The Review of Criminality Information

By Sir Ian Magee








ROCI
Review Of Criminality Information








ROCI
Review Of Criminality Information

Contents








ROCI
Review Of Criminality Information

CHAPTER 1: INTRODUCTION

1. We live in an increasingly interconnected world. Cheaper international travel means we can reach previously inaccessible parts of the world – and be reached by those who live there. Advances in communication technology enable us to be always connected with those with whom we seek to connect – and sometimes with those from whom we would prefer to remain disconnected. In such a world simple chains of cause and effect are rare. Organisations are often one element of a complex network. Some may not even realise they belong to it. That is as true of the UK public sector as it is of the private sector and of organisations around the world. So, for example, it is necessary, but no longer sufficient to be efficient, even excellent, in what you do within your organisation: more is needed these days for success.

2. It is a small step from inter-connectedness to interdependence. It is no longer enough for organisations to operate in isolation from each other depending wholly on their own resources. We have seen this in the UK over the last decade in the drive for "joined – up government". Taking this further, the new generation of Public Service Agreements (PSAs) recognises that making communities safer or delivering a more effective, transparent and responsive criminal justice system for victims and the public, cannot be achieved by any one organisation. Many organisations in Central Government and elsewhere need to collaborate to deliver improvements, finding ways to align their differing constitutions, targets and stakeholders and each contributing what they do best.

Public Protection

3. That reflects too, the business of my Review – improving public protection. A complex network of organisations is involved in the protection of the public; some will recognise that responsibility as integral to their central purpose. For others, it may be much less explicit. An effective public protection network demands that all work together, nationally and internationally, to improve public protection while continuing to deliver on their own specific remits.

4. The objective of "public protection" is one which many would support in principle. During the course of this Review I have had many debates with those involved in delivering it so as to determine a precise definition. Public protection, I have concluded, is the safeguarding from harm of our communities and individuals within them. There is a large range of organisations – the complex network referred to above – which contributes to the required safeguards. The public expects them to do so efficiently, cost-effectively and with proper regard to their rights.

5. The specific focus of this Review is the recording and sharing of information on criminality for the purposes of public protection. I define information on criminality as any information which is, or may be, relevant to the prevention, investigation, prosecution, or penalising of crime. The Review does not address those arrangements which are focused on counter-terrorism or the intelligence services more generally as these areas, by necessity, often operate using a wider range of information and intelligence. However my findings and recommendations should apply to these services in their use of criminality information.

6. Some would argue that data should only be used for the declared purpose for which it was originally collected. So, for example, information collected for social security purposes such as address details should not, on this view, be permitted to be shared with the police. However, others argue that this position unreasonably constrains the ability of agencies to protect the public – especially since the Information Commissioner is empowered to adjudicate where there are concerns that the re-use of data outside its original purpose is inappropriate or illegal.

7. I found a useful analogy in The Australian Privacy Act 1988 which makes transparency a key requirement of data sharing. The Information Privacy Principles (IPP) contained in section 14 of that act regulate data sharing between Government Departments. IPP 11 is about the disclosure of personal information and permits data sharing "where it is reasonably necessary for criminal law enforcement, or for the enforcement of all law imposing a fine, or for the general purpose of the protection of public revenue." It also provides that the disclosure of personal information is permissible where "… the individual concerned is reasonably likely to have been aware… that information of that kind is usually passed to that person, body or agency".

Dilemmas

8. The question of whether information collected for one purpose may properly be used for another is only one of several dilemmas which the Review has surfaced – some of which have been given greater prominence by recent, well-publicised incidents of data loss:

   - Individuals are entitled to know what use may be made of the data they provide BUT it is not always possible to know that in advance – data provided / collected for one purpose may subsequently be found likely to be relevant to public protection
   - The public wants, and is entitled to have, personal information protected BUT public protection may require it to be shared, which adds risk
   - Organisations have responsibilities / accountabilities specific to their remit BUT public protection may require them to collaborate with others, which is not part of their accountability

- Initiatives need to be introduced to address specific problems BUT such initiatives may have unanticipated consequences elsewhere
- Crime is global and so international sharing of criminality information is essential BUT quality standards and definitions differ widely

9. My recommendations cannot resolve these dilemmas. But I hope that the discussion within later Chapters will contribute to a well informed public debate. In particular, the balance between what may be good for society, as against individual rights and the demands of public protection, as against the priorities of individual organisations, are recurring themes throughout this Review.

Guiding Principles

10. The principle at the forefront of my mind in conducting this Review has been that the public must have confidence in the arrangements made for the recording and sharing of criminality information for their protection. They must feel that action taken is proportionate to the risks being addressed, that there are sufficient checks and balances in place and that governance arrangements will ensure high standards. The public must also have confidence that the complex network of public protection organisations is collaborating to meet the new challenges posed by advances in criminality information and the problems and opportunities presented by international information.

In compiling these recommendations I have attempted to ensure that they meet the following criteria:

- A coherent package rather than a menu
- Focus on those areas where significant improvements can be delivered
- Practical measures that will command support from relevant agencies

I have focused on addressing problems faced by front-line professionals who require timely, accurate information in order to make their contribution to public protection. Looking to the future we can:

- Learn the lessons of the past so as to take a strategic approach to issues such as risk management, investment, governance and accountability
- Take a view of criminality information as a whole
- Ensure strategy drives technology

The Case for Action

11. Following an inquiry early in 2007 into the handling of notifications by other European countries of criminal convictions for UK citizens, the Association of Chief Police Officers (ACPO) wrote to the Home Secretary suggesting that there might be a number of wider issues around the effective use of information about criminality. The Home Secretary asked me "thoroughly to examine this whole area and recommend necessary improvements for recording and sharing information about criminality within the UK and between the UK and other countries and the way in which this information is used to protect the public and the relevant procedures and responsibilities".

The Terms of Reference for this independent Review are as follows (at Annex A):

- To scope the problem and assess what is broken and where the deficiencies lie
- To test understanding of the problems and issues with key stakeholders, and seek consensus on where the principal roles and responsibilities should lie at a strategic level
- Draw conclusions and make recommendations for improving the recording and sharing of criminality data, with a clear eye on what is realistic and achievable

12. It is clear that the public protection network and the whole area of criminality information is extremely complex. The multiplicity of databases listed in Annex D is itself evidence of that – and there are many more not listed there. The international dimension adds an additional layer of complexity.

13. Even if it were possible, which in my judgement it is not, no one designing a comprehensive database on criminality information and processes for effective sharing in the interests of public protection would choose to start from here. What we currently have is far from comprehensive; there are significant gaps, overlaps and basic errors in the data. Data is too often entered inaccurately, or repeatedly (which in itself can cause inaccuracy if, for example, an arresting officer has to enter personal details on numerous forms and databases in a short amount of time). For example, the Police National Computer (PNC) contains some errors and omissions in basic data such as names, addresses and dates of birth, as well as numerous unhelpful duplications of the same information. A certain level of errors is inevitable in such a large and complex system, but the 2006 audit by Her Majesty's Inspectorate of Constabulary (HMIC) found that police forces were not reaching the basic quality assurance targets for PNC arrest / summons data input (the most basic data input measurable). This led to the current system of centralised monitoring which alerts an individual force if it falls below standard for a sustained period of time.

14. There is certainly room for improvement, but whatever is done, no set of arrangements will prove totally effective in providing for the protection of the public. There is no criticism implied of those who have developed and are responsible for what we now have; each database and process was designed for a specific purpose, and many continue to serve that purpose very well. But there is no overarching architecture for criminality information and no individual or organisation that could reasonably be held responsible for its absence. Each of the many organisations in the public protection network has its own accountabilities but none is accountable for the whole. It follows that the recommendations that emerge from this Review cannot offer solutions to every issue. Nor am I suggesting setting up some umbrella organisation through which all criminality information will pass – that would merely add to the complexity. Rather, my recommendations seek to focus on those aspects where improvements can be made that will have the maximum effect on improving public protection – which is the purpose of recording and sharing information on criminality - while remaining within the bounds of proportionality and respecting privacy.

My Approach

15. I felt it important to engage with the broadest possible range of organisations in the public protection network. These include organisations such as the police and other criminal justice agencies, the EU, child protection agencies and also, perhaps less obviously, organisations such as teachers' trades unions and the Department for Transport (DfT). A full list of those we have contacted is at Annex F and illustrates the enormous range of those who have a part to play.

16. In addition I was keen to gather views and ideas from those who might not feature on any list of those essential to interview. To that end the Review had a presence on the Home Office website and I am grateful to all those who have taken the trouble to approach us with their thoughts.

17. Having developed my thinking, as a result of our initial discussions, the Review team and I revisited many of the key players across the public protection network to check whether they thought we had identified the right areas for further investigation. Later in the process I sought the views of senior players as to our emerging recommendations – to see if they thought they were realistic, practicable and would command support from the relevant agencies and services. I also spoke to those working on developing policy and future systems within the UK and EU including those working on possible future biometric developments and systems already underway such as the Intelligence Management, Prioritisation, Analysis, Co-ordination and Tasking Programme (IMPACT), the Police National Database (PND), the Schengen Information System (SIS) II etc, to ensure we took account of what is in the pipeline.

18. In order fully to understand what is needed by the front-line staff the team also met with several key groups: those working in custody suites; in courts; in prisons; in probation areas; in the UK Border Agency; in immigration detention centres and the Asylum and Immigration Tribunal (AIT). We sought to establish that we understood the existing business processes, had mapped them correctly and to identify key decision points of the processes at which changes might significantly benefit the whole system. Later in the Review, the team checked the feasibility of our developing recommendations for change with a number of frontline staff. I am grateful to all who participated in meetings, interviews and workshops and hope that the implementation of our recommendations will remove some of the frustrations that they currently experience in carrying out what are often difficult and challenging roles.

Other Reviews

19. I also took account of other relevant initiatives and reviews. Information handling in support of public protection is central to many of the recommendations which emerged from Sir Michael Bichard's Soham Inquiry. In 2004, he highlighted issues around information sharing, particularly in relation to police intelligence and international data, which remain important. I hope this Review can help drive forward towards resolution. Progress against some of his most important recommendations has been disappointing. We have tried to learn from that, and to develop a comprehensive strategy, strong governance recommendations, and mechanisms to resolve funding and other issues.

20. The Review of Policing by Sir Ronnie Flanagan reported in February 2008. My Review shares many of his themes, for example in terms of the need to identify and embed good practice around information handling and to work in more effective partnerships across agencies. He also focuses on the need to move to a less risk-averse culture and reduce the extent to which essential recording and documentation shades over into unhelpful red tape. I agree with this. It links to the importance of understanding why specific data needs to be recorded and communicating that understanding at all levels. If we can be clear about what information is really necessary, we can be equally clear about what is unnecessary.

21. Effective use and sharing of information is a key theme of the work which has emerged from the Fraud Review, with implementation of that Review's recommendations being led by the Attorney General. The National Fraud Reporting Centre and Intelligence Bureau will be the hub in which knowledge about fraud is collated and managed. This set of initiatives is a helpful and positive example of improving the use of criminality information in support of public protection and can offer lessons for other operational environments.

22. The Data Sharing Review by Dr Mark Walport, Director of the Wellcome Trust and Richard Thomas, the Information Commissioner has highlighted that there are risks both in sharing and not sharing information. It has pointed the way towards a simpler legal framework governing data sharing, with appropriate safeguards. I am strongly supportive of this.

23. We have also been conscious of the work underway to review information security across Government in the light of high-profile data losses, notably by Her Majesty's Revenue and Customs (HMRC). There is a fundamental responsibility on the public services to keep personal information secure, which must be balanced against the public protection benefits from sharing. Achieving and maintaining that balance is very difficult, but I hope this Review can make a positive contribution towards doing so.

24. There are several other reviews that have a bearing on the focus of this work. That provides further evidence of the complexity of the public protection network and its history of new organisations, procedures and processes being introduced to meet specific, and often compelling, requirements for action.

25. What is striking is the ad hoc nature of these. There is no common agenda or standards for dealing with the sharing of criminality information. As a consequence, we are not always making best use of the national and international information that is available and can legitimately be accessed. The following Chapters seek to address the most significant problems arising from the lack of such an agenda. It is important to start examining the need for a coherent, strategic approach so that we can capitalise on future developments and ensure they are available to those who carry the responsibility for protecting the public.







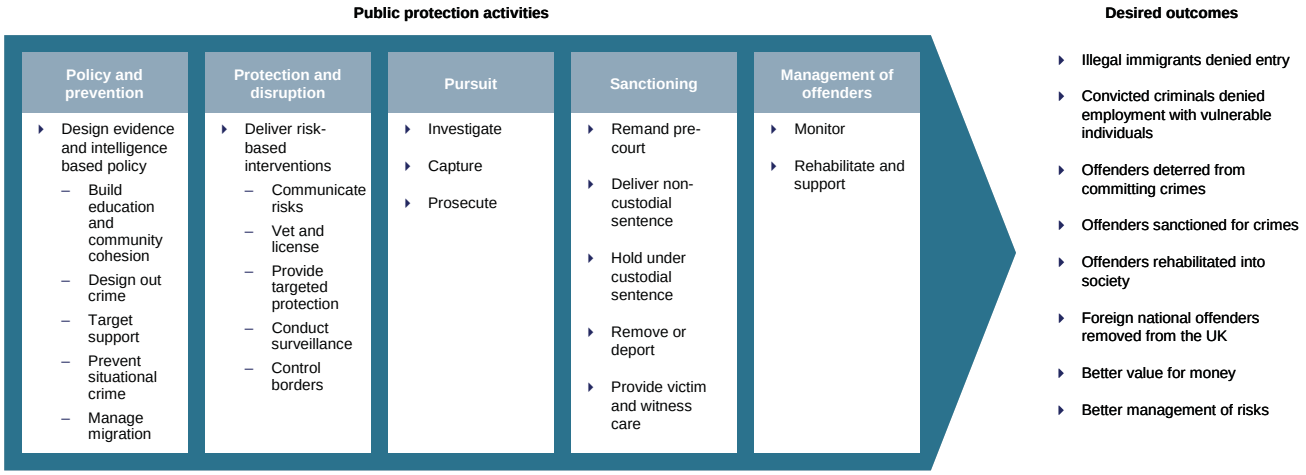


CHAPTER 2: STRATEGIC DIRECTION

The Challenge of Protecting the Public

26. Protecting the public is a fundamental role of Government, but the process by which this is achieved cuts across many Government Departments, Agencies and other institutions. I have sought to assess the collective performance of those entities dedicated to public protection so as to ascertain whether any improvement in the use of information might contribute to the desired outcomes. I conducted this assessment against a holistic definition of the main public protection activities and their outcomes.

Public Protection Assessment Framework



Recent Performance Against that Objective

27. Given the central role of Government in public protection, we were not surprised to see many examples of extremely strong practice. In fact, you cannot help but be impressed by the courageous and extremely effective efforts of those in the front-line of public protection.

28. Nonetheless, we also observed several areas for improvement. Many of these improvement areas would benefit from better management of information, and what struck us most was how co-operation, often leading to rapid joint working, will be integral to addressing them.

29. This is an important finding, and illustrates the importance of managing the collection and sharing of criminality information not as a set of delivery silos, but as an inter-linked network. While progress has been made in this area, it lags behind the continued rapid advance of available information management technologies and capabilities.

Public protection performance assessment	
Positive outcomes	**Evidence**
• Steady reduction in illegal approaches to immigration over recent years	• 75% reduction in unfounded asylum claims between 2002 and 2007 • 110% increase in proportion of failed asylum seekers removed between 2002 and 2006
• Improvements underway around the vetting of employees destined to work with vulnerable individuals	• Based on the Bichard Inquiry and following the Safeguarding Vulnerable Groups Act 2006, plans are underway to launch the Independent Safeguarding Authority (ISA) in 2009 to provide better protection for those working with children and vulnerable adults
• Steady reduction in overall crime statistics	• Overall level of police recorded crime down by 12% in Oct–Dec 2007 as compared with same quarter in 2006 • 23% risk of being a victim of crime (down 1% from previous year) in the year to December 2007. At lowest level since 1981
• Recent reduction in drug use – particularly amongst young people	• 28% reduction in Drug Harm Index (DHI) between 2002 and 2005 • Eight-fold increase, between 2004 and 2007, in drug offenders entering treatment through CJS • 47% reduction between 2003 and 2006 in frequent drug use by vulnerable young people • 28% reduction in frequent drug use by young people (between 2002 and 2007)
• Steady increase in the number of offenders sanctioned for crimes	• 0.14m more offences brought to justice (in 12 months to June 2007) than targeted by 2004 PSAs
• Increase in the professionalism of the Criminal Justice System	• 3% increase in public confidence in CJS (up to 42%) between 2002 and 2007 • Decrease from 33% in 2001 to 29% in 2007 of those feeling that CJS would treat them worse due to their race • 77% of court results loaded onto PNC within 10 day target in October 2007, up from less than 70% in 2005

Public protection performance assessment	
Negative outcomes	**Evidence**
• Room to improve information sources related to immigration	• UK unable to access EU immigration data, as does not participate in Schengen Acquis • Average of 600 checks made by the UK per year of the Interpol Stolen and Lost Travel Document database, as opposed to 7.4m per year by France and 3.6m per year by Switzerland • According to our interviews, illegally entering or overstaying one's visa is rarely recorded on the PNC • 7,000 Security Industry Authorities (SIA) security employees were found to be illegal immigrants and had their licences revoked in December 2007 • Multiple attempts by Home Office to count immigrant workers and dependants
• Information delays when international data sources are involved	• Delay of 12 months in checking DNA profiles from crime scenes provided by the Netherlands to the Crown Prosecution Service (CPS) • Interviews with practitioners describe a lack of standardised processes for international sharing
• Limited reduction in violent or antisocial behaviour – indicating an opportunity for better risk-based crime prevention and situational crime prevention	• Violent crime, burglary, vehicle theft and vandalism all remained stable in September 2007 compared to previous year • 4% increase in firearm offences between year ending September 2006 and year ending September 2007 • 5 children under 16 shot dead in 2007, zero in 2006 • No change in 2007 overall levels of perceived anti-social behaviour compared to previous year
• Continued challenges around offending while on bail – an area dependent on rapid sharing of information around patterns of offending	• Several incidents of criminals on bail or early release, committing further crimes – for example four time repeat offender Adam Swellings murder of Garry Newlove in August 2007 • Average waiting times while on bail for the Crown Court increased steadily from 9.5 weeks in 2000 to 14 weeks in 2006 – a relevant statistic as separate studies have identified a link between time on bail and likelihood of re–offending • Over the past 3 years, the number of persons bailed while accused of "violence against the person" fell from 71,800 to 64,800. However, the proportion of those bailed who failed to appear at court remained static at 9% over the same period
• Examples of weak or defective information sharing procedures	• In October 2006, 15% of court results still taking over 28 days to be put on PNC • In December 2007 four CDs were lost from the MoJ containing sensitive court information
Source: Recent Departmental Performance Reports	

The "Public Protection Network" (PPN)

30. I have found it helpful to think of the many organisations involved in protecting the public as belonging to a network. As a network, a requirement exists for common understanding, a common approach to sharing information, and an agreed agenda for improvement to which I hope all will subscribe.

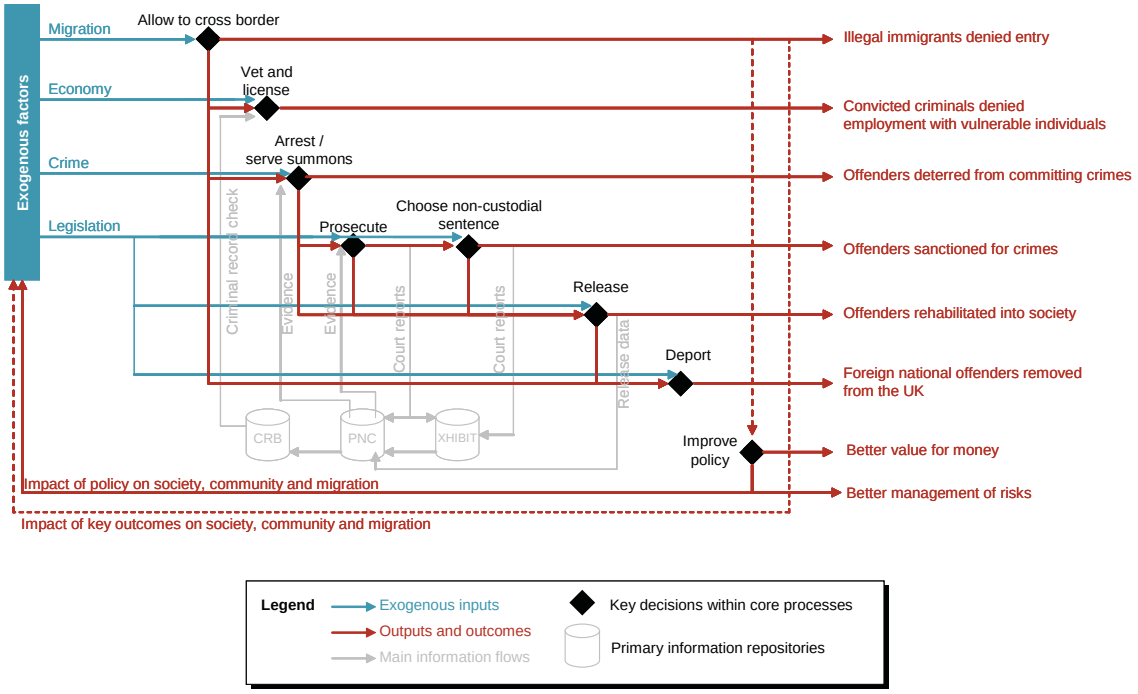
31. At present there are dozens of UK organisations which capture information potentially relevant to criminality for their own legitimate and proper purposes in the areas of health, education, or taxation, for example, to say nothing of the more than 50 UK police forces. All these organisations will have an information strategy to ensure that they capture and record the information they require to meet their own responsibilities, and all will have protocols and safeguards designed to ensure the integrity of their data collection processes. In some cases, explicit arrangements exist to coordinate the planning of the collection of criminality information. But the focus of that planning is inevitably narrower than the very broad territory of public protection.

32. On further analysis, however, the entities serving public protection also demand consideration as a single network owing to the density of interconnections between them and the interdependence between one public protection outcome and the next. For example, the decision to prosecute a potential criminal depends heavily on the information available before and after his or her arrest. This in turn depends upon the preventative measures in place to increase information available to the police or to deter criminals from committing crimes in the first place. Finally, the direct outcome of the decision to prosecute might be a fine or a custodial sentence, but it typically affects other outcomes such as the number of offenders deterred from committing crimes, the cost of holding offenders in custody, and the pressure to release or deport prisoners. Put another way, most organisations in the network act independently yet depend greatly upon information supplied by each of the others, and not surprisingly their outcomes are heavily co-dependent.

33. Recognising the existence of the network has important implications for how best to achieve the desired public protection outcomes. At a network, no matter how highly an individual organisation performs, the overall outcomes depend substantially upon having the right standards for communication, the overall network architecture, the security and access standards applied at every point in the network and the level of investment in data accuracy and storage. The purpose of this discussion is not to make a network computing analogy, but to illustrate the need for management oversight across the whole of the PPN.

34. I have also considered to what extent a single network applies to the whole scope of public protection information. Merely by considering the highest level decisions taken in support of the desired public protection outcomes, it becomes clear that every activity from border control to rehabilitation in society sits within the same network. The image below is intended to illustrate this co-dependency.

Public protection – a network of interlinked processes, decisions and outcomes



35. Developing a strategic approach in such an environment requires improved co-operation between a collection of interlinked, but independent activities. A number of criteria need to be met for successful co-operation across public protection organisations:

- First, effective co-operation requires common purpose among those who contribute. While conducting this Review we have tested the strength of common purpose amongst senior stakeholders across the PPN. There is clearly a strong sense of common purpose, though it is sometimes overwhelmed by a dedication to the immediate challenges of delivery and budgets
- Second, effective co-operation requires careful management in the sensitive area of personal information sharing. In particular:
    - Capture, use and security of all personal information raises anxieties, as exemplified by the debate on identity cards, the investigation into recent losses of personal data, and the recent reaction to a senior member of the Judiciary advocating extending the UK's DNA database
    - The critical importance of several PPN outcomes, for example, the need to protect children from paedophiles. This tends to lead to what could be termed "a zero tolerance" approach to risk – something that is well known in the business world either to halt progress or to generate exorbitant costs

- Public and political concern around the nature of immigration into the UK

- Third, all those involved in managing elements of the PPN must understand the full network and their position in it. Part of the challenge with conducting this Review is the lack of a clear map of the PPN and its interconnections. I have begun to develop a version of this, as shown at Annex CI, for further development as the recommendations of this Review are implemented

- Fourth, to secure full support, all concerned must be convinced of the value of co-operation and joint working

The Case for Co-operation

36. A decision to foster co-operation across the PPN will require assurance that the financial and societal benefits outweigh the costs. We have produced broad estimates of the financial costs and benefits of implementing my recommendations. These will need to be refined. We cannot say how many criminals may be prevented from entering the UK rather than having to be tracked down having done so – with the resultant costs and added risk to the public. We cannot say how many attacks on front-line officers will be prevented by better sharing of information on offenders. However, we are able to bring together a view of the potential benefits likely to be identified over time, and high level estimates of the costs of realising such benefits. We do this based on an understanding of the improvements in effectiveness and efficiency that would result from a co-ordinated implementation of the overall package of recommendations in this Report.

Based on this, the team has produced an overview of potential benefits and costs. As with most business cases, two types of benefits exist, namely the one-off and continuing benefits that are regularly returned over a period of time.

I have also differentiated between the various types of cost:

1. Upfront costs arising from the setting up of the respective programme or initiative, and any initial deployment of resources.

2. Continuing costs of the particular improvement being suggested.

3. Indirect costs that result from the positive PPN outcomes in question that place a strain on the operating budgets of entities elsewhere in the PPN, as highlighted by the case study below. Examples of indirect costs to organisations concerned with public protection will include:

- The need to process more criminality information because more is available

- Potential increase in numbers of court cases

- Potential increases in convictions

Indirect costs case study

Improved use of biometrics in prosecuting and convicting, could lead to 1% more convictions of those tried at court. Of this figure, an average of 7% are sentenced to custody. According to our preliminary research, this could reduce the cost of crime by tens of millions of pounds, for a modest outlay of a few million pounds.

However, this would also mean, for the possible numbers affected (at an average stay in custody of 252 days) a potential increased "downstream" cost to the Prison Service of £1.7m per annum.

This does not include the logistical problems that an already over-stretched service would have in finding the necessary accommodation to house this many offenders. We have not attempted to quantify this challenge.

Initial Estimate of Potential Benefits and Costs

	Potential benefits		Implementation costs		
	One-off	Continuing	Upfront	Continuing	Indirect
Improved effectiveness across core processes	£30 – 50m	£23 – 65m	£3 – 29m	£0 – 6m	Important trade-off to consider (see above case study)
Increased efficiency benefits		£110 – 332m	£22 – 53m	£6 – 12m	
Cost of co-ordinated governance and initial implementation	Above benefits depend on co-ordinated governance and implementation		£1m	£1m	
Source: Review of Criminality Information (ROCI) estimates					

37. These figures have been derived from repeated interaction with stakeholders across the PPN, and detailed examination of economic and accounting data.

Benefit and cost estimates are necessarily tentative. In compiling our figures we have extrapolated from available data on comparable initiatives, but in those cases where it would have been misleading to calculate an overall benefit to the whole network we merely counted the benefits of an example initiative. This suggests that our overall calculation of benefits is likely to be an underestimate.

