professional judgement, and t**he value of the information must not be exaggerated to encourage that action be taken**. The assessment of the reliability of the information will be based on the person recording it and their knowledge of the circumstances at that time.* [emphasis added]

f) As with source evaluation, this is done on a scale of 1 to 5. 1 was for material that was unquestionably accurate – generally for technical surveillance such as listening devices – while 5 was for information suspected to be false. Much of the reporting by undercovers appears to be classed as 2:

> *Information under this grading is believed to be true by the source although is not personally known to be so by the person recording the information. The source has first hand knowledge of the information. **Care must be***

taken to differentiate between what a source knows to be a fact and what a source reports they have heard or been told*.* [emphasis added]

g) The body of the information being passed on is in the main part of the form. The guidance noted that separate items of information, even those coming from the same source, should be filed separately:

> *Items of information from the same source but concerning totally different matters should be recorded on separate information/intelligence reports. Where a single source of information provides several items of information relevant to the same issue, separate 5x5x5 reports should be submitted. This is to avoid a single source being identified who may be the only one to know the sum total of the information submitted. This is particularly important when intelligence reports are prepared from a sensitive source, for example, CHIS or a technical device. The purpose of this procedure is to ensure that an adverse decision on 'disclosure' of a 5x5x5 would only put a single sensitive source or a single record at risk of compromise.*

The code on the right-hand side, "S, I, H" refers to the three strands of the 5x5x5 intelligence grading. **S** is **Source**, **I** is **Information Evaluation** and **H** is **Handling,** which comes next.

h) Handling:

> *Handling codes are designed to provide an initial risk assessment prior to recording material into an intelligence system. They allow recording officers and others involved in the dissemination of intelligence material to easily record their decisions on the suitability or otherwise of sharing the intelligence with other parties.*

Usually, for undercover police of the NPOIU or SDS, the handling ranks at grade 5: This meant the material could be disseminated but there was a condition applied. Usually the forms specified which bodies could receive this information, for example

‘C’ Squad and relevant heads of Special Branch (HSB) ‘for information only’. Most added the line

> *Please refer to originator where further dissemination is considered or where executive action is likely.*

The guidance noted:

> *In cases where handling codes ‘4’ or ‘5’ are considered necessary, a Risk Assessment Form ‘C’ must be completed. The Form ‘C’ should be attached to the 5x5x5 when it is submitted. Unless concerns are raised, the intelligence unit will review the information/intelligence report and apply the appropriate handling code. It is, therefore, important that Form ‘C’ contains a comprehensive evaluation of the risk; as without this, the intelligence unit may lack the information to make an appropriate determination of the handling code.*

Risk Assessment Form C

FOR THE USE IN DISSEMINATION OF INFORMATION/INTELLIGENCE

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

i) The guidance also noted the need for audit trails for the reports, and for review by the officer responsible for quality assurance in the intelligence unit.

> *Reliance should be placed on the person submitting the report with regards to the source reliability and information evaluation unless there is an obvious discrepancy or incompatibility. If further clarity or corroboration is required on any issue, contact should be made with the person who submitted the report.*
>
> *If the intelligence unit needs to sanitise the 5x5x5 before dissemination or inputting into an intelligence system, a new 5x5x5 should be submitted. The new report should not only be given a new unique reference number (URN) but also be cross-referenced to the original report to identify provenance and provide an audit trail. The original report should be retained but stored securely to ensure that the source is not revealed.*

j) **Sanitisation**: the guidance also noted the need to take care that the phraseology of the reports would not indicate how the information had been gathered:

> *Reports should be sanitised for onward transmissions by removing material which explicitly or implicitly identifies a source or police methodology. The text (as opposed to the source reference) should give no indication of the nature of the source, whether human or technical or the proximity of the source to the information. Words such as "seen" "saw" or "heard" should not be used. The proximity of the source may be compromised by using words such as "come" "turn up" or "appear" or "arrive at". Alternatives may be "attend" or "go to".*
>
> *Persons should not put material into a 5x5x5 that adds no value or leads to the identification of the source or any sensitive operational details. For example, care should be taken not to reveal sensitive police tactics such as observation points, surveillance, covert human intelligence sources or other confidential information.* ***The term "intelligence suggests" at the beginning of a report is no longer encouraged. This phrase detracts***

from the grading and calls its accuracy into question. In addition, this phrase may allude to the fact that the source is human *and most likely not to have come from a police officer. Where this phrase is used in some reports and not in others, a distinction is able to be drawn. Persons should report only the facts of what was told to them and not place any additional interpretation within the report, changing the meaning of what was told to them. This is essential to maintain the integrity of the information.* [emphasis added]

E. Undercover Sections

1. The National Intelligence Model does not address undercover policing per se, generally referring to intelligence from the broader category of Covert Human Intelligence Sources. However, units dedicated to undercover policing are generally referred to as Undercover Sections. There is less publicly available documentation on these. However, a number of sources do provide some useful material, particularly in relation to Special Branch undercover sections, assembled below.

2. It was clear that, within the NIM and in undercover policing generally, a distinction was drawn between operations needing intelligence and the Undercover Section itself. This was reflected in the Manual of Standards for The Deployment of Undercover Officers (2003).[97]

   Undercover Unit

   2.10 Is a unit which has been established exclusively or mainly for the conduct of operations involving the deployment of undercover officers. … The units, which must be recognised by the National Undercover Working Group, must be staffed principally by officers who have successfully completed a national approved Undercover Training Course as either a student or have attended as an observer.

[97] This manual is dealt with further below.

HM Inspectorate of Constabulary reports

3. A series of reports from HM Inspectorate of Constabulary between 2011 and 2014 helpfully clarify a number of points regarding governance and structure of an Undercover Section, albeit with its focus on the NPOIU. These reports set out the guidance in general terms.

4. **The HMIC report Undercover Tactics in Public Order,** (2011) notes among its recommendations that an operational security officer (OpSy) should review operations lasting longer than one year as part of the authorisation process.[98]

5. **The HMIC report A review of national police units which provide criminality associated with protest**, 2012:[99]

   In practice the tactic [of undercover policing] is directed against serious crime, because in 2003 ACPO restricted the deployment of such officers to serious crime (and then only on the authorisation of an officer of at least Assistant Chief Constable rank).

6. **The HMIC report An inspection of undercover policing in England and Wales** (2014) writes:[100]

   The most important feature of an undercover unit is that its staff do not instigate their own operations. An undercover officer should only ever be deployed to support an existing intelligence-gathering or evidence-gathering operation, the procedures in relation to which are set out in the National Intelligence Model.

---

98 HM Inspectorate of Constabulary, *Undercover Tactics in Public Order,* 2011 ('HMIC 2011'), page 16. HMIC also notes:
The primary role of the operational security officer (OpSy) is to quality assure issues of legality, integrity, ethical conduct and standards of covert operations, while contributing to the overall effectiveness of such operations. For example, an OpSy can independently and objectively review the relationship between cover officers, support staff and undercover operatives.

99 HM Inspectorate of Constabulary, *A review of national police units which provide criminality associated with protest*, 2012 ('HMIC 2012'), page 47.
https://www.documentcloud.org/documents/6596673-Review-of-National-Police-Units-Which-Provide/

100 HM Inspectorate of Constabulary, An inspection of undercover policing in England and Wales, 2014 ('HMIC 2014'), page 53.

It added:[101]

The separation of the undercover unit from the team that is responsible for the investigation in which the unit's members may be deployed enables an important series of checks and balances to be put in place and is seen by the police and law enforcement agencies as good practice. We agree. The undercover officers are kept away from the day-to-day running of the investigation. The separation, in line management terms, of the officer from the investigation tries to ensure that the senior investigating officer does not overstep the mark in what he or she demands of the undercover officer.

