
Her Majesty's Inspectorate of Constabulary for Scotland
COMMON KNOWLEDGE
A Report on a Thematic Inspection of Information and Intelligence Sharing

Her Majesty's Inspectorate of Constabulary for Scotland

COMMON KNOWLEDGE

A Report on a Thematic Inspection of Information and Intelligence Sharing

Scottish Executive, Edinburgh 2007

© Crown copyright 2007

ISBN: 978-0-7559-5227-4

Scottish Executive
St Andrew's House
Edinburgh
EH1 3DG

Produced for the Scottish Executive by RR Donnelley B48411 03/07

Further copies are available from
Blackwell's Bookshop
53 South Bridge
Edinburgh
EH1 1YS

100% of this document is printed on recycled paper and is 100% recyclable

Contents

Executive Summary

To deliver the Scottish Executive's vision of safer communities, public services need to develop and maintain effective, user-focused and inclusive partnership frameworks for service provision. Intelligence and information sharing is one of the key ways in which individual agencies must combine with others to do just that, and so achieve the joined-up services which can improve the lives of everyone living and working in Scotland. The converse is also true: there is a growing awareness across the public sector that inefficient processes and procedures in intelligence and information sharing can have serious consequences, as highlighted by reviews and inquiries over at least two decades.

The importance of this theme is reflected in current developments at national level, where a number of initiatives and legislative changes are being introduced to address at least some of the need.

This report has examined the existing position of intelligence and information sharing, both within the police service in Scotland and between the service and its principal partner agencies, against the fertile landscape of these national developments. While the recommendations are directed at the police service, some suggestions are also made for principal partners in an effort to enhance intelligence and information sharing arrangements across agencies.

Nowhere is this need more apparent than in the high risk areas involving the protection of children and vulnerable adults. Though here the requirement for quicker identification and relevant information sharing is paramount, some practitioners need to retain control over this information. The progress already made by the 'Getting It Right For Every Child' agenda must be commended for pointing out ways in which one agency's interest in a child can be 'flagged up' to other agencies. It is disappointing that, at the time of writing, proposals to impose a duty upon organisations to share information for the purposes of child protection are likely to be dropped from the legislative programme. However, HMIC believes that there are even greater gains to be made by overcoming well-intentioned reluctance to share lower-level information at an earlier stage. No public service or public servant can know everything and so processes and procedures within and between organisations need to make information sharing easier and safer, not a matter of guesswork or exception. The Inspectorate recommends that practical possibilities which have not yet been considered, but which could offer significant progress here, are given some thought. These should amount to a means of maintaining client/patient/victim confidentiality for the most sensitive information, right up to the point at which the need to share becomes obvious.

One of the important pieces of work currently being undertaken at national level is being led by the Scottish Executive. It seeks to establish common data standards through the work of the National Data Sharing Forum and local data sharing partnerships. This presents the prospect of a standardised method of gathering, storing and sharing intelligence and information for all public service providers.

Throughout the inspection HMIC found many examples of good practice being applied by the police in the field of intelligence and information sharing. However it is felt that if the Association of Chief Police Officers in Scotland (ACPOS) were to adopt a strategic overview and corporate approach, this would help to ensure that each of its business areas takes cognisance of the Scottish Executive strategic vision for intelligence and information sharing in the public sector. This approach could be further strengthened by each Scottish force and the Scottish Police Services Authority producing and publishing an intelligence and information sharing strategy that defines organisational structures and management responsibilities.

HMIC acknowledges that the development of information communications technology (ICT) in the police service in Scotland over the last three decades has been challenging and difficult at times. A number of different and unconnected systems have been introduced throughout the country. However, within the last year ACPOS and the Scottish Executive have embarked upon a new approach to business change, specifically focusing on the way ICT development is managed and integrated in the police service. HMIC strongly supports the positive steps taken by ACPOS towards ICT convergence and future integrated development. Indeed HMIC believes that the Scottish Executive's promotion of enhanced ICT information sharing, through its 'Getting It Right For Every Child' (GIRFEC) agenda and the National Data Sharing Forum, should be incorporated into the ACPOS vision for Information Communications Technology development.

This inspection has revealed that, across the public sector, intelligence and information sharing has been partly restricted by misinterpretation of the Data

Protection Act 1998 as an inhibiting piece of legislation. HMIC proposes that there is a need to understand and promote the Data Protection Act as enabling legislation which encourages information sharing. One of the changes which could contribute to that change of outlook would be to re-align the data protection function/expertise within forces from an administrative to an operational role, in order to encourage a more pragmatic approach to intelligence and information sharing. In addition, an improved programme of targeted training is required to assist in delivering an enabling ethos in support of front end service provision.

HMIC believes that the opportunities which exist at national level to add value to information sharing between partner agencies, should also be grasped in order to achieve efficiencies in working practices. A significant step in that direction might be achieved by reviewing the role of chief constables as data controllers of Scottish Criminal Record Office (SCRO) databases, and by allowing specialist reporting agencies (SRAs) and the Crown Office and Procurator Fiscal Service (COPFS) greater access to the Criminal History System (CHS). HMIC acknowledges that this is a departure from the traditional police view of owning and managing intelligence and information. However, most police leaders today appear to accept that meaningful progress can only be achieved by acknowledging that many challenges within the criminal justice system are shared and require shared solutions for the benefit of all.

HMIC commends the use of the National Intelligence Model (NIM) as the business model for policing in Scotland. This inspection has identified that adoption of the NIM by partner agencies, such as the Scottish Prison Service (SPS), has delivered tangible benefits to both organisations and the wider public. HMIC believes that greater information and intelligence sharing between all public services requires a common framework and language. The National Intelligence Model has proved its adaptability and usefulness beyond policing and HMIC proposes that this model be extended to all relevant public services.

Much has been accomplished in improving intelligence and information sharing within and outwith policing. But for any further meaningful progress to be achieved the Scottish Executive, ACPOS and its partners need to build on existing strong relationships and work together to a common plan aimed at agreed outcomes.

Summary of Recommendations

RECOMMENDATION 1

HMIC recommends that forces review the position of data protection officers and their staff within their organisational structures, with a view to aligning these more closely to the management of operational policing so as to promote an enabling attitude that will assist core business. (Page 17)

RECOMMENDATION 2

HMIC recommends that the Scottish Executive consider nominating or establishing a single agency with responsibility for creating a confidential child and vulnerable adult protection registry for each child protection committee area (or combination of two or more) for the purpose of:

(a) collating all information and intelligence from any public service which *could give rise to concern* about the welfare of a child or vulnerable adult residing in that area;

(b) regularly monitoring the information on each child and vulnerable adult;

(c) applying strict rules of confidentiality to such of that information and intelligence which cannot be shared with others unless in exceptional circumstances, and perhaps only then with the consent of the information source (e.g. health information);

(d) providing a 'single shared assessment' of concerns whenever certain criteria are met, with or without information restricted according to prescribed rules, which require joint consideration of a case; and

(e) activating the joint consideration of cases. (Page 22)

RECOMMENDATION 2B

HMIC recommends that the Scottish Executive consider legislating to place a duty on all public services to provide all and any information and intelligence about a child or vulnerable adult which has come to their notice and which could give rise to concern about the welfare of any child or vulnerable adult to the single agency proposed in recommendation 2A. (Page 22)

RECOMMENDATION 3

HMIC recommends that ACPOS consult with the Scottish Executive to determine whether chief constables should remain as data controllers of all SCRO databases, with a view to arriving at the best solution to promote the accuracy, quality and integrity of data and maximise efficiencies in working practices. (Page 27)

RECOMMENDATION 4

HMIC recommends that , as a matter of urgency, ACPOS consult directly with all relevant partner agencies with a view to giving criminal justice partners greater access to the criminal history system, while maintaining security and data quality. (Page 27)

RECOMMENDATION 5

HMIC recommends that ACPOS consider how to improve the two-way flow of intelligence between the police and the prison service. (Page 34)

RECOMMENDATION 6

HMIC recommends that each force produce and publish an intelligence and information sharing strategy which contains the core elements suggested within this report. (Page 35)

Summary of Recommendations

RECOMMENDATION 7

HMIC recommends that ACPOS provide a strategic overview for developing information sharing within each of its business areas, in order to promote a corporate approach in accordance with the Scottish Executive's vision for data sharing across the public sector. (Page 35)

RECOMMENDATION 8

HMIC recommends that forces and the Scottish Executive encourage principal service delivery partners concerned with community safety and anti-social behaviour to adopt the principles of the National Intelligence Model as a business model for this work. (Page 42)

RECOMMENDATION 9

HMIC recommends that the protocol templates from the Management of Police Information Sharing manual be adopted as the basis for information sharing protocols throughout Scotland, to promote corporacy and consistency. (Page 46)

RECOMMENDATION 10

HMIC recommends that information sharing protocols incorporate a risk assessment model, to ensure that the quality of information shared is such that the objective of the information sharing can be accomplished. (Page 54)

RECOMMENDATION 11

HMIC recommends that ACPOS and SPSA consider creating a process to ensure an outward facing approach to future information and communications technology (ICT) development, so that opportunities for electronic intelligence and information sharing with other agencies are not missed. (Page 60)

RECOMMENDATION 12

HMIC recommends the use of single points of contact (SPOC) to share sensitive information between the police and partner agencies. (Page 62)

RECOMMENDATION 13

HMIC recommends that ACPOS consult with the Scottish Executive and partner agencies to deliver a comprehensive guidance framework for public service information sharing. (Page 67)

RECOMMENDATION 14

HMIC recommends that ACPOS acknowledge a training need for information sharing and seek training aimed at establishing an enabling ethos for intelligence and information sharing across the police service. (Page 67)

Summary of Suggestions

SUGGESTION 1

HMIC suggests that forces and partner organisations identify the personal qualities of the most effective members of staff who liaise with partners as part of their front-end operational role, with particular reference to their ability to develop relationships, and use these as specifications for selecting future post-holders. (Page 18)

SUGGESTION 2

To prevent potential duplication of work and to ensure a co-ordinated approach, HMIC suggests that ACPOS recognise the existing data standards in use across the criminal justice community when seeking to introduce national standards for police data. (Page 36)

SUGGESTION 3

HMIC suggests that local data sharing partnerships work towards collecting personal (with appropriate safety measures) and aggregated data sets from all the principal community safety partners, to facilitate strategic business planning as well as individual- and location-related case management. (Page 40)

SUGGESTION 4

HMIC suggests that the business models adopted by the Edinburgh Community Safety Partnership and the Glasgow Anti-Social Behaviour Task Force be recognised as good practice, at strategic, tactical and operational levels respectively, and be considered for adoption by other community safety and anti-social behaviour partnerships. (Page 44)

SUGGESTION 5

HMIC suggests that ACPOS and individual forces could increase intelligence sharing across public service organisational boundaries by seeking bilateral agreements on the method of transfer, and by promoting awareness amongst relevant partners of the confidentiality, security and ethical standards of the NIM and the 5x5x5 assessment/risk management model in particular. (Page 57)

SUGGESTION 6

HMIC strongly supports the positive steps taken by ACPOS towards national ICT integration, and suggests that 'information push' be adopted as a key priority for the design of systems supporting operational policing. (Page 60)

SUGGESTION 7

The Scottish Executive development team responsible for establishing local data-sharing partnerships is also attempting to ensure common data standards for information systems in specific areas of public service. HMIC suggests that community information systems (such as those used for tackling anti-social behaviour) be considered for inclusion in this effort. (Page 62)

Preamble

Her Majesty's Inspectorate of Constabulary (HMIC) has a statutory duty under section 33(3) of the Police (Scotland) Act 1967 (the 1967 Act) to report to the Scottish Ministers on the effectiveness and efficiency of the police service in Scotland. It discharges this duty through an inspection programme which involves primary and review inspections of individual forces and common police services, and through conducting thematic inspections on areas of particular interest or concern simultaneously across all of the police service in Scotland.

The objective of thematic inspections is to establish the state of current practice in the subject area. It does this by consulting widely with stakeholders and then formulating comment and recommendations which should aid and promote improvement. Recommendations may be directed at individual forces or organisations, representative bodies and the Scottish Executive. HMIC revisits recommendations arising from thematic inspections during subsequent force inspections. Occasionally, a further thematic will be undertaken specifically to measure general progress made. Specific progress in-force should be assessed regularly through action reviews.

The Need

The sharing of case-specific information by the police and other public services in the UK has been the subject of considerable scrutiny in a number of high profile public inquiries in recent years. These have tended to involve those who are at risk of harm or those who pose a risk of causing deliberate harm, and sometimes both. The latest in a long line of inquiries was conducted by Sir Michael Bichard, following the murders of Holly Wells and Jessica Chapman. The Bichard Inquiry sought to identify lessons to be learned and point a way to minimise similar risks in future. The recommendations from his report published in 2004 are presently being progressed by a number of public bodies including, for the police service in Scotland, the Association of Chief Police Officers in Scotland (ACPOS), through the structure of a Scottish National Working Group.

Although protecting children and other vulnerable people and managing certain offenders in the community are probably the most important aspects of information and intelligence sharing to get right, there are many other purposes for which police engage, or should engage, in that sharing activity. These include:

- providing case-specific information or intelligence to public service partners, to allow them to carry out their statutory duties by identifying other risks and/or minimising other threats to public order or safety (e.g. information to local authorities about anti-social behaviour, or to procurators fiscal about persistent offenders);
- providing non-personal information or intelligence to community planning or community safety partnerships, to assist collaboration and co-operation in efforts to reduce or prevent crime and disorder;
- providing non-personal information or intelligence to other public service partners, to assist them in fulfilling their responsibilities and achieving their objectives (e.g. strategic assessments of crime and disorder threats to criminal justice partners to help inform their views of 'the public interest').

Scottish Ministers, the Westminster Government and all public service providers are aware of the need to improve information sharing. The Bichard recommendations are just one of a number of positive actions currently being undertaken to enhance information sharing across organisational boundaries, for the benefit of all communities.

Work is currently being completed at national and local levels to develop data sharing fora in order to achieve national data standards: the Macleod short-life working group recommendations seek to improve information sharing between the National Health Service (NHS) and partner agencies, the Getting It Right For Every Child (GIRFEC) agenda to enhance child protection.

This diversity of work being completed provides clear evidence of the commitment of all public service providers to develop greater information sharing. However, it also demonstrates the complexity of the subject matter and therefore the challenges that lie ahead.

The inspection looked at each of these areas, to ascertain what the strengths and weaknesses were and where opportunities and threats might emerge in the evolution towards greater intelligence and information sharing.

Existing and Emerging Systems and Structures

There is now a single integrated intelligence system for the police service in Scotland, i.e. the Scottish Intelligence Database. Nevertheless there are still many other police information systems in which intelligence and information (which may ultimately appear on SID) is collated, or analysed, or assessed, or disseminated or stored (most but not all of them, yet, using electronic technology). There are different systems in different forces and even some differences within forces.

However, there is welcome consistency and a degree of constancy in the structural backdrop against which police information sharing operates. This is provided by the fact that every police force and policing organisation in Scotland is committed to five key developments which, in their own ways, contribute or will contribute to facilitating and improving information and intelligence sharing:

1. **the national intelligence model (NIM)** – a business structure adopted by the police service which uses information in its widest sense to enable managers to determine strategic direction and make tactical and resourcing decisions;
2. **convergence and future joint development of police information and communications technology**;
3. **community planning** – the means by which police forces and other public services combine, at local authority level, to plan and deliver joint and co-ordinated efforts to achieve shared aims;
4. **national and local criminal justice boards** – established to provide a means of improving the efficiency and effectiveness of the criminal justice system at local (Sheriffdom) and national levels;
5. **the integration of Scottish criminal justice information systems (ISCJIS)**.

Within policing, the collection of appropriate information, its accurate assessment and timely exploitation are essential for efficiency. For this to happen all police information must be treated as a corporate resource. It is, therefore, important that information can be collected, recorded, evaluated and stored in a consistent manner across police boundaries. The bullet points above show the main enablers for achieving this. However there are also blockers which need to be addressed. Issues and factors which might be considered to be obstructive are as follows:

- lack of common standards for recording and evaluating information;
- incompatible information technology;
- inconsistent information sharing arrangements with partner agencies;
- a culture of protectionism applied without proportionality.

In England and Wales, a Code of Practice and Manual of Guidance on the Management of Police Information (MOPI) was introduced in 2006. This work recognises the requirement to share information not just across UK policing and its partner agencies, but also further afield. In Scotland, ACPOS was working on a Scottish version at the time of this inspection.

Sharing information between partner agencies in support of community planning is being progressed by the Scottish Executive, which has established a National Data Sharing Forum. The processes and procedures facilitating such exchange have also been considered by the inspection team.

Inspection Value

This inspection has examined current arrangements for sharing intelligence and information and has sought to identify good practice both nationally and internationally. The report contains a number of recommendations and suggestions for improvement where considered appropriate.

A significant aspect of the thematic inspection methodology was consultation with internal and external stakeholders. The views of many participants and partners on the process of sharing intelligence and information have been canvassed and contributed to the final report.

HMIC anticipates that this report will be of significant interest to police leaders and managers. However the Inspectorate hopes that it will also be of interest and assistance to those in partner organisations who believe that information and intelligence sharing is critical to improving delivery of service and safety to some of the most needy members of our communities.

Project Aim

The aim of the project was to examine the current state of intelligence and information sharing within the police service in Scotland.

Project Objectives

The objectives of the project were to:

- Consider the leadership, strategy, people, resource management and key processes of intelligence and information sharing and accountability across Scotland.
- Examine the use of intelligence and general information in developing strategies and policies, business planning and accountability.
- Consider the attributes of successful systems.
- Identify instances of good practice.
- Make recommendations designed to promote continuous improvement of the service provided by the police service in Scotland.

Methodology

HMIC methodology is to conduct inspections using protocols aligned with the business excellence model created by the European Foundation for Quality Management (EFQM). This allows a structured and comprehensive examination of key organisational functions and ensures that HMIC inspections are evidence-based. The approach is now established HMIC practice.

This thematic inspection of intelligence and information sharing adhered to principles of project management, establishing the aim, objectives, methodology, resources and timescale involved. Mr Andrew Brown, HMCIC, issued a project mandate to undertake the inspection and the project initiation document set out the approach adopted.

The project was undertaken in a phased approach, based on a strategic planning model which identified key stages and milestones. Following an initial literature review and desktop research, liaison was established with representatives of relevant Scottish Executive departments, the Association of Chief Police Officers in Scotland (ACPOS), the Information Commissioner's Office, the Scottish Information Commissioner, Audit Scotland, Crown Office and Procurator Fiscal Service (COPFS), Scottish Children's Reporter Agency (SCRA), Association of Chief Police Officers in England and Wales (ACPO) and the Serious Organised Crime Agency (SOCA).

In previous thematic inspections value has been derived from seeking out good practice internationally. In light of the ever-increasing global context to intelligence and information sharing it was felt that HMIC should endeavour to explore how the police service shares information in an international context. The major international policing event during the summer of 2006 was the Federation of International Football Associations (FIFA) World Cup, and HMIC took the opportunity to study the intelligence and information sharing structures and processes put in place for this world event.

The inspection of all eight Scottish forces and the four common police services, namely the Scottish Police College, the Scottish Crime and Drug Enforcement Agency, the Scottish Criminal Record Office and the Scottish Police Information Strategy, was conducted in June and July 2006. Prior to this, each organisation completed a comprehensive 29 question protocol.

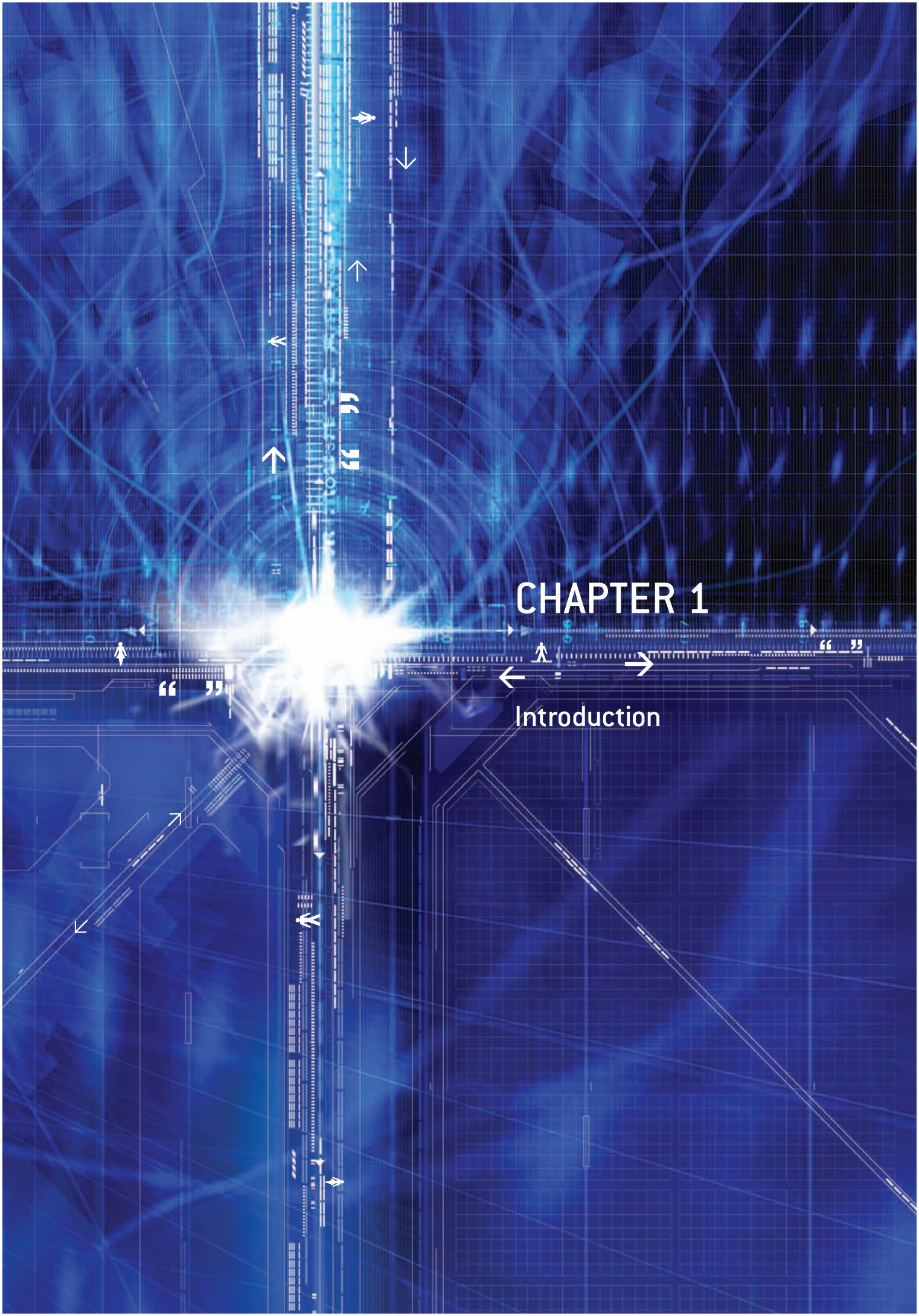
The protocol was adapted from the standard HMIC inspection format, based on the EFQM model. Although adhering principally to this format, the main headings of this report have been amended slightly to reflect more appropriately the scope of intelligence and information sharing.

Analysis of the responses provided a wealth of detailed information, permitting the inspection team to focus on the most relevant issues during the fieldwork visits. Fieldwork consisted of an examination of systems and reports, as well as interviews with police and support staff across a range of levels and responsibilities. Owing to the nature of the subject under inspection, interviews were conducted with principal partners in criminal justice, community planning, community safety and anti-social behaviour partnerships, to give a clear picture of the intelligence and information sharing landscape. An important aspect of this work was face-to-face interviews with chief constables, directors of common police services and executive officers of partner organisations.

HMIC acknowledges the valuable assistance of nominated liaison officers from each of these organisations, in collating protocol returns and negotiating workable timetables for subsequent visits. HMIC would also like to acknowledge the assistance of partner organisations in facilitating the inspection team and arranging interviews with key personnel.

At various points the report highlights a range of activity in the police service in Scotland and in principal partnerships involving the police, much of which can be considered transferable good practice.

The inspection was carried out by HMIC staff under the direction of Mr Andrew Brown, CBE., QPM., Her Majesty's Chief Inspector of Constabulary and Mr Malcolm R Dickson, QPM, MA, Assistant Inspector of Constabulary.



CHAPTER 1

Introduction

Intelligence and information sharing are the foundation of every aspect of policing. As a service, policing is dependent upon sharing information with partners in order to achieve shared and individual objectives. Similarly, partner agencies are, to lesser or greater degrees, dependent on sharing police data to achieve their own goals.

This co-dependency should be what drives and promotes intelligence and information sharing. No organisation can meet the needs of its users or deliver a complete service without a comprehensive, consistent and professional framework of data sharing.

Continuing advances in technology present both opportunities and challenges. More and more information and intelligence becomes available for use, but with this comes ever increasing work in terms of collating, storing, assessing, analysing and disseminating it. Incompatible information communications technology (ICT) between organisations is sometimes seen as an obstacle (or excuse); a more constructive view is that technological linkages are and will continue to become easier as the science and ICT market advance.