Ultimately, costs and benefits will depend on:

- The pace of implementation of these recommendations
- The extent to which Ministers choose to implement solutions when more detailed business cases are available – for example, once the cost of individual multilateral information sharing processes are better understood on a country by country basis, or once the cost of re-using specific technologies, which I recommend elsewhere, is better understood

- The order in which they are implemented
- The extent to which implementation costs can be shared across related improvement initiatives

38. Decisions on each will be influenced by the specific implications for the organisations affected. For example, the development of standardised international information sharing arrangements might initially focus on low cost standards applied for all international transactions plus a few detailed arrangements which would bring the greatest net benefit to the PPN, perhaps arrangements with Interpol along with those countries which currently supply the greatest number of migrant workers to the UK. In a sense, you get what you pay for, as follows:

39. Effectiveness Spend

Implementation spend			Relevant benefits	
Low	£3m upfront Minimal continuing	Minimal upfront investment on basic standardised processes to update UK databases with the highest value for money international data sets Applicable to UKBA, CRB and the UK DNA database Assumes no fees required given reciprocal access to the relatively high quality UK data sets Minimal costs incurred to streamline FNP release and deportation processes	£30m one-off £23m continuing	Greater access to a few international data sets best suited for sharing with UK systems and containing data on individuals most likely to offend in the UK More intervention required to handle exceptions to the standardised processes
High	£29m upfront £6m continuing	Further process fixes to handle any complications and in response to the core PPN principles of information management Creation of more international interfaces Continuing costs increased to reflect the above	£50m one-off £65m continuing	Greater access to other nations' data sets, with resulting improvements in PPN outcomes Less intervention required to handle non-standard information sharing and related processes Further reduction in risks associated with PPN outcomes

40. Efficiency Spend

Implementation spend			Relevant benefits	
Low	£22m upfront £6m continuing	Business process design to reduce future IT spend across the PPN Oversight cost for relevant initiatives Assumes lower scenario of business and IT change volumes across the PPN	£110m continuing	Reduction in IT spend Greater change programme success in response to a better cross PPN oversight capability Other benefits with less financial impact include paper reduction and improved sharing
High	£53m upfront £12m continuing	Assumes higher scenario of business and IT change volumes across the PPN	£332m continuing	Above benefits increase with the greater baseline of PPN-wide business and IT change

41. We expect the benefits and costs to lie within the ranges estimated above. I recommend that the implementation team looks at the specifics of each recommendation and puts a fully-costed action plan to Ministers, setting out which initiatives offer the best value improvements to the PPN. Indirect costs and the balance of risk should also be considered.

42. On this basis, it is clear to me that the benefits of co-operation can vastly outweigh the associated costs, as illustrated by the above table. In the remaining Chapters I recommend how these outcomes may be achieved by building a coherent approach to delivery of the strategy. In particular, the case for co-operation will need to be made to the front-line by those in a position of leadership, and with reference to a coherent governance framework and a strong set of enablers to support delivery of this improvement agenda.

Recommendation

- By January 2009, the Government should agree, across Departments:
  - A strategic direction for the improvement of criminality information management across the Public Protection Network (PPN)
  - Prioritised immediate objectives for improvement
  - The embedding in relevant Departments' goals and objectives of the principles in this report

  The strategic direction should articulate clear goals for the role of criminality information management in supporting public protection and be based on an objective assessment of performance against those goals. Regular performance reviews should update this initial assessment, and also assess implementation progress with respect to the recommendations of this Review.

  The improvement agenda should respect the following principles. It should:

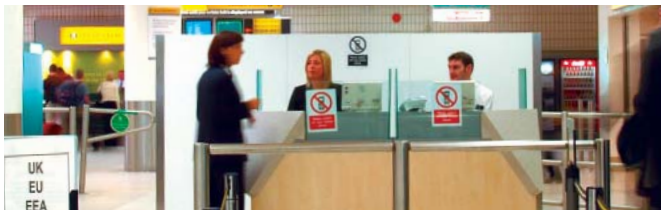
  - Adhere to all existing governance around information management – in particular: Data Protection Act (DPA), Freedom of Information (FOI)
  - Provide for collaboration only where the total benefits to public protection exceed the total cost, recognising that some benefits may be realised outside the funding organisation's area
  - Maintain delegated authorities wherever possible to allow delivery units to own core processes and thereby deliver agile responses to criminal activity
  - Institutionalise key aspects of the PPN only as needed to deliver clarity and value to PPN participants **(recommendation 1)**

43. This is a preliminary list, and should be developed further as improvements are implemented. In so doing, it should have regard to the following challenges inherent in the public protection network:

- Public protection touches society at all levels and in a wide variety of ways
- Multiple operating units are responsible for delivery, often with a premium on rapid local decision-making
- There is heavy dependence on similar information about individuals
- Interlinked outcomes may generate virtuous circles (such as a reduction in persons in custody initiated by a sustained reduction in re-offending) but also unintended consequences (such as downstream pressures on PPN organisations caused by an increase in arrest rates)

44. The new strategic direction will therefore include the key principles of information management and sharing that will span all public protection organisations and will specify where needed the ways in which criminality information should be recorded, secured, used, exchanged and shared to support public protection.




UK
EU





CHAPTER 3: GOVERNANCE AND DELIVERY

The Challenge of Governing Across the Public Protection Network

45. As will be clear from the previous Chapter, the size and complexity of the PPN presents real challenges to effective governance. On the one hand we need agile, empowered organisations that can respond swiftly to specific and local needs. On the other we need mechanisms that will ensure the safe and appropriate capture, sharing and use of criminality information between these organisations – including between nations – and which will command public confidence. This latter point is critical. Public confidence is fragile. Criminality information is sensitive. If that information is to be shared more effectively in the interests of public protection we must have a governance framework which will satisfy the public that proper safeguards are in place and that accountability is clear.

46. Effective governance requires an appropriate balance of ownership, process and control. Where ownership is shared a clear process may enable safe handoffs. Where process is vague strong ownership by an experienced practitioner may ensure delivery. And where processes are strong the control regime may be minimal. The key requirement is for a governance mechanism that is aligned to the purpose it serves.

47. When I reviewed the PPN against this definition of effective governance I found several examples of strong governance. However I also found gaps that were not addressed by ownership, processes or controls.

	PPN Governance Assessment	
	Strengths	Weaknesses

Ownership	• Clear ownership of the improvement agenda achieved for large portions of the PPN, eg, NPIA, OCJR (now strengthened further under the MoJ's new Criminal Justice and Offender Management Directorate)
	• National Criminal Justice Board (NCJB) owns a strategic challenge and performance assessment agenda across the Criminal Justice System
	• National Crime Reduction Board owns a policy and oversight agenda for the reduction of crime
		• Limited clarity of ownership for operational and information management issues across the PPN
		• Lack of a network - wide view to inform key resource allocation decisions across the PPN
		• Responsibility for effective use of international data exchange is unclear
		• Staff incentives typically exclude important PPN information management role – equally true for both senior managers and frontline staff
		  • Eg limited time spent by senior managers on this issue
		  • Eg people may fail to take the time to match different crimes to the same person

Process	• Where procedures are documented, substantial successes have been achieved
	  • Eg MAPPA
	  • Eg Police Forces which perform highly on Arrest Summon Notification (ASN) and Court Report data entry
	• Implementation of new custody suite software has brought increased quality to ASN completions
		• Strategy documentation spanning the PPN is typically aimed at senior audiences only and fails to address the complexity of managing the network, eg Departmental strategies
		• Processes for seeking and handling international data are largely absent for routine criminality information
		• Processes for sharing PPN information across organisational boundaries are often absent and contribute to limited use of important information, eg UKBA data of relevance to the police
		• Several data formats are incompatible, eg between CRB and MOPI

Control	• New software is introducing a series of mandatory fields to fill out	• Where processes are lacking for sharing of data (both domestically and internationally) multiple examples of data loss indicate an inadequate control regime • Where PSAs are cascaded and tracked at the operational level, a dogged focus on a narrow target may take the underlying process "out of control" eg Asylum cases are targeted for deportation and therefore dealt with quicker than foreign national prisoner deportations

48. Given the size and diversity of the PPN these gaps are not surprising. For good reason the network includes substantial delegated authority to those best able to react with agility. Mapping existing arrangements has been an important part of this Review so that we can see the PPN as a whole. In order to understand the key accountabilities and responsibilities across the entire network I have reviewed three aspects of the existing governance framework:

    1. Cross-departmental PSA relevant to public protection
    2. Existing accountabilities and responsibilities across the network
    3. Role played by the major entities responsible for managing information across the network

Cross-Departmental PSAs Relevant to Public Protection

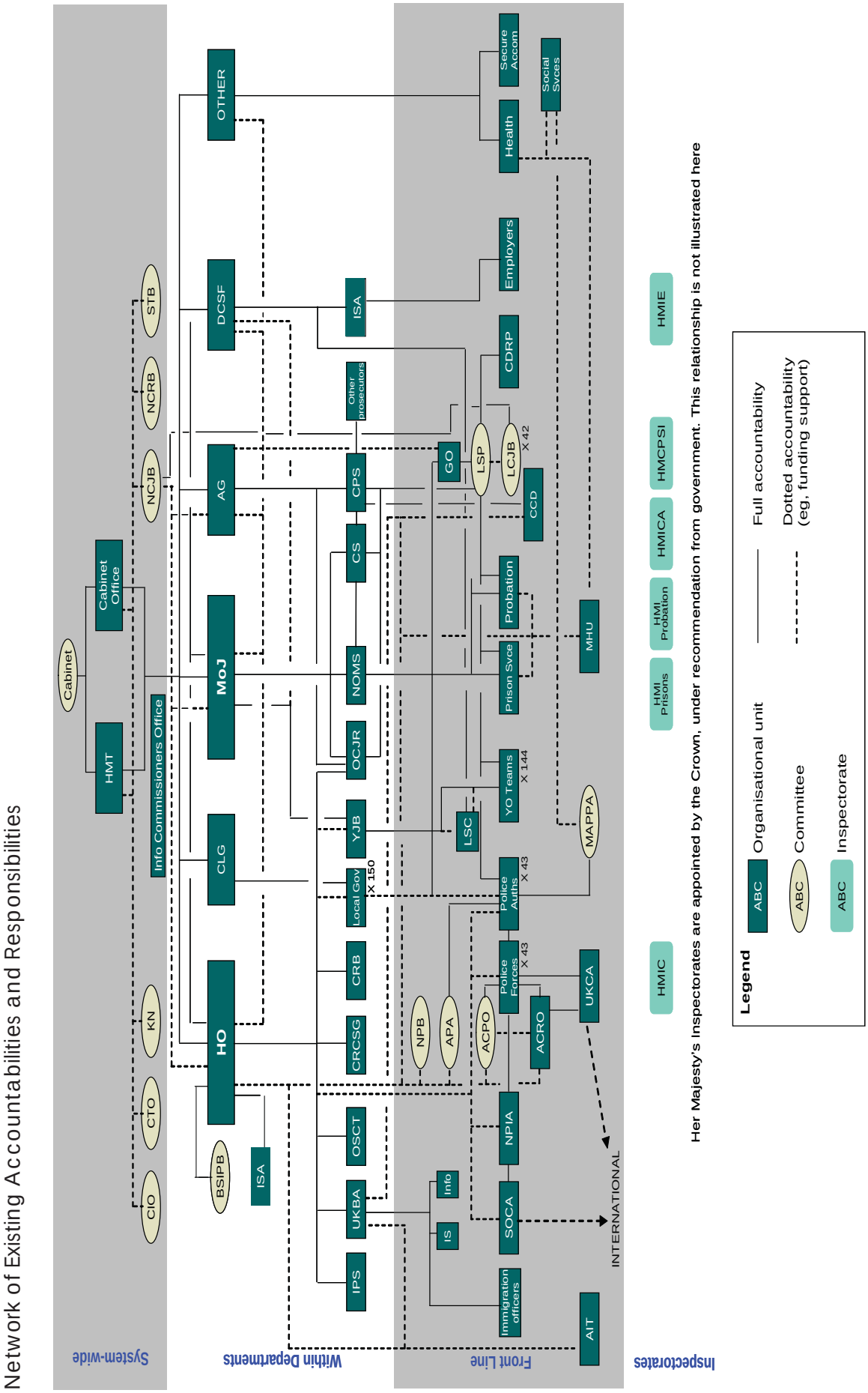
49. The PSAs were announced in October 2007 by the Chancellor of the Exchequer in his Pre-Budget Report and Comprehensive Spending Review, and represent a major effort to co-ordinate Departments' activities in support of the most important cross-departmental outcomes. The intent of the PSA framework is to allow individual entities to prioritise their efforts – empowered to act independently, but focused on the coherent objectives listed above.

50. Public protection spanned three of the four priority performance areas identified and leadership of its delivery was allocated to four owners. Each lead organisation depends on multiple entities to deliver effective public protection. For example, to deliver against the PSA to "make communities safer", the Home Office leads yet depends heavily upon many other units inside and outside of the Department, including: UK Border Agency, Criminal Records Bureau (CRB), Police Forces, SOCA, Courts, Prisons, Probation, Social Services, DCSF, Department of Health, CLG, Local Authorities, Victim Support and other Third Sector partners.

Existing Accountabilities and Responsibilities Across the PPN

51. Each oganisation within the PPN may already have clear terms of reference for conducting its business. Consideration of the whole network, however, reveals a highly complex web of reporting lines, dotted line relationships, coordinating committees and inspectorates. This is partly a natural response to the need for delegated authority, but equally it provides a powerful illustration of the challenge of ensuring effective co-operation between these entities in support of shared outcomes.

Network of Existing Accountabilities and Responsibilities



Role Played by the Major Entities Responsible for Managing Information Across the PPN

52. Aside from the overall governance challenge, how is information managed? Several entities and agreements within the above governance framework serve to coordinate key aspects of criminality information management. To assess this I have mapped relevant elements of governance against the activities of the overall PPN (as defined in the Strategy Chapter) and the key information management governance needs, defined as:

- Develop strategy
- Set funding
- Prioritise investment
- Manage delivery
- Deliver service
- Assess delivery

Against this mapping it is clear that many entities exert influence over information management across the PPN, that their roles overlap in many cases, and that some white spaces exist. The relevant map is at Annex C.

Governance of Information Management Activities at the Next Level of Detail

53. In addition to these high level assessments of governance around information management across the PPN, there is also room to bring clarity at the next level of detail. This should draw on best practices to require absolute clarity of ownership and decision rights for each key aspect of information management, including:

- Capture – what information do we seek, for what purpose, and how do we gather it?
- Store – where do we store it, for how long, and under what security?
- Access – how can it be accessed, who has the right to do so, and do they have the ability to change the information?
- Share – what interconnections should and do exist between repositories of information, what is the nature of those connections? For example, does one master copy of the record exist, or is the information broadcast to multiple repositories? How rapidly is information available to those who need it?

- Analyse – is information available in a format suitable for its intended use and when it is needed?
- Act – do decision-makers act on the basis of the information available, and do their actions result in successful outcomes?
- Manage – do managers understand the performance of the PPN, the contribution of information to this and are they able to communicate it to staff?

It has not been possible to provide an exhaustive assessment at this level of detail in this Review. Instead, we focus first on an exhaustive response to the higher level challenges around the "manage" aspect within the early Chapters. Several detailed recommendations began to emerge where we considered immediate next steps at the front-line and in the technology domain. These recommendations are discussed further in the Technology and At the Front-line Chapters of this report.

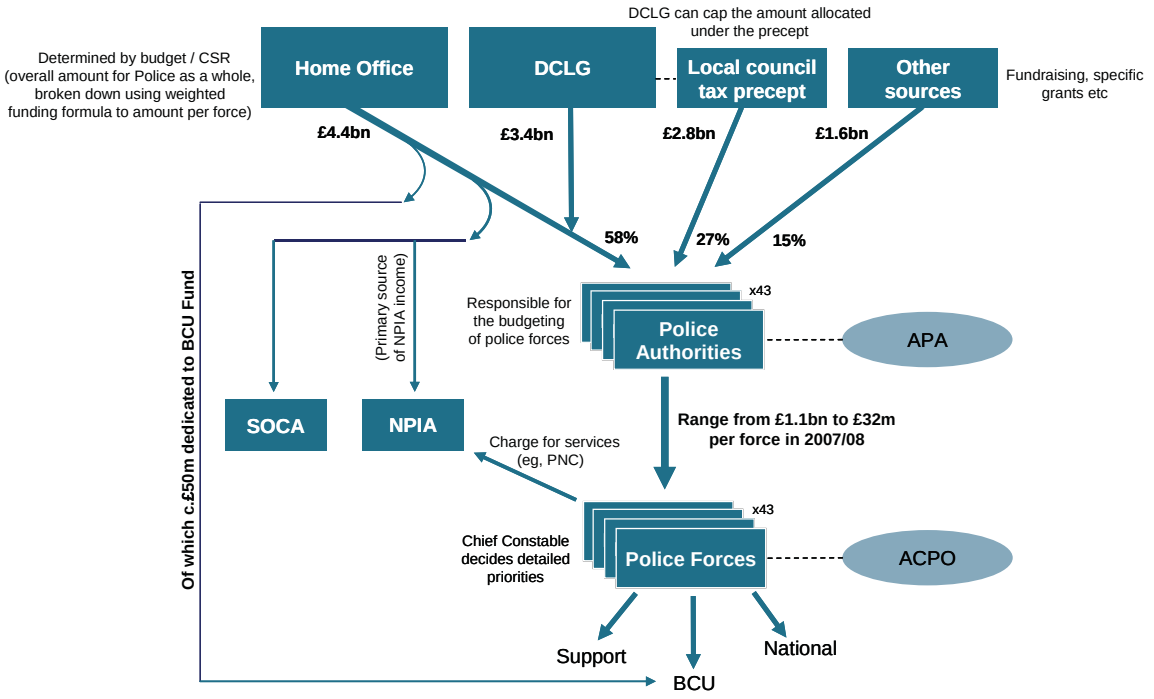
Seeking to Address the High Level Challenge – Case Studies

54. These findings are largely to be expected as the PPN has evolved over a number of years with new organisations being created and the responsibilities of others adjusted to meet specific needs. PPN governance reflects that history and the requirement to provide for the freedom to act with local agility.

The following case studies are examples which help to explain current governance arrangements, and to assess their contribution to the effective management of the PPN as whole:

- **Dotted line accountability** – as illustrated by the funding and performance assessment regime for the local Police Forces of England and Wales
- **Devolved local accountability** – as illustrated by the role played by three local initiatives: Local Criminal Justice Boards (LCJBs), CDRPs and Multi Agency Public Protection Arrangements (MAPPAs)
- **Senior accountability** – as illustrated by the NCJB
- **Independent oversight** – as illustrated by the Information Commissioner

Case Study 1: Dotted line accountability – national funding and performance assessment regime for local Police Forces



Sources: Police Grant Report 2007/08, ROCI team interviews and analysis

Strengths	Weaknesses
• Effective – the money gets to where it is needed • Embodies delegated authority • Combines elements of central prioritisation of resource with local prioritisation of resource • Allows Chief Constables to exercise their delegated authority as professionals on local partnerships / Boards (see Case Study 2) where further local co-ordination is required • Brings economies of scale in information management via NPIA ownership of the PNC	• Indirect national accountability in most matters (excluding PNC development) • Divides national resources, whereas the more challenging aspects of public protection may require greater combination of resources • Contributes to the co-ordination challenge facing the PPN

Conclusion

Dotted line accountability represents a fundamental element of the current position across the PPN that any proposed governance solution will need to take into account.

Case Study 2: Devolved local accountability - three local initiatives

Three examples of local initiative are particularly relevant to the PPN. For each, I identify their unique characteristics, and then their respective strengths and weaknesses with respect to the governance needs of the PPN.

1. Local Criminal Justice Boards (LCJBs)

Key characteristics
• 42 LCJBs established in England and Wales in 2003 • Core membership includes: Police, Youth Offending Teams (YOTs), CPS, Her Majesty's Court Service (HMCS), Prisons and Probation • Responsible for delivering local improvement against agreed criminal justice performance targets • Guidance and oversight provided by NCJB and OCJR

Strengths	Weaknesses
• Good track record of collaboration, determination of relevant local strategies and local delivery success • Broad coverage across most core PPN organisations • Grouping into 42 areas helps ensure strong ownership	• No formal link to UK Borders Agency, although some local partnerships forged in areas of high immigration • In some cases, links to Prisons are also missing – although this should be resolved by the proposed move to one NOMS representative (to cover prisons and probation) • Already stretched to deliver against a broad range of existing targets

2. Crime and Disorder Reduction Partnerships (CDRPs)

Key characteristics
• 352 CDRPs in England, and 22 Community Safety Partnerships (CSPs) in Wales came into being following the Crime and Disorder Act 1998 • Responsible authorities in these statutory partnerships are: Police Forces, Police Authorities, Local Authorities, Fire and Rescue Authorities, Local Health Boards (Wales) and Primary Care Trusts (England) • Statutory responsibility is to tackle crime and disorder, including antisocial behaviour and drug abuse

Strengths	Weaknesses
• Broad coverage across the full range of public protection outcomes • National standards for each CDRP introduced in 2007, including areas closely related to our PPN governance objectives: • Strategic resource allocation process • Information and intelligence gathering business processes • Information sharing protocols • Some central control from the Home Office might support PPN implementation efforts	• 374 local arrangements would be hard to manage to achieve national co-ordination of the PPN • Already stretched to deliver on targets

3. Multi Agency Public Protection Arrangements (MAPPAs)

Key characteristics
• 42 MAPPA Strategic Management Boards (SMBs) review, monitor and manage risks posed by sexual and violent offenders in the community • Core membership of SMBs includes: Police, Prisons and Probation • Supporting agencies have a duty to co-operate with the SMB: Local Health Authorities and Trusts, Housing Authorities and registered social landlords, Social Services, Social Security and employment service, Youth Offending Teams, Local Education Authorities, and electronic monitoring providers • Data on sexual and violent offenders is maintained nationally on ViSOR database • Guidance and oversight provided by the Public Protection Unit (PPU) of National Offender Management Service (NOMS) and the National MAPPA Strategic Management Board

Strengths	Weaknesses
• Track record of operational delivery • National co-ordination achieved via two operationally focused Boards • Not set up to develop local strategies, but includes a strong continuous improvement focus • Discussions underway about the potential inclusion of UK Borders Agency	• Costly to operate • Resources fully stretched to meet the primary focus of the arrangements – unlikely to welcome or dedicate further resource to a broader PPN remit

Conclusion

Existing local arrangements contain many examples of good practice, but their remits fail to meet the needs for co-ordination of information management across the PPN by being either more narrowly focused than that required by the PPN as a whole, or too high level to impact directly on the key information management activities.

Case Study 3: Senior accountability – as illustrated by the National Criminal Justice Board

Key characteristics

- Senior Ministerial committee composed of 33 leading members of the Criminal Justice System (CJS), including the Home Secretary, the Secretary of State for Justice, and the Attorney General
- The National Criminal Justice Board (NCJB) is responsible for supporting local boards to bring more offences to justice and to improve public confidence. It does this by:
    - Removing barriers to joint working, focusing in on particular concrete aspects of the CJS business process
    - Strategic direction of resources to secure achievement of objectives
    - Horizon scanning to identify longer term opportunities and threats
    - Learning and transferring the lessons from local areas and agencies which have successfully innovated and which offer lessons for the rest of the system
- The National Criminal Justice Board also has specific responsibility for:
    - Combating inequality and discrimination in the CJS
    - Communication across the CJS
    - The Board reports to the CJS Cabinet Committee on progress. The CJS Cabinet Committee retains overall responsibility for tracking delivery of the CJS PSA targets. The Board takes on other remits from the CJS Committee as the Committee decides

Strengths	Weaknesses
• Maintains a single system view across the whole of the CJS and much of the PPN • Brings Ministerial clout and buy-in to major issues requiring joint ownership across Departments	• Broad remit makes it difficult to maintain a management focus on the CJS, let alone the rest of the PPN • Urgent political issues are a necessary distraction from operational management issues • Operational members lack the time to step back from their immediate leadership roles to consider system-wide challenges • Remit has recently broadened further as LCJBs are increasingly not just reporting performance statistics but also successes and failures from local improvement initiatives or "Beacons" • Limited visibility or direct influence over detailed operational issues, for example, information management – even if they are cross-cutting

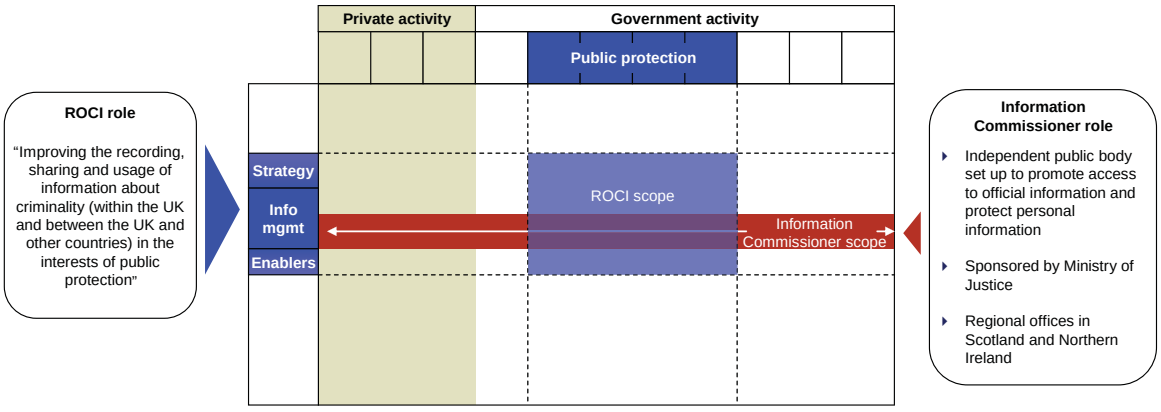
Conclusion

A degree of Ministerial oversight is a necessary element of any effort to work jointly across Government Departments, but the scope of any Ministerial group needs to be very tightly defined if it is going to engage at the right level of detail. The PPN's information management challenge is sufficiently detailed that it will require an intermediate layer of management challenge and oversight responsible for escalating only those issues and decisions worthy of Ministerial discussion.

Case Study 4: Independent oversight – as illustrated by the Information Commissioner

This review shares an interest in information management with the Information Commissioner. The scope of interest in information management does, however, differ substantially – although there is some overlap.

Comparison of the scope of the Information Commissioner with the scope of this Review



Key characteristics

- Independent public body set up to promote access to official information and protect personal information, founded as the Data Protection Registrar in 1984
- Sponsored by Ministry of Justice
- Employs more than 200 staff, with regional offices in Scotland and Northern Ireland
- Remit confirmed by the DPA 1998 and the FoI 2000

Strengths

- Clear remit and focus, supported by a solid track record has built a strong brand within and outside of Government
- Effective UK-wide coverage
- Strategic development capability via provision of advice, development of policy and management of internal improvement projects

Weaknesses

- Role is functionally narrower than that of improving information management across the PPN
- Objectives are more specific than the improvement of PPN outcomes – little time to focus on areas outside of the core Data Protection and Freedom of Information remit

Conclusion

Focused, independent and long-running accountability is a strong answer to a goal of consistent behaviour by a large, dispersed set of entities and individuals. However, the remit of the Information Commissioner addresses only some aspects of the overall information management challenge faced by the PPN, for example, the need to maintain a sufficiently robust data set to respond to Freedom of Information requests. It does not address how this information can best meet the operational requirements of front-line officers. Work to decide how information might be put to better use in the interests of public protection is therefore beyond the scope of the Information Commissioner's role.

A Coherent Approach to Governance

55. In recommending a strategic approach to information management and oversight across the PPN we identified four principles. In practice, each has implications for governance.

Principle	Requirement for an approach to governance coherent with the PPN strategy
• Adhere to all existing governance around information management – in particular: DPA, Freedom of Information Act	• Where possible embed DPA and FIA compliance within core processes, or if not within a light touch control regime
• Collaborate only where the total benefits to public protection of co-ordination exceed the total costs	• Minimise governance overhead – eg committee time, process inefficiencies, additional inspection regimes and other compliance costs
• Maintain delegated authorities wherever possible to allow delivery units to own core processes and thereby deliver agile responses to criminal activity	• Tailor governance recommendations to specific co-ordination need • National co-ordination to steer interlinked PPN outcomes • Need for coherence within existing organisational entities, but limited external intervention • Local co-ordination to manage interlinked PPN outcomes
• Institutionalise key aspects of the PPN only as needed to deliver clarity and value to PPN participants	• Maintain a clear distinction between continuing governance arrangements and project based interventions required as a result of this Review

In addition, it is also clear that delivery of the strategy will require effective incorporation of several key enablers, for example, the approach to investment across the PPN. Governance will have an important role to play in terms of connecting these enablers to the overall PPN strategy.