7. The same report also noted that an undercover unit itself would have a number of roles, as distinct from the individual undercover officer:[102]

a) *Operational head*

an officer of at least inspector rank or equivalent who has day-to-day responsibility for the investigation or operation using undercover operatives. He or she is responsible for setting clear objectives for the investigation. He or she consults the covert operations manager or cover officer for tactical advice on undercover operative deployments. He or she is sometimes referred to as the senior investigating officer

b) *Covert operations manager*

an officer of at least inspector rank or equivalent who has day-to-day responsibility for the investigation or operation using undercover operatives. He or she is responsible for setting clear objectives for the investigation. He or she consults the covert operations manager or cover officer for tactical advice on undercover operative deployments. He or she is sometimes referred to as the senior investigating officer.

---

[101] HMIC 2014, para. 4.17, page 53.
[102] HMIC 2014, Annex C - Glossary, pages 184, 186.

c) *Cover officer*[103]

a police officer who acts as the conduit between the operational team and the undercover operative unit. The cover officer is responsible for ensuring arrangements exist for the proper oversight and management of the undercover operative and tactics. Under sections 29(4A)(a) and 29(5)(a), Regulation of Investigatory Powers Act 2000, the cover officer has day-to-day responsibility for managing an undercover officer and for his or her security and welfare.

Authorisations

8. This briefing has not addressed material that relates to the authorisation of undercovers, as the information is not publicly available so we are unable to go into much detail.. However, it is possible to draw on the statement of Sir Stephen House in the Kate Wilson case at the Investigatory Powers Tribunal.[104] He noted that applications for authorisation included:[105]

   Subject(s) of the deployment including such information as is known about them, namely any aliases, DOB, address, gender and where applicable, PNC or CRO reference numbers, warning signals, NCIS and Force Flag Folio Numbers;

   Intelligence case detailing the nature of the offence and details of the investigation/operations.

   ***Operational objectives / strategy** including the purpose and sequence of what the UCO/CHIS will be tasked to do; location where contact with the subject(s) might take place; comments on collateral intrusion and plans to minimise the same; an explanation of the information that is expected to be obtained from the activity; and, where renewal is sought, the necessity for continuing with the activity.*

---

[103] This position was only formally established within undercover policing by the Regulation of Investigatory Powers Act 2000.
[104] First Witness Statement of Stephen House, Metropolitan Police, 2019 ('SSH1 2019'), unpublished.
[105] SSH1 2019, page 32, sections 93.3, 93.4 and 93.5 respectively.

9. This indicates that NIM processes were being applied to making the judgement on whether a deployment was justified and met a particular strategy. References to these strategies are to be found in intelligence reports, via ‘Control Strategy’ numbers. Further details however are not available.

F. Extracts from the Manual of Standards for a UCO pertaining to NIM

1. This manual, issued in 2003, can be found in a NUTAC document disclosed in the Kate Wilson IPT case.[106] Although it does not mention the NIM directly, it does refer to the European Convention on Human Rights (ECHR) and codes of practice, and refers to terminology from the NIM. It notes that all police forces have agreed to adopt the standards as policy, and that an ACPO-rank police officer will be appointed in each force to oversee adherence to RIPA, the Public Code of Practice and standards set out in the manual (Section 1.4). This should be read with Section 3.27 which explicitly notes that:

   > *Only officers who have successfully completed an Undercover Training Course approved by the National Undercover Working Group may be used as undercover officers.*

   If an officer was authorised to be deployed as an undercover without successfully completing a NUTAC following 2003, this would breach their own guidelines.

Legal regime

2. Section 1.2 notes that the Manual is to be read in conjunction with the Covert Human Intelligence Sources, Public Code of Practice ("The Code") and the ECHR. Section 1.5 notes that the previous, non-statutory, Code of Practice for Undercover Operations and their Minimum Standards for Guidance has been superceded by RIPA.