Across all public sector agencies the landscape for information and intelligence sharing is evolving on a daily basis, providing solutions to local and regional problems. Whilst many of these local arrangements are noteworthy, the evolution of an ad hoc approach to data sharing engenders an element of risk.

Without a corporate approach to intelligence and information sharing, there will always be the potential for a vital piece of information to be overlooked with potentially disastrous consequences.

Acknowledging this, this inspection had the potential to touch every aspect of policing. The focus of the thematic report was therefore limited to an overview of the strategic issues involved in sharing intelligence and information, and on providing direction to the service for the next steps. The report also identifies some areas which will be of interest and perhaps assistance to partner agencies.

There are many possible definitions of intelligence and information. Those most recently adopted within the police service in Scotland are useful for internal purposes but may also be of interest to partners and other readers of this report.

- Information refers to all forms of information obtained, recorded or processed by the police, including personal data and intelligence.
- Intelligence is defined as information that has been subject to a defined evaluation and risk assessment process in order to assist with police decision making.

HMIC also suggests that there are broadly three distinct types of intelligence and information *sharing*:

- Case-specific information sharing that usually contains personal information (for use at operational level).
- De-personalised, non-specific information, such as statistics. This type of information is incorporated into planning how specific partnerships will deliver services (at tactical level) and formulating strategies and policies (at strategic level).
- Non-personalised information such as locations and courses of conduct.

It is accepted that whilst there are moral and ethical grounds that fully justify not sharing some personal information, there should be no justification for failing to share aggregated records. In incidents where it is justified not to share all the information, caveats or conditions should be incorporated to allow appropriate sharing. Conversely, where unnecessary barriers are identified, they should be removed to facilitate the free flow of information.

The distinction between intelligence and information is illustrated by their different development within Scottish forces. With regard to intelligence, all the forces have robust systems for managing and analysing intelligence through the National Intelligence Model (referred to in Chapter 2, page 24), and use the Scottish Intelligence Database, which is a national electronic database used for collecting criminal and community intelligence (referred to in Chapter 2, page 24).

The landscape is not quite so clear when considering information. Forces have developed information sharing protocols with partners in order to pursue individual and joint aims. However this process is currently limited, with existing protocols restricted to a defined number of business areas, such as community safety (referred to in Chapter 4). No force has developed a central register or over-arching structure for the governance of information sharing protocols.

Formalising a framework for managing information would enable forces to provide central governance and aid accurate assessment. This in turn would allow information to be shared in a consistent and professional manner, thereby achieving maximum effect on service delivery.

Nowhere is this more apparent than in the headline, high-risk areas of child protection and the management of sex offenders. Here the risk of sharing as opposed to keeping information confidential must be very carefully considered to ensure the most proportionate approach (referred to in Chapter 2, page 19).

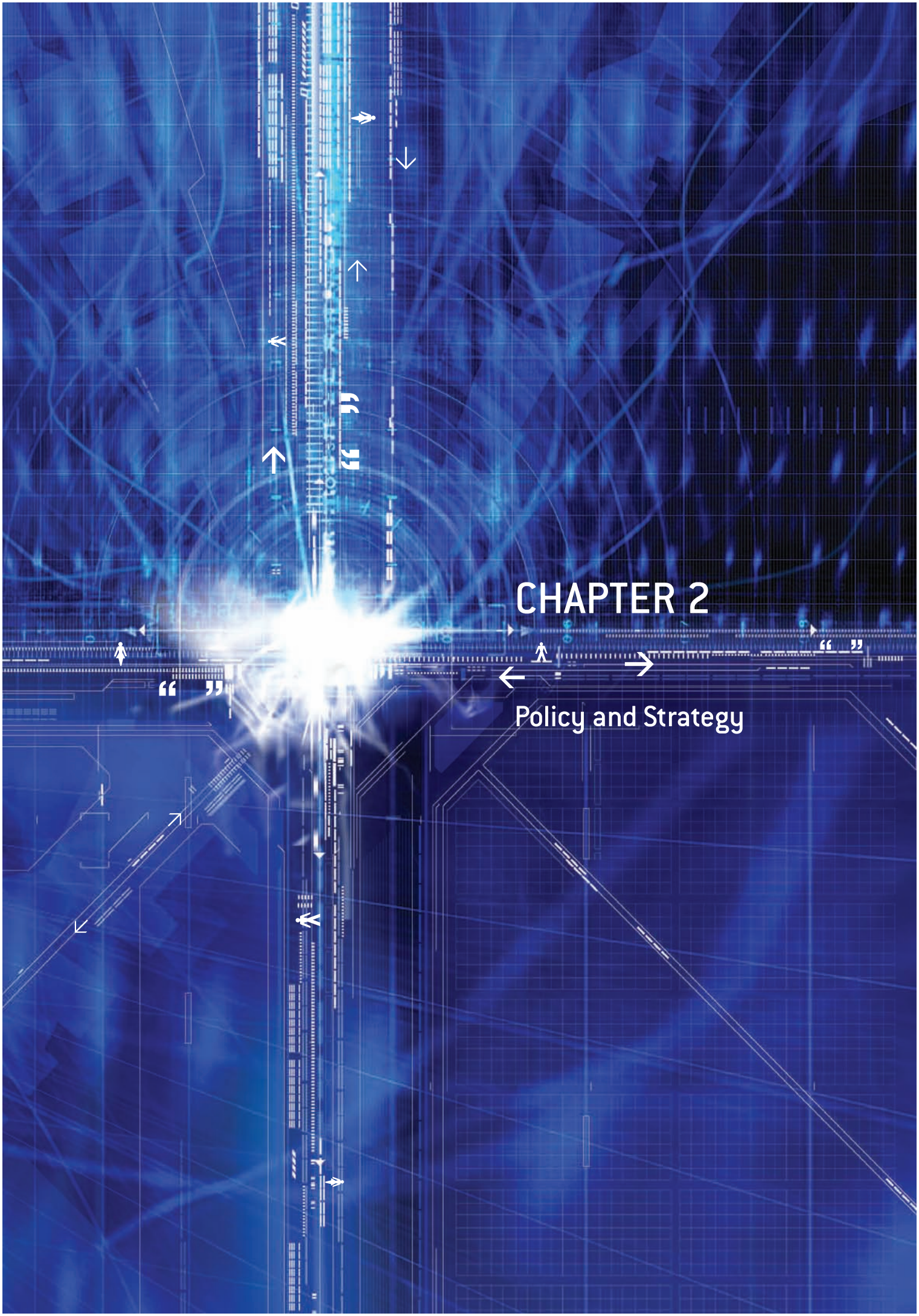
This thematic inspection report would be incomplete without reference to how partner agencies can assist and benefit from enhanced intelligence and information sharing with the police service. HMIC's statutory role means that these comments can be no more than advisory. But it is hoped that the suggestions made will be discussed and that partners will subsequently engage with policing organisations to take these matters forward.

In this context, this thematic inspection should be viewed within the national agenda for the wider reform of public services. Intelligence and information sharing is key to addressing the desire for greater co-ordination in delivering public services and doing so with greater focus on the user.

The development of information and intelligence sharing within the police service should therefore be designed in collaboration with partner organisations, using the clear principles of the Scottish Executive's reforms for public services.

All public sector organisations acknowledge the collective need to improve the ways in which information is shared. However, HMIC recognises that whilst the concept of greater information sharing is simple to accept, "[g]aining the agreement of many different agencies with different professional cultures, some more reluctant than others to share information....is a complex task." (Cleaver H, Cleaver, D Cleaver, D & Woodhead V. Information sharing and assessment: The progress of 'non-trailblazer' local authorities. Research Report 566, London DfES 2004). Enhancing information sharing will require a better understanding of the factors enabling and constraining inter-organisational information exchange. This report attempts to identify unjustified barriers and some means of either removing them or at least minimising their effect.

HMIC acknowledges that many of the recommendations contained in this thematic are aspirational. However, the possibilities for advancement presented by the current environment create opportunities that the service must endeavour to exploit.



CHAPTER 2

Policy and Strategy

2.1 The National Perspective

The Scottish Executive Criminal Justice Plan for Scotland sets out a vision for the criminal justice system in which services work effectively and coherently in the interests of justice to protect citizens, safeguard their rights and help create communities which are stronger and safer. The main challenge set out in this strategy is for criminal justice partners to work together more effectively and coherently. It focuses on the key areas of anti-social behaviour, reform of court processes, reducing re-offending rates and tackling drug addiction. Better intelligence and information sharing between the criminal justice community partners will be essential to delivering this vision.

The Scottish Executive believes that improving joint working in public services will bring about consequential improvements to the quality of these services, thereby making a positive difference to the people who access them. The community planning process, acting as a framework for making public services responsive to, and organised around, the needs of communities, also has a critical role in ensuring that these challenges are met.

2.2 Community Planning

As a result of the Local Government in Scotland Act 2003, community planning has already led to the creation of joint strategies in most areas in Scotland, and has provided the basis for impressive examples of partnership working. The community planning process puts joint visions and plans into practice with the intent of achieving a tangible improvement in services across Scotland. It is an evolving process involving ongoing changes to working cultures, behaviours, skills and attitudes to achieve effective partnership working with a genuine community focus.

HMIC acknowledges the findings of the recently published Audit Scotland Report 'Community Planning: An Initial Review', and the recommendations contained therein for both the Scottish Executive and community planning partnerships to develop a shared vision and priorities. Although this report does not deal directly with information sharing, it does state that "significant progress has been made in the availability and use of robust data to inform community planning" and that "there is evidence of increased sharing of information on service use between partner organisations".

Partnerships bring together key participants, and so can act as a bridge to link national and local priorities better. This should be a three-way process, whereby local community planning partnerships can influence national direction and help to co-ordinate the delivery of national priorities in a way that is sensitive to local needs and circumstances. Local or neighbourhood priorities should also be able to influence priorities at the community planning partnership level.

2.3 Anti-Social Behaviour

During this inspection HMIC found that a significant contributory factor in developing partnership working and information sharing arrangements across agencies, had been the maturing approach to tackling anti-social behaviour. The Anti-social Behaviour etc (Scotland) Act 2004 has specifically addressed the need to share information in tackling local problems in terms of Section 139, which states that to manage anti-social behaviour effectively the relevant agencies must share information at a local level.

Under the provisions of section 139, any person has the power to release information to a relevant authority where that is necessary for the purposes of any measure in the 2004 Act or any piece of legislation which relates to tackling anti-social behaviour. Clearly this includes exchanging information in relation to ASBO (anti-social behaviour order) investigations, applications and other relevant matters.

Section 139 also provides that, where confidential information is released to a relevant authority under this section, the receiving authority must respect that need for confidentiality.

HMIC believes that including this section in the Act paves the way for an environment where a wider and even more frequent exchange of information and intelligence is possible in the future, in order to strengthen communities and make them safer.

2.4 National Data Sharing Forum

The launch in April 2006 of a National Data Sharing Forum and Local Data Sharing Partnerships offered a governance structure for personal data sharing in Scotland, with the aim of providing a framework within which Scottish Ministers and local partners can collaborate to facilitate inter-agency data sharing. The National Data Sharing Forum was developed from the Scottish Executive eCare framework, which is the name given to the technology developed by the Data Sharing and Standards Division of the Scottish Executive to enable information sharing between agencies for the care and protection of citizens. (See Model 1)

The purpose of the National Data Sharing Forum is to develop coherent and integrated national approaches to data sharing. Fourteen local data sharing partnerships are planned, each based in a health board area. The two main priority areas for these partnerships in the first year are to complete a roll-out of the use of single shared assessments to all adult care groups and to implement information sharing for child protection purposes. This work is closely associated with the Scottish Executive's 'Getting It Right For Every Child' (GIRFEC) initiative, which is discussed later in this chapter (page 18) It is intended that each of the local data sharing partnerships will appoint a data sharing manager to facilitate the work of the partnerships.

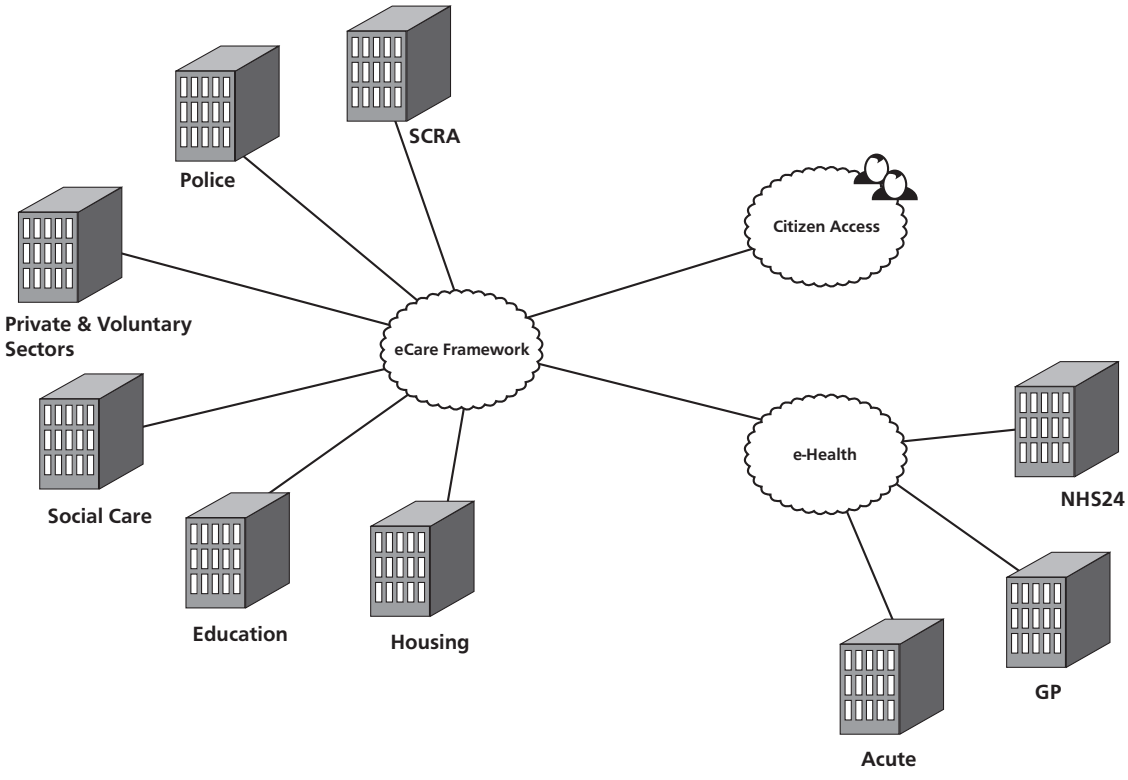
In the 2003 Inquiry into the death of Victoria Climbie, Lord Laming's report noted that information sharing is "a matter that Government must address. It is not a matter that can be tackled satisfactorily at local level" (Lord Laming, The Victoria Climbie Inquiry 2003, paragraph 1:44). HMIC acknowledges the progress made since then towards greater information sharing, and supports the view that this issue reaches across all organisational and geographical boundaries.

2.5 The Data Protection Act 1998

The Data Protection Act 1998 (DPA) became effective on 1 March 2000 and replaced the provisions of the previous 1984 Act. The DPA contains the following eight principles:

1) Information must be processed fairly and lawfully

In most cases this relates to an individual's consent to having his or her personal information processed – for example, data protection notices in application forms. When the information contains sensitive data, e.g. trade union membership or health details, then explicit consent must be obtained and recorded. There are exemptions to this requirement that can be applied to information processing for 'policing' purposes, e.g. for preventing or detecting crime, or apprehending or prosecuting offenders.



Model 1

2) Information must be obtained for one or more specified and lawful purposes (as per the notification)

Data obtained for a specific purpose, e.g. personnel/employee administration, can only be used for that purpose. The purpose(s) of obtaining and retaining the information, arrangements for processing it, as well as the sources and disclosures for the data, must be notified to the (Data Protection) Information Commissioner. Such notification provides the basis for retaining and using the data.

3) Must be adequate, relevant and not excessive for the purpose

4) Must be accurate and, where necessary, up to date

Obviously information should be appropriate for its intended use and maintained accurately. Information that is not necessary for the purpose, which could therefore be classed as 'excessive', should not be requested or retained.

5) Must not be kept longer than necessary for the specified purpose

There should be retention policies for the information retained, in accordance with the purpose identified.

6) Must be accessible to the individual concerned

Individuals have a right to access and obtain copies of their own personal data – though not that relating to a third party. This provision is to allow individuals to check that information retained about them is accurate and appropriate.

7) Must be surrounded by proper security

Processors of personal data are obliged to ensure that appropriate technical and organisational measures are taken to protect the data held. Where government protective marking is used, further security implications may apply to certain information.

8) Must not be transferred out with the European Economic Area (EEA) except in certain circumstances

If there is a requirement to process or share information with a country not within the EEA, steps should be taken to ensure that the data protection principles are taken into account.

From an information sharing perspective, organisations which process personal data must take due cognisance of the data protection principles at every stage. Each organisation is expected to adopt appropriate guidelines or protocols, within the lawful authorities, to process, secure and retain data. In light of Principle 6 regarding access by individuals, and following the introduction of the Freedom of Information (Scotland) Act 2002 (FOISA) on 1 January 2005, the process for dealing with requests for information from an organisation other than the one the information originated from, must be clarified from the outset. The timescales for dealing with requests under either Act must be adhered to.

Historically the police service has viewed the DPA as an inhibiting piece of legislation. This position, whilst perhaps understandable when first adopted, has undoubtedly had a negative effect on the quality and quantity of information being shared between forces and with partner agencies. The Bichard Inquiry commented that misinterpretation of the DPA prevented partner agencies from delivering an effective service. The report advocated that "better guidance is needed in the collection, retention, deletion, use and sharing of information, so that police officers, social workers and other professionals can feel more confident in using information properly" (The Bichard Inquiry 2004, 4:23).

The police service was not alone in its restrictive interpretation of the DPA. Partner agencies have also used the Act as an excuse for not sharing information. The recent MacLeod short-life working group was established to examine the national guidance on information sharing between the National Health Service (NHS) and police. This group was set up as a result of uncertainties over the extent of any duty of confidentiality placed upon NHS staff, identified during inquires into the deaths of Rory Blackhall and Simon Harris in West Lothian in 2005 (referred to in Chapter 3 page 32).

As recently as September 2006, an HM Government document - 'Information Sharing Vision Statement' - identified that "[w]e must, of course, properly use the provisions of the Data Protection Act as a safeguard to protect privacy and confidentiality but it must not be used to justify unnecessary barriers to sharing information" (HM Government Information Sharing Vision Statement 2006, point no. 8).

HMIC also concurs with the vision statement's assertion that the DPA contains sufficient safeguards and that "within the law, it is possible for there to be greater information sharing than currently occurs – and this can be combined with proper respect for the individual's privacy" (ibid, point no. 9).

The Inspection has revealed issues relating to legislative competency and compliance in respect of the Data Protection Act 1998 at operational levels within the police service. The question of training is discussed later in this report and HMIC accepts that improved training on data protection issues may go some way to resolving this difficulty. However, it is suggested that positioning data protection sections within force organisational structures as administrative, as opposed to operational, functions has not helped to discourage an inward facing tendency. The effect can be a negative, protectionist attitude towards data sharing within the force concerned as a whole. HMIC believes that there is a need to ensure that the DPA is interpreted as *enabling* legislation which encourages data sharing, especially in the high-risk business areas of child protection and vulnerable adults. Achieving this will require a change of culture within the police service in Scotland: that is, moving from a default position of data custody to one where the presumption is in favour of data disclosure. HMIC considers that one way of contributing towards that change would be to realign the position of data protection departments within forces.

RECOMMENDATION 1

HMIC recommends that forces review the position of data protection officers and their staff within their organisational structures, with a view to aligning these more closely to the management of operational policing so as to promote an enabling attitude that will assist core business.

2.6 Safeguarding Vulnerable People

Policing is a continuous risk management exercise. It is therefore essential to recognise that fundamental elements of intelligence and information sharing present some of the areas of highest risk. The need to deliver effective data sharing is most apparent in the headline-making, high-risk areas of protecting those vulnerable people in society who are most at risk.

Safeguarding vulnerable adults and children is a multi-agency function, where inter-agency working is essential to ensure that those concerned are protected effectively. The Laming report identified that "[t]he future lies with those managers who can demonstrate the capacity to work across organisational boundaries. Such boundaries will always exist... the safeguarding of children must not be placed in jeopardy by individual preference" (Lord Laming, Victoria Climbie Inquiry 2003, paragraph 1:37).

2.7 Child Protection

There have been many high profile cases and subsequent inquiries in which the arrangements for intelligence and information sharing have come under scrutiny. These include events in Cleveland, Orkney, the Western Isles and Edinburgh, along with the more recent inquiry into the deaths in Soham and the report by Lord Laming referred to elsewhere in this document. Most of these reports have identified, among other matters, that inadequate information sharing across organisational borders has been a contributory factor in the failure of public services to protect the public in these high-risk areas. Lord Laming's report proposed that "[i]mprovements to the way information is exchanged within and between agencies are imperative if children are to be adequately safeguarded... each agency must accept responsibility for making sure that information passed to another agency is clear and the recipients should query any points of uncertainty" (Lord Laming, The Victoria Climbie Inquiry 2003, p.9).

During the inspection HMIC found that, while all the relevant agencies involved in child protection in Scotland are moving towards greater information sharing, this is being undertaken on an ad hoc, regional basis. What is equally apparent is that the commitment of individual practitioners, in all services, is impressive. But that fact in itself, when viewed alongside some of the lingering cultural obstacles, means that there can be an over-reliance upon personal relationships in establishing the basis and format for information sharing.

The Inspection revealed that information sharing between agencies is often conducted through local information sharing protocols that take into account the relevant legislation from the Data Protection Act 1998, Freedom of Information Act 2002, Human Rights Act 1998 and the Children (Scotland) Act 1995. However, there is no universal structure for these protocols and no formal register to monitor their effectiveness.

HMIC recognises the importance of relationships in establishing foundations for enhanced information sharing. Strong relationships will normally build trust between individuals that will lead to greater information sharing. HMIC considers that the ability to develop effective working relationships by personnel who possess strong interpersonal skills, are effective communicators and have good negotiating skills, is vital for personnel working in partnership or in outward-facing positions. These necessary qualities should be reflected in the personal competencies or person specification for such positions. This is especially true for posts within co-located units, but also applies to all posts which involve a significant degree of direct contact between agencies.

SUGGESTION 1

HMIC suggests that forces and partner organisations identify the personal qualities of the most effective members of staff who liaise with partners as part of their front-end operational role, with particular reference to their ability to develop relationships, and use these as specifications for selecting future post-holders.

Nonetheless, whatever the role of relationships they cannot be allowed to dictate the framework for information sharing. Any data sharing structure which is overly reliant upon relationships creates an unnecessary additional degree of risk. Information sharing on this basis has no consistency. No individual, or group of individuals, can or should be relied upon to determine the quality and thresholds of when to share information. Irrespective of the pressure this system places upon these individuals, it would represent a clear failure if information was only to be shared when a specified person was on duty. This would not be an effective method of protecting the public. The Inspectorate also cautions that over-reliance on the quality of individual relationships and levels of trust can be catastrophic to critical information sharing systems when post-holders move. There have to be systems and channels of information sharing that operate effectively, no matter who the post-holders are.

Information sharing protocols give individuals within each organisation the security to share data. However, they do not of themselves create an environment for sharing. Such an environment can only be engendered through strong strategic leadership and commitment, training and confidence. One of the means of consolidating training and achieving that confidence is to apply a formal decision-making process to data sharing that is based upon sound analysis. Consistent information sharing across an organisation and over time can best be achieved within a formalised structure.

Ad hoc arrangements which are overly reliant upon relationships can create a lottery for public safety.

Scenario

Information relating to a child in Area A is shared by health professionals with the police. The combination of this with other information known to the police leads to action being taken by the relevant agencies using the powers conferred on them. An initial referral discussion is called, and the child is removed to a place of safety.

Identical information relating to a child in Area B is not shared by health professionals with the police. This results in the child remaining with the people who pose the risk. This lack of information sharing culminates in the child suffering serious harm.

Whatever the strength of any existing individual framework for child protection, no single agency is able to know the true value of any single individual piece of information it possesses. This creates a situation where sharing decisions necessarily start from a position of incomplete information, and so might well only be directed at those partners indicated by that incomplete information. This can introduce an element of guesswork which exacerbates the risk.

2.8 'Getting It Right For Every Child' (GIRFEC)

Following the 2004 review of the Children's Hearing system, a consultation document 'Getting It Right For Every Child - Proposals for Action' was published in June 2005. This led to the 'Getting It Right For Every Child: Implementation Plan', which was published on 22 June 2006. The plan contains proposals for reforming the delivery of children's services, including the Children's Hearing system. The aim is to place a greater focus on improving outcomes for children.