In the absence of a robust governance arrangement, the PPN would continue to run the risk of core processes and decisions at the front-line being taken independent of either the strategic intent of the PPN or its supporting enablers. Governance should therefore be regarded as the "glue" that will hold my other recommendations together.

Recommendations

- The action to deliver specific parts of this agenda should be led by the agencies concerned, but with support from a central implementation team located in the Home Office but with cross departmental staffing. This unit should be substantially in place by September 2008 **(recommendation 2)**

- Based on an objective assessment of the governance challenge, the lessons learned from existing governance arrangements around criminality, and the requirement for coherence with the overall PPN strategic direction and its core principles, the work of Agencies and the Unit should be governed by a Home Secretary-chaired Ministerial group with external challenge and advice from a Commission for Public Protection Information

  The Commission for Public Protection Information should be set up as a body to champion efficient and appropriate criminality information management across the PPN. It is not responsible for implementing this report but should contribute by:

  - Maintaining pressure on public agencies to take forward action in a difficult area, and holding them and Ministers accountable for progress, eg by publishing the external reviews of progress
  - Being a critical friend for Government as difficult issues and choices arise within or between Departments
  - Acting as a champion to help advance public understanding and debate about the policy issues and dilemmas **(recommendation 3)**

56. I recognise that implementation of my recommendations will not be easy – even with the support of the Ministerial Group and the heads of the Departments, Agencies and Services. The task is complex and will require adequate resourcing if it is to succeed. This report points to the difficulty of achieving fully collaborative and productive working across the whole territory of public protection. I am convinced that more will be required to act as a catalyst for change - hence my recommendation that a Commission for Public Protection Information be established.

57. The proposed new Commission will not take over the responsibilities of existing bodies or, as outlined above, be responsible for implementation of my recommendations. Nor will it constrain the agility of response which is essential for the effective operation of organisations in the PPN. Rather, the Commission will be independent of them, with no organisational agenda, no conflicts of interest and capable of taking a wider view, including balancing the requirements for data sharing with those for data privacy and competing investment priorities. It will be led by a part-time Chair and accountable to the Home Secretary as Head of a Ministerial group representing several of the Government Departments which have a role in public protection. It will be supported by a very small team drawn from across the Departments and other Agencies that have a part to play in public protection.

58. The objective is to provide a catalyst for better information management across the PPN, and to embed practices, processes and behaviours that will secure it. The Commission should, in three years' time, review whether there has been the significant improvement called for in this report to ensure that the concept and practice of sharing criminality information – where appropriate and with stringent safeguards – is firmly embedded in the PPN.

59. While Ministers will wish to consider the Commission's remit, I suggest that the Terms of Reference might include the key tasks set out in the chart.

	Type of role	Key tasks
Ad Hoc Ministerial Group	Ad hoc group composed of: • Home Secretary • Secretary of State for Justice • Attorney General • Secretary of State for Children, Schools and Families • Secretary of State for Health	• Determines the remit of the Commission • Sets Government priorities in response to recommendations from the Commission

	Type of role	Key tasks

Commission for Public Protection Information	• New, non-statutory body, sponsored by the Home Secretary to enhance the effectiveness and the efficiency of the PPN through the use of criminality information
	• Consists of a small committee led by a Chair and supported by a small secretariat of expert and administrative staff
	• Independent reporting as the primary source of authority (barring detailed operational commentary that might be of value to criminals) – with an initial recommendation for annual reporting
	• Relevant information sources include:
	  • Minutes of Board meetings
	  • Investment decisions
	  • Risk registers
	  • Audit and inspection reports
	  • Limited internal budget, and will work through others, such as the Implementation Team and calling for delivery support from the appropriate Department (as required)
		• Advising - to advise Ministers on the developing strategic agenda for improving criminality information management in the interests of public protection. Also, pushing for resolution of differences between organisations in the Public Protection Network on funding and other priorities
		• Champion and challenge – advocating improved management of criminality information, challenging developments, processes and behaviours that inhibit the appropriate sharing of criminality information and reporting objectively on the Government's progress on the improvement agenda. In particular, ensuring that the interests of the front line are being looked after, by for example, ensuring that there is a focus on significant front-line risks as appropriate
		• Good practice – highlighting examples of good practice across the public protection network and commissioning in-depth studies in areas of particular interest; working with the Information Commissioner to ensure adherence to legal requirements and also advising on interaction with international bodies
		• Establish clarity on PPN issues – a capacity to commission more detailed studies of any particularly difficult or intractable problems, and to make recommendations to Ministers
		• Act as a champion to help advance public understanding and debate about the policy issues and dilemmas

Delivery units	• Existing Departments, Agencies, Police Forces and other entities (eg, NPIA, OCJR)	• Implement the key enablers proposed within this Review and in future recommendations made by the Commission to ensure effective core processes and control regimes

60. The Implementation Team should get on quickly with putting the arrangements in place to begin to realise the substantial recommendations made in this report. It might also initiate work on the early practical steps which form the recommendations of the At the Front-line Chapter. Further aspects of implementation are discussed more fully in the next section.

	Type of role	Key tasks
Implementation Team	• Cross-Departmental Implementation Team • Senior sponsorship from the Home Office, in line with overall sponsorship for the Commission • Relevant support pulled in from other agencies and other Departments as necessary to implement those recommendations of the Commission agreed by the Ministerial Group	• Provides initial support to set up the Commission and Ministerial Group roles following publication of this Review • Developing an agreed agenda for criminality information, respecting the principles already set out in law and in my main report. This should articulate clear goals for the role of information management in supporting improved public protection and be based on an objective assessment of performance against those goals. It should also include working with Ministers to develop a strategic direction for the UK on international exchange of criminality information • Initiate work on all other recommendations, either itself or by identifying those accountable

61. By successfully supporting the outcomes listed above this recommendation will draw upon all of the elements of good practice identified in the case studies and required by the PPN strategic principles. Implemented as a whole, this arrangement will also address each of the core governance challenges raised at the start of this Chapter and act as the glue between the strategy of the PPN, its enablers and the front-line who deliver its desired outcomes.

Path to Implementation

62. Subject to the Home Secretary and her colleagues agreeing to proceed with my recommendations, I would urge swift progress towards implementation. I know this will be difficult and require resources to be dedicated, but if this challenge is not met then the benefits to public protection I have outlined in this report will not be realised.

63. I have given an indication of the sort of progress I expect on implementation (in the Executive Summary) by the time I revisit this area in early 2009. It is clear that management of criminality information across the PPN will remain relatively weak until these recommendations are implemented.

64. It is also clear that several parallel initiatives are underway and governance regimes in place, the most notable example being the continued presence of the Bichard Implementation Team and their remit to support the overdue implementation of several recommendations from the June 2004 Bichard Inquiry. I suggest that senior Home Office management consider consolidation as they set up implementation of this Review.




PRE-SENTENCE
REPORT





CHAPTER 4: LEADERSHIP AND CULTURE

65. The effectiveness of the new arrangements I propose, particularly the new Commission, will require the support of leaders in all the organisations involved in public protection. While information management is not usually a priority for leaders of these organisations, the potential benefits and problems for public protection that we have identified from reviewing the capture and sharing of information on criminality suggest that it is an issue that demands their attention.

66. Until recently information management has featured rarely, if ever, on Board agendas and is often seen as the responsibility of the Chief Information Officer (CIO) alone. It only becomes a priority when there is a crisis. It is unsurprising that, in general, leaders of public protection organisations have not sufficiently recognised the importance of information management. It does not feature in the key competencies of the Professional Skills for Government, which are relevant to senior civil servants. Nor is it included specifically in the agenda of the Strategic Command Course for the Police – the course that has to be taken prior to being promoted to a senior Police role. There is some inclusion of issues pertaining to the exchange of criminality information – such as public protection & the Child Exploitation and Online Protection Centre's (CEOP) inputs – although there is an opportunity to make the subject more explicit within the course. However, several Chief Constables are well qualified and understand the subject.

67. Sometimes, CIOs are members of organisational Boards. This can give some recognition to the importance of data issues. But the role is often misunderstood and the focus of discussion is on IT systems and other technical issues. Further, in today's world, ownership of information management should be shared across the whole Board and not be the sole responsibility of the CIO. This is because, in many organisations in the public protection area, information is crucial to their business.

The Climate for Sharing Criminality Information

68. There have been a number of crises involving loss of information recently, which means information management issues have been given greater prominence. The HMRC loss of discs containing the personal information of 25 million families, understandably, received widespread media coverage and caused much public concern. And there have been other incidents – indeed the Information Commissioner said in April 2008 that he had been notified of 94 data breaches over the past five months.

69. Leaders' responses to data loss included investigating what went wrong and issuing apologies; pan-Whitehall reviews were instituted with measures introduced to prevent the recurrence of such incidents. In the case of HMRC, the leadership accountability was recognised by the resignation of the Permanent Secretary.

70. This Review was itself commissioned following an inquiry early in 2007 into the handling of notifications by other European countries of criminal convictions for UK citizens. An independent review of the sequence of events and Home Office procedures provided a full explanation and pointed to lessons for the Home Office, including in the area of leadership. Expressions of public concern were then less vociferous than when sensitive data was lost. But the real point for public protection was that the information had not been shared and could not be acted upon.

71. Understandably, the response to data loss incidents across Government has been to introduce a range of measures aimed at preventing future occurrences: locking down data; new rules on transmission of data and how it may be stored; and encryption. This needed to be done. Of itself, however, it could militate against the effective sharing of criminality information between organisations. Even before the recent spate of data loss incidents, the climate was not conducive to sharing information. There are few incentives and many disincentives. In some cases, there are individual legal penalties for inappropriate sharing of information, though I have found none for people who fail to share when they should have done.

72. The framework drawn up by the police, the Management of Police Information (MOPI), in 2006 is a good example of efforts to address this and implement a structure to facilitate the sharing of criminality information. MOPI was instigated following a Bichard recommendation to improve the handling of information by the Police. The Police have until 2010 when they are obliged to have fully implemented MOPI into their day-to-day management of criminality information.

DPA 1998

73. The principles of the DPA are clear and helpful in respect of sharing information for public protection. The DPA aims to ensure that information is processed fairly and lawfully and must meet a condition to be disclosed such as:

- The data subject has given his consent to the processing
- Processing for the administration of justice
- For the exercise of any function of the Crown, a Minister of the Crown or a Government Department

74. The DPA does provide a number of exemptions such as for the prevention or detection of crime (section 29). However one must be satisfied that the disclosure is specifically for that purpose.

75. However, the DPA rules and exemptions are not always well understood and often over-complicated by local rules, procedures and misconceptions. For example, the Department for Work and Pensions (DWP) currently share information with UKBA using their common law powers for the purpose of the prevention and detection of crime. There have been occasions where DWP has not provided the requested information though there is a memorandum of understanding between DWP and UKBA which covers disclosure of information for immigration offences.

The Purpose of Information on Criminality

76. Within the public protection network, criminality information is owned by each organisation and designed mainly for its specific purposes. There can be a lack of understanding from those entering data about its wider use and fundamental purpose – public protection. For many hard-pressed public servants – police officers, immigration officers or court staff for example – this is yet another form to be filled, yet another file to be created. In some cases, the accuracy of the data being collected – perhaps from an asylum seeker, or someone charged with a criminal offence – cannot be verified and the individual is reluctant to provide it. Filling out the form may appear an exercise with an unknown purpose in trying to elicit information which may be inaccurate in any case. For example, a custody officer may take information on an individual's nationality at face value; in part because of the difficulty of verification, but also because the information has only limited value at this stage of the criminal justice process (indeed, the PNC provides for up to three nationalities to be recorded). It is hardly surprising that information collection is not at the top of the officer's priority list. On the other hand, this information may prove critical to the management of an offender who has completed their sentence.

77. Across the PPN, people charged with capturing and recording information may not be clear as to the purpose and use to which the information is put – and the importance of ensuring it is accurate and available when required. In this, as in some other areas, leadership is crucial. All those who are charged with capturing information which may help to protect the public need to understand that is its purpose, and to be helped to make the exercise as easy and effective as possible.

Barriers to Sharing

78. Business processes are not designed with a view to sharing beyond an organisation's own priorities. Processes for appropriate sharing are sometimes unclear and inconsistent, and potential sharers need confidence and competence in information management. Sharing is not the most natural process for some front-line staff, who are focused on using and protecting the data they assemble for their own purposes. Where there is a lack of understanding about what shared data is being used for, this will inhibit willingness to share.

79. Even within organisations there are numerous criminality databases and there is limited sharing of information between the various databases – often because of technological issues rather than reluctance. A number of public protection organisations have a range of legacy systems within each area in their organisation. An example is the 43 England and Wales police forces which are estimated to hold over 70 million operational records between them, split across more than 350 systems.

Changing the Culture

80. So, the picture we find is:

- Criminality information across the PPN as a whole is often a low management priority – except in a crisis
- A presumption not to share information, in some cases for fear of criminal penalties for doing so
- Confusion about legal provisions
- A focus on information owned by a single organisation – or part of it – and designed for its specific purposes
- A lack of understanding from those entering data about its fundamental purpose – public protection

81. Changing the culture across the public protection network is not about introducing a new overarching database or implementing a cross-Whitehall process guide. It is necessarily about dealing with the network as a whole and addressing each of its facets in a coherent and consistent way. It involves adopting new processes, policies, practices and, necessarily, behaviours throughout organisations.

82. It is essential that the case for change is accepted wholeheartedly by those who will have to lead that most difficult of exercises – culture change. Many problems have occurred, and will continue to occur unless the culture is changed, so that criminality information is shared appropriately. For example, SANE, the mental health charity looked at 69 inquiries into killings by people in contact with mental health services reported between January 1996 and March 2001 and found that there had been a breakdown in communication between Health, Social Services and the Criminal Justice System in 90% of cases. The report stated that it was evident that vital information was not shared between professionals, carers, families and voluntary support agencies.

83. Recognition of the importance of appropriate sharing of good quality data to improve public protection must come from the top. But to embed a culture of sharing criminality information – when appropriate and with proper safeguards – it must be championed by leaders and managers at all levels within and across the organisations. Changing culture within an organisation is hard enough but achieving significant change in a range of organisations, each of which has its own strong culture, including different national cultures, is particularly challenging and will require the highest standards of leadership. There are already examples where staff are reluctant to co-operate even with the well-established and generally effective UK MAPPA arrangements.

84. The health sector is perhaps the most sensitive. Healthcare staff have an absolute duty of confidentiality to their patients. Yet, there may be occasions when absolute adherence to that duty may place individuals in particular or the public in general at unnecessary risk. We found one excellent example of leadership in this difficult area.

Case study – Cardiff Accident and Emergency

An initiative which started in Cardiff in the mid 1990's illustrates the challenges of changing the culture of organisations and the importance of leadership. Many victims of violence have to go to Accident and Emergency for medical treatment. A surgeon in Cardiff found that 75% of woundings that resulted in Accident and Emergency treatment did not appear in Police records. A data analyst combined anonymous information from Accident and Emergency with Police intelligence to provide regular summaries of hotspots for violence in Cardiff. The police and local authorities then targeted their interventions in these hotspots. Implementation of these measures was followed by an overall decrease of 35% in numbers of assault patients seeking Accident and Emergency treatment (2000-05), and a 31% decrease in assaults inside licensed premises in Cardiff city centre. Following the success and subsequent evaluations of the Cardiff pilot in 2004 and 2006, it began to be implemented by other CDRPs. The initiative is now being rolled out throughout the country and has been included as a key part of the Government's new Violent Crime Action Plan published in February 2008. The Plan recommends all CDRPs develop methods of sharing information from health services to help police and local authorities target resources more effectively.

85. This case study of leadership illustrates how someone who recognises the bigger picture of public protection can make a real difference. He had the confidence to tackle the status quo (without compromising confidentiality as he used anonymous data) and the authority and determination to bring colleagues on board, despite inevitable setbacks. Experience in trying to replicate the initiative illustrates the challenges that leaders have to overcome. There may be many other examples of leadership on sharing criminality information within and across organisations which are delivering real benefits to public protection. These need to be identified, recognised and their lessons applied more widely.

Impact on the Front-Line

86. Decisions about when it is appropriate and proportionate to share personal and, in the case of criminality information, highly sensitive information are often left by default to those at the front-line of our PPN – who may be ill equipped to make those decisions. This can be dangerous to them, the person they are dealing with and the protection of the public more generally.

Case study – Prisoner Escort Contractors

Though Prisoner Escort companies are seen by leaders in the Criminal Justice agencies as simply providing transport for suspects and offenders from A to B, they make critical day-to-day public protection decisions on how to handle them safely and effectively whilst in custody. Because their role in this process has not been properly recognised, they often do not have direct access to the information they need to do this job, so they have to rely on a circle of friendly contacts on the end of a phone to provide them with necessary information. Contractors at a magistrate's court the team visited regularly checked with police and prisons to determine whether individuals released by the court on one matter needed to be held on other matters. The manual checks were necessary because the information they received through formal mechanisms was not always sufficient; if these contractors had not made additional informal checks, offenders could have been released incorrectly.

87. Practical issues present themselves daily to front-line staff in a whole range of circumstances. For example, the police can still sometimes encounter reluctance from organisations to answer factual questions about their members of staff, with both sides taking different views about data protection requirements. Healthcare staff may have evidence suggesting that someone is a victim of domestic abuse but be uncertain about how disclosing information to the police would sit with their professional obligations of confidentiality. The unavoidable delay in seeking advice from more senior management may expose individuals to real danger. No code of guidance or training provisions can cover all eventualities. Those faced with requests for information need to be helped to understand the positive value of their co-operation as well as the all too obvious negative aspects and to have the confidence to make difficult judgements, often under pressure. They also need to have swift access to others who can help them with the most difficult judgements – and confidence that they will be backed if their judgements are reasonable even if the outcomes are not what was desired or intended.

Recommendations

- I see leadership as a most important aspect of improving the capture and sharing of criminality information in the interests of public protection. I believe the burden of leadership falls to individuals at all points in the network, from Ministers to those leading the front-line. An approach which saw Ministers working with leaders of the organisations involved proved most effective around criminal justice in 2003. It was necessary for successful outcomes to criminal justice to get alignment in achieving a set of objectives which transcended organisational boundaries. The establishment of the trilateral Office for Criminal Justice Reform (OCJR) at national level and LCJBs at local level helped the police, Crown Prosecution Service, the courts, probation, and the prisons to pioneer a new way of addressing the resolution of problems together. The success of this approach should be built on in the wider arena of public protection. I recommend:
    - Leaders at all levels within the PPN need to demonstrate awareness of the importance of information flows across the network and of managing them with their partners, so as to improve the capture of accurate data and ensure the appropriate sharing of criminality information in the interests of public protection **(recommendation 4)**
    - Leaders should make a statement of intent in this area, before December 2008 to ensure that at all levels of leadership there is:
        - Recognition of their accountability for the improvements in criminality information capture and sharing, by including this in their key objectives
        - Simple, straightforward communication to staff of the importance of accurate data capture and appropriate sharing of information (within the law) as fundamental to public protection **(recommendation 5)**
    - The importance of information management should be explicitly included in leadership training and development programmes such as the Police Strategic Command Course, the PSG framework and other equivalent programmes before September 2009 **(recommendation 6)**
    - Within one year of publication of this report, Leaders should also assess, with peer review, their provision of organisational training, guidance etc on criminality information for staff and commit to deliver:
        - The necessary tools, agreed protocols and processes so that staff may capture, share and use criminality information appropriately. (This links with other recommendations, particularly on Investment and At the Front Line)
        - Improved capacity and confidence of staff through training, guidance and sharing good practice **(recommendation 7)**







ACCIDENT AND EMERGENCY DEPARTMENT


CHAPTER 5: RISK AND RISK MANAGEMENT

88. Risk management is one of the key enablers to support the strategic direction proposed in earlier Chapters. The Review is concerned here with risk and risk management in one specific context: the risk of harm to the public, and to the people who protect them, when accurate information is not available to the right people at the time when they have to make decisions. Every organisation has to identify risks and decide which are to be accepted, how to manage them and how to mitigate the rest.

89. However, the concept of public protection is not well or widely understood. The public protection network involves a variety of organisations. For many, their responsibility to protect the public is integral to their central purpose but for others, it is less explicit. Data is largely owned by individual organisations. Risk identification and management tends to be undertaken within each organisation rather than across the public protection network and in practice is front-line operational rather than strategic in nature. As a result, unnecessary risks are taken, and their management is inefficient.

Corporate Risk Management

90. All organisations in the PPN now have corporate risk management processes. These are based on:

- "The Orange Book", Management of Risk – Principles and Concepts' issued by HM Treasury in 2004 which is used by central Government organisations; and
- "Worth the Risk" issued by the Audit Commission in 2001 which is used by police forces and other local government organisations

91. Their main purpose is to deal with threats to the operation, change plans and reputation of the organisation.

92. Typically risk management processes provide for:

- identification of a wide range of threats to the organisation's business plans which are then listed in a risk register and weighted according to likelihood and potential level of disruption
- assignment of risks with high weightings to an "owner" who is responsible for deciding on and overseeing action to deal with them, alerting colleagues and escalation to more senior management as required

93. The processes themselves are all very similar and are also widely used in the private sector. They are becoming more sophisticated and are increasingly used to escalate risks through organisations. In the private sector best practice corporate risk management focuses on business risk. But the focus for public protection organisations seems to be on risks to their internal processes and their reputation rather than on the business of public protection itself.

94. Both the Home Office and MoJ have mechanisms for identifying risks to public protection – predominantly financial and reputational in nature. Those sponsoring organisations such as NPIA, SOCA, Criminal Injuries Compensation Board and LCJBs, recognise that serious risks identified by these bodies should be included in their own departmental risk register. In practice, it is mainly financial and reputational risks that are handled in this way. A Home Office Directors' risk group meets monthly chaired by a Home Office Director General and with representatives of NPIA, CRB and OCJR. However, the group was not created to deal with strategic public protection risks and is primarily concerned with near-term reputational threats. This group decides which risks need discussion at the Home Office Board or to be brought to the attention of Ministers. It has also taken action in relation to some risks – as when business planning in the Home Office showed that there was an increased risk of it trying to do too much with the resources available and action to reduce the level of risk was taken.

95. Alongside corporate risk management, many front-line professionals – police, probation officers, prison officers, health professionals, social workers and the security services – carry out sophisticated risk assessments of individuals (eg sex offenders), and of specific situations (eg children in homes with health risks). These assessments are standardised to enable safe, consistent decisions to be made. Most of the techniques used are based on past evidence and experience. All take account of criminality information available to the professionals involved and have a clear focus on public protection. However, weaknesses in these risk assessments – including information gaps and deficiencies – are not always, as a matter of course, fed into corporate risk management processes.

Collaboration

96. A good example of effective multi-agency working and information sharing is the Multi-Agency Public Protection Arrangements (MAPPA) involving police, probation service, and prison service. Their purpose is to protect the public from violent and sexual offenders who have been convicted of one or more specified offences and are now in the community. Exploratory discussions are underway about whether to include the UK Borders Agency.

MAPPA Case Study

MAPPA arrangements were introduced in 2001 and operate throughout England and Wales in 42 areas. Central guidance issued by the National Offender Management Service explains how the agencies are to work together to assess and manage risks and also addresses data sharing and data protection. It is supplemented by specific guidance for the each of the three services which form the "Responsible Authority" in each area: police, probation and prison service.

As they come into the community, each offender has a risk assessment made by one of the three services. A risk management plan (involving all the necessary services) is prepared for each individual identified as falling within one of the MAPPA categories. The plan is agreed by the Responsible Authority and implemented. Other agencies (health, education, housing, etc) have a statutory duty to share information and co-operate in this process.

Cases of the most serious re-offending by offenders subject to supervision under MAPPA are now subject to serious case reviews. If those reviews throw up any wider and national learning, the NOMS PPU will ensure the learning is disseminated.

The Strategic Management Board in each area reviews the operation of MAPPA annually and develops plans to improve the arrangements. The continuous improvement cycle - learning from experience of previous cases and improving arrangements – is a key feature of MAPPA.

97. The MAPPA arrangements are unusual in that:

- their focus is on specific risks to public protection
- they involve multi-agency collaboration
- organisations that would not immediately appear to be part of the public protection network are involved – and have a statutory duty to share information;

98. The MAPPA arrangements are not a panacea and have resource implications but nevertheless offer lessons for collaboration in the interests of public protection

99. Elsewhere, the lack of collaboration and information sharing creates avoidable risks for public protection. For instance, many public protection organisations keep "watch-lists" – for very good reasons – but there is no concept that these lists should operate in an integrated and complementary way. Significant risks can arise from failure to contribute to specific lists, and to check against the right lists at appropriate points. We have identified some examples where specific risks could occur and have informed the Heads of the relevant agencies and services so that swift action can be taken to mitigate these risks. I am confident that these risks will be closed as a result. The Home Office CIO has identified a total of 77 watch-lists, some of which are consolidations of other subsidiary watch-lists, which suggests that the lack of an integrated approach is

inefficient as well as unhelpful in minimising risk. The CIO is undertaking further work to assess the relevant risks and consider whether there is scope to consolidate the number of watch-lists and improve the efficiency with which they are used in support of public protection.

100. Risks – except those that have far-reaching reputational consequences – are not generally discussed between organisations. In part that is because if the risks became widely known, they could be exploited by criminals. There are not always established arrangements for drawing risks together and sharing them and so front-line organisations do not have a clear picture of the mechanisms that exist to escalate risks through the Public Protection Network.

Acceptable Risk

101. As risk management in the public protection network does not generally address the issue of public protection itself, organisations are not accustomed to determining what level of risk is acceptable despite the fact that, in practice, their decisions about priorities and funding determine what risks society will have to live with. Front-line managers use risk-based assessment for incident management, and in other well-defined circumstances such as admitting offenders to prison. However, risk management does not feature in setting priorities, developing business plans or strategic decision-making. Risk management is a "process" rather than a criterion for prioritising and managing. A "zero tolerance" approach to risk in public protection is not practical, desirable (on the ground of personal freedoms), nor affordable. Determining what level and type of risk is "acceptable" is therefore an important responsibility of decision makers across the public protection network. This responsibility is not always recognised.

102. One example is the implementation of the recommendations made by Sir Michael Bichard in June 2004. His recommendations were accepted in full by the Government but, after four years, 9 of his 31 recommendations have yet to be implemented. One of the outstanding recommendations- the urgent introduction of a national IT system for England and Wales to support police intelligence- is still under development. While some interim measures such as the Interim Police Local Exchange (which supports CRB disclosure) have been put in place, the delay in full implementation means that we are still living with at least some of the risks. Ministers believe they have taken action to remove the risk by accepting the recommendation and launching the programme to implement it. Furthermore, front-line police officers see little or no tangible action and may conclude therefore that this cannot be a priority.

103. Public protection is a complex business. Action taken in one part of the network can cause unexpected consequences in another. The acceptability or otherwise of these risks is not determined. They are not even anticipated. For example, in sentencing, the courts try to ensure that drug addicts will spend sufficient time in prison to undergo detoxification. Detoxification takes 14 days. On release, prisoners are given a discharge grant to fund their immediate accommodation and other needs. However, because

of prison overcrowding, such prisoners may now be released into the community after only 7 days, on licence with a discharge grant. So, sentencing specifically aimed at reducing the risk of re-offending by allowing time for detoxification and public funding intended to prevent recourse to crime in order to subsist instead can result in the state funding the drug habits of convicted addicts. Each of the individual decisions taken by different organisations in the public protection network – length of sentences for addicts, early release for lesser offenders, and limited financial support for prisoners on release – makes perfect sense but their combined effect is far from helpful.

104. Industries that provide critical services to the public are familiar with the concept of acceptable risk. They identify the specific types of risk that critically affect them – continuity of supply in electricity and gas; safety in the nuclear power industry – and make explicit decisions about the level of risk that is acceptable to their business. For the PPN this would mean organisations specifically addressing public protection risks, so as to help managers to think beyond immediate threat to smooth operation and reputation and, to focus on systemic weaknesses in their business operations. The CRB have already made good progress in this direction by distinguishing between operational risks and the risks to their strategic business plan.