3. Section 1.9:

   > *The primary purpose of undercover operations is to secure evidence to bring offenders before the Courts. Such operations may also be conducted in order to gather intelligence in support of the prevention or detection of crime.*

[106] National Undercover Working Group (ACPO), *Manual for Standards for the Deployment of Undercover Officers*, January 2003, unpublished.

4. Section 1.23 covers the ECHR and the Human Rights Act 2000, stating:

   every operational officer must be conversant with the Act and Convention and every officer responsible for the authorisation and supervision of investigations will need to be able to justify decisions taken in the light of the Convention and the Act.

   The following two sections spell this out further:

   1.24 There are essentially two key issues for law enforcement in the Convention. The first is the guarantee of rights to fair trial contained in Article 6. Where the prosecution seeks to protect covert sources through a Public Interest Immunity application, particularly if the procedure is 'ex parte', Article 6 issues are likely to arise. [...]

   1.25 The second issue concerns Article 8, which guarantees rights to privacy. The infringement of someone's right to privacy should be justifiable on the grounds of proportionality and necessity. The degree of intrusion proposed should be proportionate to the seriousness of the crime being investigated. The technique adopted should also be a necessary means of obtaining the desired result.

   Section 3.26 is also explicit:

   (7) Undercover officers must be fully conversant with Article 6 (Right to Fair Trial) and Article 8 (RIght to Respect for Private and Family Life) of the European Convention on Human Rights.

5. Section 3 provides information about those officers managing an undercover. The following extracts should be read in light of requirements set out by the NIM:

   3.18 The Operational Head of the investigation for which an undercover officer is to be deployed will be of at least rank of Detective Inspector… Wherever possible they should have had management awareness training in the deployment of undercover officers or successfully completed a nationally recognised Undercover Training Course as a student or attended as an observer. However, if this is not the case,

they must be fully conversant with current legal issues and guidelines that are relevant to undercover operations. [emphasis added].

3.20: The Operational Head will be responsible for the direction and general oversight of the use of the undercover…

3.21 Intelligence gathered by the undercover officer will be passed to the Operational Head. It is the responsibility of the Operational Head to deal with it in an appropriate manner, having regard to the security of the operation and those involved with it. No intelligence will be disseminated without the prior agreement of the Operational Head and after consultation with the Cover Officer.

3.24 Cover officers will… be fully conversant with current law, procedures and guidelines that are relevant to undercover operations including aspects relevant to disclosure and revelation issues.

3.25: The role of Cover officer may not be performed by a member of the operational team.

3.36 Following an application for the deployment of an undercover officer, the Undercover Unit will assess the feasibility of the deployment and advise the investigation's Operational Head accordingly. The Operational Head will also be directed as to the required support structure to be in place in order to conduct the proposed operation effectively. Upon the deployment being deemed feasible and agreement to the support structure requirements, the Undercover Unit will submit an application to the authorising officer.

6. The Manual makes two further references that show that undercover deployments were expected to follow the NIM and related regulations.

5.5 All product gained from undercover deployments will be evaluated, kept securely and only disseminated in accordance with the code of practice for the recording and dissemination of intelligence material. The Manual of Standards for

Recording and Disseminating Intelligence Material provides advice on the components and systems requirements for a sound intelligence environment. [redacted line] ***The manual provides a description of systems and procedures which underpin the ACPO National Intelligence Model.*** [emphasis added]

Sections 5.6 and 5.7 address the need for Review, Retention and Deletion policies that reviewed keeping intelligence gathered in line with the law.

G. Questions

1. Section 5.7 states that all material gained/recorded for intelligence purposes must be subject to review, weeding and destruction principles. To retain this material, there had to be a public interest justification, access appropriately restricted, and the information subjected to periodic review.