Implementation was originally intended to involve a three-pronged approach of the following:

- Practice change: developing the tools professionals need to do their jobs better – a single assessment record and plan, practice guidance and skills development.
- Removing any barriers that get in the way of joined up working and prevent more timely and appropriate responses for children.
- Legislation: placing new duties on agencies to co-operate with each other and share information.

The aim is to deliver a child-centred approach by ensuring that agencies work together to assess, plan and deliver improved outcomes for children, particularly those who are vulnerable or at risk. All children should get the help they need, when they need it, from services that are planned and delivered in an integrated way at a local level. It is intended that the agencies and practitioners working with children will work together to ensure that children's needs are met in the most appropriate, proportionate and timely way.

In order to achieve the GIRFEC agenda there is a proposal for developing a 'prototype' ICT system that could facilitate information sharing. The system will be designed to enable the existing systems of individual agencies to be adapted to support the single assessment record and plan. Entries made on the single assessment by any agency and input into the system electronically will have the potential to populate a multi-agency electronic 'store'. Relevant partner agencies can then access this when they have concerns about a child and wish to check who else may be involved (see also Model 1 on page 15). Depending on the information and *its* assessment of the child's needs, the agency can then proceed either to take action or to consult with relevant agencies over what plan may be needed for the child.

The new Executive will consider legislation to support 'Getting It Right For Every Child' after the elections in May 2007. The proposals for legislation were set out in the consultation document on Getting it Right. It is expected to place duties on all agencies to be alert to the needs of every child and to take appropriate action as required, if necessary on a multi-agency basis. It is also anticipated that, where multi-agency action is necessary, the legislative proposals will require a lead professional to be appointed to ensure that the agreed action is taken forward and improved outcomes for the child are secured.

A principle of 'Getting It Right For Every Child' is that the consent of parents/carers to share information should be secured wherever possible. HMIC accepts this principle, but believes that "wherever possible" ***must*** be taken to mean that consent should not be sought where there is any reasonable suspicion that doing so will put a child at further risk. Nor is there any requirement in either the Data Protection Act 1998 or the Children (Scotland) Act 1995 to seek consent. It follows that, in circumstances where the act of seeking consent might increase the risk of harm to a child, discretion must be deliberately exercised NOT to seek consent.

HMIC acknowledges the ambition and vision of the GIRFEC agenda, and supports the progression towards greater integration of public services in delivering public safety.

2.9 Protection of Vulnerable Groups (Scotland) Bill ('Bichard Legislation')

Provisions to disclose information where a child is at risk are the subject of proposed legislation currently before the Scottish Parliament, in the Protection of Vulnerable Groups (Scotland) Bill. The aim was to remove any existing confusion and conflicting information in order to place a primary duty for information to be shared to protect children from harm.

This obligation was not to be placed on the individual professionals but upon their organisations, which would have been held corporately accountable for any failures to share information. Simultaneously, there was to have been a parallel obligation on each agency to provide a concurrent support framework for their staff. Unfortunately, in HMIC's view, at the time of writing, this part of the legislative proposals appears likely to be dropped during Parliamentary consideration of the Bill in early 2007. Nevertheless, Scottish Ministers still intend to produce a code of practice with guidance on sharing child protection information. Although the code will not specifically oblige professionals to share information electronically, there will clearly be training and ICT implications for the police service in Scotland in order to comply with the code. (Referred to in Chapter 6, page 66)

HMIC recognises that these and any future proposals will require direct action from the police service if it is to meet its responsibilities. ACPOS is already working on this and is seeking to clarify some of the issues associated with the legislation.

HMIC strongly supported the direction in which advances in child protection were heading as part of the GIRFEC agenda and the Protection of Vulnerable Groups (Scotland) Bill. While imposing a legal duty to share information in the interests of child protection is apparently no longer on the table, Ministers have not ruled out that possibility for the future, and the Parliamentary objections appear to have been based on a perceived lack of consultation on the subject. HMIC is therefore hopeful that publication of this thematic inspection report will afford all interested parties the opportunity to discuss an alternative approach to achieving the same end, as proposed below.

The issues considered during this Inspection suggest a need both to lower the threshold for information sharing even further than originally proposed by the Scottish Executive, and to give greater assurance to professionals on the security of that information. The GIRFEC programme may still require this to be addressed, as 'Getting It Right For Every Child' applies to all children and not just those who are most vulnerable or at risk. Relying on the criterion of "risk of serious harm" or "significant need" (HMIC understands that these definitions are still being considered at the time of writing) may be correct in so far as taking action to intervene. But HMIC believes that this sets the bar too high for information sharing. It means that little things which, considered in isolation, may not mean very much but which might be part of a much more serious picture, could be ignored at great risk. A far better approach to protecting children and vulnerable adults in the future would surely be one involving more assessments, a higher proportion of which resulted in no interim action, rather than one which in concentrating only on critical cases allowed other serious cases to be missed.

In considering the implications of this HMIC has noted the finding of many reviews of protection failures in the UK (including the most recent in Scotland) that, while each of the separate pieces of information about the risk to the child was known to public services, no one agency or person was aware of all the information. Protection failures often occurred because these isolated pieces of information may not have, in themselves, given cause for concern that the child (or vulnerable adult) was at risk of *serious harm*. The Inspectorate assesses that, even if all the Bichard and GIRFEC reforms had been implemented, failures as a result of not integrating available information could still have occurred.

Scenario

Kirsty is a 10-year-old child. Her teacher observes that she has recently been consistently absent from school. The teacher notices that this is unusual.

At the same time local police officers have information relating to domestic abuse between Kirsty's mother and her new partner.

The social services have information about the adverse home conditions in which Kirsty is currently living.

Health professionals have concerns over a non-accidental injury that has been inflicted on Kirsty's younger brother.

No element of information viewed in isolation gives a clear picture, and some of the elements might not suggest a need for contact with another agency. The true value of the information can only be ascertained when all elements are put together and a collective, shared assessment of the information is undertaken.

While acknowledging the protection afforded to all by the European Convention on Human Rights, it may be that we need to remind ourselves that the state, through its public services, has a greater duty of protection for children and vulnerable adults than it does for other people.

Police experience and skills in this area have developed over recent decades. But neither the police service in Scotland, nor HMIC, would claim that police staff are the most proficient in recognising the first signs of possible risk in children and vulnerable adults, nor in knowing how to protect them once they are identified. What the service is incrementally developing a leading expertise in is managing intelligence. This has required a cultural shift away from the idea that one practitioner seeks, collects, assesses and decides upon the action merited by his/her own intelligence. Instead, the more rational, effective view now is that intelligence cannot be assessed in isolation, that the intelligence gatherer may not be the best person to make use of that intelligence, and that assessing risk to subject and source is best carried out by those who have been specifically trained and have an aptitude for doing so. This has led to the creation of structures and frameworks in which to achieve this *and* to preserve and protect sources. The most recognisable part of this structure to the layman is perhaps the 'intelligence cell' - the hub of trained staff who provide that professionalism, consistency and confidence.

The current multi-agency structures for protecting children and vulnerable adults do not yet facilitate a holistic view of all existing information held by partners about an individual. Partners need to provide a joined-up service which removes organisational, professional and cultural barriers without compromising safety and standards. As reported in 'It's Everyone's Job to Make Sure I'm Alright', which was the 2002 Report of the Child Protection Audit and Review: "The current strengths of Child Protection Committees lie in their role in co-ordinating information exchange, procedures and training". The subsequent Scottish Executive guidance for these committees, contained in 'Protecting Children and Young People: Child Protection Committees', made clear that "[t]he CPC is the primary strategic planning mechanism for inter-agency child protection work in each area". More recently the Scottish Executive vision for overall public service reform is for a 'user focused' climate which advocates greater partnership working and integrated service delivery. HMIC believes that the combination of these imperatives is particularly relevant to information sharing between separate professions, and that there are opportunities for all public service providers to contribute to real improvements in public safety.

The advantages of collaborative working include improved services, preventing people from falling through the gaps, and reducing overlap and duplication. All agencies need to be flexible and work together across common boundaries to meet agreed priority goals. This requires cultural change within agencies and may require the removal of barriers to joint working through the type of government interventions currently being pursued, with some further refinement.

HMIC suggests that an effective system for information sharing to protect children and vulnerable adults would involve all of the following key elements, some of which are based on the proven concept of the intelligence cell:

- a lower threshold of concern as part of the criteria for sharing information on children and vulnerable adults;
- lead agency responsibility for collating information;
- lead agency responsibility for initial consideration of collated information;
- the most sensitive information 'locked' until the source agency or some independent arbiter agrees that further sharing is necessary;
- an equivalent duty on all agencies to share information on children and vulnerable adults; and
- agreed 'trigger' criteria, leading to a single shared assessment that generates co-ordinated and informed action.

This would suggest that for every one of the 30 child protection committee areas (or for some in partnership with neighbouring areas), a central pool of information would be collated from, and accessible with appropriate degrees of access to, all the agencies involved. Only when *all* the available information about a child is collated from *every* agency – i.e. not just from those agencies that initially recognised the need – can a single shared assessment be achieved. The difficulties in achieving this at times when not all the agencies involved are available, i.e. 'out of office hours', is acknowledged. However, this may need to be addressed as a result of the recommendation below.

HMIC is also keenly aware that there are many public service generalist practitioners in Scotland who have contact with children and vulnerable adults, but who do not specialise in protecting these vulnerable groups and may only very rarely be involved in dealing with critical cases. Creating a system that could overcome this lack of experience and exposure would be extremely expensive. Moreover, it is doubtful to what extent training could instil the requisite skills and knowledge to recognise and act upon 'trigger' criteria on the infrequent occasions that these practitioners are faced with them. A better solution would be to raise awareness amongst this group, as recommended by 'It's Everyone's Job to Make Sure I'm Alright', and to implement a system which encourages them to offer information; assurance could be given that the information they give will only be shared if additional information is forthcoming, and sometimes only then with their subsequent permission. Decision making could then be restricted to a limited number of key personnel who can be properly trained.

The Inspectorate believes that the following recommendation contains all of the key elements identified in the paragraphs above, and takes account of the need to focus decision-making on experienced and skilled personnel. However HMIC has not scoped the volume of work which either this recommendation, or the suggestion above for lowering the thresholds for sharing information, would create. It stands to reason that low thresholds for information sharing (not necessarily for taking action) in this area of public safety will inevitably entail greater costs than higher

thresholds would. A solution that falls somewhere between what HMIC recommends and the status quo may be more practicable, but would be a matter more of affordability and efficiency than effectiveness.

The proposal is aimed at gaining the co-operation of those professionals who are properly concerned about the confidentiality of personal information and the effect of unjustified disclosure on public welfare. That co-operation can only be obtained by creating a secure and carefully guarded system which is transparently trustworthy and over which the professionals themselves have ultimate control.

RECOMMENDATION 2A

HMIC recommends that the Scottish Executive consider nominating or establishing a single agency with responsibility for creating a confidential child and vulnerable adult protection registry for each child protection committee area (or combination of two or more) for the purpose of:

(a) collating all information and intelligence from any public service which *could give rise to concern* about the welfare of a child or vulnerable adult residing in that area;

(b) regularly monitoring the information on each child and vulnerable adult;

(c) applying strict rules of confidentiality to such of that information and intelligence which cannot be shared with others unless in exceptional circumstances, and perhaps only then with the consent of the information source (e.g. health information);

(d) providing a 'single shared assessment' of concerns whenever certain criteria are met, with or without information restricted according to prescribed rules, which require joint consideration of a case; and

(e) activating the joint consideration of cases.

RECOMMENDATION 2B

HMIC recommends that the Scottish Executive consider legislating to place a duty on all public services to provide all and any information and intelligence about a child or vulnerable adult, *which could give rise to concern* about the welfare of any child or vulnerable adult and has come to their notice, to the single agency proposed in recommendation 2A.

It might be argued that concentrating too much on improving information sharing in this difficult field shifts attention away from the more important business of agreeing on and executing whatever action is necessary. HMIC is in no doubt that providing the most appropriate and effective service to a child or vulnerable adult, or deciding not to act as the case may be, is the most important aspect of protection. However, it is also true to say that public services and their practitioners across Scotland may fail children and vulnerable adults if they do not have the means of consistently and more frequently getting to the point at which an informed decision to act can be made. Lack of judgement may well be a weakness, but failing to gather available information when the need to do so has been recognised is difficult to defend.

These recommendations aim to overcome the challenges involved in personal, case-specific data sharing between agencies. However there is still a need to recognise the value in greater sharing of aggregated, non-personal data. There is no need for legislation to enable this. Proper analysis of trends and volume across organisational boundaries should help to make effective service delivery decisions and overcome the historical effects of 'silo working'.

2.10 Vulnerable Adults

Safeguarding vulnerable adults is a priority for the Government and all relevant public services. A growing awareness and documentation of the range, level and frequency of abuse towards vulnerable adults has resulted in a national drive for improved protection, led by the Scottish Executive.

The Adults with Incapacity (Scotland) Act 2000 changes the system for safeguarding the welfare, and managing the finances and property, of adults aged 16 and over who are unable to make some or all of these decisions for themselves because of mental disorder or inability to communicate by any means.

In order to provide suitable protection for vulnerable adults, multi-agency guidelines have been developed and currently operate on a regional basis between partner agencies across Scotland. These guidelines rely on regional information sharing protocols, similar to those used in child protection.

The benefits and risks associated with regional information sharing protocols and the role of relationships are almost, if not, identical to those addressed earlier in this Chapter with regard to child protection.

Notwithstanding the specific legislation that relates to protecting vulnerable adults and children, HMIC accepts that both require a collaborative response from the partners involved. Improved intelligence and information sharing between these partners is central to enhancing service delivery in these high-risk areas.

2.11 Health Service Records

HMIC is aware that the confidentiality of health records presents a particular challenge when considering the wider needs of everyone. The earlier recommendation for a single agency to collate child protection information does not resolve that issue for adults. There may be a need to look at the feasibility of applying to adults the type of sharing arrangements recommended for children and vulnerable adults at recommendations 2A and 2B, but with a higher criterion of risk of harm.

Considerable progress in information sharing between the NHS and police service has been achieved through the MacLeod short-life working group recommendations, discussed in depth in Chapter 3 (page 32). These recommendations advocate that police requests for information should not be refused solely on the grounds that *all* health information is confidential.

HMIC recognises that further significant consultation is required to deliver these recommendations successfully. Creating an information sharing group between the police and Health to advance these discussions would be of considerable benefit.

2.12 The Policing Perspective

The preceding paragraphs have discussed the national perspective with reference to Scottish Executive and UK Government policy issues, taking account of the impact on policing matters. The remaining part of the chapter examines the issue of intelligence and information sharing from a police strategy and policy viewpoint.

Strategy and policy development within the police service in Scotland is overseen by the Association of Chief Police Officers in Scotland (ACPOS), whose structure is organised around a range of specific business areas. Policy is agreed at the ACPOS Council, which comprises all chief constables and other relevant representatives. ACPOS and the Scottish Executive regularly liaise over a wide range of policy development.

During this inspection HMIC observed that the weight of ACPOS activity in relation to intelligence and information sharing has concentrated on intelligence. This is understandable given the development of the National Intelligence Model and the Scottish Intelligence Database, which are discussed in the following paragraphs, and the Bichard recommendations as already mentioned.

The increased threat from terrorism and other imperatives has brought a firmer focus to this work and a recognition of the importance of information sharing as a separate but linked matter. To date information sharing has been practiced widely, but with an unstructured approach. ACPOS is now developing improved arrangements for police ICT convergence across the eight forces in Scotland simultaneously with improved business change arrangements. These developments are discussed in the following paragraphs, and provide real opportunities for improving the way in which information is handled in the service.

2.13 The National Intelligence Model

Historically the police service has had some difficulty in effectively collating and analysing information and data on crime and disorder across the organisational boundaries of both police forces and other agencies. The lack of common ICT systems and common standards has made comparisons and the aggregation of data difficult. Recent work by the Violence Reduction Unit in Strathclyde, provides a good example of how some of these obstacles can be overcome.

The police service has adopted a national business model - the National Intelligence Model (NIM) – which facilitates improved business planning. The NIM ensures that information is used in a way that enables managers to determine strategic direction, make tactical and resourcing decisions and manage risk. It is an intelligence-led model which encourages proper examination and analysis of all available information, and decision-making based on sound evidence.

Four main products emerge from the NIM process and these are:

- The strategic assessment. This drives the business of the NIM and provides an overview of current and long-term issues.
- The tactical assessment. This defines short-term issues, comparing current figures to seasonal averages and makes recommendations in accordance with the control strategy (see below).
- Target profiles. These bring together information leading to a greater understanding of a person or group of people, for example a gang of people engaged in criminal or anti-social behaviour.
- Problem profiles. These provide information leading to a greater understanding of a problem, perhaps involving a series of crimes or incidents or a hot-spot location, and make recommendations for tactical resolution.

The NIM is simply the framework that links all aspects of business planning. Having completed a strategic assessment from a comprehensive environmental scanning exercise, a control strategy will be set for the area concerned at a ***strategic*** tasking and co-ordinating group meeting. The control strategy is derived from the strategic assessment and sets the long-term priorities to be tackled under the headings in the tactical assessment document (crime prevention, intelligence and enforcement).

The NIM operates over three geographical levels. Broadly speaking, level 1 deals with local issues as found in a police division or command unit, level 2 with force and regional issues, and level 3 with national issues.

Information used by the NIM is gathered from a variety of sources, including reports of criminal activity, reports of road accidents, criminal intelligence and, in the forces which have adopted this good practice, relevant statistical information from partners. Once collated, this information is analysed by the intelligence unit, which produces the four 'products' indicated above. After analysis, the NIM aims to ensure that the information is used in an effective and efficient manner by identifying problems, prioritising them and allocating an appropriate response.

Central to the NIM is the tasking and co-ordinating group (TACG) process, which operates at all three levels. A tasking and co-ordinating group comprises key representatives from the geographical area under examination, who consider the resources available and prioritise activity for a specified period in a focused fashion. Resourcing decisions are generally aligned to priorities identified within the control strategy and take into account the nature of crimes and or incidents, what is known of the suspects/perpetrators/victims, and any hot-spot locations.

The NIM is not just about intelligence or policing. The principles are very similar to those used in other risk businesses in the public and private sectors, like public health or fund management. It follows that the NIM business model can be applied beyond crime and anti-social behaviour to deliver more effective community safety and partnership working. In some forces, relevant partners are invited to the strategic and tactical tasking and co-ordinating group meetings. HMIC commends this as good practice.

The development of neighbourhood policing has led to the introduction of local action groups. These are multi-agency groups that co-ordinate local neighbourhood operations aimed at the effective tactical resolution of local priorities within the NIM parameters. It is at this level that problem-solving partnerships or the problem-oriented policing model sits. Problem-oriented policing is where partners work together to identify and tackle specific problems, usually short term and connected with either a location, a victim, a perpetrator or perpetrators, e.g. a known anti-social behaviour hot spot. HMIC believes that any community intelligence opportunities arising from these meetings must be tied into the police intelligence system using the Scottish Intelligence Database.

2.14 Criminal intelligence and Community intelligence

The police service in Scotland has a single over-arching system for the storing data that have been assessed as intelligence: the Scottish Intelligence Database (SID). This provides clear unambiguous rules, conventions and data standards in accordance with the Guidance on the Management of Police Information 2006 © ACPO 2006 and the forthcoming ACPOS version of that document, the Human Rights Act 1998 and the Data Protection Act 1998. The SID system is the single repository for all criminal intelligence and HMIC is aware of the work currently being undertaken by ACPOS to advance new and improved versions of the SID. This will allow interfaces to be developed with other national information and intelligence systems, including the Violent Offender and Sexual Offender Register (ViSOR) and the Criminal History System (CHS), with links to

Automatic Number Plate Recognition (ANPR) and individual force data warehouses.

Intelligence across Scotland was previously held in disparate databases within each force. There was no ICT mechanism to share intelligence and officers had no knowledge of the intelligence requirements of other forces or whether a piece of intelligence they possessed might assist in securing an arrest in a neighbouring area. The SID system means that Scotland is the first country in the UK to exploit technology successfully to achieve true cross-border policing and intelligence sharing. SID delivers a unified approach and facilitates communication across traditional boundaries, improving the consistency and accessibility of information and allowing Scottish forces to deliver improved value for money and safer communities.

SID is also the nationally recognised method of recording what has become known as 'community intelligence'. The definition of community intelligence recognised by ACPOS is: *"Local information which, when assessed, provides intelligence on issues that affect neighbourhoods, and informs both strategic and operational perspectives in the policing of local communities. Information may be direct or indirect and come from a diverse range of sources including community and partner agencies."* HMIC is aware that this definition of community intelligence will also be adopted in the Scottish version of the Management of Police Information (MOPI) guidance document, which is discussed later (page 27).

One of the ways of promoting consistency and integrity of intelligence data on SID is to apply nationally defined standard grounds for entry. Standard grounds are established where it is believed that recording and disseminating intelligence material is likely to be of value in:

- the interests of national security;
- preventing or detecting crime and disorder;
- maintaining community safety;
- assessing or collecting any tax or duty/imposition of a similar nature; or
- otherwise serving a significant public interest.

The standard grounds form the basis of the Rules, Conventions and Data Standards, which is an ACPOS document governing the way in which data is entered and retained in the SID.

During the inspection, HMIC noted the proposal to record community intelligence entries under one of several related sub headings, refined to differentiate between different types of community intelligence, such as Antisocial Behaviour, Feuds, Gang Activity, Licensing Issues, Community Tensions and Youth Disorder. In addition a new heading of 'lifestyle' has also now been created to manage a specific type of Community Intelligence relating to an individual(s), but which will require further development. Such entries would cover instances when entities (such as telephone numbers, vehicles and addresses) are identified in the absence of any other information which would justify retention under the Standard Ground, but where the entities are linked to 'nominals' who are worthy of note.

Using these headings will make the quality of life issues and tension indicators associated with community intelligence easier to assess. The information gleaned from this process will result in action being taken to address these issues through the National Intelligence Model (NIM) tasking and co-ordination process described earlier.

HMIC welcomes this clear and straightforward guidance. However, the inspection found that where community information does not meet the standard grounds for recording in the SID, it is routinely retained in other data repositories, e.g. command and control or crime management systems. If a force cannot extract this type of information from systems easily, for example due to technological difficulties, it is clear that collecting such information may be wasted effort or that the potential to use the information will be lost. Similarly, where such information cannot be shared in a national system, the inherent dangers of geographical boundary constraints come into play.

Partner organisations also often hold community information. Forces should adopt strategies that allow them access to this information, in order to assess its suitability for inclusion on SID. HMIC has noted that when partner agencies are aware of the purpose of storing this information on SID, and of the integrity of the system, they are more likely to assist than when they are unaware of these factors.

2.15 Scottish Criminal Record Office

The Bichard recommendations and Laming Report have, properly, imposed additional demands and expectations on the wider criminal justice system in terms of efficient and effective sharing of accurate data within the areas of child protection and public safety.

This environment creates an opportunity to review the existing data sharing arrangements involving the Scottish Criminal Record Office (SCRO) and partner agencies, regarding access to the Criminal History System (CHS). Developments to existing business practices could result in improved efficiency savings.

Currently, the Crown Office and Procurator Fiscal Service (COPFS) is given restricted access to CHS. The result of this is that individual force record offices provide CHS information to COPFS on both accused and witnesses. Whilst HMIC accepts that some movement has been made in this area, a forthcoming pilot scheme that will allow COPFS access to previous convictions of witnesses suggests that the current level of access is too restrictive.

The proposed pilot will allow COPFS to access criminal histories using an individual's SCRO number only. To facilitate this police forces have adapted their reporting procedures so that, where applicable, statements will include the SCRO number of each individual. This process means that the administrative and resource burden of completing the task still rests with the police.

Scenario

Under the existing system, when a police officer reports an offender for a crime or a series of crimes where there were civilian witnesses, the relevant police force has to:

- *use trained staff with access to an SCRO terminal to search CHS under the nominal for each individual witness*
- *if a CHS record exists, print the record*
- *physically deliver 'hard' copies of each record to the relevant prosecuting authority.*

The proposed pilot, allowing COPFS greater access to CHS, would still result in the police service having to:

- *use trained staff with access to an SCRO terminal to search CHS under the nominal for each individual*
- *add the relevant SCRO number to each witness statement.*

Once in receipt of the relevant SCRO number, a COPFS employee will duplicate the work already completed by searching CHS using the SCRO number, to print a copy of the relevant record. Clearly this approach will not assist in improving the timeliness of the overall criminal justice process.

In practice in both situations police human and ICT resources are being used without delivering a tangible policing product.

Many agencies have a legitimate need to access CHS. For example, when a Specialist Reporting Agency (SRA), such as Her Majesty's Revenue and Customs (HMRC) or the Driver and Vehicle Licensing Authority (DVLA), wants to report a case to the procurator fiscal, a force record office has to create the record on CHS and then supply a court print for the procurator fiscal. These overly complicated procedures slow the reporting process for these agencies and generate wasted effort by record offices at the expense of police authorities.

The needless bureaucracy in both these examples illustrates the potential efficiency gains that could be realised by allowing greater access to CHS.