Challenges

105. Directors in the UKBA and OCJR told us that at a managerial level risk management is often seen as a set of administrative processes, which are not very useful. Surveys in the Home Office and some of their satellite bodies – in common with other parts of Government – suggest that this view is widespread.

106. Public protection risks are clearest at the front-line, whereas the means to address them often lie in the business planning processes of their own or other organisations. The implications of prioritising and funding decisions for risk to public protection as a whole – not merely reputational and not confined to the remit of one organisation – must be given explicit consideration. The experience of those who manage at the front-line should be used to help identify public protection risks and bring them to the attention of policy-makers and those who determine where investment is to be directed. This is a significant change in attitude to risk and will require strong leadership within organisations and across the whole network of organisations involved in public protection. A "map" of the Public Protection Network will give leaders an overall context for identifying risk and determining priorities: As a number of managers said to me; "It is very difficult to think about whether the system is working properly when you aren't sure what it is and who is in it".

107. Cost is always a factor in implementing the recommendations of a Review such as this. Making better connections within and between organisations in order to minimise risk to public protection is bound to incur some cost. In my view this is so fundamental to the responsibilities of public protection organisations that the necessary costs must be met. But I would also argue that better risk management will be cost effective.

Knowledge that a newly admitted prisoner is dangerous – to himself or others – is used to prevent problems that are costly to investigate and resolve and may also have tragic consequences. Co-ordinated pre-release programmes minimise the risk of re-offending which benefits the public purse as well as public protection. Stopping criminals from entering the UK is much cheaper than tracking them down after they have done so. The recommendations that follow are made with an eye to cost-effectiveness as well as to minimising risk to public protection.

Recommendations

- Those responsible for strategy, business planning and risk management within each department or organisation belonging to the PPN should give explicit consideration to the potential impact of their decisions on risks to public protection as a whole. (This links to the Governance recommendation as the proposed Commission should have an oversight role on PPN risks and be provided with organisations' risk registers) **(recommendation 8)**

- Each agency within the PPN should institute by January 2009 a regular mechanism to enable escalation of significant front line risks to public protection. These processes and their outcomes should be reported in department / agency annual reports, and the risks in them should be considered and managed alongside corporate risks **(recommendation 9)**

- The Home Office and, where necessary, the Ministerial Group should facilitate mechanisms to encourage senior managers to share their analysis and assessment of public protection risks and vulnerabilities, and proposed action, with other organisations. This should enable joint action to be organised where appropriate **(recommendation 10)**

- The concept of the PPN brings a new dimension to the need to assess risk. The Ministerial Group should ensure that an assessment of the effectiveness of risk identification and management is included in the inspection framework of public protection organisations **(recommendation 11)**

- Agency heads, as part of the action under Leadership recommendations, should ensure that adequate training in risk assessment and management as it applies to interchange all criminality information should be provided for managers at all levels **(recommendation 12)**









CHAPTER 6: INVESTMENT

108. Investment, like risk management, is another key enabler to achieving the proposed improvement agenda. My concerns with investment focus on the financial resources invested in processes, databases and systems for sharing and accessing criminality information. Generally, priorities for investment are determined within individual organisations rather than across the Public Protection Network.

109. I have looked at how funding is allocated and the decision-making processes for carrying through investment programmes and projects. I have also looked at the speed with which investment decisions are turned into practical tools for action in the public protection context.

Investing in corporate priorities

110. Funding is allocated to organisations with responsibilities for providing public protection – or providing facilities and services to those bodies – from Central Government votes and grants and from council tax allocations.

111. At national level, individual Government Departments, Services and Agencies decide how best to divide their funding between operating costs and investment priorities (with reference to their own business strategy, plans and expected funding). Locally, Police Authorities and, in future, Probation Trusts will make their own decisions about how funding is best divided between current services and new capabilities. In deciding their priorities, national and local bodies take account of priorities set out in Government strategy, objectives in PSAs and expectations set by governance machinery such as the National Policing Board and the National Crime Reduction Board.

112. There are constraints on national organisations' freedom to proceed with investment programmes. Both the Home Office and MoJ operate investment approval boards for high-cost investments. The UKBA and NPIA have similar bodies. All these carry out checks to ensure that developed investment proposals are sound and are aligned with strategic priorities. The focus is on whether each case for investment is strong in itself. This can mean that investments which would be of wider benefit to public protection, but do not necessarily benefit the main funding organisation, have problems getting approval. E-Borders is a good example of such a programme as the main benefits are to the police and counter-terrorism operations – not necessarily to UKBA who lead. However the investment board recognised the wider benefits of the programme to public protection and agreed funding. The e- borders pilot is proving its worth and has already led to over 1300 arrests.

113. The overall level of funding available to organisations concerned with public protection has grown significantly in the past 10 years, and this has been accompanied by an increase in investment in databases and IT systems. Departments and their Non Departmental Public Bodies (NDPBs) and agencies have invested to solve particular

problems with the result that there are many – perhaps too many – IT systems developed independently which then need to be connected together, or to exchange data. For example, the IT systems involved in the Joint Border Operations Centre (which will become e-BOC in July 2008) do not "talk" to each other making the automated transfer of information from one to another difficult. This is resolved in unsatisfactory fashion by staff having two or more PCs on their desk. Contracts have been put in place by the Home Office to develop and implement e-Borders; suppliers are in the process of developing a more integrated IT system to overcome this issue. And in the Risk and Risk Management Chapter of this report, attention is drawn to the proliferation of watch-lists which, for example, e-Borders is having to deal with, to have available a comprehensive database of wanted people to use for border enforcement. As e-Borders moves forward, a more rigorous approach to information management will be developed, involving a degree of cleansing of watch-lists to make them more manageable. This complexity increases costs and makes it difficult for operational staff to know what information and data is available and how to get it.

Investment Decisions do not Reflect Public Protection Priorities

114. We have found that it is problematic for organisations involved in public protection to align their investment plans with others and to see where they have similar priorities which would benefit from joint investment. This is because there is no map of the landscape, or overall strategy, to support public protection which shows where investment is, and should be, targeted to improve criminality information. There isn't even a comprehensive "map" of the existing infrastructure: though the NPIA have a useful starting point in their diagram of England and Wales Policing Systems & Information Flows. It is not surprising therefore that investment decisions do not generally reflect public protection priorities.

115. This Review has undertaken some mapping work which will help to clarify the landscape (see Annex C) and the CIOs of the various organisations are also building a comprehensive picture of the information flows in place, and the IT systems which support them, across the Public Protection Network.

116. In addition, while there are bodies that deal with large parts of the system including the National Crime Reduction Board (though this doesn't become involved in investment issues) and National Criminal Justice Board there is no single organisation with the authority to develop or broker a set of Public Protection Network investment priorities. And there is no machinery to give effect to them which means that there are few incentives for organisations to work together on investment priorities, to design complementary processes and to invest in facilities to make them work.

Delays in Programmes with a Significant IT Element

117. The approaches that have been taken to the implementation and enhancement of national programmes have resulted in long delivery timescales during which frontline staff have had to cope with information gaps and deficiencies and poor tools for accessing information that should be available to them. While we acknowledge that some interim solutions – both technical (IMPACT Nominal Index, INI) and clerical (court reporting) – have been put in place, the major programmes, for example to deliver solutions to the Bichard recommendations, are still not delivered (as detailed in the Technology Chapter).

Suppliers Need to Understand Wider Priorities

118. Because investments are cost-justified on their individual merits, and suppliers do not understand the wider public protection priorities, the technology is not developed in a way that helps with linking different IT systems together. Linking systems into PNC is a good example of this: in the past, interfaces between PNC and others needed to be individually engineered: only now is a technological means of interfacing systems in a more universal way (using web services) being implemented. And though national standards which will make police systems easier to connect together were issued in 2006, the target date for police forces to have plans for implementing them is not until 2009. A more cost-effective approach would include the capacity for timely information exchange in the original design.

119. There is no generally accepted way of dealing with the issue of how best to share and link together data for public protection purposes: for instance, whether to hold datasets in a national database for use by all, or whether to keep data local where it is collected and have tools for searching across local systems. As a result, there is a mixed picture of some data on national databases, some on local databases which are incompatible with each other, while other data is held on such old technology that it cannot be integrated with any other systems / data (eg UKBA casework). Other public services have faced this difficulty and have found different ways of tackling it. For example, in education the data needed nationally and the functions required locally have been clearly defined – for local authorities, schools and suppliers. The local organisations acquire whatever systems they wish – as long as they can provide data to national systems and have the necessary facilities for local services. Some similar combination of overall strategy and defined connections between systems would improve information flows in public protection.

120. I make a recommendation about better engagement with suppliers at the end of the Technology Chapter as this is the area of investment where the greatest benefits and savings may lie.

Challenges

121. Over the next three years, and probably beyond, reduced levels of funding will make it impossible to sustain the current rate of investment, and by implication, make it increasingly important to direct the available investment at the highest priorities, and ensure that any IT systems that are built will work well together to improve public protection. But the tight fiscal climate will also make it harder for individual organisations to divert resources from their own organisational priorities to those that cross organisational boundaries. It will therefore be challenging to change funding priorities. Indeed, many organisations are already facing very difficult choices about which programmes to fund and which to scale back.

122. There are nevertheless examples elsewhere of getting "system wide" investment to work better – and at the same time stop investment happening in an unco-ordinated way: in the criminal justice system (Criminal Justice Information Technology, CJIT), in Youth Justice and in education (as mentioned earlier). In the case of CJIT, the investment budget was initially centralised, though, from this year, more has been devolved to LCJBs. In youth justice, very modest investment has been used to make significant incremental improvements in getting critical information to move with the young offender across organisations at the right speed. In the present financial climate, the youth justice approach, or that adopted in education, could be useful across the Public Protection Network.

123. There is likely to be some resistance to taking more account of wider public protection priorities when making investment decisions, because most organisations in the public protection field view dependence on others to meet their information needs as adding to the risk that they won't get what they want in a reliable and acceptable timescale. Strong leadership will be required to change this view and build confidence.

Recommendations

- Investment Boards in the various public protection organisations should always take account of wider public protection priorities in making funding decisions. I am encouraged by work being done to create an assessment process at inception for new projects and programmes, particularly where there is a substantial IT component. I recommend that the consideration of wider public protection benefit is embedded in that process **(recommendation 13)**

- The Implementation Team should facilitate mechanisms to ensure better joined up investment across the PPN. This should include unblocking problems quickly to prevent delays in implementing solutions to improve the flow of criminality information **(recommendation 14)**







ACCIDENT AND EMERGENCY DEPARTMENT


CHAPTER 7: THE INTERNATIONAL DIMENSION

124. This Review came about as a result of the handling of notifications of convictions imposed by other European countries on UK citizens. As we found, there are many difficulties surrounding the collection and sharing of criminality information within the UK. The international issues bring further complication. However, our focus is on the difficulties involved in exchanging criminality information across borders and frontiers.

125. The world is increasingly interconnected and one of the negative impacts of this is an increase in crime across borders. The internet plays a part in this, as does the advent of cheaper flights and direct travel links via improved rail and road networks which mean that people travel more than ever before. Large numbers of people are taking up their right to live and work in this country and many UK nationals are increasingly spending periods of time abroad.

126. But this flow of people is not always accompanied by a flow of information about criminal activities in different countries. We often know little about the criminal convictions of people who are foreign nationals or UK citizens who have spent time abroad – as the work we have undertaken on "vetting and barring" has shown (see separate Chapter At the Front-Line).

Current International Data Sharing

127. There is no clear UK strategy for sharing international information on criminality which sets out what we want to achieve, or our preferred routes for doing so. The public protection organisations within the UK need to be clear on what we require from international criminality information exchange as part of a wider strategy on public protection.

128. There are numerous mechanisms in place by which countries share criminality information across the world. The UK participates in some arrangements with groups of countries: for example, the EU or the "Four Countries Conference" – our partners there being the USA, Canada and Australia. Another example is the UK's involvement in a pilot scheme with a growing number of EU countries to enable electronic exchange of criminal records data. The pilot was started between Germany, Spain, Belgium and France in 2005 and UK joined in 2007. It aims to create an interface linking the criminal records systems in each individual state, but with full regard to issues around the protection and security of personal data. We also have bilateral arrangements with a number of countries. Some of these, such as the USA, are at the national level and others are at a more local level, for example Hampshire police with the French police. The UK also participates in arrangements which encompass the wider world, for example Interpol.

129. Although some of the arrangements are bound by EU legislation (for example, the 2006 framework decision for electronic exchange of criminal records), others are determined by Service Level agreements. This results in a complex picture of data sharing mechanisms for which no clear governance structure exists. (The maps in Annex C illustrate the complexity. Definitions of each of the current mechanisms can be found in Annex D.)

130. The existence of so many different mechanisms and initiatives means that the transmission of information is inefficient; the same criminality information may be sent several times. During the work that was done to clear the backlog of notifications of overseas convictions of UK citizens it became apparent that information about these convictions was being sent to the UK using arrangements established under the relevant Council of Europe Convention, using Interpol facilities, with the intervention of the FCO and also through direct communication between police staff in the sending country and the UK. Many convictions were not transmitted at all, but others found their way to the UK down more than one of these routes.

UK Participation

131. The evidence we have collected suggests that, for a variety of reasons, which we explore below, the UK does not make best use of the international mechanisms available.

132. We know less about foreign nationals, or UK nationals who have spent time abroad, and so more information needs to be shared between countries. However, the number of combined requests to Interpol and the UK Central Authority for the Exchange of Criminal Records (UKCA-ECR) is very low. For example, in the first two months of 2008, an average of 7 requests per day were received by UKCA-ECR from UK police forces for conviction information relating to EU nationals, and Interpol estimate that they receive on average just over 20 requests a day (8000 per year) for conviction information about foreign nationals from outside of the EU. It is worth noting, however, that through both the implementation of the electronic pilot for record exchange and the continued efforts of the UKCA-ECR's communication strategy, in particular their work with the Cambridgeshire force, the volume of notifications and requests handled by the UKCA-ECR is anticipated to increase dramatically.

133. The Interpol Secretary General has claimed that the UK is not making use of his agency's list of 11,000 terror suspects and the UKBA does not yet have a link to Interpol's Lost and Stolen Documents database whereas France makes approximately 7.4 million checks on it per year. However, progress has been made to establish this link which should allow automatic download of the Interpol data by the end of 2008. Other organisations should follow the example of UKBA and make better links to Interpol.

134. The UK is currently unable to access alerts on data from across the EU for wanted and missing persons, stolen and missing property, or European arrest warrants. While we will gain access when we join the second phase of the Schengen Information System, this will not be until 2010 at the earliest. But being a partial member of the Schengen agreement, means that we will still be unable to access the EU immigration data provided and accessed by other Member States. From the perspective of public protection, this is unsatisfactory.

135. The UK does not have a very good reputation in the EU in terms of responding to requests for information from other countries. This results in an understandable reluctance on the part of other countries to co-operate as efficiently and effectively as they might with

the UK. For example, when a UK official attended a bilateral with the Belgian Central Authority recently they were told "if I received a request from the UK and a request from France at the same time, I would prioritise the French request as the UK take a long time to respond to requests". One factual example illustrates the point. A Belgian magistrate enquired about a Belgian national arrested in the UK. A request was made to the UK via Interpol for some information from a police force outside London. It took six months before this information was sent back to Belgium. Some time later an urgent request was made to Belgium via Interpol from the Metropolitan police about a high level crime. Belgium were reluctant to action the request urgently given their previous experience.

Confusion on the Front-Line

136. I have found that front-line staff involved in public protection often lack awareness and understanding about international exchange of criminality information. This is perhaps not surprising considering the many and complex arrangements available. However, many police officers simply do not know what is available. For example, some of the officers the team spoke to had not heard of UKCA-ECR. Or if they have heard of the various bodies, they do not know enough about them to feel comfortable exchanging information.

137. Ad-hoc decisions are sometimes made that can result in data being treated in an insecure and inefficient manner, instead of using established arrangements, or formal treaties and conventions. For example, in January 2007, Dutch investigative authorities sent CPS a disc containing a large number of crime scene DNA profiles from unsolved crimes. From the Inquiry into this incident, which was published by the Attorney General in May 2008, it is clear that the package was not addressed to a specific person or section within the CPS, nor was the operational purpose for the disc explained clearly. The lack of protocols surrounding the arrangement meant there was no standard procedure in place at CPS for dealing with receipt of the information. As a result, and in combination with the lack of an urgent approach from CPS staff, the data was not sent to the police for the process of matching the crime profiles against the national database until a year after it had been intially received in the UK. Established channels for sharing information offer more reassurance that data is exchanged in a secure manner, with a clarity of purpose, and international data protection principles are adhered to.

138. There is no international element in core police training. And it is not only junior officers who lack the necessary knowledge. Unless senior police officers have had experience of international data sharing, usually through involvement in a particular operation, they are also unsure what is available and how to make best use of it. A superintendent we spoke to admitted "I don't know the difference between Europol and Eurojust". And a Chief Constable recently said it would be good if the UK could undertake cross-border surveillance in the EU – something which is already possible via Europol.

139. There is no single source of information on international data exchange for front-line officers in the UK – unlike in France where there is a central hub which directs officers' requests to the correct organisation.

140. There is even confusion around the respective roles of the UK – based centres facilitating the exchange of criminality information. UK Central Authority for Mutual Legal Assistance (UKCA-MLA) is in the Home Office. Scotland has a separate Central Authority and HM Revenue & Customs is a Central Authority in relation to certain matters. UKCA-MLA processes requests from overseas for legal assistance in obtaining evidence or the service of summons and judgements within the United Kingdom and it transmits requests from the United Kingdom for evidence to be obtained overseas. However, this unit is often confused by other countries with the UKCA-ECR, which receives notifications of UK nationals in other EU Member States and notifies relevant EU Member States of any convictions of EU nationals in the UK. Since the launch of the UKCA-ECR in 2006, UKCA-MLA estimates that is has received over 200 notifications of UK nationals convicted in European countries by post, which it has then had to forward on to the UKCA-ECR in Hampshire.

Examples of Good Practice

141. However, once awareness of the various organisations' roles and responsibilities is raised, then the existing mechanisms have been used to good effect. For example, the Scottish Crime and Drug Enforcement Agency (SCDEA) have said that they were initially nervous about using Europol for data security reasons, but as they used it more and more they have gained such confidence that they have seconded a member of staff there. Using Europol, SCDEA identified a common theme in the marketing of ecstasy which enabled them to link back to the source of supply.

142. As mentioned earlier, the Cambridgeshire police force has been working closely with UKCA-ECR. They are now running UKCA checks on all non – UK EU Nationals arrested and are finding them a useful source of criminality information. For example, they recently stopped a man for erratic driving who then attacked the arresting officer. On carrying out a UKCA check, they discovered that he had served 14 years for murder in Poland, was on his second 6 – year driving ban, and was wanted in connection with another violent crime in Poland.

Case study – Child Exploitation and Online Protection Centre (CEOP)

143. CEOP works against UK nationals who travel either to avoid the offender management system within the UK or to abuse children. CEOP shares intelligence and information on these high risk individuals with international law enforcement through tried and tested channels – in addition, CEOP works to build relations with law enforcement counterparts and officials internationally. Examples of the successes that can be achieved when information is shared across international boundaries building on good working relationships include: a high risk paedophile had absconded from prison in France and had been missing for several years. CEOP had previously worked with the French authorities to try to locate him but without success. The offender was placed on the Most Wanted website and within a short period of time, had been identified in France. Within 24 hours of the tip – off, he had been arrested by French police and was subsequently brought back to the UK.

A More Proactive Approach is Needed

144. The UK should look ahead to where trends in criminal activity suggest future threats lie – taking a proactive, risk based, approach in setting up any new arrangements necessary with countries with whom we do not currently exchange criminality information. To date countries have tended to react to incidents and only seek to agree data sharing after the event. But this leaves us unprepared to deal with the increasing tide of criminal activity across borders.

145. This approach is already being taken by some organisations within the public protection network. For example, the CRB is to undertake an overseas vetting pilot for which countries have been identified using a risk – based approach. Analysis of disclosure applications received by the CRB over a 12 – month period showed that the applications where an overseas address had been given were mainly from the Republic of Ireland, Poland, France and Australia. CRB has approached these countries to take part in a pilot exercise.

Earlier Consideration of Costs and Benefits would Lead to Smoother Implementation of New Legislation

146. The implications of signing up to EU legislation for UK front-line staff are not always considered in full until after the decision on whether to participate has been made. It is in my view especially important to engage delivery organisations at an early stage in the policy formulation process – not only to ensure that emerging policy is built on sound operational foundations and practicability, but also to allow realistic estimates to be made about implementation, time and cost.

Case Study on Prüm Treaty

147. The Prüm treaty is an agreement between certain EU States which will enable signatories to access DNA and fingerprint databases, plus vehicle registration data, across the EU to help fight serious crime. Germany and Austria are already exchanging DNA information as a pilot arrangement in advance of the Prüm Treaty being formally implemented. In the first two months of this arrangement, German searches of Austria's DNA database turned up 1510 matches or "hits" (enabling a request for further information to be made),with the Austrian authorities able to connect 710 open criminal cases in Germany with known suspects. The hits in the Austrian database were made in connection with 14 homicides, 885 thefts and 85 robberies or cases of extortion.

148. This demonstrates the potential benefits to the UK when Prüm is implemented here in 2010. Great effort was put into ensuring policy makers, technical experts and negotiators engaged effectively before the UK signalled its agreement to the Council Decision, with cross-Whitehall Ministerial clearance secured from all departments in advance of the final decision. However, it was not agreed at the time where the budget would come from to implement the initiative, nor was it agreed between delivery bodies and policy makers who would take ownership once negotiations were complete.

149. Although the delivery agencies that are fundamental to the delivery of this initiative seem to recognise the practical benefits that it can provide, difficulties are now arising on implementation as a result of the failure to identify the funding sources.

Prioritising and Resourcing International Work

150. International work is not seen as a high priority for the front-line officer. Not only is there a lack of training but the absence of performance indicators and targets on international work in the police performance framework also suggests it is low on the list of priorities. None of the 27 standard custody forms include requesting international information – individual forces have to devise their own forms for this purpose.

151. Further, increased volumes and complexity of international work have not been matched by increased resources. For example, the number of evidential requests coming into the UKCA-MLA has almost doubled in the last seven years: In 2000, 1288 evidential requests were received from EU member states. In 2007, 2572 requests were received. As a result the response time from the UK is increasing. I understand that restructuring and changes to the funding base are underway to enable more efficient responses to be made, but this area may need more attention as workloads continue to grow.

152. Closer to home, improvements are also required on data sharing within the UK – between England and Wales, Scotland and Northern Ireland – and between the UK and the Crown Dependencies. For example, there are still only limited links between

PNC and Northern Ireland police information. This means that only information relating to sex offences and some other very serious offences in Northern Ireland is currently put on to PNC (although PSNI have access to PNC for their purposes). Essentially, it has been unclear who is going to pay for a more comprehensive link. I welcome the fact that a feasibility study has just been conducted by NPIA and (as recommended in the Technology Chapter) by the time I revisit these issues in early 2009, I expect this issue to have been resolved.

153. Another example is that employers based in Jersey, Guernsey and the Isle of Man are not covered by the CRB regime for vetting prospective staff. They have to rely on such applicants exercising their rights to obtain details of their own criminal records from the police and passing those records on.

International Differences

154. Experience of dealing with overseas convictions highlights the different standards which apply to criminality information in different countries – in terms of data quality and completeness, definitions of offences etc. This all adds to the confusion staff face when dealing with international criminality information.

155. The Overseas Crime Taskforce (which was set up by the Home Office to address the backlog of UK citizens' overseas convictions not recorded on the PNC) identified difficulties in translating / recording notifications of convictions from abroad for the following reasons:

- A number of countries use offence terminology which is difficult for translators to interpret and define. Examples include the varied interpretation of the word "coercion", the offence of "Intentional Manslaughter" and particularly the German offence of "Total Intoxication". This does not equate to drunken behaviour and refers to circumstances where the actual offence committed is not specified and cannot be determined due to the level of intoxication of the offender
- Convictions notified from some countries may refer to the country's foreign penal code only and do not actually specify the offence, and so time has to be taken to research the country's penal code to discover what the actual offence was, to correlate it to our own systems
- Translation of foreign offence details: Abbreviated terms and offence details, together with foreign "slang" require a level of interpretation from the translator. The degree of accuracy in such a translation is inevitably uncertain

156. The roles of key players are often different in other countries. For example, in many European countries, the police have to refer to the judiciary to conduct the investigation into the offence whereas in England & Wales the police carry out the investigation.

157. The law differs from country to country which means that sometimes behaviour in a foreign country might be a crime there, but would not be in the UK. Commonplace examples include: in Germany, sunbathing in a public park is a criminal activity; the

penalty for entering or bathing in a fountain in Italy is a heavy fine; and, it is illegal to make rude gestures or swear in public in Bahrain, the UAE (United Arab Emirates) and Kenya.

Recommendations

158. There is much to be gained from a concerted effort to improve the flow of information between the UK and other countries, both within the EU / EEA and beyond. But this will not be a simple or a quick task, given the complexity of the current position and the number of potential countries and initiatives involved. Recognising this complexity and the scale of the task, I recommend the following:

- The Home Office led Implementation Team should support Ministers in developing by January 2009 an agreed approach for the UK on international exchange of criminality information. This agreed approach should cover:
  - Priorities for expanding agreed information flows with other countries, based on a more proactive, risk based approach to identifying the countries with which it needs to exchange data. Vetting and barring should be a priority area
  - A plan to rationalise the number of channels for international criminality information to flow in and out of the UK, improve any timeliness issues, and increasing staff awareness of the UK's obligations and the opportunities available to it
  - A plan to provide training and guidance explicitly covering international issues for staff across the public protection network
  - The development of options for the future structure and governance of international criminality information exchange **(recommendation 15)**
- Police forces, individually and collectively, and other PPN organisations should nominate a lead official for international criminality information issues (links to Governance and Delivery Chapter) and the resulting network should be maintained by the Implementation Team **(recommendation 16)**
- The Implementation Team should ensure that all international proposals on the management of criminality information, whether from the UK or elsewhere, are evaluated by a combination of international experts, senior policy makers with an interest and those key delivery organisations who would be affected or required to put them into effect. The agreed position should be re-visited periodically, as negotiations progress **(recommendation 17)**
- Subject to reaching agreement with Jersey, Guernsey and the Isle of Man, the earliest opportunity should be taken to bring them within the CRB regime **(recommendation 18)**

159. Successful implementation of these recommendations, and the subsequent benefits to public protection in the UK, will require an increase in the priority of, and dedicated resources allocated to, international work – including within the Implementation Team to bring a focus to the International response.









CHAPTER 8: TECHNOLOGY

160. Whenever people discuss information, technology seems to be an assumed part of the conversation. While I believe that the technology is an important enabler, it must be driven by the needs of the business and it forms a significant, but certainly not the main, part of the changes needed to deliver the benefits of better criminality information management. Criminality information cannot be dependent on IT delivery. IT should be an enabler rather than a dependency. My focus is on what is needed to ensure that IT moves in the right direction, rather than trying to fix existing IT programmes.

161. A key tension in many environments is the business demand for expediency and priority for functional delivery over the "greater good" of the whole. This is reflected in the approach to IT as it is used in the public protection network. Sometimes IT is too narrowly business driven, and the businesses fail to think about the broader landscape in which they operate. Resolving this tension requires the businesses to accept and govern adherence to standards. CIOs are already aware of this, but other business leaders need to recognise the issues as well. My proposals on risk management and investment should help to bridge the gap. However, Board level awareness of the application potential of IT is not always evident.