2. A number of documents indicate that the SDS did adopt the National Intelligence Model in part and used it in setting priorities and taskings for the Undercover Section. Regardless of points made by undercover police and their managers that the undercover officers had to be self-directing, to be in accordance with the legislation and the National Intelligence Model, they would still have to be providing material in accordance to meet predefined objectives as defined by the NIM, particularly the intelligence requirements. The fact that there were authorisations implies that the undercovers were being deployed to advance a pre-defined intelligence need or requirement, which by 2005 at the very latest, ought to have been in line with the NIM This opens up multiple questions to be put to undercover officers and managers that include:

   a) Adherence to NIM Standards:

      i. To what extent were undercover officers and their managers trained in the NIM, or aware of the new regulatory regime post-2000?

ii. To what extent did the SDS and related squads within the MPSB/MPS Counter Terrorism Command follow the model set out in the NIM, particularly with reference to Tasking and Co-ordination Meetings (T&CG)?

iii. What changes were made within the SDS and NPOIU to align these units as a whole to the NIM, its required control strategies and T&CG meetings?

iv. To what degree did the NPOIU and its undercover unit adhere to the NIM?

b) Who appointed the senior management team of the SDS / NPOIU for the period concerned, or otherwise made staffing decisions in relation to it?

i. What requirements were made of senior management team knowledge of undercover policing guidance and/or the NIM when they were being recruited? What training were senior managers offered?

c) Compilation of NIM products relating to the SDS/NPOIU:

i. To what Control Strategies, if any, did these deployments relate?

ii. Where S/TT&CG meetings took place, was intelligence derived from SDS/NPOIU undercovers placed before those meetings?

iii. What tasking and input from the undercover section was used to compile personal profiles of targets?

d) Proportionality of undercover deployments:

i. What was the wider intelligence gap to which undercovers were deemed to be necessary?

ii. To what extent were less intrusive alternatives considered?

e) Explore the degree to which SDS was allowed to sit outside the new regime that the NIM envisaged. To what extent did its lack of adherence to the NIM play a role in its closure?

f) Were operational security (OPSY) managers appointed for the SDS/NPOIU; if not, why not? If so, did they do their job sufficiently well?

g) Who in the SDS/NPOIU held the position of intelligence manager? What training did they have and were they otherwise equipped to carry out their role?

h) It is clear that for both the NPOIU and the SDS the envisaged good-practice distinction between the operational head, who would supervise the undercover operation, and the undercover section itself became quite blurred. How and why did this occur, and, if so, why did senior managers permit it?

i) Given that many of the named targets were groups without formal membership lists, how were the restrictions on the authorisations in any way meaningful?

H. Conclusion

1. Post 2000, the changing legislative regime imposed a new world on policing, itself under pressure to find savings and efficiencies by moving to an intelligence-led model. This gave rise to a lot of practical considerations which resulted in various new protocols and policies being adopted – some of which were later given a statutory basis. The Management of Police Information and the National Intelligence Model were two key aspects of this, covering all policing activities.

2. They created an entire new structure for intelligence gathering, not least of all undercover policing. As the Undercover Policing Inquiry moves to examining the later periods of its investigation, this aspect is going to become far more important. Understanding this changed regime is important to both interpreting the documents but also the degree to which the police were operating within their own guidelines. And these guidelines were there to ensure that the intelligence gathering was itself lawful.

3. By understanding the NIM one can give better context to the authorisation process on one hand, but also ask questions about what the very processes by which the undercovers were supposedly being tasked. In a crude sense, the deviation of the NPOIU and the SDS from this model is a measure of how far they were out of control. A question for the managers is how, as the people responsible for authorising and enforcing it, how they allowed this to happen on their watch. Previous managers could claim there were no formal processes to guide them. This excuse entirely falls away once the NIM is firmly in place, and a significant question is why it was allowed to continue.

4. As the NIM remains in force, the recommendations the Inquiry Chair is due to make on how to prevent the spycop scandal happening in the future, need to take this regulatory regime into account. While much focus is naturally on the Regulation of Investigatory Powers Act 2000 and later legislation, this briefing has covered the practical implementation of this law. Going forward, recommendations must also be at this level as well. It is by understanding where the NIM is flawed or was ignored that the Inquiry can make substantive recommendations that will have direct impact on the actions of future undercover officers and those responsible for them.