HMIC is aware that ACPOS previously decided that creating and updating offender records should be the sole remit of force record offices. The rationale behind this decision was to preserve the integrity of data standards. HMIC also recognises ACPOS' decision to review the 'create and update' work of individual force record offices on behalf of SRAs. The proposal to establish an Agency Support Bureau within SCRO, to accommodate the work of SRAs, would certainly represent progress.

However HMIC believes that police authorities can no longer afford to subsidise other criminal justice partners by absorbing these inefficiencies. Both require more fundamental changes of approach. It must be possible for partner agencies to introduce vetting, training and systems to achieve the integrity required for the CHS. Equally, the introduction of an Agency Support Bureau within SCRO perpetuates the misapprehension that resolving the problem of SRA access rests within and at the expense of the police service alone. Allowing identified partners in the criminal justice process greater access to CHS would enable all partners to work more efficiently, consequently improving the criminal justice process.

HMIC believes the traditional view that the police alone should manage the CHS should be reconsidered. The needs of criminal justice partners must be more carefully considered against the efficiency of the whole criminal justice process.

During the HMIC inspection of SCRO in 2004 HMIC recommended that:

'ACPOS consult with the Scottish Executive to determine a formal framework which protects the interests of all stakeholders in maintaining accurate CHS, but which facilitates the increased efficiency in working practices which ISCJIS offers (paragraph 5.109).'

In light of opportunities now emerging at national level, not least the creation of the Scottish Police Service Authority from 1 April 2007, it may now be appropriate to return to this.

HMIC accepts that any extension of access to the CHS would have to be supported by a robust structure of governance. This structure should include common data standards and universal protocols, and be underpinned by a rigorous auditing system. However, all such conditions of access must be reasonable and must not create unnecessary disincentives to deter partner agencies.

Meaningful progress in this area may require re-visiting the debate over the role of the eight chief constables as data controllers of SCRO. HMIC has already recommended, in a Review Inspection Report on the Scottish Criminal Record Office (published in December 2006) that the ownership of data on the CHS be reviewed. The additional reasons given here simply give greater weight to that recommendation and so it is repeated here. Seeking Scottish Executive leadership in this matter (perhaps with the assistance of the National Criminal Justice Board) for the benefit of the criminal justice community could be the practical development that is needed to deliver the necessary changes.

RECOMMENDATION 3

HMIC recommends that ACPOS consult with the Scottish Executive to determine whether chief constables should remain as data controllers of all SCRO databases, with a view to arriving at the best solution to promote the accuracy, quality and integrity of data and maximise efficiencies in working practices.

RECOMMENDATION 4

HMIC recommends that as a matter of urgency ACPOS consult directly with all relevant partner agencies with a view to giving criminal justice partners greater access to the criminal history system, while maintaining security and data quality.

2.16 Management of Police Information (MOPI)

A manual of guidance on the Management of Police Information is being developed for the Association of Chief Police Officers in Scotland. It is derived from a similar document produced by the National Centre for Policing Excellence on behalf of the Association of Chief Police Officers in England and Wales, following the publication in July 2005 of the associated code of practice. The code of practice formed part of the government response to recommendations made by Sir Michael Bichard, following his inquiry into the circumstances around the murders of Jessica Chapman and Holly Wells in Soham. The IMPACT Programme, discussed later in this report, is responsible for delivering on the Bichard recommendations for ACPO and the Home Office. ACPOS is working closely with the programme and this work includes delivering a replacement for the PNC by 2010. This is also the latest timeframe for achieving the standards associated with the guidance on Management of Police Information according to the IMPACT Programme.

ACPOS has endorsed the use of the adapted ACPO guidance manual as the Scottish framework for managing police information, a key element of which is the need for common standards in high-risk areas of activity.

The manual defines policing purposes in terms of information management. Policing purposes have deliberately been described at a high level and are intended to be inclusive. The definition does not incorporate every policing activity and no existing legal power or duty on the police is superseded. The fact that these policing purposes do not specifically refer to an activity, e.g. road policing, protecting vulnerable persons or counter-terrorism, does not in any way imply that this is not a legitimate activity for the purposes of police information management. It is important to distinguish between information that is collected for a policing purpose which is covered by the guidance, e.g. crime records or custody records, and information ancillary to a policing purpose, e.g. personnel, pay or invoice records, which are not covered.

This guidance is subject to a nationally agreed implementation strategy, oversight of which lies with the ACPOS NIM Development Project. This involves attaining associated threshold standards, which will be subject to a phased implementation. These standards sit outside the guidance itself, but are part of the overall package for chief officers to take account of in terms of police information management.

The phased implementation of the guidance on the Management of Police Information recognises the challenge for the police service in Scotland at this time. The focus of activity in the initial phase will be on the following six areas, considered to present the highest threat and risk to the service in terms of information management:

- crime
- intelligence
- domestic violence
- child abuse investigations
- firearms revocations and refusals
- custody.

The emphasis for the first phase will be on the standards relating to infrastructure, policy, processes and procedures. Further phases are likely to follow which will progressively raise standards across the whole area of police information management, subject to understanding the full impact across the police service.

Once implemented it may be useful to conduct a thorough review of the guidance, to ascertain users' views and experiences of it in practice.

It is intended that a timetable of compliance for the initial phase will be agreed in March 2007, once force and SCDEA capability assessments are complete and have been considered by ACPOS.

HMIC commends the work undertaken so far in this regard, and the prioritisation of areas of highest risk for the first phase.

2.17 The Scottish Police Services Authority (SPSA)

An important development in Scottish policing, which should coincidentally assist forces in working more closely together by way of information and intelligence sharing, will be the creation of the SPSA.

The SPSA will come into being on 1 April 2007, as a result of the Police, Public Order and Criminal Justice (Scotland) Act 2006. It will bring together several existing support services that operate at a number of different locations throughout Scotland and which have developed separately with different cultures and practices. It will also be responsible for establishing a new Scottish Forensic Science Service and providing future national ICT development and support. It is envisaged that in due course SPSA could take on responsibility for an increasing range of police support services on a national basis.

This is an ambitious and high profile initiative which will require strong leadership and change management skills. The challenge is to forge a new, dynamic and expanding organisation as a single national service with its own identity, and to create a platform for developing and improving further support services.

The SPSA will bring together the existing common police services and some entirely new services into a single national body. The support services provided will be:

- training and education - the Scottish Police College (SPC) at Tulliallan currently provides most formal training for the police service in Scotland. It accommodates up to 650 residential students and a further 3,500 students on short professional development courses each year;
- the development, provision, procurement, maintenance, management, support and oversight of national data and IT systems and records - the Scottish Police Information Strategy (SPIS) is the body which currently co-ordinates national ICT projects across the police service in Scotland, such as the replacement Criminal History System (CHS), the Violent and Sex Offenders Register (ViSOR) and Automatic Number Plate Recognition (ANPR). The Scottish Criminal Record Office (SCRO) provides governance for the Scottish Intelligence Database (SID) and ANPR along with the CHS. The latter system also holds electronic references for fingerprints and images, although these are physically stored at the same location. The convergence and subsequent integration of all police ICT development and procurement will add to this critical mass and should help to create an information synergy which will substantially increase public safety and enhance service;

- a national system for collecting, identifying and verifying forensic evidence (to be known as the Scottish Forensic Science Service).

The SPSA has a duty to provide these support services mentioned, but it will also maintain the Scottish Drug Enforcement Agency (SDEA). The SDEA was established in 2000 to tackle drug trafficking and other serious organised crime in Scotland, such as hi-tech crime and money laundering. The Police Act re-designates the SDEA as the Scottish Crime and Drug Enforcement Agency (SCDEA), with new and expanding statutory powers and functions.

HMIC is aware of and welcomes developments that will improve the way business change in the police service in Scotland is co-ordinated. This is particularly relevant to the development of a single ICT directorate and common ICT systems, discussed later in Chapter 5 (page 59).

The SPSA may also take on other shared services over time which do not need to be provided at a local level and may be more efficiently, effectively and consistently delivered by a single organisation.

CASE STUDY – FIFA World Cup 2006

One of the objectives of examining information and intelligence sharing in this report was to consider the issue from a UK national and international perspective. In light of the increasingly global context to intelligence and information sharing, it was felt that HMIC should explore how the police service shares information on an international platform.

One of the major policing events of 2006 in Europe was the Federation of International Football Association (FIFA) World Cup. This event involved 32 competing nations, with matches taking place at 12 venues across Germany. Studying the intelligence and information sharing for the event would be beneficial to the inspection, it was felt, in two ways:

- *by clarifying the protocols required to allow intelligence and information sharing between nations and how this is managed; and*
- *by observing the extent to which sharing good quality intelligence and information can identify and limit the activities of those intent on committing crime and disorder.*

2.18 Data Sharing Arrangements

Prior to the start of the tournament, a bi-lateral agreement between the German government and the governments of each participating nation was signed. This covered all policing aspects associated with the event and included the facility for information sharing.

In the case of the UK, the Home Office decided to provide the German police with the details of all 3,700 people previously issued with football banning orders under the terms of the Football Disorder Act 2000. These banning orders can be applied for either on conviction for a football-related offence in a criminal court or through a civil court. It is a criminal offence to breach the terms of such an order. The Home Office also gave details of people with football-related convictions. Although no criminal intelligence was provided, such an exchange was permissible under a section of the bi-lateral agreement that allowed the National Football Policing Unit to consider cases on an individual basis.

Where personal information was provided, this was accompanied by a letter signed by the head of the National Football Policing Unit. This letter articulated the terms by which the information was provided, what it could be used for and how long it could be retained. In this case, all such information had to be deleted at the conclusion of the FIFA World Cup.

2.19 Risk Supporters Data Base

In 1994 the German police set up a 'risk supporters database'. All persons with football-related criminal convictions, German football banning orders, convictions for a number of relevant listed offences, or suspected of being involved in football-related violence had their details included on this computer database. For the period of the FIFA Word Cup, all the information concerning risk supporters that had been requested from participating nations was added.

The inspection team discovered that the database was also linked to the principal German police criminal records database, which covers all 16 states and federal police authorities. Any new nominal details could be input by the processing police officer at the same time that he or she was amending or creating a nominal criminal record file, in a single entry data capture process. Thus a standard 'person check' on a nominal in Germany could generate a computer link to relevant information held on the risk supporters database.

2.20 National Police Intelligence and Information Centre (ZIS – Zentrale Informationsstelle Sporteinsatze)

The role of the ZIS was to:

- collect, evaluate and disseminate all relevant information and intelligence from national and international sources;
- summarise and update the information in a Situation Report;
- integrate central foreign liaison officers;
- deploy and give logistical support to international police delegations.

Strengths

- Effective organisational structure constructed around an existing and proven effective national system.
- Documented strategy for information management.
- Evidence of a co-ordinated effort by all the agencies involved, including the 16 German state police forces, the German Federal Police Force and the international police forces represented, towards the common intelligence and information sharing aim.
- General international information sharing conditions set out in the bi-lateral agreement, which also articulates the conditions for sharing personal information.
- Personal information shared in written form, with an indemnity clause included.
- Agreement to share intelligence via a single point of contact and each case considered on its own merits.
- Guidance for intelligence and information sharing contained in the EU policing handbook.
- Single point of data capture into the computerised intelligence system, including the risk supporters database.
- A computerised intelligence system that could be accessed by all German police services.

Weaknesses

- No process for evaluating the intelligence.
- No evidence of tasking liaison officers as a result of the intelligence.
- Insufficient detail of arrested persons conveyed to the ZIS to allow for further action by the arrested person's national police force.

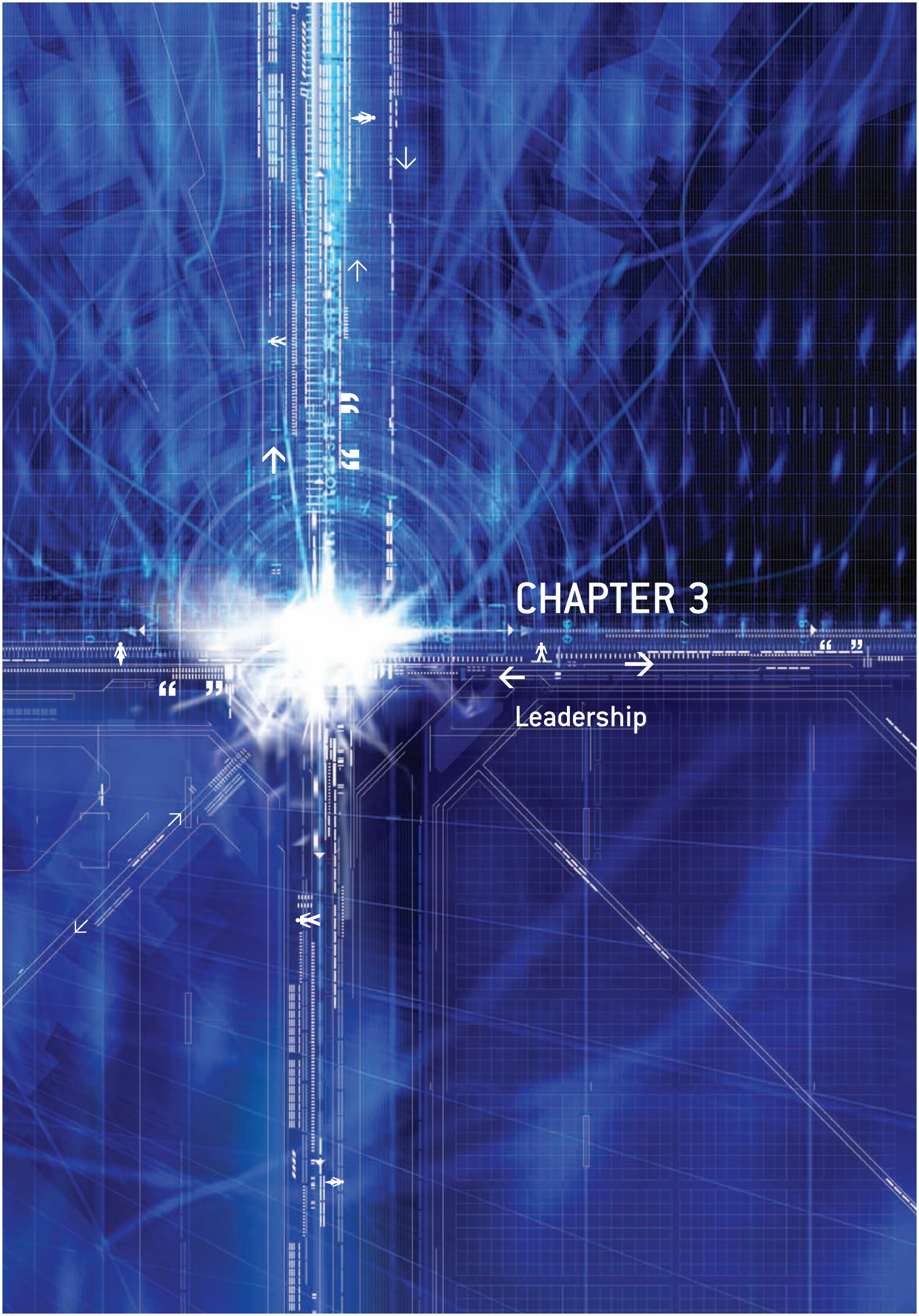
2.21 Conclusion

There is no doubt that the German police worked closely with other countries and established a significant information and intelligence sharing system for the FIFA World Cup. This operation was built around existing police information and intelligence management arrangements, and included the facility to share information and intelligence between the competing nations.

HMIC is of the opinion that several areas of good practice can be identified. Notably, from a strategic viewpoint, bi-lateral agreements between the German government and the governments of each of the participating nations facilitated the official exchange of crucial information, and, on an individual basis, intelligence relating to the proposed activities of prominent known hooligans.

This process was assisted greatly by a national ICT system, established and provided centrally by the German government and common to all 16 federal state police forces, the national force dealing with cross-border policing, ports and railway policing and the Federal Bureau of Investigation. Incorporated in this national ICT structure is a risk supporters database which contains details of all persons with football-related convictions. This database is linked to the principal German police criminal records database, and these two systems can be updated and cross-populated using a single entry data capture process.

This integrated, single-entry information technology for one aspect of policing demonstrates the type of thinking which the police service in Scotland aspires to for *all* its systems.


CHAPTER 3
Leadership

3.1 Introduction

The previous Chapter described current opportunities across the public service for enhanced intelligence and information sharing through strategic and policy developments. These provide a number of challenges for the police service in Scotland and its key partners.

HMIC acknowledges the strategic lead that the Association of Chief Police Officers in Scotland (ACPOS) has demonstrated to date in developing more efficient and effective methods of intelligence and information sharing within its individual business areas. However, HMIC believes that much of the effort has focused on intelligence management and less on information sharing. It is in this latter area that further progress can be achieved.

3.2 Criminal Justice

ACPOS involvement in information sharing is well illustrated by ongoing work in the relatively new Criminal Justice Business Area.

The establishment of a Warrants Action Team and the development of a shared warrants database will provide tangible benefits to all partner agencies. HMIC also notes ACPOS involvement in current reforms of the criminal justice system, through engagement with the Justice 1 Committee of the Scottish Parliament and particularly through participation in the National Criminal Justice Board.

3.3 Freedom of Information

During the inspection HMIC noted that ACPOS had appointed a Freedom of Information (FOI) co-ordinator, on a pilot basis. HMIC looks forward to seeing an evaluation of the benefits of this encouraging development. This role should provide a strategic oversight and corporate view, promoting national consistency in FOI issues across the police service in Scotland.

3.4 Sharing Health Records

Earlier in this report the issue of confidentiality with regard to health records was referred to briefly (Chapter 2, page 23). HMIC is aware of the work undertaken by health and justice partners in this area and believes that the evolution of this work is of particular relevance.

These developments followed the murder of Rory Blackhall in West Lothian in 2005. In a statement to the Scottish Parliament regarding this case, the Lord Advocate said:

> *"Simon Harris admitted himself to St John's Hospital, Livingston in the early hours of 22nd August 2005, the day he was due to appear in court. He was discharged later that day. During the period he was in the hospital some of the nursing staff thought he may have been a person of interest to the police. They passed on that information on the 26th of August 2005. The delay appears to have been due in part to some uncertainty over the extent of their duty of confidentiality. It is unlikely that the information, even if it had been supplied earlier, would have changed the course of events but the uncertainty suggests that further clarification in this area is required."*

Subsequently the Minister for Health and Community Care agreed that a short-life working group should be established to:

- examine the national guidance on information sharing between the NHS and the police, and the way it is applied across the agencies; and
- ensure that it provides clarity for staff who may have to make decisions which call for them to balance issues about patient confidentiality, public safety and the investigation of serious crime.

The short-life working group was chaired by Mr Andrew Macleod, Head of Patients and Quality Division, Scottish Executive Health Department, with representation from the NHS, clinical professions, the Crown Office and ACPOS. Its recommendations are currently being taken forward by the Executive, ACPOS and other relevant interests.

The key recommendations of the Group were as follows:

- National guidance for information sharing between the NHS and the Police should be reviewed and updated.
- The NHS Code of Practice on Protecting Patient Confidentiality should be revised to reflect the Group's recommendations.
- NHS Boards should establish an Information Sharing Partnership Group, involving Police, Procurator Fiscal Service and other key partners (for example, local authorities). This group should do the following: develop and implement a local information sharing procedure based on the revised national guidance; establish arrangements for ensuring that senior NHS staff have round-the-clock

access to senior police staff when required to balance issues of patient confidentiality, public safety and the investigation of serious crime; develop arrangements to ensure the safety of NHS staff who make decisions to share information; and oversee multi-agency education and joint training arrangements.

- Police forces and NHS Boards should agree arrangements to facilitate liaison and data sharing – including two-way secondments.
- An inter-agency information and training programme should be developed to support NHS, Police and Procurator Fiscal staff – which may include 'easy-to-read' posters, on-line interactive programmes and an awareness-raising DVD.

As a result of further discussion following the Group's report, it has been agreed that the responsibility for ensuring effective local arrangements between the NHS and the police, and for developing local processes, should rest with the Local Data Sharing Partnerships discussed earlier in this report. This will ensure close co-ordination with other developments in improved information sharing, including the GIRFEC agenda.

The Scottish Executive Health Department, in discussion with ACPOS, has drafted a revised protocol on information sharing between the NHS and the police. Consultation on this within the NHS and with other key interested parties is planned for the near future.

HMIC commends the Scottish Executive on the progress being made to improve information sharing arrangements with the NHS. It is important to ensure that information is effectively shared where there is a clear public interest and benefit to public safety in doing so. Sometimes this will require difficult decisions to be made in terms of striking a balance between protecting individual privacy and the public interest; strong working relationships and arrangements at a senior level between the NHS and the police will be critical to achieving a shared and agreed approach. It will also be important to establish strong links between the various national improvement initiatives underway for information sharing, so that 'user' benefit is maximised and opportunities are not lost.

3.5 Scottish Prison Service

During the inspection HMIC found a great deal of evidence of improved intelligence sharing with partners, including the Scottish Prison Service (SPS), local authorities and the United Kingdom Immigration Service (UKIS) at both regional and national level.

HMIC considers that some of the ongoing work with the Scottish Prison Service provides an excellent example of the promotion of intelligence and information sharing between the police service in Scotland and key partner agencies.

While the Inspectorate acknowledges the valuable local arrangements in place between a number of Scottish forces and the prison establishments situated within their geographic boundaries, of particular note is the work being progressed by Grampian Police and Her Majesty's Prison (HMP) Aberdeen.

CASE STUDY – Scottish Prison Service

Following significant research and consultation between Grampian Police, the Scottish Prison Service and HMP Aberdeen, a Grampian police officer was appointed as a dedicated Prison Liaison Officer (PLO) as part of an initial pilot project which began on 4 April 2005.

The role of the PLO is primarily to ensure the effective exchange of intelligence and information which may benefit both agencies. Any intelligence or information exchanged between the two services must be treated confidentially and take cognisance of the provisions of the Data Protection Act 1998. Matters of a sensitive nature, including issues such as surveillance and interception, are governed by the provisions of the Regulation of Investigatory Powers 2000, Regulation of Investigatory Powers (Scotland) 2000 and Part III of the Police Act 1997.

It was agreed from the outset that both organisations would independently evaluate the project after six months. Some of the key points identified through the evaluations are as follows:

- *Significant improvement in the intelligence flow between the two organisations, which has helped to reduce intelligence gaps in ongoing operations at National Intelligence Model (NIM) level 1 - local issues and level 2 – cross-border issues.*
- *Development of liaison and information sharing between the PLO and the Scottish Crime and Drug Enforcement Agency (SCDEA), to reduce intelligence gaps in relation to NIM level 3 – serious and organised crime.*
- *Implementation of a NIM compliant tasking and co-ordinating structure within Aberdeen Prison.*

- *The introduction of a standard '5x5x5' intelligence management system (Chapter 4, page 54) and an Intelligence source register within Aberdeen Prison to facilitate robust submission and source protection processes and meet best practice in this area.*
- *The ability to provide enhanced risk assessments both for prison establishments prior to admissions and for Scottish police forces in advance of prisoner releases.*

Both services have identified clear business benefits from this project, which ACPOS and the Scottish Prison Service are currently developing at a national level. Since adopting the NIM process, the Scottish Prison Service now contributes to the Scottish national strategic assessment. In addition, a police officer will be seconded to the National Intelligence Bureau of the Scottish Prison Service, where a Scottish Intelligence Database terminal will be installed in an effort to promote intelligence and information sharing on a national basis.

HMIC recognises that there is considerable potential for a greater flow of criminal intelligence between prisons and the police for the purpose of preventing and detecting crime, and promoting safety; similarly, it recognises that intelligence flowing in the other direction can help with prison safety and encourage future crime preventing intelligence. The Inspectorate also appreciates that one means of addressing this is to locate police staff in prisons as dedicated liaison officers. However other points to bear in mind include human rights and ethical issues, as well as the fact that intelligence from individual prisons will be of varying value to the police forces in which those establishments are located (e.g. the Women's Prison at Corntonvale houses prisoners from well beyond the boundaries of Central Scotland Police). It is therefore necessary that ACPOS consider how best to improve the intelligence flow without incurring disproportionate cost, and thereafter liaise with the Scottish Prison Service to achieve this.

RECOMMENDATION 5

HMIC recommends that ACPOS consider how to improve the two-way flow of intelligence between the police and the prison service.

3.6 Management of Police Intelligence

This inspection has confirmed that throughout all eight Scottish forces and the SCDEA there is clear and robust leadership in the management of police intelligence.

ACPOS firmly supports the National Intelligence Model (NIM), described in the previous Chapter, as one of the key business processes for policing within Scotland. HMIC has found that at strategic, tactical and operational levels there is an understanding of the tasking and co-ordinating processes and a realisation of how effective a tool the NIM has become in defining and delivering service to meet specified demand and need.