Major Programmes

162. In the field of criminality information, experience suggests that big IT programmes are not necessarily the answer. Some projects and programmes have been delivered to time and to budget, such as the Crown Prosecution Service's case management system and the Scottish Intelligence Database. But many others – for example, NSPIS Case Preparation, Libra, Impact, and C-NOMIS – have had their troubles with delays, funding problems, cost overruns and delivering fewer business benefits than originally envisaged. These problems arise in part from the scale of the programmes themselves. Furthermore continuity of accountability has not always been a feature of these and other major government programmes. Frequent changes of senior responsible ownership are not desirable and have happened too often for comfort in these and other areas. And changing business priorities contribute to the difficulties. For example, the Libra contract was signed in 1998, before the unification of crown and magistrates' courts; and before the largely successful attempt to get criminal justice organisations to enter into more active partnership with one another. Partnership between business and IT, including suppliers, is the key to success, avoiding the potential for confusion between the business owners and those delivering the technology. Libra is an example of a programme that has re-established clear business ownership.

163. But more is required. As I have pointed out, the landscape of criminality information is heavily populated, and so some collaboration between the many different players, with an eye to the needs of the public protection network, is essential. The NPIA – which is currently carrying out a review of ICT – and the Home Office CIO have a pivotal role to play. At the time of writing, it is unclear whether there is to be one or several focal points for IT within the Ministry of Justice. The MoJ, however, with its responsibilities for

prisons, probation, courts, and criminal justice IT, have a big part to play in helping to resolve issues which stretch beyond the Department itself in the context of criminality information.

164. It is a matter of particular concern that those programmes which arose from the Bichard Report have not yet been fully delivered. The electronic transmission of Magistrates' Courts results on to the Police National Computer is one example. The solution depends on Libra, which as well as having its own difficulties was not designed to send results to the PNC. There is some encouragement from the fact that three court areas will be testing the technology which has now been developed to enable the transfer of data from August 2008. However, the delays to the roll-out of Libra have inevitably impacted on implementation of this important Bichard recommendation.

165. The second example is IMPACT, which includes the electronic sharing of police intelligence, the first phase of which is not due to be nationally available until 2011, though a partial interim solution is in place. A third area, improving information about criminal records where the information is held overseas, seems not to have progressed very quickly despite the efforts of the CRB (see Vetting and Barring section). All of these taken together suggest that some of the recommendations in the Bichard report most likely to have an impact on public protection have yet to be fully delivered.

Criminal Justice IT

166. There has been a significant (£2bn) investment in criminal justice IT since 2001, which has addressed infrastructure and IT applications across the system; the police (through their case and custody preparation system), the CPS and the courts have all benefited.

167. However, there is a problem in the way that information sharing has been implemented using IT solutions. Connecting IT systems together has often been an afterthought, as the initial focus has been on developing specific functionality to support immediate business needs. This results in increased costs, timescales, and system complexity. Secondly, where sharing does occur, the mechanism has often been to copy data between systems and then extend the functionality of those systems to deal with that data. One example is the electronic transfer of case information from the Police to CPS. The two main IT systems involved – NSPIS Case Preparation and COMPASS CMS – were neither designed nor built to share case information. It was recognised that electronic interaction would help to improve the efficiency of the CJS and so significant additional development was undertaken to pass a copy of police data to the CPS system; the CPS system then needed further development to be able to absorb the data and present it in a meaningful way to the prosecutors.

168. Duplication of IT systems is inefficient. In the past few years over £1bn has been spent or committed on a number of case management systems, including those for the Police (NSPIS Case Preparation), the CPS (COMPASS CMS), the Courts (Libra, XHIBIT and CREST) and the Prison Service (NOMIS). Whilst all of these systems will have functionality

that is specifically suited to their own business needs, at their heart they all involve the processing of something (cases, offenders, hearings, etc.) and they all need to store and share information. Creating separate case management systems involves duplication and creating post-hoc links between them increases that duplication further.

169. There are many other examples of duplication such as the watch-lists mentioned in the Risk Management Chapter. All this contributes to the problems with criminality information sharing across the network. Though such a review goes beyond the scope of my task, I recommend that a full review is undertaken of IT systems as they relate to criminality information management, drawing on the expertise of NPIA and the CIO of the Home Office. This Review should look to quantify and deal with overlapping case management systems; whether there is a need for as many databases and watch-lists as currently exist; how IT innovation could be applied to support appropriate sharing of criminality information; and how an approach to criminality information technology might be brought together with the governance arrangements I recommend for the public protection network as a whole.

170. Furthermore, IT systems developed for one purpose may turn out to have importance far beyond that initial purpose. The Police National Computer is one. Built to service policing, it is crucial for a number of processes across the Public Protection Network, such as CRB checks. PNC data is owned by Chief Police Officers, while NPIA run the system on their behalf. I am aware that the NPIA, in developing the PND, are concerned about the transparency of governance – and indeed are also seeking to clarify the governance of PNC. I think this is the right approach given the importance that the PNC has, and PND will have, to a number of processes across various organisations concerned with public protection.

171. IT projects generally and understandably focus on the immediate business requirement rather than the overall requirements of public protection. As a consequence, a new database is often created for new business initiatives. The sheer number of databases means that duplication of information is inevitable. An example lies in SOCA, which inherited over 350 databases from the predecessor organisations. SOCA is currently reducing the number of databases to between 50 and 60.

Recommendations

- A full review should be undertaken of IT systems as they relate to criminality information management, drawing on the expertise of the National Policing Improvements Agency (NPIA) and the Home Office Chief Information Officer (CIO), with others including the Government CIO and the Ministry of Justice (MoJ) CIO where appropriate, to address any duplications, inter-operability issues and overlaps **(recommendation 19)**
- Each CIO should consider as a matter of urgency giving effect to any simple tactical IT fixes that will support my recommendations elsewhere on improving criminality information management **(recommendation 20)**
- Building on the governance, processes, standards and architectures that will flow from my recommendations elsewhere to facilitate information sharing, increasing IT integration should be an objective and programmes that increase information sharing should be accorded a degree of priority **(recommendation 21)**
- Looking to future requirements, all IT developments in the sphere of criminality information should pass through an assessment process of the kind set out in my first Investment recommendation. This process should explicitly address use and reuse of IT capacity, making the maximum use of existing technology **(recommendation 22)**
- There should be better engagement with IT suppliers so that they understand priorities and respond to the need for processes and IT systems to be able to share criminality information across departments and agencies. This should help to ensure their understanding of the cross-cutting requirements of the public protection network, and to encourage their active help and expertise in making suggestions as to how re-usability can be achieved, rather than the building of fresh systems. (This links with the comments made in the Investment Chapter) **(recommendation 23)**
- By Spring 2009, ACPO working with NPIA and stakeholders, should clarify the governance of PNC and develop a clear and agreed approach in the light of the issues this report identifies as to who in which organisations should have what access to PNC. (This links to one of the early practical steps regarding CCD access to PNC and to the recent joint Inspectorate report on the Peart / Joseph case which recommends that prisons should have direct access to PNC.) The long-running dispute about funding of the Northern Ireland link should have been resolved **(recommendation 24)**
- The SROs for the remaining Bichard recommendations should urgently re-consider the timetables for implementation with a view to expediting them. I expect to see greater progress when I revisit these issues in early 2009, and in particular to see that the court resulting recommendation will be fully implemented by April 2009 **(recommendation 25)**









CHAPTER 9: AT THE FRONT-LINE

172. The earlier Chapters of this report focus on the need for a clear strategic direction and coherent governance arrangements to improve criminality information across the whole public protection network. And while the ultimate responsibility for public protection rests with the Government, the reality is that significant decisions – for example, on deportation or access to employment with the vulnerable – are taken every day by front-line staff. The fact that these decisions are sometimes based on inadequate information impacts on public safety. This Chapter focuses on finding practical ways to improve criminality information management to ensure front-line staff have better information on which to base their decisions.

173. To understand better the operational impact of decisions taken in these circumstances, we decided to look in detail at some of the processes where the appropriate use of criminality information is critical to minimising risk of harm to the public and those who protect them. We focused on three areas:

- Processing foreign national prisoners
- Releasing detained persons from custody
- Vetting and barring for roles with children and vulnerable adults where the applicant is a foreign national or UK national who has spent time abroad

174. Members of the Review team interviewed a number of front-line staff who make key decisions in these processes. I set out here our findings about the current processes and the information management issues which interviewees raised with us. Some of these issues are specific to particular processes while others cut across all three business areas. We identified common issues in each aspect of information management:

- **Capture** – there are particular problems in establishing identity and nationality
- **Store and access** – accurate information is sometimes hidden behind inconsistent data formats or unavailable to those who most need it
- **Share** – multiple instances were found where information exists but processes or systems are not in place to share it quickly
- **Analyse and act** – those responsible for interpreting criminality information and taking key decisions sometimes lack the required decision framework or expertise
- **Manage** – these issues have been addressed in the earlier Chapters of this report

175. In proposing what actions might be taken to help improve matters, I have focused on practical steps that can be undertaken to amend existing practices and procedures, rather than fundamental change. Other proposed actions will require or be part of wider, long term – changes – some of which have been addressed in other Chapters.

Overview and Background to Business Areas

Processing Foreign National Prisoners

176. There are currently around 11,000 prisoners who are identified as foreign nationals. The actual number of foreign nationals in custody may be higher but, as explained below, there are often problems in establishing true identity and nationality. The processing and managing of these individuals, particularly with regard to deportation (2784 in 2006 / 07, 4000 expected for 2007 / 08), is therefore a significant task. Continued increase in international mobility and migration means that the numbers are likely to grow.

177. Following a review in 2007 of the deportation of foreign nationals released from custody, there have been some significant changes to the deportation processes, which focus on the work of CCD of the UK Border Agency. These changes have been designed to better ensure that Foreign National Prisoners (FNPs) are appropriately considered for deportation and, if conducive to public protection, deported on the recommendation of the courts and the decision of the Home Secretary. This review has looked at the wider processes involved and my recommendations should complement the changes already underway.

Releasing Detained Persons from Custody

178. Ensuring that individuals released from custody are both released and subsequently managed appropriately is critical to minimising the potential risk of harm to the public, those who protect them and the individuals themselves. With around 90,000 sentenced offenders received into custody in 2006 and a probation service caseload in the same year of 235,000, reducing re-offending rates has been put at the centre of achieving this aim and offender management has undergone substantial reform in the last few years to this effect. The introduction of the National Offender Management System (NOMS) in 2004 and the adoption of a more effective end-to-end approach have been important in bringing the prison and probation services closer together.

Vetting and Barring for Roles with Children and Vulnerable Adults where the Applicant is a Foreign National or UK National who has Spent Time Abroad

179. Protecting the most vulnerable in society is key to public protection. The vetting and, if necessary, barring of those who apply to work with such individuals is critically important. The Bichard Report has been the most significant driver to reforms in this area leading to the 2006 Safeguarding Vulnerable Groups Act (SVGA), the establishment of the ISA and a much greater appreciation of the importance of sharing and taking account of criminality information.

180. The International Dimension Chapter describes some of the work underway to improve the exchange of criminality information internationally – which is hugely important to vetting and barring. The CRB, the main body responsible for undertaking criminal record checks in England and Wales, carries out approximately 2.8 million criminal

record checks a year. Around a quarter of a million are for foreign nationals and 80% are for roles that will be classed as regulated activity under the SVGA, activities in which around 8.8 million people in total are currently employed. Some 5000 Registered Bodies can process applications for a CRB check (some on behalf of many other employers), ranging from large public sector organisations such as the NHS to small employment agencies.

Findings

Capture – There are Particular Problems in Establishing Identity and Nationality

181. Correctly establishing the nationality of FNPs has important implications for deportation eligibility. While their deportation depends primarily on sentence length (either single sentence or sum of several short sentences) the criteria are different for citizens of the European Economic Area compared with other countries. EEA nationals will only be considered for deportation if they have committed a serious offence, or offences, and been sentenced to more than 24 months, while non – EEA nationals are eligible for deportation if they have a sentence of 12 months or more. This means that it may be in the interests of an FNP to falsely claim EEA nationality to seek to avoid consideration for deportation. A wrong determination of nationality therefore has the potential to lead eventually to wrong release in the UK instead of deportation.

182. Determining who should be referred to CCD for consideration for deportation is the responsibility of prison staff. However, they often lack supporting nationality identification for their decision and, as prison staff have no method for cross checking with other immigration records, they have limited means of verifying nationality. FNPs may claim that their passports are lost or stolen or documents may have been taken by the police on arrest and the details of those documents not passed on. Whenever a deportee does not have travel documentation, CCD must go through the often extremely lengthy process of applying for emergency travel documentation (to the deportee's country of origin) in order to remove them from the UK.

Validating and Verifying Identity

183. Ensuring that an identity is a valid one and that it belongs to the person claiming it, is also critical to vetting and barring. This issue was identified in the Bichard Report and can compromise the rest of the process. Validation and verification is the responsibility of Registered Bodies and employers. With large volumes of applicants, often complex immigration paperwork, unfamiliar ID documents, little supporting biographical information (such as addresses, bills etc) and little means of cross checking against other data this is a particular problem with non-EEA foreign nationals.

184. In the eight months to February 2008, following several UKBA operations in the South East region, 130 immigration offence prosecutions were made on foreign nationals working in the care industry and education, all with clean, valid CRB checks issued under false identities. While use of false identities may be largely for immigration purposes, there is the potential risk that individuals, who would otherwise be deemed unsuitable, could be employed with vulnerable adults or children.

185. Changes by the Identity and Passport Service (IPS) and UKBA to the way identity and immigration are managed are already underway and identity cards for foreign nationals applying for leave to enter or remain in the UK may also prove helpful in more effectively establishing identity and nationality.

Store and Access – Accurate Information is Sometimes Hidden Behind Inconsistent Data Formats or Unavailable to Those who Most Need It

186. A Prisoner Escort Record form (PER) accompanies an offender every time he or she is transferred from one part of the prison estate to another – or to court, hospital etc. A fresh PER is completed for every transfer journey but we were told that PERs often contain inadequate information. As a result, staff guarding or escorting individuals in custody may be unaware of previous incidents and unable to guard against their repetition. One example cited was of a prisoner who had previously attempted to escape during a medical visit, but was allowed to do so again because that information was not passed on. In part response to these issues, a positive development is the work currently being undertaken in the West Midlands to pilot a revised PER form that includes improved information on risk.

187. The multiplicity of reference numbers for individuals used across public protection organisations means there is no reliable way for different organisations to ensure that they are sharing information about the same individual. Staff spend a lot of time chasing up the location of individuals elsewhere because they do not have the relevant reference number needed to search for them on that organisation's database

188. With few consistent and robust mechanisms for obtaining and passing on data, many information sharing channels identified by staff are ad hoc and informal, relying wholly on staff establishing good working relationships. The team found many examples where this worked relatively effectively but where, for example, a member of staff is absent, changes jobs or their casework is moved to someone else, informal channels prove vulnerable.

Examples of Good Practice

189. The police and prison service in the Isle of Wight provide a good example of an effective formal relationship to share information at the local level, particularly in helping to detect and prevent criminal activity between those inside and outside prison. In other areas such as between the police and CRB, formal liaison roles have made obtaining consistent information less time consuming, while bringing together information in a single place and better managing some of the cultural barriers inherent in working across organisations.

The Police National Computer (PNC)

190. IT systems can help to enable the consistent availability of information. The PNC plays a central role in all three business areas we looked at, including providing offending case history in considering FNP deportations, checking for outstanding warrants prior to release from custody and checking for convictions by the CRB as part of the vetting and barring process. However, delays with getting information onto PNC, gaps in information on issues such as foreign convictions for UK nationals and limited access to PNC by front-line staff were all issues raised by interviewees.

191. Thus there are delays in processing FNP cases because CCD staff do not have access to PNC – they have to fax requests to other UKBA staff – offenders with outstanding warrants may be released when they should have been taken back into custody and individuals may be wrongly employed following apparently clean vetting checks. CCD staff estimate that having more effective access to PNC would make workflow 60% faster.

192. These issues are well known and work is in hand to improve matters – especially following the Bichard report. However, it is not clear to what extent front-line staff from organisations other than the police and courts are involved in helping to shape this work.

Additional Sources of Information

193. One additional helpful development identified was the police use of prison offender location and release information through the Prisoner Intelligence Notification System (PINS). This IT solution cross-references prisoner data to databases of known offenders or suspects, reducing the risk that offenders will be overlooked while in prison. So far 20 police forces have taken up the system and feedback is very positive. According to one police force, the time spent obtaining information on outstanding warrants for offenders due for release has reduced from between 1 and 14 days (using paper and fax) to 3 minutes and the number of warrants outstanding has drastically reduced as a result.

194. An additional important source of information for vetting and barring is relevant local police force intelligence. CRB have limited and variable access to this data. Drugs offences for example are regarded by some forces as relevant to disclose but not by others. CRB has already begun the Police Volume Management Project, working with four police forces to improve and coordinate the way in which this information is made available.

Sharing Information – Multiple Instances were Found where Information Exists but Processes or Systems are not in Place to Share it Quickly

195. A consistent theme identified by interviewees with regard to FNPs was the delays in the deportation process resulting from information not being shared effectively. For example, there was no direct mechanism for communicating the outcomes of appeals between the AIT and prisons, probation, IRCs, or the case worker in CCD. When asked how a prison found out the determination of AIT appeals against deportation for an individual, one FNP coordinator stated "if they don't come back, chances are the appeal has been successful".

196. CCD also do not routinely inform the Detention Escort Population Management Unit (DEPMU) quickly when something happens in a case that means deportation cannot be effected, such as judicial review. This means that DEPMU are often unable to follow through with planned removals. This is costly and also delays other deportations that could otherwise be successfully effected.

197. Given that individuals may lodge repeated appeals, and deportation cannot be carried out while an appeal is still being processed, prompt communication of results is vital. In one case, an individual had exhausted his in-country appeals rights three times and simply kept on appealing. We were told that delays led to greater case complexity, greater likelihood of individuals having to be moved within the prison and immigration removal estates (giving more opportunities for information on them to be lost every time they are moved) and an increased possibility of immigration bail being granted, with the potential public protection risk that this introduces.

Ineffective Sharing of Information

198. Ineffective information sharing when individuals are moved between prisons and IRCs, and from one IRC to another, is a common problem. There is no shared information system linking IRCs with one another and with DEPMU, and 70% of IRCs (run by contractors) do not have access to prison service IT systems. However IT is only part of the problem – there are also governance, culture and process issues which can act as barriers to information exchange. Staff at one IRC told us that on several occasions, prison files (including medical, behavioural and procedural information) had arrived up to 3 months after detainees had left the centre. In one IRC, if a deportee had to be moved back into prison – due to violence or severe mental health problems, for

example – the file built up in the IRC was not routinely passed to the prison. And when individuals were moved from one IRC we visited to another, the paper or electronic file of information built up about that person was not always passed to the receiving IRC. While I recognise these are only examples of ineffective sharing of information, and do not necessarily represent the norm, they serve as indicators of where more systematic, routine methods of sharing would be of benefit.

199. Poor sharing and loss of risk assessments on an individual can present a potentially serious risk to public protection when they are bailed or released. While current NOMS and MAPPA are supposed to include higher risk individuals on immigration bail, staff at one IRC told us they had never been asked to provide any information about individuals to help inform any subsequent supervision or monitoring. Furthermore, information is not consistently provided to inform monitoring procedures on release.

Health Assessments

200. There are particular problems in sharing health assessments, especially in relation to mental health and drugs related issues, when prisoners are released from custody. Given the prevalence of mental health and drug problems affecting many in custody, this is an important area highlighted by several interviewees. The duty for, and emphasis on, information confidentiality by health professionals (combined with the confusion over DPA requirements, mentioned in the Leadership and Culture Chapter) was identified as a barrier to information disclosure for the purposes of public protection. Currently the limited mental health information recorded in OASys is not regarded as fit for purpose by many mental health practitioners. A greater shared understanding and more effective sharing of risk information could be encouraged by involving mental health practitioners in the development of the planned replacement for OASys.

201. Information sharing is less of an issue when specialist forensic psychiatrists are involved, given their expertise and understanding of public protection issues. The inclusion of mental health practitioners in domestic violence Multi Agency Risk Assessment Conferences (MARACs), where health considerations may be relevant for both victim and offender, has also proved effective in improving understanding and information sharing.

Analyse and Act – Those Responsible for Interpreting Criminality Information and Taking Key Decisions Sometimes Lack the Required Framework or Expertise

202. Many of the findings in this Chapter have so far focused on getting the right information in the first instance. Understanding and interpreting this information and matching it to the management of risk and priorities (as identified in the Risk and Risk Management Chapter) is also an issue in all business areas.

203. AIT has targets for asylum cases but not for FNPs – the latter are often referred to as "non-target cases" – despite the fact that, being offenders, they are potentially a higher risk to public protection than non-offending asylum seekers. From an appeal being received to substantive court case, the average time for asylum cases is six weeks. For FNPs, it is 14 weeks. This adds to pressures on the wider prison estate, including the impact on the effective rehabilitation of other offenders.

204. Interpreting information wrongly can also lead to problems. For example, when first processing foreign national offenders, police will run checks using the LiveScan system against UKBA databases. We found that a nil return is routinely interpreted by the police as the individual being of no interest to UKBA, whereas no record in a range of cases might well suggest that the individual is in the country illegally.

205. Probation service risk assessments are often based on complex mental health information. One study of probation hostel residents carried out by the probation service working together with mental health professionals identified significant differences in the assessment of levels of risk carried out by probation staff compared to trained mental health professionals – reinforcing the need for greater specialist mental health involvement.

Information to Help Make Critical Decisions

206. At several key stages in processing offenders, such as in custody suites, front-line staff have to use and interpret information quickly to make critical decisions. Retrospective review to learn lessons can help to improve the quality of these decisions. In 2003 the Parole Board established its own Review Committee, responsible for reviewing decisions to release prisoners where those prisoners were subsequently alleged to have committed violent or sexual offences on licence. The Committee is perceived to have been successful in identifying learning points for the Parole Board and other PPN organisations and the initiative offers lessons for other areas such as deportation, bail or employment and barring decisions based on offending history and risk.

207. In vetting and barring, doubts over the information on an individual impact on risk assessment. It is the responsibility of employers to understand the purpose and importance of complementary and supporting checks and the implications of the information they receive in support of this. However, understanding and practice amongst employers is patchy.

208. CRB provides advice to employers on the type of information they can request to check for possible foreign convictions. But as well as lacking expertise, employers often have little means of verifying the robustness or completeness of this information. Proof of good conduct for one job applicant, for example, was in the form of a letter the applicant brought from a local Chinese police force. In these circumstances, employers have to make hard choices on the basis of such evidence as is available.

The Need for Good Quality Guidance

209. Lack of understanding and inconsistency in practices and standards is compounded by the variable quality and accessibility of guidance provided to employers by different organisations. Furthermore, such guidance is often focused on the initial decision and does not cover subsequent risk assessment and monitoring. For foreign nationals and UK nationals who have spent time abroad in particular, there will always be limits to the extent to which an applicant's information can be quality assured and so monitoring or supervision during employment is required. Some employers in the care industry, however, regard a clean CRB disclosure as effectively a "green light" rather than simply a part of wider employment risk assessment. Concern was expressed by one umbrella body that some employers view CRB checks as merely a required step in the employment process while others over-estimate their value.

210. New SVGA and ISA arrangements should help; new criminality and risk information received on an ISA – registered individual will cause their status to be reassessed, with employers informed if that reassessment results in barring. Building on this work, CRB are considering the possibility of offering a broader monitored disclosure service where employers could be notified of any status change on an individual.

Recommendations

211. Many examples of good practice already exist within the main front-line processes specific to existing agencies. General recommendations in this area across the whole PPN are unlikely to be helpful. Nonetheless, there are several overall areas for improvement, which can be summarised as follows:

- Where justified by the risk to the public, proffered identification should be checked against relevant databases, and relevant information sought at each decision point as offenders move through the criminal justice system **(recommendation 26)**
- Clear accountability and standard procedures should be developed to manage storage and access to all key PPN information **(recommendation 27)**
- Where information sharing is both necessary and proportionate to support effective public protection, arrangements should be systematic, proactive and accountability clear **(recommendation 28)**
- Clear frameworks should be developed for decision making on individual cases appropriate to the staff member taking the decision, and indicating clear escalation paths where required **(recommendation 29)**

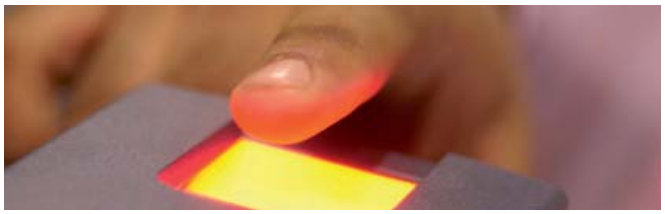
212. For each overall recommendation there are several specific areas for improvement. Detailed recommendations are summarised in the table overleaf.

Information management activity	Issue	Overall recommendation	Initial steps recommended	Longer term recommendations
Capture	Particular problems in establishing identity and nationality	Where justified by the risk to the public, proffered identification should be checked against relevant databases, and relevant information sought at each decision point as offenders move through the criminal justice system	• UK Border Agency to ensure that both pre and post sentence, all individuals who cannot prove UK nationality and who meet minimum sentencing and non – EEA (ie 12 month) criteria are referred for consideration by CCD, with CCD verifying and applying nationality criteria for deportation eligibility [FNP] • Police, prisoner escort companies, courts, prisons and IRCs to ensure that the details and whereabouts of identity documents obtained on first processing are passed on with the individual [FNP] • Where identity / travel documents are not available, CCD to start initial stage of Emergency Travel Documentation process on receipt of an eligible referral [FNP]	• The process of identifying people applying to work with children and vulnerable adults should more robustly verify and validate identity documentation such as with the issuing organisation. IPS should consider how it can best support Registered Bodies with this process as part of the roll-out of the National Identity Scheme and Identity Verification Service [V&B]
Store and access	Accurate information is sometimes hidden behind inconsistent data formats or unavailable to those who most need it	Clear accountability and standard procedures should be developed to manage storage and access to all key PPN information	• All police forces to implement prisoner location and release information solutions [RDP, FNP] • CCD to be provided with dedicated, appropriately resourced access to relevant PNC information for assessing offending history [FNP] • The reference number used to identify an individual by the transferring / referring organisation as well as all previous reference numbers, ie PNC reference number, Prison Number and Home Office number (for FNPs) to be included on all transfer forms / individual records [FNP]	• Introduce revised standard and consistent escort record form and process across police, courts, prisons, prisoner escort providers and IRCs (for FNPs) that ensures more robust onward transfer of relevant risk and historical information. [RDP, FNP] • Each PPN organisation to review information channels between them and put in place single contact points and robust business continuity arrangements, where needed {RDP / FNC} • Each PPN organisation to review formal liaison with key partners and establish formal liaison wherever possible • All police forces to participate with CRB's Police Volume Management Project to centralise disclosure of low level intelligence [V&B]

Information management activity	Issue	Overall recommendation	Initial steps recommended	Longer term recommendations
Share	Multiple instances were found where information exists but processes or systems are not in place to share it in a timely fashion	Where information sharing is both necessary and proportionate to support effective public protection, arrangements should be systematic, proactive and accountability clear.	• UKBA to lead on implementing oversight and governance arrangements to manage the criminal casework, appeals and immigration detention process between Police, Courts, CCD, AIT, Prisons, DEPMU and Probation as a whole [FNP] • Determinations from tribunals of Foreign National prisoner appeals should be passed on to caseworkers in UKBA CCD, Prisons, Probation and IRCs [FNP] • Communication between CCD and DEPMU to be improved, particularly around cancellation of planned deportation [FNP] • Release and licence / probation or MAPPA arrangements for FNPs to be reviewed and appropriate arrangements put in place. In cases where it is clear that FNPs who have completed sentences cannot be deported for human rights or other reasons, these cases to be identified at the earliest opportunity to facilitate such arrangements [FNP, RDP]	• UKBA to consider bringing together and providing a more integrated information system to improve the interface between DEPMU, the Immigration Removal estate and CCD – AIT – to facilitate better information access and more effective oversight and management of processes [FNP] • NHS to ensure that medical practitioners who are required to contribute to information sharing and / or assessments of those in the public protection system have appropriate guidance and legal understanding on the sharing of medical information [RDP] • Mental health practitioners to be engaged in the development of the planned replacement for OASys [RDP] • Specific provision should be made for the inclusion of health practitioners in MARACS which should be rolled out more widely [RDP]
Analyse and act	Those responsible for interpreting criminality information and taking key decisions sometimes lack the required decision framework or expertise	Clear frameworks should be developed for decision making on individual cases appropriate to the staff member taking the decision, and indicating clear escalation paths where required. .	• ISA with support from CRB to provide centralised core application to termination of employment standards covering continuing risk assessment, monitoring and referral to the ISA – Standards to be incorporated into relevant employer guidance (eg Department for Children, Schools and Familes, DCSF) and existing employer inspection regimes (eg Ofsted) [V&B] • Primary Care to work with local probation services to identify appropriate mental health liaison and support arrangements for the purposes of risk assessment and identifying appropriate interventions [RDP] • AIT with UKBA to review and clarify risk prioritisation of FNPs [FNP] • UKBA and police to agree correct procedures when interpreting Live Scan checks against immigration data [FNP]	• PPN organisations to review areas of decision making (eg vetting and barring, FNP bail, probation) that would benefit from review board arrangements and establish these arrangements where appropriate [RDP] • CRB to provide broader monitored disclosure service to employers [V&B]
Manage	Key challenges and recommendations discussed in other Chapters of this report			

213. Abbreviations: V&B refers to vetting and barring; RDP refers to release of detained persons from custody; FNP refers to foreign national prisoners









CHAPTER 10: THE FUTURE

214. All the recommendations in this report are for the future and my focus has been on the strategic direction, governance and leadership that will ensure improvements to public protection through better approaches to risk management, investment and technology, recognising the increasing significance of the international dimension and the critical need to help and support those on the front-line. This final Chapter looks in some detail at particular developments on the horizon. As well as ensuring that we tackle the criminality information issues which are currently a problem, we must learn and apply the lessons which they offer for future developments.