The NIM framework allows forces to share intelligence with partner organisations in confidence, and provides clear examples of the strategic lead being given by the executive members of each force. The model contains unambiguous roles, responsibilities and common themes that can be incorporated into improving performance in joined-up areas of business. (NIM policy Chapter 2, page 23)

3.7 Management of Police Information

In several forces, executive members regularly chair regional community partnerships whose aim is to deliver joint services across organisational boundaries, and tackle shared problems. To achieve their goals, protocols for intelligence and information sharing have been developed at strategic level. However, there is some feeling that, although these protocols exist, their effectiveness in delivering the joined-up services for which they were designed can be limited. One of the factors contributing to this shortfall is the lack of an efficient police information management structure.

HMIC recognises the requirement for each force to ensure that all the information it controls is managed effectively and that information management policies and strategies are embedded into its organisational structures. Police forces are data-rich organisations. Nevertheless all data, whether information or intelligence, must be properly managed before it can be used effectively.

HMIC believes that all police information should be treated as a corporate resource. Therefore, information must be collated, recorded and evaluated in a consistent manner across organisational and force boundaries. Failure to meet or even apply these standards is likely to result in unnecessarily over-complicating information sharing both within the police service and with key partners.

HMIC acknowledges ACPOS' decision to endorse and circulate a Scottish version of the Management of Police Information (MOPI) guidance manual (referred to in Chapter 2, page 27). The MOPI was developed by the Association of Chief Police Officers in England and Wales (ACPO) as a direct response to recommendations in the Bichard enquiry on the need for a code of practice governing the management of Police information.

The Scottish version of the MOPI will confirm that the management of police information is an organisational function for each force and that every force needs to be the guardian of the information it stores. This will require a more structured approach to considering information management than there has been until now. Ensuring that a corporate approach to managing all police information is undertaken, both within and between police forces and functions, will enable the service to share data consistently and effectively with partner agencies.

Effective leadership should ensure that all forces have information and intelligence sharing strategies, influenced by the ACPOS and Scottish Executive visions for data sharing, which share core elements such as: the aims of information and intelligence sharing within the force and with other police organisations, and how the force will pursue the idea of 'information push' (see Chapter 5); the aims of data sharing with generic and specific external organisations; organisational structures which delegate management responsibilities for information and intelligence sharing throughout the organisation; and how the force will promote and support sharing, and monitor the effectiveness of its strategy.

RECOMMENDATION 6

HMIC recommends that each force produce and publish an intelligence and information sharing strategy which contains the core elements suggested within this report.

3.8 Development of Intelligence and Information Sharing

HMIC recognises the developments being progressed by ACPOS and advocates that individual forces plan effectively to make the most of opportunities presented by implementation of the MOPI and enhanced information sharing with partner organisations, as previously described in this Chapter.

The very nature of the actions embarked upon by ACPOS and executive members of individual forces demonstrates the valuable work being done within individual business areas to improve intelligence and information sharing. However, HMIC is concerned that the diversity of work currently being undertaken is not supported by a structure of overarching governance.

Improvements in information sharing cannot be achieved in isolation. It must be acknowledged that this is one of the key themes within the wider public reform programme and that an appropriate strategic response is required.

It is important that the variety of good work taking place can be captured and developed within a common strategic approach. This will be fundamental to the contribution which policing can make to wider information sharing in the public sector. HMIC believes that ACPOS is best placed to provide this strategic oversight.

RECOMMENDATION 7

HMIC recommends that ACPOS provide a strategic overview for developing information sharing within each of its business areas, in order to promote a corporate approach in accordance with the Scottish Executive's vision for data sharing across the public sector.

3.9 National and Local Data Sharing Fora

HMIC believes that the advancement of national and local data sharing fora presents a significant opportunity for developing improved intelligence and information sharing between the police service and partner organisations .

A National Data Sharing Forum has been established under the chairmanship of the Minister for Finance and Public Sector Reform, with the intention of moving towards National Data Standards. The purpose of the Forum is to collaborate with local partners to develop coherent and integrated approaches to data sharing at the national level (referred to in Chapter 2, page 15).

National data standards are necessary to ensure that when two separate databases containing information are joined together, or searched simultaneously, the data is compatible and comparable. For example:

Adult A is recorded on all systems as John SMITH, not Smith John or John Smith.

Failure to record all data in a uniform manner creates the potential for information to be lost.

The structure will include 14 local data sharing partnerships, based on the existing Health Board areas. Membership will come from the principal partners: local government, NHS, police and other agencies. Each will plan for electronic data sharing in the partnership area within the national policy priorities and frameworks. They will also implement national data and technical standards using the eCare technical framework to allow partners who hitherto could not converse electronically, to communicate.

The intention is for each partnership to have a multi-agency store, or hub, where a unique biographical record will be used to identify individuals whose records are held. Messages containing information about the individuals concerned will then be sent between the partner agencies via this multi-agency store or hub.

The two main priorities for Local Data Sharing Partnerships established for 2006-2007 are:

- to complete the roll out of single shared assessment for all adult care groups; and
- to implement information sharing for child protection.

HMIC is aware of work currently underway to identify business processes and any existing best practice. The intention is that any messages generated as a result of the Getting It Right For Every Child (GIRFEC) initiative, mentioned in Chapter 2 of this report, could be passed through the multi-agency store as described above. It also follows that any decision by the Scottish Executive to pursue recommendations 2A and 2B of this report could be supported by the concept of a multi-agency store or hub.

SUGGESTION 2

To prevent potential duplication of work and to ensure a co-ordinated approach, HMIC suggests that ACPOS recognise the existing data standards in use across the criminal justice community when seeking to introduce national standards for police data.

The drive towards improved national and local data sharing requires the police service to provide robust leadership at national level, through ACPOS, and at local level through individual forces. However the response must be corporate, to ensure that all development opportunities across all business areas are realised. This is further complicated by the need to take account of the way partners are approaching this area, and the pace of progress in other agencies, the voluntary sector and with private sector partners.

It is clear that strong strategic leadership is necessary to demonstrate commitment, clarify direction and discourage parochialism in tackling information sharing. The liaison and co-ordinating role of ACPOS is crucial in developing wider and better information sharing, and HMIC strongly encourages its members to accept a leadership role in this important work.


CHAPTER 4
Partnership Working

4.1 Introduction

As previously indicated within this report, HMIC acknowledges the opportunities which currently exist to improve the services delivered by partnerships through enhanced intelligence and information sharing. It is now more apparent than ever that meeting customer needs can most effectively and efficiently be achieved through partnership working. The outcomes reached by partnerships will be enriched if successful systems and procedures for intelligence and information sharing are achieved.

4.2 Community Planning

The Local Government in Scotland Act 2003 places a statutory obligation on local authorities to initiate, facilitate and maintain community planning. It also requires other key partners, including the police, to participate in the two main aims of the community planning process, which are to ensure that:

- people and communities are genuinely engaged in the decisions made on public services that affect them; and
- organisations are committed to working together, not apart, in providing better public services.

The main components of the Act include a duty to secure Best Value, a power to advance well-being, a statutory basis for community planning and a framework for the better delivery of public services.

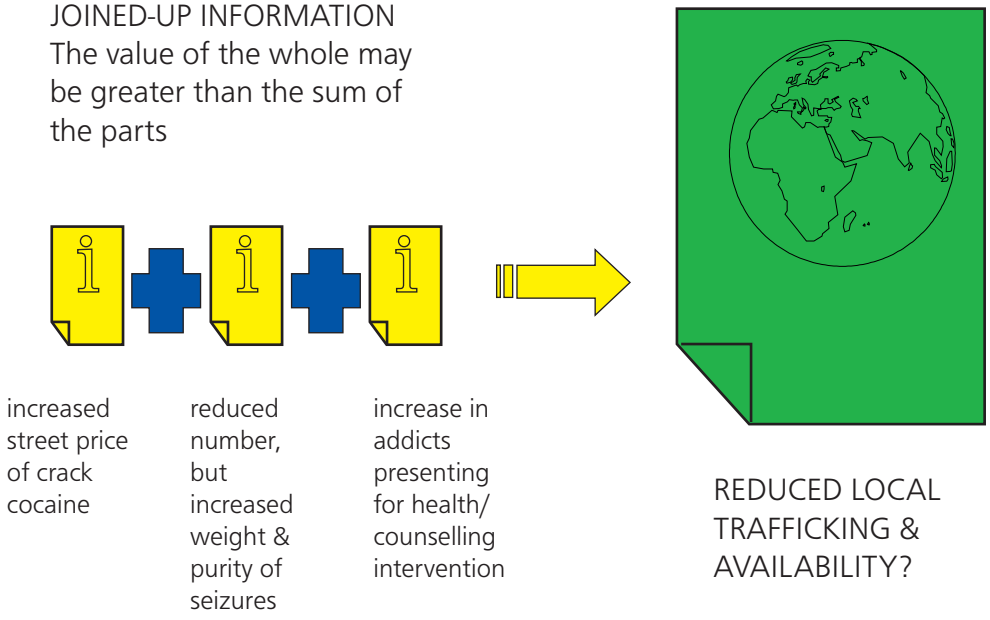
The aims of community planning are supported by two further principles:

- that community planning is the key over-arching partnership framework helping to co-ordinate initiatives and partnerships and where necessary acting to rationalise and simplify a cluttered landscape; and
- the ability of community planning to improve the connection between national priorities and those at regional, local and neighbourhood levels.

Recognising community planning as the key overarching partnership framework reflects the fact that it should not be an additional or parallel process. Rather it should should act as the umbrella partnership arrangement for other partnerships and initiatives at regional, local and neighbourhood level. The essence of community planning is collective or collaborative working, as well as the integration of the various planning and service delivery functions of the local authority and other community planning partners for the purpose of identifying and solving problems, improving services, and sharing resources.

Community planning operates at various structural levels within local authority areas, from the pan-authority strategic partnerships to local, neighbourhood or thematic partnerships. The importance of having effective information sharing structures within this process is obvious, even though delivering information sharing arrangements in practice can sometimes be complex.

At a **strategic** level, information from various sources is used to inform policy and evaluate the outcomes of policy and practice. This allows strategic partners to pose the question: "Is what we are doing separately and in partnership having any effect?"



At the **tactical** or themed partnership level, where community safety partnerships, drug and alcohol action teams, anti-social behaviour units, criminal justice and child protection inter-agency committees operate, data sets from the various statutory, community and public bodies involved in the community planning process can be over-laid. This contributes to a greater shared knowledge of the topic under scrutiny, so that cause and effect, or correlation, can be better understood and joint tactical operations planned. An example of this might be to examine how drugs trafficking enforcement and heroin seizures are related, if at all, to issues such as availability, socio-economic landscape, methadone prescription rates, uptake of counselling services, reports of heroin dealing activity and drug deaths, and whether this understanding will lead to a total knowledge which is greater than the sum of its parts.

At the **operational**, local or neighbourhood level, partnership groupings will include local anti-social behaviour task forces, case-specific conferences, neighbourhood management groups, problem-oriented policing partnerships sometimes known as problem solving partnerships, and so on. In these groups, information sharing arrangements between partners will focus mainly on data concerning locations, victims, offenders or suspects. It must be acknowledged that there is the likelihood of an overlap, as some of this information will also be discussed at the tactical level. It is vital that each partner brings all the relevant data to the partnership table so that the full picture can be viewed. However, much of this information will be of a personal or sensitive nature; caveats must be in place to ensure that it is only used for the purpose intended and complies with all the relevant legislation, or that information is redacted to conceal identities. It is perhaps at this level, when dealing with personal or sensitive information, that the greatest challenges exist.

During the inspection HMIC found that all forces were engaging in the community planning process, with perhaps the most developed information sharing partnership structures being found in the work associated with anti-social behaviour. This progress has no doubt been assisted by the introduction of the Crime and Disorder Act 1998 and the Anti-Social Behaviour etc (Scotland) Act 2004, both of which articulated processes and procedures and gave power to share information to further the main purposes of the legislation.

4.3 Community Safety Partnerships

HMIC found that, unsurprisingly, community safety and anti-social behaviour have emerged as core themes in most community plans. Community safety partnerships have become important decision-making and delivery mechanisms within community planning. In the report 'Threads of Success' (Scottish Executive, November 2002) the following COSLA definition of community safety was recognised as being accepted by the majority of community safety partnerships:

> *"protecting people's right to live in confidence and without fear for their own or other people's safety".*

This embraces a range of issues including crime reduction, domestic abuse, drug and alcohol abuse, road safety, fire safety and accident prevention. As intimated in HMCIC's Annual Report for 2005-06, the Inspectorate believes it is unrealistic to use the incidence of total recorded crime (or the crime rate as it is more commonly known) as a measure of police performance. So many factors outwith the control or influence of policing activity affect the crime rate that it makes more sense for *reducing crime* to be seen as a partnership responsibility - shared at national level between Government and national public services as well as the crucially important private sector, and at local level between those engaged in community planning.

'Threads of Success' recommended that community safety partnerships build a platform for partnership by establishing a three-tier structure, not unlike that used within the National Intelligence Model:

- senior partners group (to commit the organisation, direct, agree and review action);
- operations group (to manage, task and implement); and
- task groups (to deliver on key priorities).

Local data sharing partnerships, referred to in Chapter 2 (page 15), are being established in the 14 health board areas across Scotland. Their role is to provide electronic data sharing in the partnership area within the national policy priorities and frameworks.

HMIC believes that an opportunity exists to develop the use of the local data sharing partnership structure further in the future, to facilitate data sharing arrangements for community safety partnerships. A challenge too, will be reconciling the differing boundaries that exist between the 32 community safety partnerships in each local authority area with the 14 health board areas.

SUGGESTION 3

HMIC suggests that local data sharing partnerships should work towards collecting personal (with appropriate safety measures) and aggregated data sets from all the principal community safety partners, to facilitate strategic business planning as well as individual- and location-related case management.

4.4 The Edinburgh Community Safety Partnership

During this inspection HMIC found a range of effective models for managing community safety issues. Elements of particularly good practice were observed in the Edinburgh Community Safety Partnership (ECSP) business model. The Partnership was restructured in 2004 to reflect the recommendations for a three-tier structure in 'Threads of Success'. It is important to note that Lothian and Borders Police re-organised itself some three years ago to create one large policing division for Edinburgh, co-terminous with the City of Edinburgh Council boundary. One of the main aims of this re-organisation was to facilitate effective partnership working of this kind.

The ECSP meets quarterly and is made up of elected members, chief officers and heads of service representing the partner agencies. The main function of the partnership is to provide scrutiny and leadership as well as to monitor the performance and delivery of the key targets laid out in its community safety strategy, including priority elements from the police divisional control strategy. This is effectively the 'senior partners' or **strategic** steering group.

In addition to the strategic meeting, there are a number of strategic working groups for main work areas such as anti-social behaviour. Scrutiny of the partnerships work is provided through the City of Edinburgh Council Communities Scrutiny Panel as well as the Council Executive.

The ECSP has invested in two dedicated partnership analyst posts which are funded by the partnership and employed by Lothian and Borders Police within its divisional intelligence unit. These analysts have access to information from all of the partners and are responsible for creating a number of information products that are essential to the effective working of the National Intelligence Business model in force.

The community safety strategy was developed following a comprehensive audit of relevant aggregated or non-personal data gathered from many of the partners, undertaken by the Community Safety Unit of the City of Edinburgh Council.

The information collated included:

- Lothian and Borders Police: incident data, road traffic accidents statistics and crime statistics.
- City of Edinburgh Council Housing Department: anti-social behaviour data.
- Council Environmental and Consumer Services: noise nuisance data.
- Education Department: information on school exclusions.
- Lothian and Borders Fire and Rescue Service: dwelling house fire data, statistics regarding attacks on fire crews and data on secondary fire setting.
- NHS Lothian: information on household accidents.
- Edinburgh Royal Infirmary Accident and Emergency Department: relevant data concerning admissions as a result of violence, accidents in the home, alcohol consumption, drug deaths, road collisions and poisonings.
- British Transport Police: data regarding crime and incidents both at stations and on routes.
- The Youth Justice Partnership: findings from an academic study of youth transitions and crime and SCRA data on relevant referrals to the Children's Reporter.
- Victim Support: information on certain referral categories.
- Edinburgh Drug and Alcohol Action Team: data on the arrest referral scheme and child alcohol consumption information.
- Edinburgh Racial Incident Monitoring Project: information on the remote reporting of racially motivated incidents or crimes.

By analysing this extensive range of information, priority areas for ECSP activity were established. These priority areas form the basis for the partnership control strategy, as well as the focus for activity in the partnership tactical assessment document which the analysts produce monthly. Policing priority areas, identified from the police divisional level 1 tactical assessment document, are also included within the partnership tactical assessment document. This enables

a degree of joint or complementary objective-setting as well as providing a structured basis for partnership tasking and collaborative working arrangements.

A monthly tactical tasking and co-ordinating group meeting provides a tactical focus to the delivery of key initiatives and targets from the strategy. The group is made up of service managers from the range of partners, is jointly chaired by police and local authority officers, and provides a responsive function to ongoing events. The group has sought to adapt the principles of the National Intelligence Model, described in Chapter 2, into a partnership business model so that its agenda is set by a monthly 'partnership' tactical assessment document. This allows the group to remain focused on action.

As well as identifying actions to tackle particular incidents and events, the partnership tactical tasking and co-ordinating group manages a problem-solving fund. This is accessible to all agencies through an established problem-oriented policing or problem-solving partnership (PSP) structure.

This formal problem-solving partnership approach is now in its third year in Edinburgh. Though primarily aimed at council, police and fire and rescue officers, formal training is given to all agencies. Centred on the 'SARA' model, which involves the scanning, analysis, research of and selection from, a range of possible responses, and assessment of the results, locally based officers are encouraged to form PSPs. Each is supported by the partnership analysts and is required to be registered with the City of Edinburgh Council Community Safety Unit. A problem profile document is created at the start and end of the PSP so that input can be assessed against output and outcomes. Although encouraged to use available resources where possible, PSPs are able to make bids for additional resources to the monthly partnership tactical tasking and co-ordinating group, and link with the police divisional tactical tasking and co-ordinating group.

CASE STUDY

In one area of Edinburgh a web of walkways and cycle paths is intended to provide safe routes for travel and for leisure. It became apparent that the walkways were attracting youths congregating in groups, abusing alcohol and carrying out low level drug abuse. Other problems included harassment of cyclists and pedestrians, fire raising, vandalism, motorcycle use and abandoning stolen cars.

Edinburgh's multi-agency NIM approach addressed this problem. Having initially been highlighted in the partnership and divisional level 1 tactical assessment, the partnership TACG requested that a problem profile be produced by the partnership analyst. Information was obtained from the Fire and Rescue Service, Anti-Social Behaviour Dept of the City of Edinburgh Council, British Transport Police, bus companies and NHS Lothian. By assessing the collective information the extent of the problem could be fully appreciated and appropriate recommendations made to address concerns.

The partnership TACG decided that a problem-solving partnership (problem-oriented initiative) should be established. As well as police, the partners for the PSP were: City of Edinburgh Council Departments – Housing, Cleansing, Environmental Wardens, City Development, Anti-social Behaviour teams and Recreation Dept; the local Youth Centre; Edinburgh Leisure; two local Community Councils; the local secondary school; Lothian and Borders Fire and Rescue Service and local elected members.

The main objectives of the PSP were to reduce the following:

- *instances of vandalism to the walkway;*
- *youth calls associated with the walkway;*
- *people using stolen motor vehicles on the walkways and/or abandoning vehicles there;*
- *harassment of cyclists and pedestrians; and*
- *instances of wilful fire-raising.*

Actions taken included the following: increasing security at a derelict building; cutting back all foliage and shrubbery; upgrading lighting; providing extra services at local youth clubs and leisure centres; enforcing licensing legislation; increasing patrols by Environmental Wardens; giving educational inputs at local schools; implementing traffic calming measures and increasing high visibility police patrols.

During the life of the PSP the group received regular problem profiles from the ECSP-funded analyst, which included information on calls relating to youths, vandalism, and secondary fires. Feedback received from two local community councils also enabled tactics to be adjusted as necessary.

Conclusion

Only through sharing information from all the partners could a complete assessment of the problem be realised. The resulting multi-agency actions as a result of this knowledge contributed to the following decreases in comparison to the same period in the previous year: vandalism -16%; youth calls -20%; abandoned stolen vehicles -50%; and complaints to police involving harassment to pedestrians and cyclists –52%. In addition, there were no reported incidents of fireraising.

The approach adopted in Edinburgh, reflected by degrees in other parts of the country, is welcomed by HMIC as a valid and successful attempt to incorporate the principles of the NIM and an effective problem-solving methodology into partnership business.

The National Intelligence Model is by no means the only way that this kind of synergy and progress can be achieved. But it is certainly the only model of its type which is used and understood by all police forces in Scotland, and by an increasing number of their key partners in community safety. It makes eminent sense for this trend to be replicated everywhere in Scotland so that a common language and methodology is understood and practiced, and so that advances and good practice can be rapidly shared.

RECOMMENDATION 8

HMIC recommends that forces and the Scottish Executive encourage principal service delivery partners concerned with community safety and anti-social behaviour to adopt the principles of the National Intelligence Model as a business model for this work.

CASE STUDY

Within the Highlands and Islands, key public service partners such as the Heads of Council Departments, i.e. Social Work, Housing, and Education, as well as the Regional Procurator Fiscal, the Reporter to the Children's Panel, Northern Constabulary and others, attend a partnership tactical tasking and co-ordinating group which meets in the afternoon immediately after the Force tactical tasking and co-ordinating group.

This means that the police can immediately share matters which affect or need to be known by one or other of the partners. The meeting operates in a similar way to the police TACG. Information on partnership initiatives, for example the progress of anti-social behaviour investigations, is also discussed at this time.

The agenda and business discussed is driven by a document which is similar to a tactical assessment, and which contains an information note on the front page reminding the readers of their responsibilities under the terms of the Data Protection Act 1998.

The partnership meeting has a joint chair which is shared by the police divisional commander and a senior manager from a partner agency.

CASE STUDY

In North Lanarkshire an edited edition of the divisional strategic assessment document, produced every three months, is shared with criminal justice and community safety partners. This document is forwarded to the Sheriffs who cover the area, the Procurator Fiscal Service and the North Lanarkshire (community planning) Partnership.

Sharing this strategic document gives principal partners the opportunity to view police priorities and consider, if they so wish, how this will or should affect their own business. Not only does it inform criminal justice partners what senior police managers perceive to be the developing external environment in which they operate, including threats and risks from crime and disorder in the medium to long term, it also tells them what these police managers are doing and intend to do about this, where they intend to prioritise their resources and why. This affords partners the opportunity to take positive and complementary action when appropriate or even to advise on alternative options.

HMIC recognises the constructive action taken by the North Lanarkshire Division of Strathclyde police as good practice because it includes all partners, encourages transparency, and clearly contributes to the assessment of 'public interest' by criminal justice partners (see also para. 49 under Criminal Justice System Partnership).

4.5 Glasgow Anti-Social Behaviour Task Force

During the inspection the development of Glasgow's approach to anti-social behaviour was brought to HMIC's attention. The model has been applied to ten Glasgow Council wards at the operational or task group level, with the purpose of tackling anti-social behaviour in these areas (there are plans to extend this to all Glasgow wards in a significant re-structuring programme for services).

The anti-social behaviour Task Force brings together all the various agencies who can contribute to the overall aim of reducing anti-social behaviour. Functions concerned with private landlord registrations, victims and vulnerable persons, community relations, Street Watch (public space CCTV), services for young people, restorative justice, neighbourhood management services, neighbour relations, Greater Glasgow Housing Association and Strathclyde Police (including an enforcement team) have established very effective and co-ordinated joint working, with information sharing arrangements which are articulated in a joint protocol.

Associated with the group is a Police Information Unit, consisting of an inspector, an analyst co-ordinator and an administrator. The Unit works very closely with the task force analyst, collaborating in the creation of intelligence products.

The Unit receives information from sources across the partnership, including the Strathclyde Police command and control (incident recording) system, the Scottish Intelligence Database, the Strathclyde Police crime recording system, pro-forma reports submitted by community support wardens, and various reports and spreadsheets updated daily from each of the sections of the Task Force and the Fire and Rescue Service. Liaison on emerging issues takes place on a daily basis between the inspector in the Information Unit and the local police divisional intelligence officers.

The principal products of the information unit are as follows:

- *Tactical assessment* – This is the main product of the Unit. It is created every four weeks and forms the basis for discussion at the Task Force tasking and co-ordinating group (TACG) meeting. The Task Force TACG meets the day after the police divisional TACGs. The inspector attends both, along with the sergeant from the police enforcement team. The tactical assessment contains information on seasonal trends and gives crime trends for the year. The content centres on a control strategy based on the anti-social behaviour priorities, gives details on suspected offenders, locations and victims and recommends preventative measures, information/intelligence requirements and enforcement options.
- *Daily briefings* – Information regarding anti-social behaviour is extracted from the force command and control system on a daily basis. It is distributed to the Task Force partners but is primarily aimed at the neighbourhood community support officers to enable tasked hot spot patrolling.
- *Weekly offending briefing* – This is a list of all anti-social behaviour offences committed during the previous week, where a suspected offender has been charged. It shows the name of the suspected offender, the offence committed and the location of the offence.
- *Problem profiles* – Work here falls into two distinct categories: 1) the Unit will help to produce police divisional problem profiles when related to anti-social behaviour in their areas; and 2) they produce their own Anti-Social Behaviour Task Force problem profiles for areas which are causing particular problems or are hot-spot locations for anti-social behaviour.
- *Target profiles* – The information contained in these documents is centred on offenders or persons suspected of committing anti-social offences. These products will also contain information on a subject's possible criminal associates and other relevant social material. Offending patterns are tied to a GIS mapping system. These documents are mainly for the use of the Task Force Case Management Unit which will be tasked with actions.
- *Communications report* – this is an internal document for use by the Task Force. It gives statistics from each Department in the Task Force and indicates who is dealing with specific cases.

The Task Force has a tasking and co-ordinating group meeting every month, with a progress meeting at two-week intervals. The agenda for this meeting is taken from the Information Unit's tactical assessment. At this meeting there is open and frank discussion about anti-social behaviour, with an emphasis on hot-spot locations, victims and perpetrators/suspects. Tactics are discussed and agreed and tasks allocated to the multi-agency team. A good example of the effectiveness of these collaborative working arrangements is given in the case study below.

The Glasgow Anti-Social Behaviour Task Force operates a business model styled on the National Intelligence Model and linked to the police divisional tasking and co-ordinating groups. It enables prompt action to be taken to address trends and challenges in the priority areas, as defined by the agreed and published strategy, and also allows for constant monitoring of performance in these areas. HMIC believes that this is an effective structure for delivering joined-up services for anti-social behaviour.

SUGGESTION 4

HMIC suggests that the business models adopted by the Edinburgh Community Safety Partnership and the Glasgow Anti-Social Behaviour Task Force be recognised as good practice, at strategic, tactical and operational levels respectively, and be considered for adoption by other community safety partnerships and anti-social behaviour partnership groups.

CASE STUDY

The problem of anti-social behaviour in a neighbourhood of Glasgow containing shops and a dental practice first came to the attention of Neighbourhood Management Services, part of the Anti-social Behaviour Task Force, in March 2006. This was as a result of persistent safety concerns raised by the immediate community. At this location were an unoccupied former take-away food store, a betting shop and a lane used as a thoroughfare to these shops from licensed off-sales premises.

In order to assess fully the extent of the problem, community safety patrol officers were tasked with patrolling the area. Their role was to speak with the public, ascertain their views and then feed these back to the Task Force, as well as to provide reassurance. Task Force members also interviewed shopkeepers and their customers, and held meetings with local youths and teachers.

The results of this consultation exercise were combined with data from police incident recording and crime reporting and other information that the Information Unit had obtained from partner agencies. A problem profile document was produced which confirmed the location to be a hotspot for group disorder and associated criminal activity. The nature of the problems and possible tactics to address them were fully explored in a free exchange of information between the partners at the tasking and co-ordinating group meeting, allowing appropriate tasks to be allocated.

A police operation resulted in several arrests and remedial action taken by partners continued to be directed and monitored by respective monthly and fortnightly meetings of the multi-agency tasking and co-ordinating group. Progress reports recorded not only the action taken, but also the effects that partner activity was having and any necessary re-focusing of activity undertaken as a result.

Conclusion

Although still at an early stage, initial analysis has shown a significant decrease in reported crime, of about 80%, and a drop in reported incidents to the police of about 60%. However a longer-term evaluation will need to be carried out to highlight any sustainable impact that these initiatives have made.

CASE STUDY

A joint Strathclyde Police and South Lanarkshire strategic assessment document was produced when the Council was preparing its anti-social behaviour strategy in 2004. Information gathered as part of this exercise from a variety of sources had indicated that vandalism might be an area for attention. Data from the police incident recording system and the crime recording system were analysed in conjunction with vandalism and property repair reports and costs from the Council Housing and Technical Resources Department, giving a more complete picture of the problem. As a result, addressing the crime of vandalism was included as a key objective in the strategy. Issues surrounding the problem were examined by the partners every month at their tasking and co-ordinating group meetings, where progress was reviewed and tasks allocated as necessary.

As part of the plan, the partners decided that neighbourhood wardens on routine patrol would carry digital cameras which they could use to capture evidence of vandalism or associated anti-social behaviour.

Wardens subsequently photographed graffiti and by marrying existing intelligence held to the new information a suspect was identified. As a result the suspect was traced, interviewed and charged.

CASE STUDY

While producing a tactical assessment document for the Hamilton area, one neighbourhood appeared to be experiencing a particular problem with anti-social behaviour.

A problem profile document was produced by analysing information gathered from the partners. This included data from police incident and crime recording systems, Council anti-social behaviour complaints, relevant complaints recorded in the Council general complaints system, related reports from the Fire and Rescue Service, reports from registered social landlords in the neighbourhood, reports of complaints and repair costs from the Housing and Technical Services Department, and the results of a consultation exercise with local residents undertaken by the Council Problem Solving Unit.

From this wealth of information it emerged that the combination of vandalism, harassment, drug and alcohol abuse and gang culture was causing great distress to the local community.

Having further analysed the collated information, the partnership tasking and co-ordinating group concentrated its attention on a particular group of youths in the neighbourhood who were thought to be responsible for most of the anti-social behaviour.

The Problem Solving Unit gathered further information on the identified youths from the Council Social Work Department, Criminal Justice Department, Restorative Justice Department, Community Wardens, the Council's Legal Team, the Anti-Social Behaviour Investigation Team and registered social landlords, as well as from Strathclyde Police.

Pooling information from partners enabled a number of actions and tasks to be identified and allocated. And by bringing their combined services to bear on the problem, a very significant improvement has been achieved – in the three month period following their joint action there has been an almost 100% reduction in calls to the police and complaints to the Housing Department concerning the behaviour of the target group.

Conclusion

HMIC is in no doubt that the free exchange of information, including personal information where appropriate, has been the basis of the success enjoyed by this kind of partnership. Free information exchange, within the terms of agreed protocols, enables

4.6 The Impact of Recent Legislation on Community Safety Information Sharing

The principles and requirements of the Data Protection Act 1998 (DPA) have been highlighted previously within Chapter 2 of this report (para 25). From an information sharing perspective, organisations that process personal data must take due cognisance of the data protection principles at every stage.

The Anti-Social Behaviour Etc (Scotland) Act 2004 introduced new provisions relating to applications for interim and full anti-social behaviour orders (ASBOs) by local authorities or registered social landlords. Section 139 of this Act makes clear provision for disclosing and exchanging information, where this is necessary or desirable to fulfil duties imposed by the 2004 Act or any other legislation relating to anti-social behaviour.

It should also be noted that the Human Rights Act 1998 and the Regulation of Investigatory Powers (Scotland) Act 2002 similarly have a significant bearing on the investigation of anti-social behaviour. The Housing (Scotland) Act 2001 further provides the statutory basis for local authorities and registered social landlords to make informed decisions about tenancies on the grounds of anti-social behaviour.

As partnership working arrangements have evolved and grown, releasing sensitive police information to partners has become an important element. There is no doubt that the DPA was initially viewed by some as inhibiting legislation and that there was reluctance to share information fully – either because of, or at least supported by, that misinterpretation. To overcome these challenges and to place information sharing on a more formal and structured footing, most forces entered into information sharing protocols with their main partners.

Such sharing is normally undertaken within guidelines or protocols agreed between organisations at the appropriate level. Accepted best practice is that the preparation of these documents should involve consultation with expert advisers (generally within the organisations concerned). These may include those who are knowledgeable in the relevant legal, data protection, freedom of information and information security matters, so as to give assurance that the ultimate 'owners' of the information, such as chief executives and chief constables, are appropriately and lawfully processing the information.

The legislative landscape can seem quite complex to the untrained practitioner, often resulting in confusion and doubt as to what information can be shared with partners. Simply explained, much information concerning community safety is already in the public domain, having been de-personalised and aggregated into statistics showing trends and patterns rather than identifying individuals. It is safe to say that this type of information falls outwith Data Protection requirements. However, any information from which a person's identity can be deduced (i.e. case-specific) does fall under the scope of the Data Protection Act and reasonable care must be taken to ensure that there are no unlawful disclosures. It is for the legitimate and necessary handling of this kind of information that the majority of protocols have been developed.

4.7 Information Sharing Protocols

Perhaps because of the way that the information sharing landscape has evolved, along with the emergence of the importance of partnership working in service delivery and the formalisation of community planning arrangements under the Local Government in Scotland Act 2003, a somewhat un-coordinated picture has emerged with regard to information sharing protocols.

This inspection confirmed that each police force in Scotland has now developed a number of such protocols with partner agencies. These range from protocols for information sharing under section 139 of the Anti-Social Behaviour etc (Scotland) Act 2004, which almost every local authority area has although the content and format differ slightly, to protocols for child protection information, for information relating to 'houses in multiple occupancy', and for sharing information with local businesses. An audit by one of the larger forces found 36 different protocols in place at the time of the inspection.

However, there was little evidence of a corporate approach to the production of these protocols within forces. The majority of forces did not maintain a central register of protocols and the protocols were not readily accessible to staff. In most cases senior officers from the partner agencies signed the protocols to activate them and most had designated signatories. There was little evidence of any auditing arrangements to ensure that protocols remained relevant and appropriate for purpose. HMIC believes that the range of protocols should be examined and a degree of uniform information management introduced.

As previously explained in Chapter 2 of this report (page 27), the police service is Scotland has agreed to adopt the ACPO manual of guidance for the Management of Police Information (MOPI). An amended version to reflect the Scottish landscape was being developed at the time of inspection, to be implemented in the near future.

One of the key features of the guidance is the requirement for each organisation to develop an overarching information management strategy, which explains how they will manage information in relation to collection, recording, evaluation, retention, review and disposal, records management and information sharing.

There are a number of identifiable benefits in adopting the guidance in the MOPI manual, including better data standards, quality assurance, integration and linking of information systems, and standardised information sharing protocols. All are intended to ensure that the risks associated with information management can be minimised.

Adopting the standardised protocol templates included in the MOPI manual should result in broadly the same protocol for the same subject being used, regardless of the locality in Scotland. The MOPI implementation team envisages that template protocols will articulate all the issues that *should* be covered and highlight the issues that *must* be covered. Slight local variations may then be applied to reflect local issues/structures. The aim is that protocols will be produced in terminology that practitioners will find easy to understand and interpret.

HMIC believes that there is merit in considering an overarching strategic, Scotland-wide 'in principle' or generic protocol, under which a 'family' of protocols would sit.

RECOMMENDATION 9

HMIC recommends that the Management of Police Information protocol templates be adopted as the basis for information sharing protocols throughout Scotland, to ensure corporacy and consistency.

4.8 Criminal Justice System Partnership

Following devolution, Scottish Ministers recognised the need to reform the criminal justice system to produce, inter alia, speedier justice and more efficient service. It is widely acknowledged that speedier justice is more effective justice, not least for victims of crime and communities, but also for offenders.

Subsequent reviews, notably the Normand, Bonomy and McInnes reports, tackled the pinch-points and the resulting 'churn' of cases. An objective of the Normand report on prosecutions was "[t]o improve efficiency and deal with cases with appropriate speed", while Lord Bonomy's remit for the High Court included "... to make recommendations with a view to making better use of Court resources in promoting the interests of justice". Furthermore, one of the recommendations of the McInnes Report was "[t]o ensure more efficient handling of cases, prepared earlier and more effectively". The Bonomy reforms, albeit directed at courts carrying the least volume (but the most serious) of cases, have already contributed to a 144% rise in early guilty pleas, a 70% saving in witness citations, and 96% of trials proceeding on the day assigned or the following day.

One of the Scottish Executive's responses to the Normand Report (published in 2003) was to set up a National Criminal Justice Board, comprising leading figures from each of the organisations/professions involved in the criminal justice system in Scotland. One of the four system goals of the national board is that:

> *"Continuous improvement is delivered by using more efficient and effective processes."*

Eleven local Criminal Justice Boards were phased in later with boundaries designed around the six sheriffdoms. At national and local level this has united major players in criminal justice in a commitment to work together to improve justice. There must always be due, proper and very visible separation of powers in the investigation, prosecution and trial of alleged offenders, and Scottish criminal justice and its practitioners have guarded and will continue to guard that separation robustly. However, HMIC is encouraged to see that, without compromising these principles, today's practitioners are showing the necessary clarity of thought and breadth of vision to make important strides forward in improving the way justice is delivered.

In order to support and contribute to these recent and continuing reforms, ACPOS established the Criminal Justice Business Area in 2005. Its remit is to build partnerships within the criminal justice community, maximise the performance of the police service in Scotland in all aspects of the criminal justice system, and engage with partners in the reform programme. HMIC acknowledges the work that is currently being undertaken at national and regional level in preparation for the proposed reforms outlined in the Criminal Proceedings (Reform) Scotland Bill.

It is widely accepted that to achieve improvements in the quality and timeliness of criminal justice processes, enhanced information sharing between partners will be essential. HMIC believes that this does not simply mean sharing more and different types of information, but also requires a more efficient exchange of existing information.

The police service has by far the largest share of resources (and so represents the most cost to the public purse) in Scottish criminal justice. It is therefore perhaps ironic that in the past the service seems to have had the least influence on justice procedures and processes. Historically police resources have been used in other parts of the CJS (e.g. in running court business, escorting prisoners, the long-term storage of productions, citing witnesses, etc.). And of course in so doing, many police hours were, and in some cases still are, diverted from front-line service.

Enlightened thinking on the part of Scottish Ministers, Law Officers and other criminal justice partners, particularly since devolution, has improved things enormously. Inroads are being made into many historical inefficiencies. However, advances in technology and in the types of information which can be secured and used as evidence in courts, mean that new challenges in capturing, exchanging and processing information between partners will continue to arise. HMIC cautions all those engaged in the constructive and co-operative work underway to learn from the past. This means taking care not to add to the administrative burden of the operational police officer, nor unnecessarily to increase demand on the support services in police forces, simply because doing so seems to present the easiest short term option.

CASE STUDY

West Lothian Criminal Justice Pilot

In a progressive effort to pursue reform, the Lothian and Borders Criminal Justice Board established the West Lothian Justice Pilot.

The aim of the pilot was to provide collective, practical solutions to many of the recommendations of Sheriff Principal McInnes' Summary Justice Review Committee. These included recommendations on improving the efficiency of police reporting to the procurator fiscal, better communication and closer co-operation between police and procurator fiscal, improvements in case preparation, the co-location of some police and procurator fiscal staff and greater use of undertakings to improve court efficiency for all partners.

The outcome is a criminal justice product, owned by all the partners, which improves the quality and timeliness of the summary criminal justice process.

Information was gathered from criminal justice partners on 11,600 cases reported between January 2003 to December 2004. Combining this information gave partners an overview of the whole, integrated process as opposed to just its individual component parts. As a result, weaknesses were identified that had not previously been apparent and which were causing time delays in the existing system.

Using this knowledge the process was redesigned, removing all waste from the system and retaining only critical matter with a view to reducing end-to-end processing times. The result is a criminal justice system that embodies efficient working practices in delivering its outcomes.

The redesigned system incorporates each individual component need in the process. It recognises the value of information held within each organisation and the value this has to others involved in the process. The subsequent exchange of information through the system is informed by what each recipient requires, thereby encouraging inter-organisational empathy.

Essentially this creates a quality assurance model that is driven by the main customer, in this case the Procurator Fiscal. The process does not extend the range of information exchanged. Rather, the data now exchanged is relevant, guaranteeing that it is of sufficient quality to deliver the final product.

The key features of the new process are:

- *Creation of a co-located case progression unit, comprising a case progression officer (police), procurator fiscal depute, clerk of the court, criminal justice social workers and administrative support for each partner organisation;*
- *Expansion in the use of undertakings;*
- *Providing officers with direct access to a PF depute to discuss reporting requirements;*
- *Access to fiscal reporting application for all officers in the pilot.*

The benefits of the new arrangements are:

- ***Removal of wasted effort.** The information supplied is now what is actually required, not what each organisation perceives the recipient needs. The Crown Office and Procurator Fiscal Service has identified that the greatest advantage of this process is the quality of the information being provided. The information is now 'fit for purpose'. This in turn has produced:*
- ***Less bureaucracy for all partner agencies.** For example, over a previous six-month period, the procurator fiscal sent 396 memoranda asking the police to clarify information already received. Since the inception of the case progression model, no such memoranda have been sent;*
- ***Efficiency saving for police.** The operational impact has been that officers no longer waste effort supplying information which is not required or having to find the correct information when it is subsequently requested;*
- ***Improved court efficiency.** Trials need no longer be adjourned on the basis of insufficient information. The system ensures that the relevant information is now available to the relevant partners, on time, allowing trials to proceed much more often at first time of asking.*

The practitioners from all the partner agencies firmly believe that co-location has improved the process, recognising the importance of relationships in generating trust between the agencies. However they agree that it is the redesigned process, not the individuals, that has led to the enhanced data exchange.

The advances in service delivery have been achieved by creating a collaborative system which improves the quality and speed of information exchange without requiring additional Information and Communications Technology (ICT).

In May 2006, giving evidence to the Justice 1 Committee, Sheriff Principal McInnes saw the work being undertaken in this pilot as being influential to reforms of Scottish summary justice procedures.

The West Lothian Criminal Justice Pilot was designed from the outset as a continuous improvement model. By extending its existing formalised structure the model is set to develop further, with the inclusion of additional partners and the move from data exchange to data sharing.

Improving information sharing requires parties to share data across organisational boundaries consistently and within an agreed framework. The structure should provide security and engender the confidence to share information in all individuals involved. The system will only operate effectively if the structure meets the needs of all the partners in delivering the final product. Achieving improved information sharing within the criminal justice business area, as with all business areas, requires a collective, unified approach.

HMIC is aware that one of the four system goals of the National Criminal Justice Board is to arrive at a state where: "continuous improvement is delivered by using more efficient and effective processes". This report underlines the need for that goal and suggests that review of existing information sharing and exchange processes will be one of the means by which it can be achieved.

The inspection identified parts of Scotland where area procurators fiscal are actively involved in the community planning tactical assessment process. HMIC suggests that sharing NIM data with COPFS should be encouraged for the benefit of both organisations. In several areas the practice of police sharing the identified top ten criminals with the procurator fiscal was helping to reduce crime and increasing public re-assurance. During interviews with COPFS representatives, HMIC noted their enthusiasm for improved data sharing with the police. COPFS recognises the value of PF involvement in the tasking and co-ordinating process, where this provides fiscals with essential information about police priorities and the reasoning behind them. Whilst not affecting their independence, such knowledge can assist PFs when formulating their decisions "in the public interest".

4.9 ViSOR – Violent Offender and Sex Offender Register

ViSOR (the Violent Offender and Sex Offender Register) is a UK information technology solution to facilitate information sharing about registered and unregistered sex offenders, violent offenders, dangerous offenders and otherwise potentially dangerous people.

Before an offender or any other person can be included on ViSOR they must either have a criminal conviction for an appropriate offence or have another valid reason for being included. Each case is determined on its own merits, following a joint-agency case conference or similar within the relevant force/agency area and based on the evidence/information available.

At present those records held on ViSOR by Scottish forces relate to both registered sex offenders and those unregistered offenders whose current behaviour is of concern. There are currently approximately 3,000 such nominals 'owned' by Scottish forces.

Where a nominal record exists on ViSOR and that individual ceases to be actively monitored by police/criminal justice social work (CJSW), then the record will be held in an archive within ViSOR. It nevertheless remains retrievable.

Each record within ViSOR has an identified owner who is responsible for the day to day management of that person. Should a ViSOR user not connected to a specific nominal view a record, then a message that this record has been viewed and by whom is sent to the owner. All users are required to enter full contact details on their initial log-in to ViSOR and must ensure these are kept fully up to date.

Each offender nominal record contains a diary page. Any appropriate dates/events relating to the individual concerned are recorded therein. These events are thereafter allocated to and populate the diaries of key workers within the appropriate organisations.

ViSOR supports the risk management and assessment process. It has the facility to record and store current and historical risk assessments using the Risk Matrix 2000 (RM2k), which is an accredited assessment model. While RM2k is a static tool, ViSOR maintains a capability to acknowledge dynamic factors when managing risk. The assessment is linked to risk

management plans where actions, decisions, results etc, can be recorded. Responsibility for designated tasks is allocated to identified individuals.

The system has two separate retrieval facilities. The 'find' page permits the user to search on the basis of known nominal details. The 'search' page is for enquiries of a speculative nature. Information about personal physical appearance, including photographs, is held on ViSOR in 'time–slices'. This allows for searches to be carried out in cases of historical complaints.

Every police force in the United Kingdom now has access to ViSOR, and information on each nominal record held within can be viewed and updated anywhere in the country. Where ViSOR nominals are known to cross identified borders, partner status can be allocated to a user in any other police or local authority area.

Trained criminal justice social workers in four local authorities (Fife, Dundee, Dumfries and Galloway and Stirling) now have access to ViSOR. Service managers of the remaining local authority CJSW units are now being engaged to roll out ViSOR to all 32 authorities.

The Scottish Intelligence Database (SID) described earlier in this report is the single over-arching database for assessed intelligence about criminals residing in Scotland (Chapter 2, page 24), although the Serious and Organised Crime Agency (SOCA) maintains an independent database which it will interrogate on request from Scottish forces. The SID contains details of criminals, associations, vehicles and activities in a single location, access to which is available to officers throughout Scotland. All information input to the SID has its provenance recorded and graded using what is known as the '5x5x5' system. This is a tool which allows the police service to manage information which has an associated risk, discussed later at page 54. It has been developed in conjunction with the National Intelligence Model and is compliant with the Human Rights Act and data protection legislation. Information held on SID is reviewed on a regular basis to ensure that it continues to meet the standard grounds for retaining and disseminating intelligence.

While ViSOR has a searchable intelligence capability, it is primarily a management and assessment tool. In the absence of an equivalent to SID, police forces in England and Wales are using ViSOR in an intelligence capacity. All ViSOR nominals being managed in Scotland will also be held on SID.

An interface between the SID, ViSOR and Automatic Number Plate Recognition (ANPR) system has been devised. But before this can be implemented, PITO (the UK serving Police Information Technology Organisation) will need to upgrade the systems. The systems will communicate by means of unique reference numbers relating to each nominal record.

It is proposed that, subject to appropriate checks and controls, relevant intelligence which is input to the SID will be electronically transferred to ViSOR, and vice versa. The information will be monitored by gate-keepers at both ends to ensure validity and quality control. Rules, conventions and data standards have been devised for ViSOR, in keeping with those already in existence for SID which were based on HOLMES standards, but final decisions had still to be taken about the detail of this arrangement at the time of writing.

Intelligence gathered by ANPR will be channelled to SID and sanitised before being transmitted to ViSOR where relevant. Conversely a ViSOR user will be able to provide SID with, for example, details of a new vehicle used by a sex offender. This intelligence can then be automatically placed on ANPR, with the results of any hits being sent back directly via SID to the ViSOR user.

HMIC acknowledges and supports the progress that has been made with the ViSOR database and its increased linkage to partner agencies.

4.10 Management of Offenders etc. (Scotland) Act 2005

A national support team has been established to lead and facilitate the significant changes in culture and joint working practices required for implementation of the Management of Offenders etc. (Scotland) Act 2005. The legislation and new structures should be a catalyst for change. In addition, new service developments such as the use of risk assessment tools, integrated case management and a single accreditation panel, are providing tools to help change take root. But success can only be assured when people commit to change. The team has therefore been given a remit to lead in developing a cultural change programme. Its make-up reflects the integrated approach necessary to achieve the objectives set out in the strategy, with members from all the key partner agencies. The team will facilitate discussion on the opportunities created by the introduction of Community Justice Authorities (CJAs) to forge stronger local partnerships which can address the wider needs of offenders and help to reduce offending.

CJAs were established in April 2006 but will not take up their full range of activities until April 2007. As a partner

body the police will have to engage with the CJAs, whose functions will include integrated sentence planning, consistent case management and improvements in information sharing.

Sections 10 and 11 of the Management of Offenders etc. (Scotland) Act 2005 introduce a statutory function for the police, local authorities and the Scottish Prison Service (SPS) to establish joint arrangements for assessing and managing the risk posed by sexual and violent offenders. These will include the National Health Service (NHS) where the sexual and violent offenders are also mentally disordered offenders. The Association of Chief Police Officers in Scotland (ACPOS), the Association of Directors of Social Work (ADSW), and the SPS are working with the Scottish Executive Justice Department to set up Multi-Agency Public Protection Arrangements (MAPPAs) in Scotland.

MAPPAs will operate on the following four principles of good practice: defensible decisions; rigorous risk assessment; risk management plans that match the identified public protection needs; and evaluation of performance to improve delivery. They will also have four core functions:

- identifying MAPPA offenders;
- sharing relevant information among those agencies involved in the assessment of risk;
- assessing the risk of serious harm;
- managing that risk.

MAPPAs are based on inter-agency working, not just between lead agencies but with other agencies such as housing and health who will have a duty to co-operate with the MAPPAs. Similarly, voluntary sector agencies will also have a duty to co-operate as appropriate. The CJAs provide the infrastructure within which the MAPPAs will sit, and each MAPPA will be responsible for reporting annually on performance through the CJA to the National Advisory Body.