215. The pace of technological change has accelerated considerably within the last hundred years or so – from the invention of the telephone, radio and fingerprinting techniques in the late 19th Century through the development of computers and mobile phone technology in the 20th century to the continuing development of technological solutions and widespread use of the internet today. However, those changes, as they relate to data and criminality information, have accelerated at an exponential rate over the past 10 years, bringing both opportunity and threat in their wake.

216. Recent incidents such as the loss of discs by HMRC containing personal data of 25 million families, and by the Northern Ireland Driver and Vehicle Agency (DVANI) of 6000 drivers' personal details would not have been possible 20 years ago. The datastores available in the late 80s could not hold anywhere near the amount of data we routinely download to discs today. Rapid technological advances have made changes in working practices possible. But, as has been shown by these and other examples, such advances need to be matched by better security and a more sophisticated assessment of risk across, not just within, organisations. In aiming to reduce the risk of similar incidents happening again, we need also to take account of the pace of technological change.

217. The increasing pace of change in scientific and technical fields is accompanied by wider demographic and environmental changes. More people are taking up their rights to live and work in the UK, which makes the task of establishing identity and the sharing of criminality information with other countries ever more important. As proposed in the International Dimension Chapter, we need to develop a risk - based approach to future sharing of criminality information internationally. Again this involves planning for the future, identifying those countries with which we need to share data and spotting potential problems before they arise.

Identity Management

218. Establishing the real identity of those who have committed criminal offences is key to ensuring that they are caught, brought to justice and denied further opportunity to offend. Unsurprisingly, the use of multiple identities (or aliases) is a core part of the armoury of criminals, both small scale and organised criminals, as well as terrorists.

219. The best way to verify an individual's identity is though a combination of biographic data (name, address, date of birth etc) cross checked with biometric data (explained in more detail below). The current difficulties of establishing identity are discussed further in the At the Front-line Chapter.

220. The Government's recently announced National Identity Scheme should help to offer a new and secure way for UK citizens and foreign nationals living and working here to protect and prove their identities. From November 2008 foreign nationals who come to the UK to work and study will be issued with biometric identity cards. These cards are intended to make it easier for employers and sponsors to check whether newcomers are entitled to work or study here and to establish whether they have criminal convictions which would make them unsuitable to take up jobs working with children or vulnerable people.

221. From 2009 people working at airports who need identity verified to a high level will be entered on the National Identity Register. High volume of identity cards linked to the introduction of fingerprint biometric passports is planned for 2011-2012.

Biometrics

222. Biometric information means physical, measurable characteristics of a person which can be used in an automated way to help establish an individual's unique identity. The most familiar Biometrics in use include:

- Fingerprints – have been used in criminal investigations for over 100 years. Regarded as the primary means of establishing conclusive proof of identity for immigration control purposes; for many years accepted as evidence in criminal courts when substantiated by fingerprint experts. Technological advances have meant that encoding and matching can be automated efficiently, to process high volumes of records. However the clarity of prints varies considerably according to age and other matters

- Facial Images – the most universal biometric, exemplified by the passport photo. These can easily highlight gross differences between an individual's appearance and their passport photo. They can be used to automate one-to-one searching at a control point but are not foolproof, as people can change their appearance relatively easily, and indeed ageing itself brings about changes

- Iris – the details of the structures in the coloured part of the eye surrounding the pupil has been shown to have a stable pattern for each person and to be highly varied between individuals, so is unique (or very close to unique). Iris recognition schemes are in operation at Heathrow, Gatwick, Birmingham and Manchester airports and may be more widely used in future
- DNA – the structure of DNA was discovered in the 1950s. It is a unique biometric now used widely (but not as often as fingerprints) and successfully in criminal cases. DNA is only partly automated in that it requires laboratory analysis (it takes a few hours at a minimum) and is therefore expensive and not practical for identification at borders

Biometrics Databases

223. Since May 2001, when section 64 of PACE was amended by the Criminal Justice and Police Act 2001, the Police have had powers to take and retain DNA samples and fingerprints from all people who are arrested for recordable offences, as well as photograph them – including those who are subsequently acquitted or where the charges are dropped. The retained DNA samples can only be used for the purposes of the prevention and detection of crime, the investigation of an offence or the conduct of a prosecution, or the identification of a deceased person.

224. DNA profiles are stored on the DNA database – which has grown over the past 12 years to contain over 4 million records. Fingerprints are stored on IDENT1; there are 13.5 million sets of ten-prints and 2.86 million palm prints.

Attitudes to Biometric Data

225. Biometrics databases, and in particular the rapid growth of the DNA database, are often raised as public concerns. The dilemmas are mentioned in the Introductory Chapter. The public may want the organisations whose job it is to protect them to use biometrics to aid quick, reliable identification of those who would seek to cause harm. But they may also worry about the DNA profiles of innocent people, particularly children, being on the database. At least part of this concern is rooted in the myths surrounding DNA which can lead to unfounded fears. For example, while potentially some DNA samples might be analysed to detect the likelihood of developing particular diseases (which would be useful information for insurance companies), the reality is that the type of profile held in the National DNA database is not analysed in this way – they are simply to establish an individual's unique identity.

226. It is clear from, among other things, the reactions to Lord Justice Sedley's reported remarks about DNA testing last year that there are widely differing public views about its desirability and applicability. This is such an important area that I believe Ministers need to lead a public debate to help improve public understanding and confidence. Given the significance of this matter for public protection, I hope such a debate would transcend political difference.

227. Media reports of criminal cases where forensic evidence, such as traces of DNA, have helped to convict a rapist or murderer generate support for such techniques and help to build public confidence.

In 2006 / 07 there were 41,717 crimes with DNA matches including:

- 452 homicides
- 644 rapes
- 222 other sex offences
- 1,872 other violent crimes and
- Over 8,500 domestic burglaries

228. DNA matches do not necessarily equate to a crime solved as some of the matches will eliminate potential suspects. However, being able to eliminate suspects quickly can save a great deal of time, money and distress – ensuring police resources are focused on finding and bringing the perpetrator to justice.

229. Familial DNA can be useful when the offender is not on the DNA database but it is suspected that the profile of a close relative may be retained. The Information Commissioner has approved use of familial searching in the UK as proportionate in DPA terms, if restricted to the most serious cases and intrusion into the private lives of individuals is minimised. It has been used successfully in helping to solve difficult, long running cases such as that of James Lloyd, known as the "Shoe rapist".

Case Study – the Shoe Rapist

Numerous rapes and other sexual attacks were committed in Rotherham, South Yorkshire between 1983 and 1986. The investigation stalled after years of using routine methods of investigation and familial searching was eventually undertaken. The search identified 42 possible relations of the rapist on the DNA database. The strongest link was through a sister who had been convicted of drink driving. This led to James Lloyd's arrest. He admitted 4 rapes and 3 attempted rapes and was convicted in July 2006. Stiletto shoe "trophies" belonging to his victims were found at his place of work.

230. However the use of familial DNA is controversial on ethical grounds – as it involves identification of perpetrators by looking at the DNA profiles of their innocent relatives. And there is the possibility of great distress being caused to people who learn that, for instance, they are adopted and had never been told. In other countries such as France and Belgium its use has been ruled out and in the USA there are legal challenges that it is contrary to the Constitution.

231. The UK has recently taken steps to provide greater reassurance in the use of biometric techniques by establishing the office of the Forensic Science Regulator and is to establish a Forensic Science Advisory Council whose members will be drawn from key stakeholders, expert bodies and others with a particular interest in the provision of forensic science to the Criminal Justice System. The Regulator's role will cover the regulation of: organisations; processes; new techniques and individuals. There is also a DNA ethics group, which examines ethical issues and provides independent advice to Ministers. Public confidence in biometric and other developments is essential to their successful application.

Inter-Operability and Standards

232. By definition, biometrics data relates to a person whereas criminality information has generally related to a case – a court case or an asylum case for example. There has been a rapid expansion of biometrics databases – both within the UK and internationally – but they have usually been developed independently for the purposes of one organisation. Inter-operability is often a problem – an issue which affects IT systems too, as outlined in the Technology Chapter. If we are to improve the future sharing of criminality information in the interests of protecting the public we need to move away from "police data", "prisons data", "immigration data" etc to the concept of "public protection data".

233. Inter-operability issues may relate to contracts let to suppliers and action is now underway to improve compliance of systems to enable business processes across organisations. For example, the OGC ensure that the wording of new contracts includes the need for compliance across Government. This is important; and I hope the supplier community will respond positively.

234. There are established rules and standards on the exchange of fingerprints as evidence with other countries – which includes verification by experts – but international standards differ considerably on DNA profiles. Interpol have produced a DNA handbook, and police forces within England and Wales all use the ACPO DNA handbook, but there is a range of standards in use across the world. Until standards are established and adopted on DNA across the world, concerns about the differences for evidence will remain.

Effective Use of Biometrics

235. Britain now leads the world in successful delivery of biometric visas, with all those coming to the UK on a visa now required to provide fingerprints. So far, more than one million biometric visas have been issued, to travellers from 135 countries around the globe. All applications are now checked before a visa is issued – and so far, more than 11,000 have been identified as people previously fingerprinted in the UK as part of immigration cases or asylum applications. The checking of fingerprints for this purpose is quick – results are generally sent back in a few minutes. A couple of case studies illustrate the benefits of this new approach:

UK Visas case studies

Two applicants in India applied for UK visit visas. Biometric checks revealed they had both previously claimed asylum in the UK as Sri Lanka nationals. One had applied as a tourist using an Indian passport showing a different name and date of birth. The other applied for settlement using a different identity. Both applicants were refused.

An applicant in Jamaica applied for a settlement visa to join his spouse in the UK. He claimed they had met in Jamaica and that he had never been to the UK before. A biometric match revealed that the applicant had previously claimed asylum in the UK in a different identity. After initially denying this, the applicant admitted that he had previously lived in the UK unlawfully. The application was refused.

Current and Future Technologies

236. Organisations in the network should ensure that arrangements are in place to keep abreast of technology development, its application, and its acceptability – horizon scanning, technology evaluation and impact analysis. Business processes and models also need to change to keep pace with what technology can do. The technology exists to locate, scan and search finger marks from a crime scene and potentially identify a suspect in less than 30 minutes, so that the arresting officer could be waiting outside the perpetrator's last known address when he returns. However, existing business processes preclude that, therefore officers at crime scenes cannot react as quickly as the technology would allow.

237. The custody suite is another area where use of technology has increased dramatically in the last few years. However, much of the technology is not joined up and without that, and business process redesign, the job of a custody sergeant is still difficult, often in a challenging environment.

Case Study – Custody Suite

We visited a Custody Sergeant at a police station in Belfast. There are several separate IT systems that support the custody staff in booking in a prisoner. The first is the custody system, then Livescan is used to take fingerprints. Other information is available through PNC. The systems are not integrated, so information is entered several times. The custody sergeant had a single computer for initial data entry, largely logging responses from the arrested person. There are a number of screens of information to get through, and he cannot move on to the next screen if he has missed an important field. For each person, this can take upwards of 20 minutes. Added to this, he has to deal with people who might be drunk, unco-operative or unable to speak English. While we were there, a Polish interpreter had to be called to deal with an arrested person. There is little waiting space, so other officers and arrested people are often kept waiting in the Station yard, adding to pressure to book prisoners in quickly. On a busy night, this can mean officers wasting time waiting for their turn to book in their prisoner.

238. There is a great deal of technology currently available, with the prospect of more in the future. It has the potential to assist with sharing criminality information across the public protection network. The point again is that business processes do not necessarily keep pace with technology and that can prevent organisations from capitalising on what there is on offer.

Schengen Information System

239. More widely, perhaps the most significant development on the horizon is the UK joining the second phase of the SIS . SIS holds alerts on wanted and missing persons, stolen vehicles and certain categories of property and operates through a centralised set of data which can be created, maintained and searched on a Hit / No Hit basis by all law enforcement agencies in member states which have signed up to the agreement. SIS I (the precursor system to SIS II) is currently in use within 24 European Countries, helping law enforcement, border and visa agencies to work more closely together to combat international crime and improve public safety.

240. SIS II is currently in development and is expected to be operational in existing Schengen member states in Q4 2009; the UK is aiming to be connected to this system in 2010. The NPIA are leading the project for the UK which should reduce the risk of interoperability problems. Via the Police National Computer (PNC), law enforcement officers will be able to share and use certain information with other police organisations from all Schengen countries. Use of this information will allow them to locate missing persons, criminals and stolen property from other countries – increasing our opportunities to deal with cross-border crime and extending their reach across Europe. When operational, officers will be able to perform PNC checks on foreign vehicles, persons and ID documents from within

the Schengen countries. If that person or object has an alert placed against them, the officer will be notified and provided with information in order to take the correct initial action. Likewise, law enforcement officers in the other Schengen countries can check for UK wanted / missing person alerts, lost and stolen vehicles, passports and driving licences. SIS II will be accessible to a range of organisations in the public protection network with data available to all Law Enforcement Officers who have access to PNC, which includes the UK Police Service, HM Revenue and Customs (HMRC), the UKBA and a number of other investigative organisations.

Capitalising on New Developments

241. In the Technology Chapter of this report I have emphasised that technology must be driven by the needs of the business and that it forms a significant, but certainly not the main, part of the changes needed to deliver the benefits of better criminality information management. Our approach to future developments in criminality management must recognise this fully. Whatever technological advances become available – whether in the science of biometrics, the data sharing technology of Schengen or the many other promising techniques that are under development – their success or failure will depend on people. Public protection and the management of criminality information to deliver it can only be effected with the support of the public themselves. Ensuring their understanding and confidence in new developments will be essential to securing that. Those who carry the responsibility of protecting the public must have the confidence and the infrastructure to capitalise on the tools that are available to help them. They will look to their leaders to provide that.

Recommendations

242. To enable the PPN to take full advantage of the opportunities the future may hold, I recommend that:

- Horizon scanning should be undertaken (on a regular basis) by the proposed independent Commission for Public Protection Information (This links to the Governance recommendations) **(recommendation 30)**
- Ministers should lead a public debate about the DNA database, and the use of biometrics more widely, to help improve public understanding and confidence **(recommendation 31)**

ANNEXES








ANNEXES

Contents

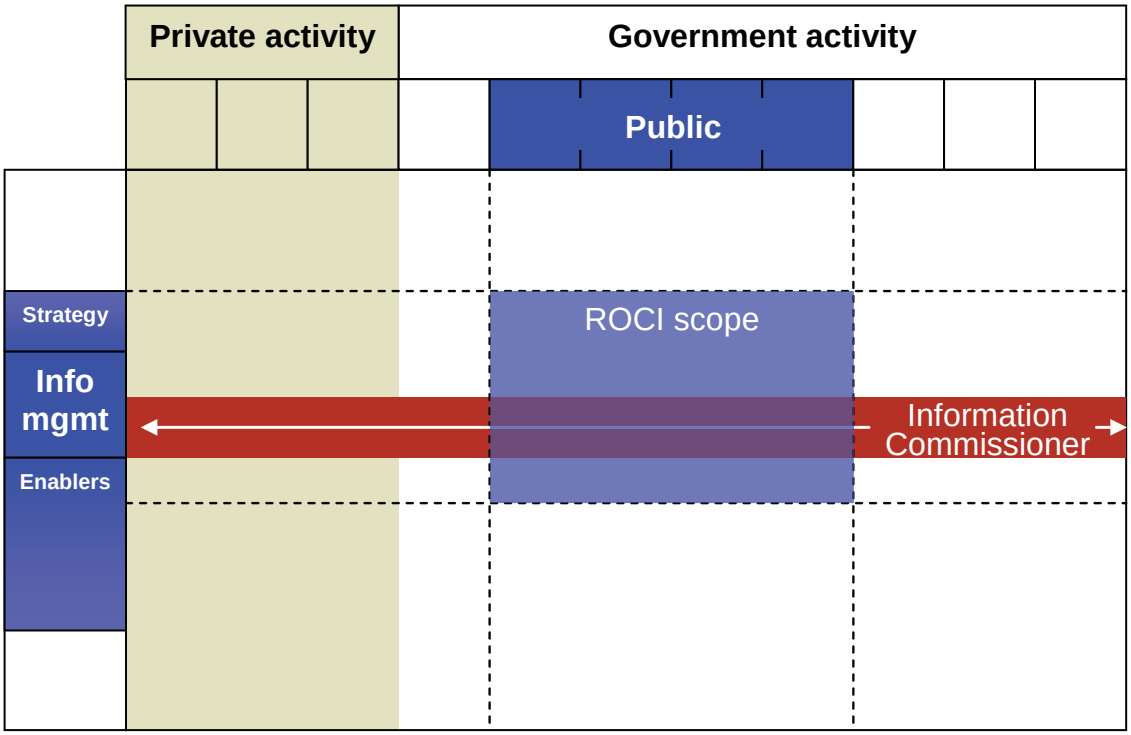
Annex A: Terms of reference for the Review of Criminality Information

Following an inquiry early in 2007 into the handling of notifications by other European countries of criminal convictions for UK citizens, the then Home Secretary took the view that there might be a number of wider issues around the effective use of information about criminality. Sir Ian Magee was therefore asked "thoroughly to examine this whole area and recommend necessary improvements for recording and sharing information about criminality within the UK and between the UK and other countries and the way in which this information is used to protect the public and the relevant procedures and responsibilities".

The Terms of Reference for this independent Review of Criminality Information (ROCI) are as follows:

- To scope the problem and assess what is broken and where the deficiencies lie
- To test understanding of the problems and issues with key stakeholders, and seek consensus on where the principal roles and responsibilities should lie at a strategic level.
- Draw conclusions and make recommendations for improving the recording and sharing of criminality data, with a clear eye on what is realistic and achievable

This review has a tightly defined scope



Annex B: Summary of recommendations

Strategic direction

1. By January 2009, the Government should agree, across Departments:

   - A strategic direction for the improvement of criminality information management across the Public Protection Network (PPN)
   - Prioritised immediate objectives for improvement
   - The embedding in relevant departments' goals and objectives of the principles in this report

The strategic direction should articulate clear goals for the role of criminality information management in supporting public protection and be based on an objective assessment of performance against those goals. Regular performance reviews should update this initial assessment, and also assess implementation progress with respect to the recommendations of this Review.

The improvement agenda should respect the following principles. It should:

- Adhere to all existing governance around information management – in particular: Data Protection Act (DPA), Freedom of Information Act (FoI)
- Provide for collaboration only where the total benefits to public protection exceed the total cost, recognising that some benefits may be realised outside the funding organisation's area
- Maintain delegated authorities wherever possible to allow delivery units to own core processes and thereby deliver agile responses to criminal activity
- Institutionalise key aspects of the PPN only as needed to deliver clarity and value to PPN participants

Governance and Delivery

2. The action to deliver specific parts of this agenda should be led by the agencies concerned, but with support from a central implementation team located in the Home Office but with cross departmental staffing. This unit should be substantially in place by September 2008.

3. Based on an objective assessment of the governance challenge, the lessons learned from existing governance arrangements around criminality, and the requirement for coherence with the overall PPN strategic direction and its core principles, the work of Agencies and the Unit should be governed by a Home Secretary-chaired Ministerial group with external challenge and advice from a Commission for Public Protection Information.

The Commission for Public Protection Information should be set up as a body to champion efficient and appropriate criminality information management across the PPN. It is not responsible for implementing this report but should contribute by:

- Maintaining pressure on public agencies to take forward action in a difficult area, and holding them and Ministers accountable for progress, eg by publishing reviews of progress described in recommendation 1 above
- Being a critical friend for Government as difficult issues and choices arise within or between Departments
- Acting as a champion to help advance public understanding and debate about the policy issues and dilemma

Leadership

4. Leaders at all levels within the PPN need to demonstrate awareness of the importance of information flows across the network and of managing them with their partners, so as to improve the capture of accurate data and ensure the appropriate sharing of criminality information in the interests of public protection.

5. Leaders should make a statement of intent in this area, before December 2008 to ensure that at all levels of leadership there is:

   - Recognition of their accountability for the improvements in criminality information capture and sharing, by including this in their key objectives
   - Simple, straightforward communication to staff of the importance of accurate data capture and appropriate sharing of information (within the law) as fundamental to public protection

6. The importance of information management should be explicitly included in leadership training and development programmes such as the Police Strategic Command Course, the civil service PSG framework and other equivalent programmes before September 2009

7. Within one year of publication of this report, Leaders should also assess, with peer review, their provision of organisational training, guidance etc on criminality information for staff and commit to deliver:

   - The necessary tools, agreed protocols and processes so that staff may capture, share and use criminality information appropriately. (This links with other recommendations, particularly those mentioned Investment and At the Front Line Chapters)
   - Improved capacity and confidence of staff through training, guidance and sharing good practice

Risk

8. Those responsible for strategy, business planning and risk management within each department or organisation belonging to the PPN should give explicit consideration to the potential impact of their decisions on risks to public protection as a whole. (This links to the Governance recommendation as the proposed Commission should have an oversight role on PPN risks and be provided with organisations' risk registers)

9. Each agency within the PPN should institute by January 2009 a regular mechanism to enable escalation of significant front-line risks to public protection. These processes and their outcomes should be reported in department / agency annual reports, and the risks in them should be considered and managed alongside corporate risks.

10. The Home Office should facilitate mechanisms to encourage senior managers to share their analysis and assessment of public protection risks and vulnerabilities, and proposed action, with other organisations. This should enable joint action to be organised where appropriate.

11. The concept of the PPN brings a new dimension to the need to assess risk. The Ministerial Group should ensure that an assessment of the effectiveness of risk identification and management is included in the inspection framework of public protection organisations.

12. Agency heads, as part of the action under Leadership recommendations, should ensure that adequate training in risk assessment and management as it applies to interchange of criminality information should be provided for managers at all levels.

Investment

13. Investment Boards in the various public protection organisations should always take account of wider public protection priorities in making funding decisions. I am encouraged by work being done to create an assessment process at inception for new projects and programmes, particularly where there is a substantial IT component. I recommend that the consideration of wider public protection benefit is embedded in that process. (This links to Technical recommendations)

14. The Implementation Team should facilitate mechanisms to ensure better joined up approaches to investment across the public protection network. This should include unblocking problems quickly to prevent delays in implementing solutions to improve the flow of criminality information.

International Dimension

There is much to be gained from a concerted effort to improve the flow of information between the UK and other countries, both within the EU / EEA and beyond. But this will not be a simple or a quick task, given the complexity of the current position and the number of potential countries and initiatives involved. Recognising this complexity and the scale of the task, I recommend the following:

15. The Home Office led Implementation Team should support Ministers in developing by January 2009 an agreed approach for the UK on international exchange of criminality information. This agreed approach should cover:

    - Priorities for expanding agreed information flows with other countries, based on a more proactive, risk based approach to identifying the countries with which it needs to exchange data. Vetting and barring should be a priority area
    - A plan to rationalise the number of channels for international criminality information to flow in and out of the UK, address any timeliness issues, and increase staff awareness of the UK's obligations and the opportunities available to it
    - A plan to provide training and guidance explicitly covering international issues for staff across the public protection network
    - The development of options for the future structure and governance of international criminality information exchange

16. Police forces, individually and collectively, and other PPN organisations should nominate a lead official for international criminality information issues (links to Governance) and the resulting network should be maintained by the Implementation Team.

17. The Implementation Team should ensure that all international proposals on the management of criminality information, whether from the UK or elsewhere, are evaluated by a combination of international experts, senior policy makers with an interest and those key delivery organisations who would be affected or required to put them into effect. The agreed position should be re-visited periodically, as negotiations progress.

18. Subject to reaching agreement with Jersey, Guernsey and the Isle of Man, the earliest opportunity should be taken to bring them within the CRB regime.

Technology

19. A full review should be undertaken of IT systems as they relate to criminality information management, drawing on the expertise of the NPIA and the Home Office Chief Information Officer (CIO), with others including the Government CIO and the MoJ CIO where appropriate, to address any duplications, inter-operability issues and overlaps.

20. Each CIO should consider as a matter of urgency giving effect to any simple tactical IT fixes that will support my recommendations elsewhere on improving criminality information management.

21. Building on the governance, processes, standards and architectures that will flow from my recommendations elsewhere to facilitate information sharing, increasing IT integration should be an objective and programmes that increase information sharing should be accorded a degree of priority.

22. Looking to future requirements, all IT developments in the sphere of criminality information should pass through an assessment process of the kind set out in my first Investment recommendation. This process should explicitly address use and reuse of IT capacity, making the maximum use of existing technology.

23. There should be better engagement between the organisations in the PPN with IT suppliers so that they understand priorities and respond to the need for processes and IT systems to be able to share criminality information across departments and agencies. This should help to ensure their understanding of the cross-cutting requirements of the public protection network, and to encourage their active help and expertise in making suggestions as to how re-usability can be achieved, instead of building fresh systems.

24. By Spring 2009, ACPO working with NPIA and stakeholders should clarify the governance of PNC and develop a clear and agreed approach in the light of the issues this report identifies as to who in which organisations should have what access to the police national computer. (This links to one of the early practical steps regarding CCD access to PNC and to the recent joint Inspectorate report on the Peart / Joseph case which recommends that prisons should have direct access to PNC.) The long-running dispute about funding of the link to Northern Ireland should have been resolved.

25. The SROs for the remaining Bichard recommendations should urgently re-consider the timetables for implementation with a view to expediting them. I expect to see greater progress when I revisit these issues in early 2009, and in particular to see that the court resulting recommendation will be fully implemented by April 2009.

At the Front-Line

Many examples of good practice already exist within the main front-line processes specific to existing agencies. General recommendations in this area across the whole PPN are unlikely to be helpful but the detailed suggestions (in the table at the end of the At the Front Line Chapter) can be summarised as follows:

26. Where justified by the risk to the public, proffered identification should be checked against relevant databases, and relevant information sought at each decision point as offenders move through the criminal justice system.

27. Clear accountability and standard procedures should be developed to manage storage and access to all key PPN information.

28. Where information sharing is both necessary and proportionate to support effective public protection, arrangements should be systematic, proactive and accountability clear.

29. Clear frameworks should be developed for decision making on individual cases appropriate to the staff member taking the decision, and indicating clear escalation paths where required.