From April 2007 the full responsibilities of CJAs will additionally include disbursement of funds provided by the Scottish Executive for community based criminal justice social work services, and monitoring the operational delivery of the services provided.

All CJAs have begun work on area plans for 2007-2008 which follow framework guidance. Every police force in Scotland is represented in the appropriate CJA and is submitting information to assist in its CJA area plan.

Although the structure of the framework guidance is standard across Scotland, each CJA has differing priorities influenced by local issues.

4.11 Integration of Scottish Criminal Justice Information Systems (ISCJIS) Development

In June 1996, as a result of the work of the ISCJIS Programme Board, the principal organisations of the Scottish criminal justice system were electronically linked for transmitting information.

At a basic level, ISCJIS is currently able to transfer information electronically between selected criminal justice partners, through what is known as the 'primary loop'. The ISCJIS programme has proved successful in allowing the information technology systems of the main criminal justice agencies to communicate with each other. However, it is accepted that this communication is far from perfect, with problems persisting over the definition and interpretation of data.

At the time of inception it was decided to concentrate on exchanging, rather than sharing, information. An unintended outcome of this decision is that IT development in individual organisations has continued to be inwardly focused, thereby constraining performance across the entire criminal justice system.

However, there appears to be a growing realisation of new burdens and opportunities in such areas as child protection and public safety, which require the criminal justice system to react quickly to supply and share accurate information. Thus, the possibility of using the loop to share as well as exchange information is currently being explored.

In March 2006 the National Criminal Justice Board (NCJB) agreed that a review of the ISCJIS programme should be undertaken. The remit of this review is to make recommendations to the Board on the future structure and strategy for integrating criminal justice information systems in Scotland. Essentially, how can ISCJIS contribute to the Scottish Executive strategy for integrating criminal justice information?

The stated aim of the review is to provide a system that can aid information sharing for Scottish law enforcement and justice agencies that:

- crosses organisational boundaries without impediment;
- where possible removes manual intervention from business processes;

- assigns appropriate responsibility for security, accuracy and timeliness.

It is commonly accepted that the most effective way to share information among criminal justice partners would be to store information on a central criminal database, giving specified permissions to each agency according to its lawful needs. Presently, no such commonly accessible database exists.

Nonetheless, the absence of such a system is no excuse for not improving data sharing between criminal justice partners.

The ISCJIS medium term strategy for improving data sharing would involve:

- common terminology with agreed data standards;
- improved data quality, with agencies assuming responsibility for own data;
- a strategy for statistics and management information which adopts common standards and definitions;
- an integrated strategy where new developments and change are discussed on an inter-agency basis;
- a strategy flexible enough to support new technology and policy areas, e.g. violence reduction, child protection, anti-social behaviour.

HMIC acknowledges current work by the ISCJIS review programme in this area, and agrees that every effort should be made to maximise existing opportunities to improve data sharing between criminal justice partners.

In light of the these developments, HMIC believes that there are clear advantages for the Scottish Children's Reporter Administration (SCRA) being brought into the ISCJIS data exchange and sharing arena. Whilst accepting that there are issues involving electronic receipting and existing contracts, it is nonetheless disappointing that the potential benefits and efficiencies to all parties, which could be achieved by SCRA having direct access to ISCJIS, are not being realised.

Scenario

Every working day, across Scotland, the ISCJIS system allows the police to send reports about alleged adult offenders electronically to the relevant procurator fiscal, literally at the touch of a button. This is one of the many advances in efficiencies between the police and procurator fiscal service which allows more time and money to be spent on delivering frontline services.

Unfortunately, with one exception in Scotland the same process does not apply when reporting alleged juvenile offenders. Juvenile offender reports still have to be physically printed off and collated by police, then delivered daily to the relevant children's reporter. Without the luxury of an electronic process, this involves a very low-tech physical transfer, usually by means of at least one daily car journey per force and personal handover.

The Scottish Executive, SCRA and ACPOS all agree that better outcomes for children can be achieved by a swifter, more efficient hearing process.

4.12 Barriers to partnership working

HMIC accepts that whilst the concept of information sharing is straightforward, its practice is more complex. There are many hurdles that can obstruct information sharing between partner agencies. This inspection has confirmed that the challenges to greater information sharing are as follows:

- **Organisational culture:** The police service has historically had a culture of not sharing information, based on a perceived need for operational independence and confidentiality. Similarly, some areas of health organisations maintain a principled reluctance to share information on the grounds of protecting patient confidentiality, without further considering the need to protect potential victims (and thus, the argument goes, ensuring that patients are never too scared to seek healthcare/treatment for fear of information then being used against them). Though patient/client/victim confidentiality is clearly of huge importance, it cannot always be the most important consideration. There have been and will continue to be instances in the UK where professionals have, for very good, exceptional reasons, and after careful, objective risk assessment which takes account of all other available information, agreed to disclose sensitive personal information.

- **Lack of training:** There are times when though there is no objection in principle to sharing, practitioners of the information-holding organisation are nervous about what will happen if they do share, e.g. a doctor sharing information about underage sex. Perceptions surrounding interpretation of relevant legislation and misconceptions about how partner agencies will use the information need to be addressed.
- **Lack of awareness:** Information is not deliberately withheld, but is not shared because it is collated and stored within distinct silos. As a result individual organisations are unaware that the information they hold is or may be of value to anyone else. Solutions to this issue have to involve much wider understanding of the information types and systems used across the public sector.
- **Information is shared and misunderstood:** This occurs where information is shared but inconsistencies in language, thresholds and data standards prevent a mutual understanding across organisational boundaries. An example is the definition of 'serious risk' in child protection as a prerequisite for sharing information. The fact that this term unintentionally leads to different interpretations by each agency may prevent information being shared in perfectly appropriate circumstances. This is one of the reasons for the lesser criteria advocated in Recommendation 2A (page 22).

4.13 Risk Assessments

Risk assessments need to be considered when sharing intelligence and information because of the potential impact upon an individual user or customer, the public at large, an organisation or an employee of that organisation. Legislation including the Data Protection Act, discussed previously (page 15), places obligations on organisations when sharing information. However, these statutory obligations do NOT justify failing to share information that should have been shared. The events that led to the Bichard and Laming inquiries clearly demonstrate the risk of not sharing information.

Broadly speaking, therefore, there are two types of risk: the risk of sharing information and the risk of failing to share information. HMIC accepts that deciding whether or not to share information can be difficult. Nevertheless, the difficulty can be minimised through comprehensive training, as discussed in Chapter 6 (page 66) and an appreciation of *both* types of risk. The recommendations of the Bichard and Laming inquiries clearly intend to teach all public service providers that the risk of failing to share information must be considered in all sensitive decisions.

Additionally, there is the risk that organisations construct processes that flood systems with excessive information, increasing the likelihood of vital information being missed. The impact that increased information sharing may have upon partner agencies must be considered. In order to improve information sharing agencies must accept that it is a collaborative process developed across organisational boundaries to achieve collective goals. It is essential that all partner agencies are aware of the final product that the improved information sharing aims to deliver. Collective awareness of 'customer/user' need is necessary at each stage of the process, to build towards the final product. This requires each organisation to be conscious of the content and quality of information the recipient needs and how they will use this information.

Building this foundation of awareness will help to prevent problems that may arise elsewhere within individual organisations, whilst overcoming barriers to information sharing. For example, in July 2006, the Scottish Children's Reporter's Administration (SCRA) reported a 10% rise in the numbers of children referred to them for offending or welfare concerns. Section 53 of the Children (Scotland) Act 1995 obliges the police to make such referrals and the increase had resulted from improved reporting arrangements for a number of reasons. Although acknowledging the requirement to share information, the negative publicity which resulted from reporting this increase highlighted the need to understand all of the implications of increased sharing. Opening the gateway to information sharing can lead to the system being swamped if there is no appreciation of the impact this may have upon the recipient organisation. This is not to say that the inability of one organisation to 'scale up' quickly to receive increased information should stop that information being shared. However, it does mean that dialogue should always take place before any anticipated increase in flow in order that possible solutions might be identified. It may be that, as in the SCRA example, there is a more appropriate destination for some of the information (implementation of recommendations 2A and 2B in this report would greatly ease this sense of single agency 'overload').

The SCRA situation also emphasises the marked difference between sharing and assessing information. Improving the general quality of information being shared requires a risk assessment to be undertaken by the practitioner providing the information (or at least by his/her organisation). The important element is managing the sharing aspect, and to achieve this it is essential that a quality assurance model is applied to the information being shared. There is clearly a need to develop a shared understanding of this process, through mutually agreed thresholds and criteria, that will give practitioners the confidence to make the decisions necessary to enhance the quality of information shared. This in turn will require the relevant practitioners responsible for managing the gateways of each organisation to undergo comprehensive training.

As previously discussed in this Chapter, a risk assessment is not a barrier to sharing information. It should be viewed as a tool that can enable practitioners to share information ethically and securely in the confidence that they will not incur personal or organisational liability.

To realise this, HMIC believe that it is good practice for information sharing protocols to incorporate a risk assessment model. For the majority of instances this will simply involve practitioners asking themselves two or three standard questions and very briefly recording the answers - the intention being to focus thoughts on the purpose of the act of information sharing.

RECOMMENDATION 10

HMIC recommends that information sharing protocols incorporate a risk assessment model, to ensure that the quality of information shared is such that the objective of the information sharing can be accomplished.

4.14 Intelligence Grading System

Information to be considered for police intelligence purposes may first be recorded in a number of business processes, such as crime reports and custody records, before being extracted and assessed for intelligence purposes. Alternatively it can come directly from a source, confidential or otherwise. Across the UK the police service uses a standard pro-forma to record and assess all information to be considered for intelligence purposes, including specific intelligence extracted from these processes. This form (now computerised when used internally) assesses the *reliability of the source* of the information on a scale of A to E. The extent to which the information or intelligence itself is *known to be accurate* is assessed on a scale of 1 to 5, while later the level of *protective measures* required to handle it is analysed on another scale of 1 to 5. For this reason the form has become known as the 5x5x5.

The 5x5x5 is a tool which allows the police service to manage information that has risk attached to it. For example, the 5x5x5 can help to assess the risk of exposure of the source or of the use of the material. This assessment can in turn help to safeguard the operation and protect the source which the information relates to, thus maintaining police effectiveness. It is the standard format for managing the evaluation, the source and the provenance of the information, and the manner in which it should be handled and disseminated. The use of a 5x5x5 proforma sets off an audit trail which is integral to the NIM process, ensures consistency between forces, and so enables forces to share intelligence more easily. Managing the 5x5x5 recording and evaluation process requires effective intelligence management processes to be in place in accordance with the National Intelligence Model.

The 5x5x5 format facilitates the mechanics of sharing information. This format can be extended beyond policing to permit secure and ethical information sharing with other parties. HMIC believes that there is now a need for other agencies to adopt a similar model, to allow and indeed encourage professional, consistent information sharing across organisational boundaries. The following fictitious scenario shows how the same format could allow, for example, social work and health practitioners to share information.

Scenario

The Divisional Intelligence Unit of a police force has an arrangement with the local Royal Infirmary Hospital for transmitting intelligence. Most, but not all, of this intelligence emanates from the Accident and Emergency Department. Occasionally the information will be non-personal, for police use in planning patrol priorities – for example "three head wound cases in white male teenagers over last weekend at separate times from the vicinity of Cooper Street, some caused by blunt instrument – believed to be the result of gang-fighting". At other times specific intelligence relating to named people will be passed on when hospital staff believe that there is sufficient cause. The staff are assured that their intelligence will be treated in confidence because they have all received an awareness briefing jointly conducted by the head of A&E and the local detective inspector.

During one night shift at A&E our fictitious subject, a young man named Craig Mitchell Ramage, attends the hospital with a puncture wound to the abdomen. He is accompanied by a male friend whose name is not known. The injured party freely admits to the nurse and doctor attending him that he received the wound in a 'square go' (mutually agreed confrontation) with someone he refers to as Jimmy. Later the doctor overhears Ramage say to his companion that Jimmy Donaldson will have his house 'torched' next week for this. The doctor then passes this information to the police-trained single point of contact (SPOC) within the hospital on that shift who submits the information that morning in an agreed format, via a secure communication system, to the police Divisional Intelligence Unit. An officer in that Unit then populates a 5x5x5 form with the intelligence and assesses it for dissemination.

CONFIDENTIAL

NATIONAL INTELLIGENCE REPORT (Form A)

ORGANISATION and OFFICER	XYZ Police DC 3271N Joe Bloggs		**DATE/TIME OF REPORT**	0600 hours on 05/01/2007	
INTEL SOURCE or INTEL REF No.	0017		**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

	PERMISSIONS			**RESTRICTIONS**	
HANDLING CODE To be completed at time of entry into an intelligence sysem and reviewed on dissemination	**1** May be disseminated to other law enforcement and prosecuting agencies, including law enforcement within the EEA and EU compatible (No Code or Conditions)	**2** May be disseminated to UK non-prosecuting parties (Code 3.7 conditions apply)	**3** May be dessimenated to non-EEA law enforcement agencies (Code 4.7 and/or conditions apply, specify below).	**4** Only disseminate within originating agency/force. Specify internal recipient(s).	**5** Disseminate Intelligence Receiving agency to observe conditions as specified below.

REPORT				
SUBJECT	**CRAIG RAMAGE – COMMUNITY INTELL – FEUD**			
		EVALUATION		
		S	I	H
Intelligence dated 05/01/2007 provides that Approximately 0020 hours on Friday 5th January 2007, Craig Mitchell RAMAGE, born 05/07/1982 of 24/3 Oxland Avenue, attended at the A & E of the Royal Infirmary and was treated for injuries, which he freely stated were the result of a fight with a Jimmy DONALDSON. During treatment, RAMAGE was heard to say to an unknown male who had accompanied him to the hospital, that Jimmy DONALDSON would have his house 'torched' next week in revenge.		A	4	5

SOURCE DETAILS

SOURCE NAME: DR Sarah Branson

ADDRESS: c/o A & E Royal Infirmary, Sometown

CONTACT NUMBER: 0191 662 111

PROVENANCE

HOW DOES THE SOURCE KNOW THE INFORMATION PROVIDED?

Source was present in the treatment room when she overheard the conversation between RAMAGE and the unknown male.

DISSEMINATION TO: SID/Confidential Unit

DISSEMINATED BY: DC 3271N Joe Bloggs

Handling Codes 2, 3 or 5? Conditions apply? Yes 5

DETAILED HANDLING CONDITIONS Unsure who else RAMAGE has mentioned his intentions to. Only RAMAGE the unknown male and source were within the room at the time. Dissemination must therefore not reveal identity, location or occupation of source nor time and location conversation overheard.

After the information has been evaluated it is 'sanitised' to prevent those who will use it within the force knowing its origin. The following intelligence entry is placed on the Scottish Intelligence Database:

Intelligence dated 05/01/2007 provides that:

Craig RAMAGE was involved in a fight with Jimmy DONALDSON recently.
It is thought that RAMAGE will seek revenge be setting fire to Jimmy DONALDSON's house.
Craig Mitchell RAMAGE, Born 05/07/1982, 24/3 Oxland Avenue, Sometown.
Jimmy DONALDSON is piw*
James DONALDSON, Born 01/01/1980, 17 Oxland Avenue, Sometown.

* piw = possibly identical with

Feedback is passed confidentially to the SPOC at the hospital, who is authorised to share this with the originator of the information for the purpose of providing assurance about confidentiality and security.

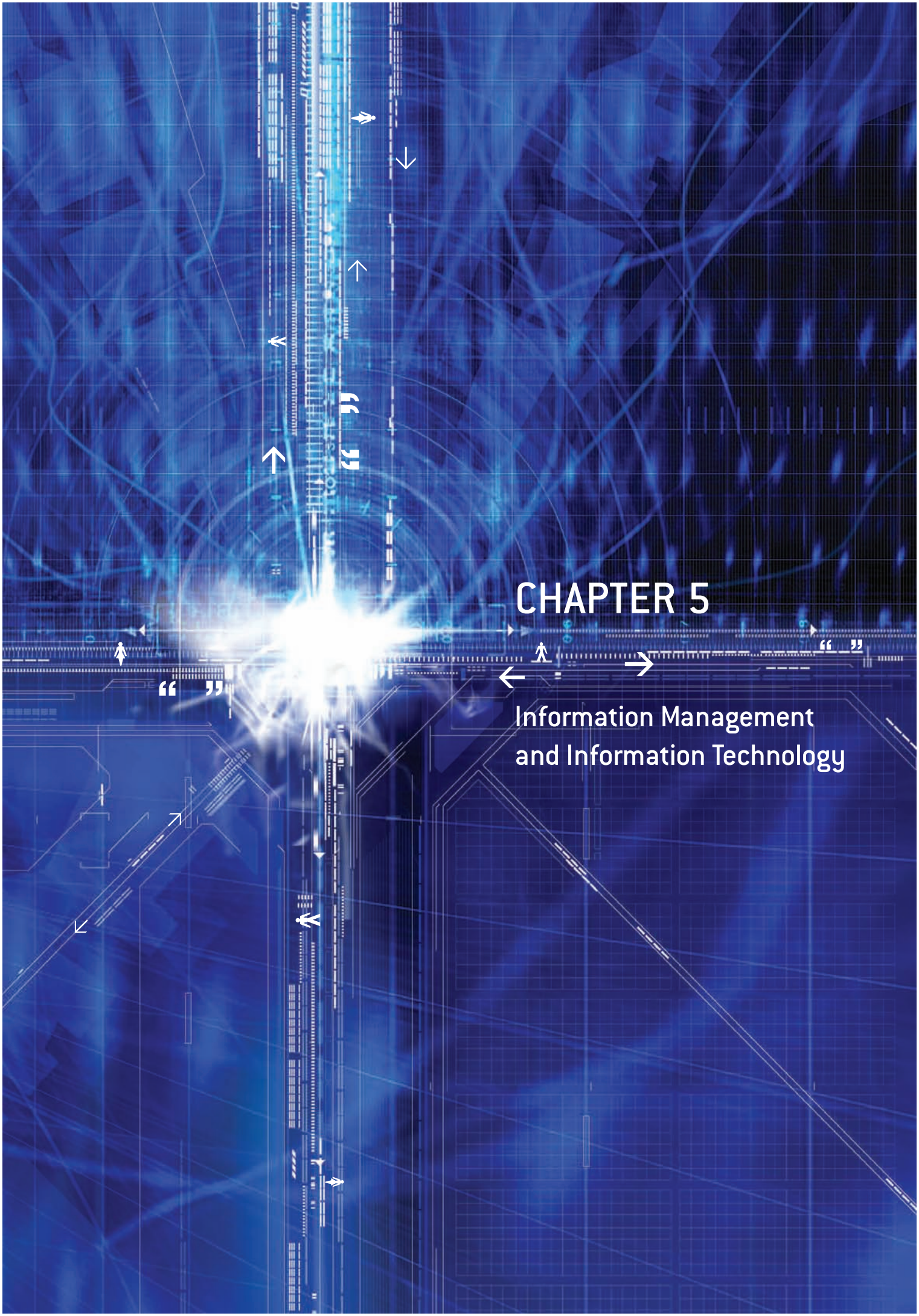
A detective constable from a different division, in whose area both males live and who knows them personally from previous professional contact, is tasked with disrupting any fire-raising. Accompanied by a colleague, he visits Donaldson to warn him. Donaldson agrees to temporary CCTV being installed within his home and to he and his family leaving the home for a few days. CCTV is installed with a live link to a monitoring centre. When suspicious activity is observed one evening, the police are immediately alerted. They arrest Craig Mitchell Ramage in the garden of the house in possession of a home-made incendiary device. Ramage is later prosecuted and convicted, without any mention being made of the intelligence which initiated police action.

As a proven tool which allows the police service to share information confidently and effectively across business areas and forces, the 5x5x5 incorporates a uniform quality assurance model. By removing non-essential intelligence through analysis it helps to prevent the system being overloaded.

The scenario above demonstrates clearly how intelligence transfer between public service partners can be justified, confidential and involve minimal risk of compromise. However, this kind of intelligence transfer has yet to become established practice across the country.

SUGGESTION 5

HMIC suggests that ACPOS and individual forces could increase intelligence sharing across public service organisational boundaries by seeking bilateral agreements on the method of transfer, and by promoting awareness amongst relevant partners of the confidentiality, security and ethical standards of the NIM and the 5x5x5 assessment/risk management model in particular.



CHAPTER 5

Information Management and Information Technology

5.1 Information Management

As was observed in Chapter 2, force intelligence and information strategies should reflect the need for a change of culture within the police service in Scotland and its principal partners, from that of data protection to that of appropriate data sharing. This change in culture is encouraged by a regulatory environment that includes the Freedom of Information (Scotland) Act 2002 and the Anti-Social Behaviour etc (Scotland) Act 2004, section 139. Changes in policy, procedures and working practices, including data sharing protocols with partner organisations, need to reflect this.

In the widest sense, organisational plans are fed by information from a variety of sources. Joint planning with partner organisations can be best informed by aggregating data sets from the various partners involved. In a similar way effective casework concerning individuals can be made possible through sharing complete and relevant information on the victim, location and offender, and including intelligence when appropriate. Ideally this information sharing would be possible using an electronic solution. It is anticipated that the Scottish Executive Data Sharing Forum and Local Data Sharing Partnerships, together with the projected eCare plan, will, through time, evolve to meet this need.

However HMIC acknowledges that these developments may take some time to become fully operational. In the meantime for those cases involving the highest risk, alternative strategies that make the best possible use of existing discrete information systems and manual or 'workaround' sharing, need to be put in place urgently.

5.2 Scottish Police Information Strategy

As with other public agencies, the development of information and communications technology (ICT) in the police service in Scotland over the last three decades has been challenging and difficult at times. There have been some areas where individual forces have made real progress and where the innovative development of IT applications has resulted in parts of the service being seen as leaders in the field. However, the nature of this aspect of policing and the pace of technological advancement has resulted in some new developments becoming quickly outdated. When these factors are added to the ever growing need for information sharing within the police structure and beyond, it seems obvious that arrangements for robust data sharing and common ICT platforms on which to do so should underpin future technological developments in public services.

ACPOS recognised the potential benefits of ICT integration in the mid 1990s, when the need for forces to combine their efforts on various projects was acknowledged and the Scottish Police Information Strategy (SPIS) was developed. The Police Information Technology Organisation (PITO) was established in England and Wales at around the same time and in similar circumstances. SPIS began as a strategic concept, but over the years grew into a funded team with the objective of delivering the strategy. This proved to be difficult, due to a range of internal and external factors.

During the period of this inspection HMIC was briefed on a new approach to business change, under the auspices of ACPOS, specifically focusing on the way ICT development is managed and integrated in the service. This represents the next stage in taking forward the original SPIS objectives and is linked in part to the imminent formation of the Scottish Police Services Authority. The Act specifies that the new Authority will have responsibility for providing police support services including data systems, IT systems and for "the development and maintenance of a strategy for the acquisition and use of IT systems by police forces".

The change management arrangements, which have been agreed between ACPOS and the Common Police Services Programme Board, are designed to integrate the work of SPIS and the eight forces under a combined ICT directorate which will become part of the SPSA from April 2008. The first phase of this work will seek to consolidate existing systems onto a common platform (convergence) and identify opportunities for joint development of applications in forces in the short to medium term. In the longer term it is envisaged that business needs and priorities will drive ICT development from a national (Scottish) perspective, thus reducing duplication and enhancing data and information sharing through the use of common systems which are fully networked.

HMIC recognises that these are still under development. It is clear however that the process of consolidating existing systems, integrating these onto a common platform, and introducing a fully functional data and information sharing arrangement will take some time. In the meantime a great deal of preparatory work is required and some interim measures are already in hand.

Much of this work will examine the fundamental relationship between ICT and core policing responsibilities. Though police forces are data-rich organisations, they can be poor in their use of information to support operational policing. This may be because of the way in which some IT systems were originally created to support management processes (e.g. recording crime and incidents) rather than the core purposes of policing (e.g. *investigating* crime and *managing* incidents). Police officers on the street sometimes feel that their relationship with IT is solely as suppliers of information – feeders of the beast. HMIC acknowledges that there will always be a need for these key intelligence gatherers to input information into police ICT systems. However, these are the frontline service providers who should also be supported by information and should not have to know where to look for it or even have to ask for it to be provided. The police service needs to aim to transform that relationship so that information is pushed out from the centre, out from the operations and control rooms and communications centres and offered to street officers to help them help the public. The development of police information and communications systems should make 'information push' a key priority for the support of frontline, core responsibilities.

SUGGESTION 6

HMIC strongly supports the positive steps taken by ACPOS towards national ICT integration, and suggests that 'information push' be adopted as a key priority for the design of systems supporting operational policing.