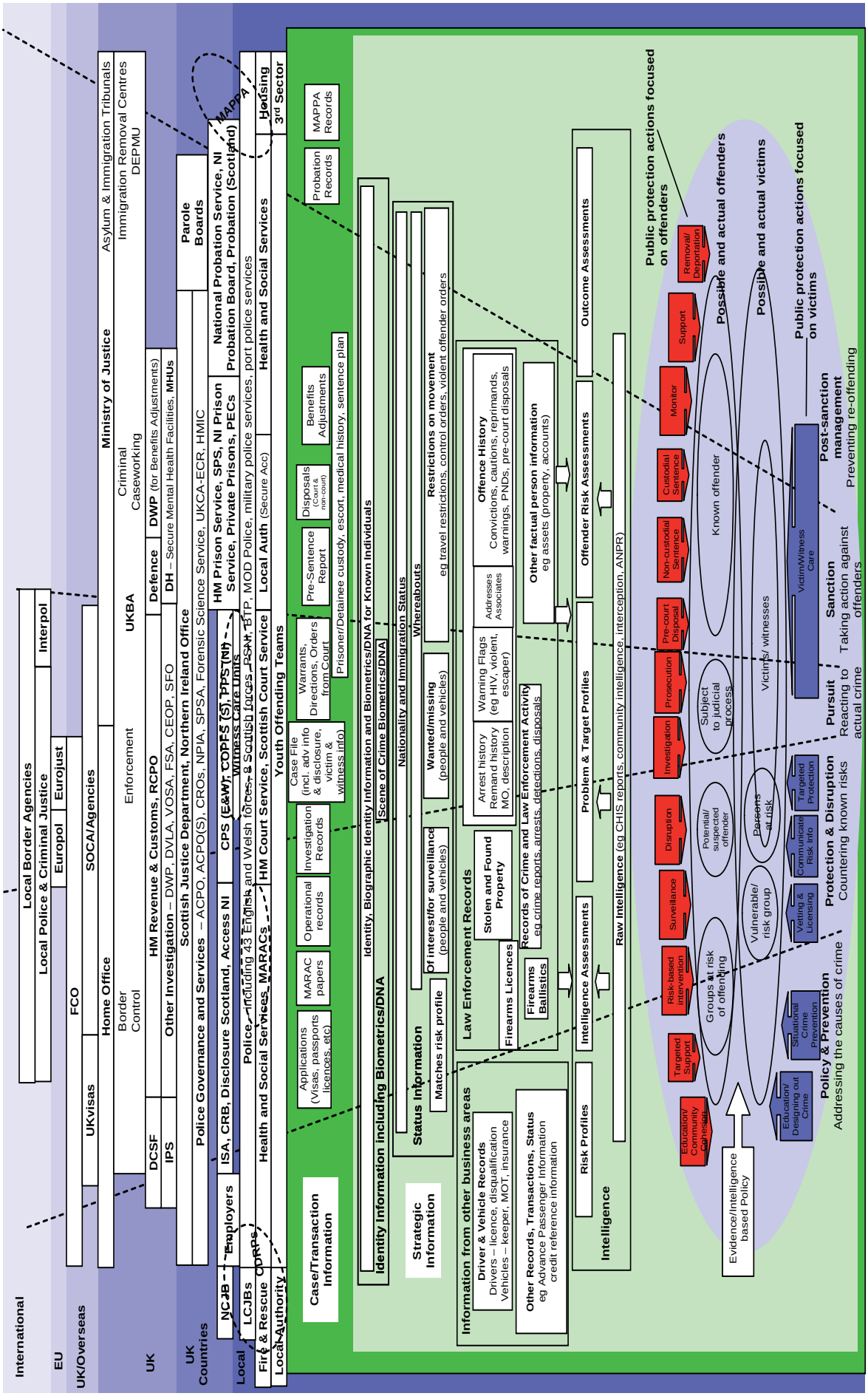
For each overall recommendation there are early practical steps and longer term action to improve information management practices as part of core front-line processes and decisions.

The Future

30. Horizon scanning should be undertaken (on a regular basis) by the proposed Commission for Public Protection Information. (This links to the Governance recommendation)

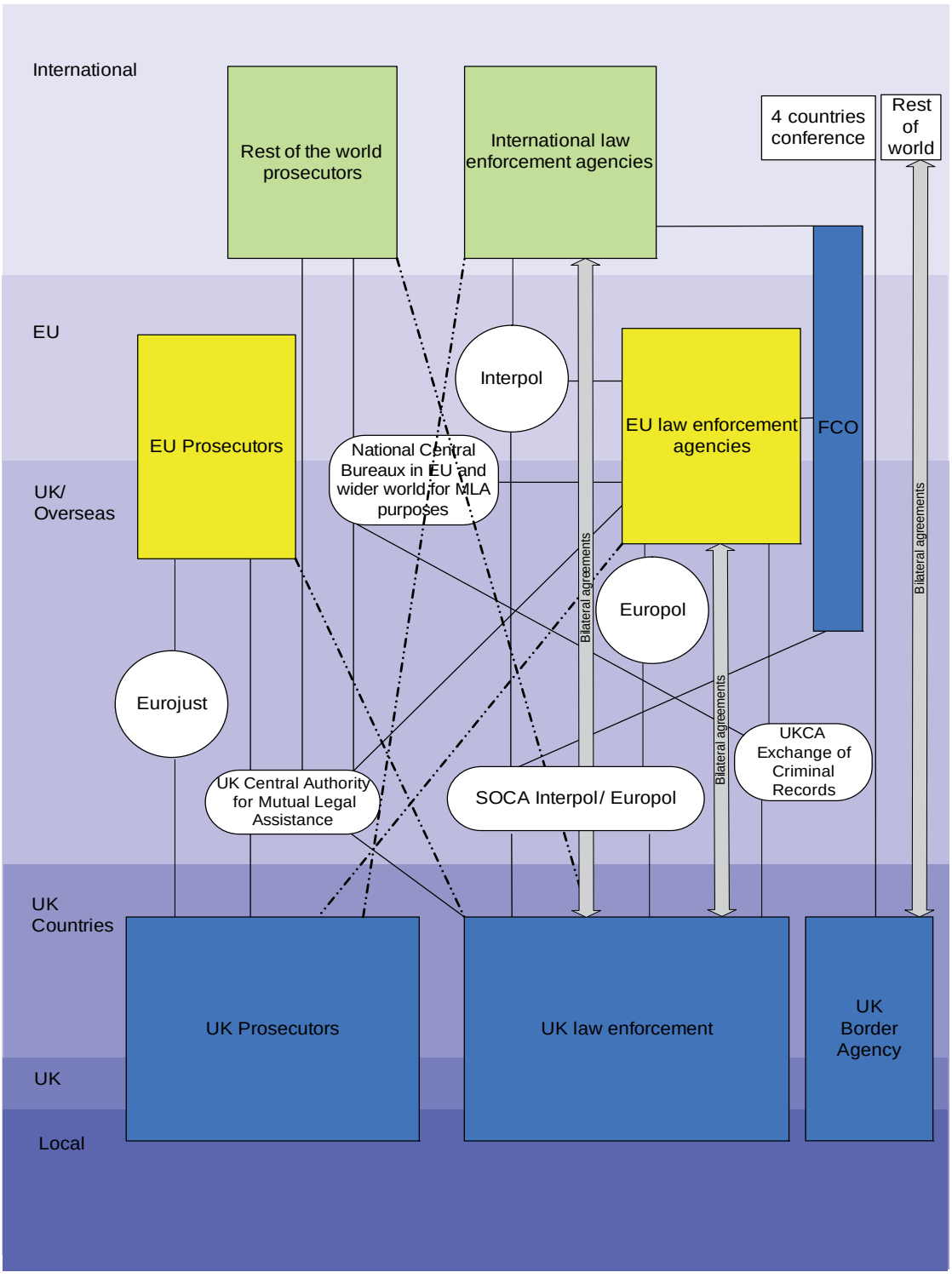
31. Ministers should lead a public debate about the DNA database, and the use of biometrics more widely, to help improve public understanding and confidence.

Annex C: Public Protection Mapping



C I. Public Protection Network map

C. II. International criminality information system flows, including bilateral and ad hoc arrangements



Annex D: Glossary of terms

UK Databases, Structures and Initiatives

ACPO DNA Handbook	The ACPO DNA Good Practice Manual provides operational guidance in using DNA for the detection and prosecution of offenders. It sets out current good practice so that police in every force can use the technology successfully to solve crimes and gather criminal intelligence.
ANPR	Automatic Number Plate Recognition is an established technology that allows vehicles observed by camera to have their vehicle registration mark "read" using pattern recognition software.
Bichard Inquiry	Sir Michael Bichard's Review and recommendations following the Soham murders.
Biometric Visas	Visas issued which record the applicant's fingerprint.
Biometrics	Biometrics is the technical analysis of biological data, such as fingerprints, to confirm identity.
CHIS Reports	Covert human intelligence sources are essentially people who are members of or act on behalf of one of the intelligence services to obtain information from people who do not know that this information will reach the intelligence service; reports are produced to provide such information to intelligence services.
C-NOMIS	The National Offender Management Information System provides central end-to-end offender management.

Commission for Public Protection Information	The proposed Commission for Public Protection Information should be set up as a body to champion efficient and appropriate criminality information management across the PPN.
COMPASS CMS	COMPASS CMS is a national case management system and management information system in use across the CPS.
CREST	Crown Court Electronic Support is an IT support Courts' case management system in the Crown Court. XHIBIT is providing a more accessible front end to this system for court staff.
Crime and Disorder Reduction Partnership	The 1998 Crime and Disorder Act established partnerships between the police, local authorities, probation service, health authorities, the voluntary sector, and local residents and businesses.
Criminal Injuries Compensation Board	The Criminal Injuries Compensation Board was set up in 1964 (CICB) to administer compensation throughout Great Britain on the basis of common law damages to victims of a crime of violence. In 1996 the Criminal Injuries Compensation Authority (CICA) was established to administer the tariff based scheme which came into effect for all applications received on or after 1 April 1996. The staff of the Board became the staff of the Authority at that time. The CICB ceased to exist after 31 March 2000 when all applications under consideration transferred to the CICA.
Criminal Justice Information Technology	The Criminal Justice System Information Technology (CJS IT) Programme harnesses new and existing systems in the Criminal Justice System so Criminal Justice professionals in the different Government CJS agencies – as well as independent practitioners such as lawyers and victim and witness organisations – can work more closely together, in particular managing cases more effectively across the CJS as a whole.
CRO	Criminal Records Offices exist in various forms at national and police force level to assist in managing and facilitating the use of criminal records.

Cross-Departmental Public Service Agreement	PSAs set out the key priority outcomes the Government wants to achieve in the next spending period. They play a vital role in galvanising public service delivery and driving major improvements in outcomes.
C-SIS	Central Schengen Information System was developed as one of the main ways to facilitate police and judicial co-operation and exchange a common set of information in order to combat exploitation of the EU travel area.
Data Sharing Review	In December 2007 the Prime Minister commissioned Richard Thomas, the Information Commissioner and Dr Mark Walport, of the Wellcome Trust, to undertake a review of the use and sharing of personal information in the public and private sectors.
DHI	The Drug Harm Index is an amalgamation of individual harm indicators, weighted according to their economic impact to allow year-on-year comparisons of the harm caused by drugs.
DNA Database	The National DNA Database contains samples taken from persons in police detention or custody who have been charged with or told they will be reported for committing a "recordable offence" (an offence subject to a term of imprisonment), and from persons convicted of a recordable offence.
e-Borders	The main purpose of the e-borders programme is to collect and analyse passenger and crew data provided by carriers (air, sea and rail), in respect of all journeys to and from the United Kingdom in advance of their travel, supporting an intelligence-led approach to operating border controls.
Forensic Science Advisory Council	The FSAC is to advise and support the Forensic Science Regulator across a wide range of issues relevant to quality standards in forensic science.
Forensic Science Regulator	The Regulator is a public appointee whose function is to ensure that the provision of forensic science services across the criminal justice system is subject to an appropriate regime of scientific quality standards.

IDENT1	Formerly NAFIS (National Automated Fingerprint Identification System), IDENT1 is used to match and identify fingerprints.
IMPACT Programme	Led by the NPIA and ACPO, the IMPACT (information, management, prioritisation, analysis, co-ordination, and tasking of intelligence) Programme is delivering several of the recommendations in Sir Michael Bichard's report.
INI	IMPACT Nominal Index is a basic index of people and intelligence appearing in police records.
Interim Police Local Exchange (iPLX)	An easily searchable index of all those on whom any police force holds information.
Knowledge Network (KN)	Knowledge Network is a cross-government project whose work helps to improve and simplify the electronic delivery and sharing of information.
Lantern	This is a pilot scheme testing mobile fingerprinting equipment linked to IDENT1 in real time.
Learning and Skills Council (LSC)	The LSC aims to improve the skills of England's young people and adults to ensure that the UK has a workforce of world-class standard.
LIBRA	The LIBRA project is intended to replace the magistrates' courts' existing information technology systems with a single, modern, national infrastructure and case and accounts management system.
List 99	List 99 contains the names, dates of birth, and teacher reference numbers of people whose employment has been barred or restricted, either on grounds of misconduct or on medical grounds.
Livescan	This is digital fingerprinting in custody suites, linked to IDENT1.

Local Strategic Partnerships (LSPs)	LSPs are non-statutory, multi-agency partnerships, which match local authority boundaries. LSPs bring together at a local level the different parts of the public, private, community and voluntary sectors; allowing different initiatives and services to support one another so that they can work together more effectively.
MAC	The Migration Advisory Committee
MAPPA	Multi-Agency Public Protection Arrangements. The aim of MAPPA is to ensure that a risk management plan, drawn up for the most serious offenders, benefits from the information, skills, and resources provided by the individual agencies being co-ordinated through MAPPA.
MARAC	Multi-Agency Risk Assessment Conference provides a platform for local agencies to meet to discuss the highest risk victims of domestic violence in their area. Information about the risks faced by those victims, the actions needed to ensure safety, and the resources available locally is shared and used to create a risk management plan involving all agencies. The aim of the MARAC is to increase the safety, health and wellbeing of the victim – adults and any children.
PNC	Police National Computer

UK Organisations, Agencies and Departments

Access NI	ACCESS NI is a new system for the disclosure of an individual's criminal history. It is being established by the Northern Ireland Office as a result of the introduction in N. Ireland of Part V of the Police Act 1997 and will replace the current system operated by the Police Service of Northern Ireland.
ACPO	Association of Chief Police Officers is an independent, professionally – led strategic body. In the public interest and in equal and active partnership with Government and the Association of Police Authorities, ACPO leads and coordinates the direction and development of the police ser-vice in England, Wales, and Northern Ireland.
ACRO	The ACPO Criminal Records Office carries out a range of functions relating to criminal records on behalf of police forces and in partnership with Government and other organisations.
AG	Attorney General (The Attorney General and Solicitor General (the Law Officers) are the chief legal advisers to the Government and are responsible for all crown litigation. They have overall responsibility for the work of: Treasury Solicitors Department, Crown Prosecution Service, Serious Fraud Office, Revenue and Customs Prosecution Office and Her Majesty's Crown Prosecution Service Inspectorate).
AIT	A tribunal that hears appeals against decisions made by the Home Secretary and officials in asylum, immigration and nationality matters.
APA	Association of Police Authorities is "the national voice for police authorities in England, Wales, and Northern Ireland".

BCU	A Basic Command Unit (BCU) is the largest unit into which territorial British Police forces are divided. This may actually be called a BCU or may have another designation, such as Division or Area.Most forces are divided into at least three BCUs and some have many more. Most BCUs are further subdivided into smaller units. The BCU is usually commanded by a Chief Superintendent.
BTP	British Transport Police is the national police force for the railways, providing a policing service to rail operators, their staff, and passengers throughout England, Wales, and Scotland.
Cabinet Office	The Cabinet Office coordinates policy and strategy across Government Departments. The Department's three core functions are: Supporting the Prime Minister; Supporting the Cabinet; and Strengthening the Civil Service.
CCD	Criminal Casework Directorate (CCD) operates under the Home Office and UKBA and aims, subject to international obligations, to deport from the UK all foreign nationals who commit serious criminal offences
CDRPs	Responsible authorities have a statutory duty to work with other local agencies and organisations to develop and implement strategies to tackle crime and disorder including anti-social and other behaviour adversely affecting the local environment as well as the misuse of drugs in their area. (s6, Crime and Disorder Act 1998 as amended by s97 & s98 Police Reform Act 2002 and s1, Clean Neighbourhoods & Environment Act 2005). These statutory partnerships are known as Crime and Disorder Reduction Partnerships (CDRPs) or Community Safety Partnerships (CSPs) in Wales.
CEOP	The Child Exploitation and Online Protection (CEOP) Centre is part of UK police and is dedicated to protecting children from sexual abuse.

CIO	The role of the Chief Information Officer (CIO) was established in the Home Office to lead the strategic development of information systems (IS) and information technology (IT) across the Home Office.
CJIT	Criminal Justice Information Technology
COPFS	Crown Office and Procurator Fiscal Service is Scotland's sole public prosecution commission. In addition to prosecuting crimes in District, Sheriff, and High Courts, the Service is also involved in enquiries into sudden and suspicious deaths. On a day-to-day basis, staff are also involved with local criminal justice partners working in their communities.
CPS	Crown Prosecution Service
CRB	The Criminal Records Bureau is an Executive Agency of the Home Office and provides wider access to criminal record information through its Disclosure service, enabling employers to make informed decisions when recruiting.
CRCSG	Crime Reduction and Community Safety Group is one Directorate of the Home Office. It contributes to all the Home Office's strategic objectives and has lead responsibility for: help people feel safer in their homes and local communities; cut crime, especially violent, drug and alcohol related crime; and support visible, responsive and accountable policing.
Criminal Justice and Offender Management Directorate	The Criminal Justice and Offender Management Strategy in the Ministry of Justice sets the strategic direction for offender management and regulates the increasingly diverse range of providers and work with the judiciary on the proposals for a Sentencing Commission.

CTO (Chief Technology Officer)	The role of the Chief Technology Officer is to lead on development, management and use of the Home Office enterprise architecture framework including the development of group IST strategy and the development of high level design authority for Home Office IT including shared services.
DCLG	Is now Communities and Local Government
DCSF	Department for Children, Schools, and Families
DEPMU	Detention Escort Population Management is a part of the Home Office which decides whether or not offenders remain in prison or be transferred to a detention centre prior to deportation.
DfT	The Department for Transport is responsible for transport issues (except when devolved), in particular railway franchising and a range of executive agencies.
DH	Department of Health
Disclosure Scotland	Disclosure Scotland is currently a service provided by Scottish Ministers to manage and operate the Disclosure service in Scotland as provided for in Part V of the Police Act 1997. From October 2007, Disclosure Scotland will form part of a (shadow) Scottish Government agency which will plan, manage, and operate the new vetting and barring service as provided for in the Protection of Vulnerable Groups (Scotland) Act 2007.
DIUS	Department for Innovation, Universities and Skills
DVANI	Northern Ireland Driver Vehicle Agency

DVLA	The Driver and Vehicle Licensing Agency is an Executive Agency of the Department for Transport (DfT). The Agency's primary aims are to facilitate road safety and general law enforcement by maintaining registers of drivers and vehicles and to collect vehicle excise duty (car tax).
DWP	Department for Work and Pensions
FCO	Foreign Commonwealth Office
FSA	Financial Services Authority
FSS	Forensic Science Service is designed to meet the needs of specific police investigation using scientific techniques. FSS is a trading name of Forensic Science Service Ltd., which is a UK Government-owned company (GovCo).
HM Crown Prosecution Service Inspectorate (HMCPSI)	HMCPSI is the independent Inspectorate for the Crown Prosecution Service (CPS), the principal prosecuting authority for criminal cases in England and Wales.
HMCS	Her Majesty's Courts Service is an executive agency of the Ministry of Justice that is responsible for the England and Wales courts system.
HMIC	Her Majesty's Inspectorate of Constabulary
HMICA	Her Majesty's Inspectorate of Court Administration
HMIE	Her Majesty's Inspectorate of Education
HMIP	Her Majesty's Inspectorate of Prisons
HMRC	Her Majesty's Revenue and Customs

HMPS	Her Majesty's Prison Service
HMT	Her Majesty's Treasury
Home Office (HO)	The Home Office is the Government Department responsible for leading the national effort to protect the public from terrorism, crime and anti-social behaviour.
Home Office CIO	The Home Office Chief Information Officer
Immigration Removal Centres (IRCs)	IRCs house those who are about to be removed from the country.
Information Commissioner's Office	The Information Commissioner's Office is the UK's independent authority set up to promote access to official information and to protect personal information.
Intelligence Services	The Security Service, Government Communications HQ, and The Secret Intelligence Service.
Investment Boards	Investment Boards advise public bodies on investment activities and monitor their performance.
IPS	The Identity and Passport Service is an Executive Agency of the Home Office which currently provides passport services and in the future will provide ID cards for British and Irish nationals resident in the UK. Foreign nationals resident in the UK will also be included by linking the scheme to biometric immigration documents.
ISA	The Independent Safeguarding Authority was previously known as the Independent Barring Board and will be the new non-departmental public body to be created to take consistent expert decisions as to who should be included in the new lists of people who will be barred from working with children and / or vulnerable adults.

JBOC	The Joint Borders Operations Centre is responsible for providing detailed information to border agencies about passengers who are suspected of crime or who are of other interest to the PPN agencies.
LCJBs	Local Criminal Justice Boards. At a local level, the work of the Criminal Justice System agencies is co-ordinated by 42 LCJBs across England and Wales. These boards bring together the chief officers of the CJS agencies to co-ordinate activity and share responsibility for delivering criminal justice in their areas.
Liberty	An independent human rights organisation which works to defend and extend rights and freedoms in England and Wales.
LSC	Legal Services Commission
MHU	Mental Health Unit
MOD Police	Ministry of Defence Police is a specialised police force that operates within Britain's defence community.
MoJ	Ministry of Justice
MoJ CIO	Ministry of Justice Chief Information Officer
NCJB	The National Criminal Justice Board is responsible for supporting local boards to bring more offences to justice and to improve public confidence. It also is responsible for supporting local boards and co-ordinating work across the whole criminal justice system.
NDPB	Non-Departmental Government Body

NIO	The Northern Ireland Office has responsibility for Northern Ireland's constitutional and security issues, in particular, law and order, political affairs, policing, and criminal justice.
NIPS	NI Prison Service
NOMS	The National Offender Management Service aims to protect the public; transform the way offenders are punished and managed; reduce re-offending; and cut crime.
NPIA	The National Policing Improvement Agency aims to support the police service by providing expertise in areas as diverse as information and communications technology, support to information and intelligence sharing, core police processes, managing change and recruiting, and developing and deploying people.
OSCT	Office for Security and Counter Terrorism
OCJR	Office of Criminal Justice Reform
Police Authorities	A police authority is an independent body made up of local people. The police authority's job is to make sure that police forces are efficient and effective. There is a police authority for each local police force – 43 in all in England and Wales – plus an additional one for British Transport Police. In Northern Ireland the police authority is called the Policing Board but it has a similar role to police authorities in England and Wales.
PPS (NI)	The Public Prosecution Service for Northern Ireland is established by the commencement of the Justice (NI) Act 2002. The Act defines the Public Prosecution Service, its statutory duties and commitments, and the legislative framework within which it provides its services. PPS is designed to incorporate good practice on a national and international basis.

PPU	Each police force has a Public Protection Unit – a specialist unit of highly trained detectives and constables responsible for the management and investigation of crimes involving adult abuse, child abuse, domestic abuse, sex and dangerous offenders and vulnerable and intimidated witnesses.
PBNI	Probation Board of NI
Probation Trusts	Six probation trusts started work as part of the government's drive to further reduce re-offending and increase protection for the public. Trust status, introduced through the Offender Management Act 2007, allows probation services more independence to focus their work on local communities and reduce re-offending while providing the same high level of service to the courts and oversight of offenders.
PSA	Police Superintendents Association
PSNI	Police Service of Northern Ireland. The PSNI was formerly the Royal Ulster Constabulary.
NASUWT	National Association of Schoolmasters Union of Women Teachers
NSPCC	National Society for the Prevention of Cruelty to Children
ROCI	Review of Criminality Information
SANE	National charity for Mental Health
SCDEA	Scottish Crime and Drugs Enforcement Agency
SIA	Security Industry Authority manage the licensing of the private security industry as set out in the Private Security Industry Act 2001.

SID	Scottish Intelligence Database was fully launched in 2003. It is a system for all the forces and agencies to share their intelligence data and open up force boundaries.
SOCA	The Serious Organised Crime Agency is an Executive Non-Departmental Public Body sponsored by, but operationally independent from, the Home Office. The Agency has been formed from the amalgamation of the National Crime Squad (NCS), National Criminal Intelligence Service (NCIS), that part of HM Revenue and Customs (HMRC) dealing with drug trafficking and associated criminal finance, and a part of UK Immigration dealing with organised immigration crime (UKIS).
SS	Security Services
SPSA	The Scottish Police Services Authority provides expert policing and support services to the country's eight police forces and criminal justice community.
UKBA	The UK Border Agency is a shadow agency of the Home Office. The Agency was formed in April 2008 to improve the United Kingdoms's security through stronger border protection whilst welcoming legitimate travellers and trade. The Agency brings together the work previously carried out by the Border and Immigration Agency, Customs detection work at the border from Her Majesty's Revenue and Customs (HMRC) and UK Visa Services from the Foreign and Commonwealth Office (FCO).
UKCA-ECR	The UK Central Authority for the Exchange of Criminal Records deals with notifications of UK citizens convicted abroad and transmitting details relating to foreign citizens convicted here to their home countries. UKCA-ECR also deals with both incoming and outgoing requests for the exchange of criminal records information. It is based within ACRO.
Victim Support	Victim Support is the independent charity which helps people cope with the effects of crime.

VOSA	The Vehicle and Operator Services Agency provides a range of licensing, testing, and enforcement services with the aim of improving the roadworthiness standards of vehicles, ensuring the compliance of operators and drivers, and supporting the independent Traffic Commissioners.
Wellcome Trust	Medical research charity funding research into human and animal health.
YJB	The Youth Justice Board for England and Wales (YJB) is an executive non-departmental public body. Twelve board members are appointed by the Secretary of State for Justice. The YJB oversees the youth justice system in England and Wales and works to prevent offending and re-offending by children and young people under the age of 18, and to ensure that custody for them is safe, secure and addresses the causes of their offending behaviour.
YOTs	Youth Offending Teams are the main vehicle by which the principal aim of the youth justice system, as set out in section 37 of the Crime and Disorder Act 1998 (to prevent offending by children and young people aged 10 to 17) is delivered, through co-ordinated work at a local level.

UK Legislation

Arrest Summon Notification	The Arrest Summons Notification is generated by the PNC for every arrest or summons that occurs. The ASN identifies a specific individual arrested or summonsed for a specific case; it is a unique identifier and the principle means of identifying a defendant within a case.
Criminal Justice and Police Act 2001	The Act makes provision for combating crime and disorder; about the disclosure of information relating to criminal matters and about powers of search and seizure; to amend the Police and Criminal Evidence Act 1984, the Police and Criminal Evidence (Northern Ireland) Order 1989 and the Terrorism Act 2000; to make provision about the police, the National Criminal Intelligence Service and the National Crime Squad; about the powers of the courts in relation to criminal matters; and for connected purposes.
Data Protection Registrar	The 1984 Data Protection Act makes provision for a Data Protection Registrar. By virtue of the 1998 Data Protection Act, this became the Data Protection Commissioner. With the coming into force of certain provisions in the Freedom of Information Act 2000, the Data Protection Commissioner became the Information Commissioner.
Data Protection Act 1998	The Data Protection Act requires anyone who handles personal information to comply with a number of important principles. It also gives individuals rights over their personal information.

International Databases, Structures, and Initiatives

EEA	European Economic Area came into being on January 1, 1994 following an agreement between member states of European Free Trade Association (EFTA), the European Community (EC), and all member states of the European Union (EU). It allows these EFTA countries to participate in the European Single Market without joining the EU.
Four Countries Conference	The Four Countries Conference consists of the UK, USA, Canada and Australia who share data on failed asylum seekers, failed visa applicants, absconder cases, and "legacy" asylum cases (where failed applicants have remained in the country for several years).
Interpol STLD	The Stolen and Lost Travel Documents Database was launched in June 2002, in response to identification of link between terrorist activity and stolen passports. It stores data from 93 countries and UN Mission in Kosovo, more than 15m records. National Police Services can access the database through Interpol's National Central Bureaux.
MLA	Mutual Legal Assistance is the formal way in which countries obtain evidence located in one country to assist in criminal investigations or proceedings in another country.