In addition, HMIC believes that the current national landscape which is promoting enhanced ICT information sharing across organisations, through the GIRFEC agenda (page 18) and National Data Sharing Forum (page 15), should be incorporated into the ACPOS vision for ICT development. The genuine need for organisations to share information and intelligence in order to promote public safety and enhance service delivery can sometimes be thwarted, unintentionally or not, by difficulties in transferring information electronically. It can often be too late to rectify this once a new system is implemented, so it makes eminent sense to insist that partnership information sharing is considered at the earliest stage of any new development in police ICT.

RECOMMENDATION 11

HMIC recommends that ACPOS and SPSA consider creating a process to ensure an outward facing approach to future information and communications technology (ICT) development, so that opportunities for electronic intelligence and information sharing with other agencies are not missed.

During the inspection HMIC discovered that one medium-sized Scottish force has at least 41 different information technology systems. Undoubtedly there were, at the time, sound reasons for the proliferation of stand-alone information systems currently operating in the divisions and departments of all Scottish forces. Nonetheless, it is imperative that these are now integrated with the main force or national framework. Only then can a comprehensive search facility be sure of capturing all relevant, available information.

5.3 Management of Community Information

HMIC found structures in place for capturing community information in several local authority anti-social behaviour investigation departments. Community information is gathered from a variety of sources, such as neighbourhood wardens, local housing departments, registered social landlords, environmental wardens and environmental officers, trading standards officers, anti-social behaviour investigation teams, housing officers, education department officers including teachers, police officers and social workers.

When tasking neighbourhood wardens with gathering community information on anti-social behaviour, some local authorities use targeted patrolling matrices to ensure that they are deployed to hot spot areas. The wardens are then able to inform other partners, such as the police, if they believe urgent attention is needed.

In South Lanarkshire the wardens electronically input the community information gathered onto a standard pro-forma report. This is received by the administration team, which then produces a written report and enters the information on an electronic spreadsheet. At this point the administration team then notifies other partners, such as the police, if they think the information would be of interest to them.

The administration team distributes the report to relevant partners including the police Local Authority Liaison Officer (LALO). The LALO then distributes this to key local police personnel such as the Divisional Senior Managers, Local Intelligence Officer and Community Officers. Both the written report and the spreadsheet are copied to the partnership analyst in the Police Divisional Intelligence Unit, who will then assess whether these should be included in their tactical assessments or problem profiles.

The Scottish Intelligence Database, as the only acknowledged over-arching repository for assessed *criminal intelligence* in Scotland, does not store wider *community information*. However it must be recognised that community information too, can be necessary to the work of police and partners. Community information can range from the occupancy of local shops and business premises, through voluntary sector services available or the opening times of doctors' surgeries, to more transient intelligence such as where the local children prefer to play football or when 'the shows' are coming to town. Some of this information, while of no interest to the police may be of significance to partners, e.g. trading standards officers would find information about someone using his dwelling house to buy and repair cars useful. Conversely some of it will clearly be useful for crime prevention or criminal intelligence. Indeed increasingly, community information or intelligence is becoming invaluable in the fight against terrorism.

The structure in place in South Lanarkshire affords the police several opportunities to assess the usefulness of an item of community information, and whether it should be regarded as criminal or community intelligence and input to the Scottish Intelligence Database. It is also the case that the usefulness of community information can change with time and information that may initially seem of no interest to the police could be regarded as useful as circumstances change. Again the structure in place in South Lanarkshire allows for this.

The Community Intelligence Unit at Tayside Police also has a structured system for managing community information and intelligence. Information from community wardens, as well as letters and e-mails from the public, are collated by the Unit administrator who assesses their value as items of intelligence. In conjunction with the Unit analyst, the information is input onto a searchable spreadsheet. From this a community impact assessment document, similar to a National Intelligence Model Tactical Assessment, is produced and distributed to strategic managers for consideration at the morning tasking meeting.

This Unit has a seconded officer from the Council Housing Department who is equipped with a laptop computer and has broadband internet access to the Housing Department database. This allows the Unit speedy access to information when investigating anti-social behaviour matters, and is viewed by HMIC as good practice.

5.4 Community Information – Electronic Applications

HMIC is aware that some local authorities have purchased, or are in the process of purchasing, computer systems for their anti-social behaviour departments which provide similar functions to police command and control systems. By their very nature these systems store community information which analysts can use when preparing products such as tactical assessments.

This capacity can be further enhanced by tasking practitioners, such as neighbourhood wardens, to seek out information to fill existing knowledge gaps. The computer applications concerned also have an effective search facility which allows searching over a number of fields: a very useful tool in the information or intelligence-led approach being undertaken by partners. HMIC views the use of such computer systems, when combined with sound procedures for processing and storing information, as good practice, as they further advance the use of information and the sharing process to the benefit of the service provider and receiver.

However, more than one manufacturer is involved in supplying these systems to local authorities in Scotland. HMIC would therefore suggest that common data standards be established, in order that systems in communities serviced by more that one local authority or in bordering local authority areas can communicate with each other. Otherwise the opportunity to share community information nationally and regionally in line with agreed protocols and authorisations will be lost.

SUGGESTION 7

The Scottish Executive development team responsible for establishing local data-sharing partnerships is also attempting to ensure common data standards for information systems in specific areas of public service. HMIC suggests that community information systems (such as those used for tackling anti-social behaviour) be considered for inclusion in this effort.

5.5 Use of Single Points of Contact

A good deal of the information police provide to partners is of a sensitive, personal nature, and only that pertinent to the case should be disclosed or made available. To ensure that there are no inappropriate disclosures, most forces have dedicated officers in information sharing positions. These posts are usually co-located within the anti-social behaviour investigation departments of the partner body which has this responsibility. This information sharing process is normally formalised and facilitated by an agreed information sharing protocol between the agencies concerned.

HMIC found several advantages of using a single point of contact. Not least was that the post-holder becomes a trusted gatekeeper between the partners and, by gaining expertise in this very specialised field, provides more accurate and consistent disclosures. The use of a single point of contact who is co-located in the partner organisation can also result in a speedier response to information requests and, being the only one with access to the partner's system, system security and integrity can be maintained. This is especially important if the applications contain sensitive personal data such as records of criminal convictions or criminal intelligence logs.

RECOMMENDATION 12

HMIC recommends the use of single points of contact (SPOC) to share sensitive information between the police and partner agencies.

5.6 Impact Nominal Indexing System

Whereas Scottish policing is served by a common intelligence system and database (the Scottish Intelligence Database), the 43 police forces in England and Wales still rely on separate systems. However a co-operative programme called IMPACT has been implemented, providing a means of flagging up possible intelligence connections across force boundaries in England and Wales.

The Impact Nominal Index (INI) is an IT system produced by the IMPACT Programme in response to recommendation 2 of the Bichard Inquiry. INI was introduced to police forces in England and Wales in December 2005. In September 2006 piloting of the INI in Scotland began in Lothian and Borders Police. The INI is scheduled to go live in the remaining Scottish forces, SCRO and the SCDEA by the end of December 2006.

The INI enables users in one force to establish whether any other force providing data to the INI holds information about a particular person. The system cannot return the records themselves, but provides the user with details of a single point of contact within the 'holding' force to whom further enquiries should be directed. The INI is a list of the names and corresponding dates of birth of individuals who are named in police records; it is not limited to suspects and offenders.

In England and Wales the nominal data is extracted by individual forces from information systems supporting six high-risk business areas:

- child protection
- crime recording
- intelligence
- domestic violence
- custody
- firearms licensing (revocations and refusals)

In Scotland SCRO provides this data from the criminal history system (CHS). The CHS has eight fields, including intelligence markers, that indicate which force or agency holds a nominal's corresponding intelligence record. The data is then passed to the Criminal Records Bureau (CRB) in Liverpool, which processes and loads it onto the INI. An INI search can be carried out using the following fields:

- forename (mandatory)
- surname (mandatory)
- date of birth or age (mandatory)
- gender
- force
- business area
- record input date

A search using the name field will return the number of 'hits' recorded against that name across the UK. For example, a search for a fictitious John Smith born 30.7.1966 could reveal a number of hits. The criteria should then be further focused by adding to the search, for example, the areas where John Smith was known to live. A request for greater detail would then be made to the nominated single point of contact in the relevant forces. The request, and any subsequent responses, would be exchanged over the secure Criminal Justice Extranet (CJX) e mail network using electronic pro-forma.

The Scottish Intelligence Database provides Scottish forces with an integrated intelligence system which is still the envy of other countries. The introduction of IMPACT across England and Wales at least offers forces south of the Border the ability to point to possible cross-force connections there. HMIC acknowledges the work completed to deliver the INI system across Scotland. The potential to share information and intelligence, not just in Scotland but across the UK, represents a significant step forward in capability.

5.7 ACPOS Common Performance Management Platform Project

In 2005, HMIC published 'Managing Improvement' – a report on a thematic inspection of performance management across all Scottish forces. In response to that report, the police service in Scotland has embarked on a major business change process. This is aimed at fully embracing a performance culture which will operate at national, force, local, and ultimately individual, level. A further aim is to provide the public and other major stakeholders with performance and related information which is much more comprehensive and meaningful than that published by forces at present. However, it has been recognised that a fully embedded and effective performance culture:

- must use common definitions and recording conventions across Scotland;
- needs access to accurate and timely information; and
- must endeavour to present the information in such a way that it is easily disseminated and understood.

To assist the business change process there is therefore a need to provide an IT platform across Scotland which can extract information from legacy systems, collect it into a data warehouse or similar, and provide a flexible and comprehensive user interface and reporting system. This platform would be used to provide performance management information at all levels within each force and service, and would be directly accessible to the Scottish Executive, HMIC and Audit Scotland in terms of force-level and command unit/support service information. Such technology is already available and is extensively used in the private and public sector.

To address this need the ACPOS Performance Management Business Area is driving a project to provide a common performance management platform for the police service in Scotland. The cost of this project has been estimated at £8.3 million.

To assist in funding this project an approach was made to the Scottish Executive's Efficient Government Fund. This is a £60 million challenge fund intended to stimulate a sustainable, more efficient public sector by reallocating resources for better front-line use. Its aim is partially to fund multi-partner projects which seek to deliver sustainable efficiency savings using a proven approach. It was estimated during the bid process that efficiency savings of more than £30 million by 2010 might be achieved through this project. In August 2006 it was announced that the bid had been successful in attracting an award of £5.4 million.

A dedicated project team is already in place, and it is estimated that a common IT platform will be up and running in all eight Scottish forces and the Scottish Crime and Drug Enforcement Agency, by April 2009.

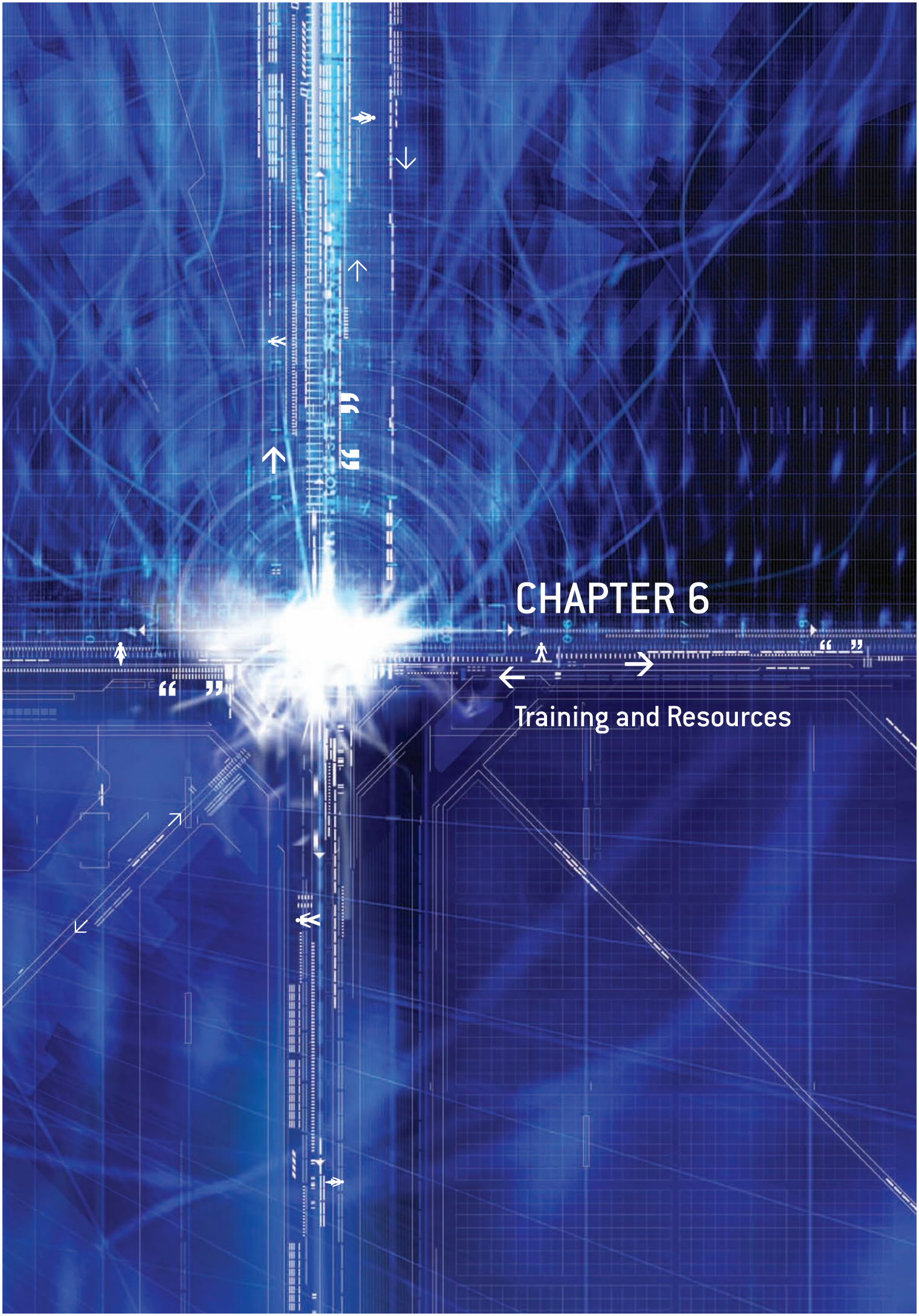
Although this project is aimed primarily at providing performance information, it will also provide easily accessible management information and information about the policing environment (e.g. demand levels, social deprivation, etc.). In addition the licences and software purchased will allow a comprehensive data warehousing structure which can then be used for other purposes. The front-end reporting tools envisaged in the bid will be flexible enough to extract, analyse and present complex information sets in a user-friendly way. The specification will also require the software to be configurable by trained staff within the service. In preparing for this common platform, forces will have to improve the quality of their data significantly.

Although the final structure and location of the data warehouses has yet to be finalised, HMIC understands that ACPOS intends to achieve this in conjunction with the ICT Directorate and that this decision will recognise the need for the information held to be shared across the police service in Scotland and with other relevant bodies.

Implementation of this technological platform will greatly assist development of the Scottish Policing Performance Framework, a collaborative approach by ACPOS, the Scottish Executive, Audit Scotland and HMIC to the creation of meaningful and useful information about police performance and the policing environment. The platform project will also support the creation and pursuit of joint performance targets with key partners and could help to streamline statistical information sharing between the police service in Scotland and partners such as the Crown Office and the National Criminal Justice Board.

5.8 Conclusion

The police service should see advancements in ICT as an opportunity to improve information sharing with partner agencies, not an excuse to prevent development. HMIC believes that the positive moves made by ACPOS towards a national ICT structure will enhance the possibilities that already exist nationally, with the development of the GIRFEC agenda and the National Data Sharing Forum. Equally, the development of the common performance management platform, supporting a new publicly available information framework, will help to demonstrate transparency and accountability, and present the opportunity to provide real evidence of improvement in policing and partnership working.



CHAPTER 6

Training and Resources

6.1 The Role of Training in Overcoming Barriers to Information Sharing

HMIC recognises the need for greater awareness amongst everyone concerned, of the concerns of, and the impact of enhanced information sharing upon, partner agencies. Narrowing this gap of awareness can only be achieved through a targeted programme of training.

The existing approach to information sharing between the police and partner organisations relies upon relationships and data sharing protocols. HMIC accepts that any information sharing structure must include protocols and recognises the importance of relationships. However, information sharing protocols cannot identify the required quality of information to be shared or engender an environment that encourages individuals to do so.

Improved information sharing can only be achieved within a formalised structure, supported by a training programme that provides relevant individuals with the requisite knowledge to share information with confidence. Without a prescribed structure, individuals will undoubtedly be reluctant to share information. The Inspection has identified that one of the primary sources of this reluctance, across all public services, is a real fear of the personal consequences of sharing information. Training can reduce this fear and empower individuals by increasing their awareness.

There is a wide range of factors which influences the decisions of professionals when making judgements about whether to share information. The existing lack of inclusive guidance, for both police and partner agencies, allows for different individual and organisational interpretations of policy documents and legislation. This then has a direct impact upon the balance between sharing and protecting information. This lack of clarity can produce a reluctance to share data.

In addition, divergent guidance can have a negative effect on the effectiveness of information sharing protocols. Protocols may exist, but if guidance on how to operate within them is incongruous, information is unlikely to be consistently shared. Data-sharing protocols are the mechanisms which facilitate greater information sharing. However, as with all tools, they can only be effectively and efficiently applied if their proper use is learned through guidance and training.

Organisations appear to approach the task of producing guidance on information sharing with a silo mentality. A greater degree of organisational empathy is required. Guidance ought to be developed in collaboration with partners to achieve collective aims. For example, there should be no difference between organisations' interpretations of the Data Protection Act 1998. However, these differences do occur and prevent information that should be shared, from being so (referred to in Chapter 2, page 16).

This matter can be compounded between internal boundaries within each service. Within the police service, not only each force, but in some forces each business area, provides guidance on information sharing. In addition, there is no formalisation, central governance or quality assurance of the guidance that is provided. The same occurs within partner agencies. For example, the MacLeod short term working group found no uniform system for the NHS to share information with the police about public safety issues or the investigation of serious crime. Without the ethical or security guidance for information sharing, it is unsurprising that practitioners are unsure about the correct procedures and are thus unwilling to share information.

It is important that individuals are empowered through training to share information across all services or across internal business areas. In this respect, training should act as a means of reducing the risk associated with sharing information between organisations. As discussed in Chapter 4 (page 54), the key element to effective information sharing is managing the sharing aspect. This can be achieved by applying a quality assurance model to information that is shared. Correctly applying such a model will ensure that only information that should be shared will be, whilst encouraging a sharing ethos by providing practitioners and organisations with the appropriate security and confidence to do so.

Though a service may publicly espouse an outward looking code of ethics and values, attitudes to information sharing may in practice reflect underlying and unofficial values at practitioner level. This in turn may result in the protocols, guidance and codes of practice being insufficient or, at worse, counter-productive. Attention needs to be paid, at the outset of training and professional development, to creating professional values which are more outward looking and which strengthen levels of inter-professional trust and empathy.

HMIC is aware of the significant progress that has been made in integrating the National Intelligence Model (NIM) within training courses at the Scottish Police College, and the inherent information sharing training which is contained therein. Nevertheless it is considered important that all police officers receive specific training in information sharing during their initial probationary training period. HMIC is also aware of work ongoing within the Scottish Executive in relation to delivering NIM training to partners, particularly in relation to problem-solving policing and partnership working. Whilst in its infancy, early indications reveal a strong desire to extend the use of the NIM to a number of partner organisations such as local authorities, the Scottish Prison Service and the fire and rescue services (referred to in Chapter 3, page 33).

It is essential that the evolution of information sharing includes *all* partner agencies. This will help to minimise lost opportunities and deliver better joined-up service. Failing to engage meaningfully and inclusively with partners may engender a protectionist response from those excluded, which would clearly thwart progress.

RECOMMENDATION 13A

HMIC recommends that ACPOS consult with the Scottish Executive and partner agencies to deliver a comprehensive guidance framework for public service information sharing.

RECOMMENDATION 13B

HMIC recommends that ACPOS acknowledge a training need for information sharing, and seek training aimed at establishing an enabling ethos for intelligence and information sharing across the police service.

CASE STUDY

Northern Constabulary found that delays in receiving information to which it was entitled was due to some partners incorrectly interpreting relevant legislation including the Data Protection Act 1998.

In an attempt to overcome these difficulties, Northern Constabulary embarked on a series of training days for its main partners. At first these training days were organised for partners in general, but more recently they have been targeted at specialist partner groups.

The programme for these days differs slightly according to the group, but all stick to the following basic format: a welcome and introduction by a senior police officer, a presentation on the Force information sharing policy, a case study based on the findings of the 'Bichard' inquiry, an outline of the Scottish Intelligence Database, a presentation on the National Intelligence Model, background to the work of Disclosure Scotland, and a plenary session to close.

Each candidate receives a pack containing a letter from the Chief Constable and a copy of the Highland Information Sharing Policy.

CASE STUDY

The Scottish Executive is currently supporting structured training in problem-solving for all 32 Community Partnerships over the next two years. Each partnership has been allocated funding to allow stand-alone training in this area. The purpose of this is to bring together practitioners from different agencies within each partnership and give them a shared understanding of problem solving principles. Ideally this would be achieved using the S.A.R.A model (Scan, Analyse, select from a range of responses, and Assess results), but partnerships have the autonomy to choose their training provider.

The training delivered so far has covered information exchange, use of analysis and formal tasking processes.

To further this aim, Central Scotland Police has embarked upon joint training with its main partners; a commercial consultancy company with expertise in the field will undertake the training. Central Scotland Police has ensured the attendance of the area chief inspector, all inspectors working in the area and the community policing sergeants. Early indications are that this training has proved very useful and has been well received.

Conclusion

HMIC acknowledges the Scottish Executive's direction for improving information sharing between all the agencies involved in child protection. The proposed outcomes of the Bichard Inquiry and Getting It Right For Every Child (GIRFEC) agenda may place dual organisational obligations on stakeholders to share information, and to ensure that their staff are suitably equipped to meet this corporate obligation.

These organisational obligations will have training and ICT implications for the police service and partner agencies across Scotland. HMIC believes that any progress on this front should be welcomed as a positive step forward, as it presents possibilities to maximise joint working with partners and an opportunity to 'get it right first time.'

6.2 Conclusions

Intelligence and information sharing lies at the heart of policing. The police service cannot operate effectively at any level without enabling processes and procedures for managing intelligence and information. For intelligence and information sharing to work properly and consistently, both internally and with partner agencies, police forces and services need to manage this area of work more deliberately and thoughtfully than has been the case in the past.

The degree of difficulty in achieving this is directly proportionate to the complexity of the subject matter. Identifying what is relevant from amongst the miasma of all incoming or available information is a daunting enough task in itself. But when some of that raw material has the potential to become intelligence, it has to be assessed and sometimes further analysed. Only then does it become useful intelligence that might enable individual interventions or inform the design of service delivery for different communities. In both cases information and intelligence is only valuable when it adds to knowledge. To do that it has to connect with existing knowledge, which unfortunately is rarely located in the same place at which the information enters the organisation or partnership. Therefore the act of sharing is the critical element in arriving at **common knowledge** which is of value.

There are some aspects of information and intelligence sharing, such as the protection of children from sexual and/or violent crime, which are literally a matter of life and death. There are also good reasons why some low-level information has not been shared between agencies in the past. But HMIC believes that it has found a way in which client/patient/victim confidentiality can be maintained right up to the point at which the need to share is obvious to all. No public service or public servant can know everything, and so processes and procedures within and between organisations need to make information sharing easier and safer, not a matter of guesswork or exception.

The Scottish Executive's continuing emphasis on improving public services encourages all public service providers to work in partnership in order to achieve more, collectively and individually. The Executive's recognition that these services need to be 'user focused' further requires public organisations to collaborate to achieve unified delivery.

This inspection found clear evidence of effective intelligence and information sharing by forces. There is also no doubting the desire across the service and amongst principal partners to move this agenda forward to deliver greater public safety and improve service delivery.

Against this positive background, nevertheless, there is much scope for clarification and development. Notable in this respect is the requirement for a corporate approach to managing police information, and the overriding need, across public services, to provide all practitioners with the knowledge, assurances and mechanisms to share information confidently, securely and ethically.

HMIC is encouraged that in these areas of weakness there is much work being undertaken at both force and ACPOS level to improve performance. However there is also clear evidence that some parts of the country are moving faster than others in specific areas, that there is inconsistent development of good practice, and that there are some matters which need to be pushed more energetically at national level. The Inspectorate therefore firmly believes that it is necessary for an over-arching, strategic approach to co-ordinate the good work already underway as well as that which should be initiated by this report.

HMIC believes that the recommendations in this report recognise and complement existing efforts across the police service in Scotland. The Inspectorate also believes that the suggestions in this report which look beyond the police service, acknowledge and supplement nationally evolving developments and aim to capitalise on the cross-fertilisation of policing with other public services in an area of work where all concerned can learn from each other.

RR Donnelley B48441 03/07

Further copies are available from
Blackwell's Bookshop
53 South Bridge
Edinburgh
EH1 1YS

Telephone orders and enquiries
0131 622 8283 or 0131 622 8258

Fax orders
0131 557 8149

Email orders
business.edinburgh@blackwell.co.uk

w w w . s c o t l a n d . g o v . u k