SIS

The Schengen Information System allows the competent authorities in the Member States to obtain information regarding certain categories of persons and property. The SIS is a computer system designed to allow police officers access to alerts issued by member states in respect of persons, vehicles and objects. It includes details of wanted and suspected persons; missing and vulnerable persons; persons whose activities pose a threat to national security or public order; stolen vehicles; stolen, lost and suspect documents; counterfeit and stolen banknotes; and stolen firearms.

In addition, it is used as the main information system to carry data which relates to immigration and asylum issues (ie, Article 96 data). This exchange of data is necessary to support the Schengen External Border policy, which the UK is not applying to join. The UK will therefore not have access to this particular category of data.

SIS II

Schengen Information System II is the successor to SIS I, updated to include more Member States. The 10 new Member States will connect directly to SIS II, as will the UK which is not currently connected to SIS.

International Organisations, Agencies and Departments

Eurojust	Eurojust is a European body established to enhance the effectiveness of the competent authorities within Member States when they are dealing with the investigation and prosecution of serious cross-border and organised crime. It is composed of national prosecutors, magistrates or police officers of equivalent competence from Member States.
Europol	Europol is the European Law Enforcement Organisation which aims at improving the effectiveness and co-operation of the competent authorities in the Member States in preventing and combating terrorism, unlawful drug trafficking, and other serious forms of international organised crime.
Interpol	Interpol is the world's largest international police organisation, with 186 member countries. Created in 1923, it facilitates cross-border police co-operation and supports and assists all organisations, authorities and services whose mission is to prevent or combat international crime.
SCCOPOL	La Section Centrale de Coopération Opérationnelle de Police

International Legislation and Conventions

Council of Europe Convention	1959 European Convention on Mutual Assistance in Criminal Matters. Article 22 of the convention requires member countries to exchange information about the convictions of their citizens in each other's states.
European Arrest Warrant	A European Arrest Warrant, valid throughout the European Union, has replaced extradition procedures between Member States. It may be issued by a national issuing judicial authority if the person whose return is sought is accused of an offence for which the maximum period of the penalty is at least a year in prison, or if he or she has been sentenced to a prison term of at least four months.
Prüm Convention	An international police co-operation agreement signed by Belgium, Germany, Spain, France, Luxembourg, the Netherlands and Austria on 27 May 2005, which has now become part of the legislative framework of the European Union and will be implemented in all Member States. It provides for designated contact points within the law enforcement agencies in the Member States to have mutual access to each other's DNA, fingerprint, and vehicle registration information systems, for serious crime purposes. The EU (including the UK) has agreed to implement by 2010. It is already operationally used in Germany and Austria to solve long-standing (high profile) cases.

Annex E: The legislative framework

This legal summary has been provided by the Ministry of Justice.

Sharing data across public services can be a complex process; there is no single source of law regulating a public body's power to collect, use, and share personal data. Rather, a range of express and implied statutory provisions powers as well as common law powers govern data sharing, and public bodies often need specialist legal advice to assess whether data sharing is permissible.

Administrative Law

Before a public body can engage in data sharing, it must first establish whether it has a legal right or power (vires) to share the data in question. Administrative law is the area of law that regulates the activities of public bodies. Where a public body acts outside of their powers, their activities can be brought before the courts by way of a judicial review. The jurisdiction of the court is regarded as supervisory and as such will generally limit its review of the public body's decision to the following considerations:

- Legality – Whether the decision falls within the remit of the public body's powers
- Rationality – Whether the activity was a rational means of achieving a stated aim
- Procedural propriety – Whether the public body acted in line with procedure when carrying out an activity

However, in cases where there are questions involving the European Convention on Human Rights, the courts will pay much closer attention to the merits of the decision.

For the purpose of data sharing, the review of the "legality" of a public body decision is the most relevant. The doctrine of "illegality" states that a public body may not act in excess of its powers. If it does, then the act is considered to be ultra vires and therefore unlawful.

Types of Government Bodies

Bodies exercising a public function are subject to legal controls. These bodies include Government Departments, local authorities, the police, the armed forces, the courts, and numerous non-departmental government bodies.

The nature of the body, and the rules that govern its activities, will play a crucial part in determining the legal basis upon which it acts and whether its activities are lawful. If a public body does not have the power or vires to collect, use, or share data, it will be acting unlawfully, and the fact that an individual may have consented would not make the activity lawful.

Government departments fall into two categories:

- Those that are headed by a Crown Minister such as the Treasury, the Home Office, the Department for Work and Pensions, the Department for Education and Skills, and the Department for Constitutional Affairs
- Those that are created by statute and are not headed by a Minister, such as Her Majesty's Revenue and Customs

Departments headed by a Crown Minister derive all of their powers, including the powers to collect, use and share data, from the following sources:

- Express statutory powers (powers that explicitly confer a power to share data)
- Implied statutory powers (the power to share is implied from a power to do something else)
- Prerogative and common law powers

Non-ministerial bodies or those created by statute do not have common law or prerogative powers. Any data sharing by them must be based on statutory powers (express or implied).

Statutory Powers

Express statutory powers, also referred to as "gateways", can be enacted to provide for disclosure of data for particular purposes. Such gateways may be permissive or mandatory. A permissive gateway describes legislation that gives a public body the power to share data, for example, Section 115 of the Crime and Disorder Act 1998. A mandatory gateway makes it obligatory for a public body to share data when requested. An example of this is Section 17 of the Criminal Appeals Act 1995.

Implied Powers

Even if there is no express statutory power to share data, it may still be possible to imply such a power.[1] To this end, where the actions or decisions of a public body are incidental to meeting the requirements of an expressed power or obligation, they can be considered to have an implied right or power to act.

Many activities of statutory bodies will be carried out on the basis of implied statutory powers. This is particularly so in relation to activities such as data collection and sharing that are not always express statutory functions.

In order to imply a power to share data, the body in question must first of all be satisfied that it has the vires to carry out the basic function, to which the sharing of data is ancillary. Without the power to do the activity there can be no implicit power to share data.

A public body sharing data under an implied power must also take account of relevant conflicting statutory provisions that may prohibit the proposed sharing (either expressly or implicitly). Similar considerations should also apply when a body is collecting data. A body should also consider whether the collection of the data is reasonably incidental to existing statutory powers (whether it is reasonable to accept that this activity is necessary and associated with their existing powers).

Common Law Powers

Where there is no express or implied statutory power to share data, Government departments headed by a Minister of the Crown may be able to rely on common law or prerogative powers to share data. The general position is that the Crown has ordinary common law powers to do whatever a natural person may do (unless this power has been taken away by statute). This principle is called the “Ram Doctrine”.

1 This point was established in A-G v Great Eastern Railway Co (1880) 5 App Cas 473 Lord Selborne LC in dealing with the doctrine of ultra vires:
“…this doctrine ought to be reasonable, and not unreasonably, understood and applied, and that whatever may be fairly regarded as incidental to, or consequential upon, those things which the Legislature has authorised, ought not (unless expressly prohibited) to be held, by judicial construction, to be ultra vires.”

Prerogative Powers

In addition to common law powers, the Crown also has prerogative powers. There is no single accepted definition of the prerogative. They are often seen as the residual powers of the Crown, which allow the executive to carry out any lawful functions without the use of statute.[2] There are several residual powers, for example, powers relating to foreign affairs, defence, and mercy. However, Parliament can override and replace prerogative by statute, where individual circumstances make that appropriate.

Data sharing under prerogative or common law has not often been considered by the courts, so there is an element of risk involved. The degree of risk involved would depend on the facts, particularly the nature of the data proposed to be collected and disclosed, the purposes for which it was to be collected and disclosed, and the identity of the bodies acting as recipients.

Public bodies like HMRC which have powers conferred on them by statute have no powers under the common law or the Crown prerogative and must rely solely on their express or implied statutory powers.

Local Authorities

Local authorities, like non-ministerial Government departments, are creatures of statute. As such, they can only reply on express or implied statutory powers and, therefore, similar considerations to those outlined above will apply. Of particular relevance to local government are the following statutory powers:

- Section 111 (1) of the Local Government Act 1972 that provides a local authority "shall have power to do anything…which is calculated to facilitate, or is conducive or incidental to, the discharge of any of their statutory functions"
- Section 2(1) of the Local Government Act 2000 that provides that a local authority shall "have power to do anything which they consider is likely to achieve any one or more of the following objects (a) the promotion or improvement of the economic well-being of their area; (b) the promotion or improvement of the social well-being of their area; (c) the promotion or improvement of their environmental well-being of their area"

2 See A.V. Dicery; Introduction to the Study of the Law of the Constitution (1898)

Other Public Authorities

Besides central Government Departments and local authorities there are, of course, numerous other public bodies that derive their powers from statute or from common law. For example, the Welsh National Assembly that derives its powers from statute and non-departmental government bodies like the Legal Services Commission. In relation to these bodies, careful consideration should be given to the particular statutory regime that might govern the activities of the particular body in determining whether or not there might be express or implied power to collect, use and share data.

What Happens Next?

Once vires has been established, a public body must then consider whether the proposed data sharing complies with the Data Protection Act 1998 and Human Rights Act 1998 and whether it could breach the common law tort of confidentiality.

Data Protection Act

The Data Protection Act 1998 (DPA), which updated the Data Protection Act 1984, is governed by EC Directive 95 / 46 / EC. The DPA regulates the collection, use and distribution of personal data. Personal data is defined in section 1 at some length, but it broadly means any data which relate to a living individual who can be identified from those data. The DPA controls the processing of personal data and provides enforceable safeguards to protect privacy rights through eight key principles. These stipulate that personal data shall be:

- Processed fairly and lawfully
- Obtained only for one or more specified and lawful purposes
- Adequate, relevant, and not excessive in relation to the purpose / s for which they are processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purpose or purposes under which data are collected
- Processed in accordance with the rights of data subjects under the DPA
- Subject to appropriate technical and organisational measures to guard against unauthorised or unlawful processing and against accidental loss, destruction, or damage
- Not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection of the rights and freedoms of data subjects in relation to the processing of personal data

The DPA also provides data subjects with rights and responsibilities and requires all data controllers to register with the Information Commissioner, an independent statutory office which is responsible to Parliament for regulating the DPA.

Human Rights Act

The Human Rights Act 1998 can also impact on data-sharing activities. Following are the key aspects:

- All legislation must be interpreted so far as is possible to do so to be compatible with the Convention on Human Rights (ECHR) (section 3(i)
- It is unlawful for a public body to act in a way that is incompatible with ECHR rights (section 6)
- All courts and tribunals are required to take account of relevant decisions of the European Court of Human Rights, and to have regard to the opinions and decisions of the Commission (section 2)
- Higher courts may make a decision of incompatibility in respect of incompatible primary legislation, and in certain circumstances, of secondary legislation. Such declarations do not, however, change the law. That is for Parliament to do, if it so wishes (section 4)

Article 8 of the ECHR is of particular importance in the context of data sharing and privacy. This provides that persons have the right to respect for their private and family life, their home, and their correspondence. Interference with this right by a public body will need to be justified by being in accordance with the law, in the pursuit of a legitimate aim, and necessary in a democratic society. Current understanding is that compliance with the DPA and the common law of confidentiality should satisfy Human Rights requirements.

Common Law Breach of Confidence

A public body must ensure that a common law breach of confidence action will not arise as a result of data sharing. A breach of confidence occurs when information carrying the necessary quality of confidence is communicated in circumstances entailing an obligation of confidence, and the information is later used in an unauthorised way.

Annex F: List of those consulted

Name	Job Title & Organisation
Dennis Adams	Detective Constable, Hampshire Constabulary
Ruth Allen	Head of Intelligence, CEOP
Levent Altan	Desk Officer, European & Global Issues Secretariat, Cabinet Office
XXXX XXXX	Detective Inspector for Field Intelligence, SCDEA
Philippe Andrieux	Immigration Liaison Officer, Police aux Frontières
Nick Apps	Business Manager, ACRO
Fragkiskos Archontakis	IT Project Manager, Directorate General – Justice, Freedom & Security, European Commission
Farahnaz Ashouri	Safety, Service Delivery & Logistics Group, DfT
Bob Ashton	Detective Constable International Liaison Officer, Hampshire Constabulary
Ahmed Azam	Head of Schengen & EU Institutions Team, International Directorate, HO
Andrew Bailey	Chair of INI Project Board, PSNI
William Bailhache QC	Attorney General of Jersey
Rosemary Bailie	Policy, Planning & Business Development Manager, PBNI
Stuart Barker	Head of UK Desk, Europol
Derek Barnett	Vice President, PSA
Damian Barratt	Detective Inspector, Public Protection Unit, West Mercia Constabulary
Toby Barratt	Inspector, Reading Police Station, Thames Valley Police
Jerry Bartlett	Deputy General Secretary, NASUWT
Sergeant Liz Barton	ACPO International Liaison Enquiry Team, Hampshire Constabulary
Pat Baskerville	Deputy Director of OPRU, HMPS
Stewart Baxter	Head of Policy, ISA
Ailsa Beaton	Director of Information, MPS
John Beckerleg	Director of Resources, NPIA

XXXXXXX XXXXXX	Head of International Counter Terrorism Strategy, Security Service
Seb Beine	Head of Bichard Implementation Team, HO
Colin Benson	Compliance Officer, CRB
Jan Berry	Former President, Police Federation
John Best	Inspector, Causeway Business Liaison, PSNI
Vijay Bhanaut	Headmaster, De Beauvoir School, Hackney
Tim Bianek	Head of Governance & Planning, OCJR
Sir Michael Bichard	Chair, Legal Services Commission
Trevor Birchall	Compliance Auditor, HO
Stuart Blackley	UKCA Casework, HO
Nick Blake	Strategy Manager, MTU, OCJR
Stephen Blake	Head of Performance and Delivery Unit, HO
Ian Bloom	Senior Policy Adviser, Information Communications Technology & Science Unit, NPIA
Pat Boshell	Head of Corporate Services, Parole Board
Iain Bourne	Thomas / Walport Data Sharing Review Secretariat, Cabinet Office
Jim Boyd	Head of Intelligence, SCDEA
Kevin Bradford	Staff Officer, Violent Crime Portfolio, ACPO
Ursula Brennan	Director General Corporate Performance , MoJ
Andrew Bridges	HM Chief Inspector of Probation, HMIP
Sue Brooks	Head of Offender Strategy, Scottish Prison Service
Roger Browell	Acting Programme Director, Bichard Implementation, HO
Alan Brown	Head of Policing Powers Team, PPPU, HO
Richard Brows	Assistant Director of Border & Visa Policy, UKBA
Nick Burgham	Head of Policy Unit, PECS, NOMS
Bridget Campbell	Director of Policing and Community Safety, Scottish Executive
Richard Campbell	Head of Person Centred Services, DoH
Elaine Carlyle	Senior Security Accreditor, CRB

Peter Charlesworth	Offender Law & Sentencing Policy Unit, NOMS
Jo Chilvers	Offender Assessment Management Unit, NOMS
Kevin Clark	Risk Improvement Manager, NPIA
Richard Clarke	Head of Police Reform Unit, HO
Simon Clarkson	Principal Officer, Multilateral Operations, SOCA
Dave Clater	Head of Information Systems , Scottish Prison Service
Alexis Cleveland	Head of Prime Minister's Delivery Unit, Cabinet Office
XXXXXXX XXXXXX	Head of Intelligence Development Unit, Security Service
Ian Cockerill	Deputy Director, Adobe
Sue Cockerill	Police Officer, Northamptonshire Police
Tunde Coker	Chief Technology Officer, MTU, HO
Matthew Cook	Thomas / Walport Data Sharing Review, MoJ
Nyla Cooper	Employment Services, NHS Employers
Brian Cox	Police Reform Programme Co-ordinator, Policing Policy Group, HO
Alan Cranston	Deputy Director, Information Strategy and Knowledge Management , DCSF
Mark Crawford	Head of Business Change, ISA
Natalie Cronin	Joint Head of Policy and Public Affairs, NSPCC
Sir James Crosby	Non-Executive Board Member, FSA
Gareth Crossman	Director of Policy, Liberty
Belinda Crowe	Head of Information Rights Division, MoJ
Peter-Jozsef Csonka	Head of Criminal Justice , European Commission
Scott Cullen	Office Manager, Absolute Recruit
XXXXXXX XXXXXX	Senior Intelligence & Security Manager, UKBA
Sam Darby	MARAC Policy Lead, HO
Anne Dardis	Chief Immigration Officer, Colnbrook IRC, UKBA
Mick Davidge	Domestic Data Sharing Policy, HMRC
Emma Davies	Head of Criminal Justice Delivery, HMCS
Katie Davis	Executive Director of Strategy Programme, IPS
Gordon Davison	Head of Public Protection & Licensed Release, NOMS

Roger Daw	Director of Policy, CPS
Mark de Pulford	Head of the Better Trials Unit, OCJR
Jane Dench	Personnel Management Business Area, ACPO
Brian Donald	Head of UK Liaison Bureau at Europol, SOCA
Graham Dore	Biometrics Programme Team, HO
Matthew Dormer	Nationality Identification Programme, UKBA
Paul Downing	Project Manager, MPS
Sarah Dring	Head of Human Rights and Assistance Policy Team, Consular Directorate, FCO
Richard Dubourg	Economic Adviser, HO
Walter Dunlop	Project Manager, NIPS
John Dunworth	Head of Interpersonal Violence Team, HO
Richard Earland	Chief Information Officer (Policing), NPIA
Peter Edmundson	Head of Police Leadership & Powers Unit, HO
Helen Edwards	Chief Executive, NOMS
Judith Edwards	Strategic Development Manager, Victim Support
Jayne Eldridge	Senior Business Analyst, NPIA
Ian Elliott	Detective Constable, PPO Lead, MPS Transport Police
John Elliott	Chief Economist, HO
Mike Ellis	Superintendent, PSNI
Paul Ellis	Biometric Programme Manager, UK Visas
Bob Evans	Head of Detainee Escorting and Population Management Unit, UKBA
Laura Fairweather	Head of OASys Team, NOMS
Louise Falshaw	Head of Research & Development, HMIP
Julie Feeney	Probation Officer (Woolwich), London Probation Service
Lyn Fereday	Former Head of FSPU, HO (currently on secondment to NPIA)
Claire Fielder	Justice and Home Affairs, UKREP
John Fiennes	Director of Borders Review, Cabinet Office

Kevin Finch	Criminality Policy Team, UKBA
Gerry Firmin	Information Sharing Support Manager, MPS
Mike Fitzpatrick	Former Programme Director, SIS
Sir Ronnie Flanagan	Chief Inspector of Constabulary, HMIC
Mike Flynn	Seconded UK National Expert, SIS Programme
James Fogg	Her Majesty's Inspector, UK Visas
Olivier Fourès	Office of Legal Affairs, Interpol
Sarah Franklin	Deputy International Liaison Officer, Hampshire Constabulary
Jonathan Freeman	Deputy Director, Preventing Extremism Division, CLG
Nick Fussell	Assistant Legal Adviser, HO
Peter Galbraith	Chief Inspector, PSNI
Jim Gamble	Chief Executive, CEOP
Vince Gaskell	Chief Executive, CRB
Sarah Gawley	Director of Policing Policy and operations, HO
Emma Gibbons	Head of EU Section, International Directorate, HO
Mike Gillespie	Head of Public Order Unit, HO
Simon Godfrey	Central Government Principal, SAP (UK) Limited
Caroline Goemans-Dorny	Office of Legal Affairs, Interpol
Peter Grant	Head of Operations, Parole Board
Bernie Gravett	Operational Command Unit, MPS
Pat Gray	Head of Security Information, NIPS
Simon Greenwood	Parole & Public Protection Unit, NOMS
Julian Gren	Customer Services Manager, Shared Services, HMPS
Edward Gretton	Head of Project Delivery Unit, Peart / Joseph Working Group, OCJR
Jon Griffin	Senior Manager, SOCA
Rachel Griffin	Strategic Development Manager, Victim Support
James Guerrier	Business Analyst, OCIO, HO (Detica)
Peter Haddock	(formerly) Head of Flanagan Secretariat, HO
XXXXXXX XXXXXX	PURSUE Unit, OSCT

James Hall	Chief Executive, IPS
Matt Harris	Business Analyst, OCIO, HO (Detica)
Stephen Harrison	Policy Director , IPS
Darren Hart	Heathrow Intelligence Unit, UKBA
Catherine Hartshorn	Business Benefits & Business Change, MTU, OCJR
Christian Henry	International Relations Division, SCCOPOL
Giles Herdale	Head of Professional Practice, NPIA
Andrea Hester	Head of Employment Services, NHS Employers
Martin Hewitt	Superintendent OCU Commander, MPS
Stephen Hickey	Director General of Safety, Service Delivery & Logistics Group, DfT
Phil Hicks	Assistant to the National Member, Eurojust
Roger Hill	Director of Probation, NPS
Rt Hon Meg Hillier MP	Parliamentary Under Secretary of State
Dr Zoë Hilton	Policy Adviser, NSPCC
Vic Hogg	Director, Policing Policy & Operations Directorate, HO
Lance Holden	Assurance & Controls Manager, HMCS
Justin Holiday	Strategic Director of Resource Management, UKBA
Bill Holland	Technical Project Manager for Causeway Programme, PSNI
Lin Homer	Chief Executive, UKBA
George Houghton	Head of Security Group Policy, HMPS
Stephen House	Assistant Commissioner. Head of Specialist Crime Directorate, MPS
Barbara Howard	Business Development Manager, CRB
Bill Hughes	Director General, SOCA
Helen Hughes-McKay	FCO (formerly on secondment to Hewlett Packard)
David Humphreys	IT Project Manager for Fingerprint Systems, PSNI
Jude Hurley	Business Change Manager, MPS
Kellie Hurst	Domestic Data Protection, Information Rights Division, MoJ

Andrea Hyde	Head of Requests, UKCA-ECR, ACRO
Glenn Jackson	Process Manager, Joint Operational Authority, SIS Programme
Liane Jackson	SIS-Sirene Programme, SOCA
Dr David James	FTAC Lead / GMC Confidentiality Review, Royal College of Psychiatrists
Clarke Jarrett	Covert Security Programme Manager, Olympic Security Directorate, MPS
Lucy Johnson	ID Management Responsibilities Review, HO
Ian Johnston	President, PSA
Chris Jones	Business Analyst, OCIO, HO (Detica)
XXXXXXX XXXXXX	PROTECT Unit, OSCT
Ken Jones	President, ACPO
Sian Jones	Information Access Team, UKBA
Nick Joseph	Dangerous Severe Personality Disorder Programme Unit, NOMS
Helen Judge	Review of Public Protection (including MAPPA), OCJR
Sir Igor Judge	President of the Queen's Bench Division, Judges Council
Peter Kane	Director, Performance & Finance Directorate, HO
Ursula Karkowska	Directorate General Justice, Freedom & Security, European Commission
Michael Katz	Planning & Project Manager, ISA
Chris Keates	General Secretary, NASUWT
Michael Keegan	Confidentiality Guidance Lead, General Medical Council
Nick Kelly	Senior Policy Advisor, NPIA
Steve Kemsley	Olympic Transport Work Stream Manager, Olympic Security Directorate, MPS
Mike Kennedy	Chief Operating Officer, CPS (formerly with Eurojust)
Commander Sharon Kerr	Commander, Specialist Crime Directorate, MPS
Chris Kershaw	Programme Director for Policing Statistics, HO
Helen Kilpatrick	Director General, Financial and Commercial Group, HO
Ailish King-Fisher	Policy Project Manager, Criminality Policy Team, UKBA

Simon Kinghorn	Inspector. Head of Criminal Justice Information Bureau Scottish Criminal Records Office
Russ Kirton	Head of PECS, NOMS
Alan Kittle	Head of Operations, Detention Services, UKBA
Lotte Knudsen	Director of International Security and Criminal Justice, European Commission
Ann Kyle	Senior Law Assistant, Public Prosecution Service, Northern Ireland
Martine Lacour	International Relations Division, SCCOPOL
Tony Lake	Head of ACPO Forensics Portfolio, ACPO Criminal Records Office
Sir Stephen Lander	Chair, SOCA
Andrew Lawrence	Criminal & Law Enforcement Policy, HMRC
Stephen Leach	Director General, Criminal Justice, Northern Ireland Office
Amélie Leclercq	Directorate General Justice, Freedom & Security, European Commission
Peter Leitch	Causeway Programme, PSNI
Luigi Leo	Regional Finance & Performance Manager, HMCS
Peter Lewis	Chief Executive, CPS
Alan Lindfield	Principal Technology Advisor, NOMS
Jonathan Lindley	Strategic Director, Enforcement, UKBA
Gary Linton	Detective Superintendent. Head of Criminal Records Office, ACPO
John Logue	Director of Policy, COPFS
Carole Lord	PPO Team, MPS
Dave Low	Technical Solutions Integration Manager, SIS Joint Operational Authority
Paul Lowton	Police Liaison and Operations, CRB
Stuart MacDonald	Identity Management Strategy Programme Manager, IPS
Ziggy MacDonald	Head of Anti-Social Behaviour and Alcohol Unit, HO
Sir Ken Macdonald QC	Director of Public Prosecutions, CPS
Mike MacKay	Chief Information Officer, YJB
Gordon MacKenzie	PNC Audit & Inspection, HMIC
Valerie MacNiven	Director of Criminal Justice, Scottish Executive

Peter Makeham	Director General, Strategy & Reform Directorate, HO
John Malcolm	Assistant Chief Constable. Secretary of the Crime Business Area, ACPOS
Mike Manisty	Director of Offender Information Services, NOMS
Keith Mannings	Deputy Executive Director, APA
Chris Marsh	Team Leader, Young People Directorate, DCSF
Lucy Mason	Executive Research Officer, Thames Valley Police
Adrian McAllister	Assistant Chief Constable. (formerly) Recording and Disclosure of Convictions Portfolio Holder, ACPO
Tom McArthur	Director Support to Policing Operations, NPIA
Sean McCann	Structures Project Manager, Access Northern Ireland
Terry McCarthy	Joint Review Panel Lead, Parole Board
David McCracken	Chief Superintendent. National Wildlife Crime Unit, HMICS
Brian McCutcheon	Head Of IT, PBNI
David McDonald	Safeguarding Vulnerable Persons Team, HO
Dr Sandy McEwan	CEO, Isle of Wight Prison Cluster, HMPS
Patricia McFarlane	Head of Policing Powers & Safeguarding, HO
Barbara McGarvie	Detective Constable, Central Authorising Bureau, SCDEA
William McGregor	PINS Developers, Saadian Technologies
Cliodhna McGuirk	PINS Developers, Saadian Technologies
Carol McLean	Scottish Criminal Records Office, SPSA
Rod McLean	Head of Criminality Policy Team, UKBA
Mike McMullen	Deputy Head, ACRO
Paul McNally	Detective Sergeant, PSNI (seconded to UKBA)
John McSporran	Intelligence Expert, ACPOS
Michael Merker	Policy Officer, Unit for Fight against Economic, Financial and Cyber Crime, European Commission
Leslie Millar	Causeway Business Liaison, Northern Ireland Court Service
Kristyn Miller	Analyst, OCIO, HO
Brian Minihaine	Head of Overseas Operations for UK, Interpol
Jonty Monteith	Assistant Project Manager for INI, PSNI

Steve Moore	Business Development Manager, CRB
Clare Moriarty	Constitution Director, MoJ
Shona Morris	Assistant Director, UKBA
Colin Morrison	Constable, PSNI
Judge Mary-Jane Mowat	Circuit Judge, Oxford Crown Court
David Mulhern, QPM	Chief Executive, SPSA
Frank Mulholland	Solicitor General for Scotland, COPFS
Jim Munro	Home Office Interface with the Forensics Science Service, HO
Eric Murch	Director of Partnerships and Commissioning, Scottish Prison Service
Helen Murray	Head of CRU, HO
Ian Neill	Deputy Programme Manager, UKBA
Peter Neyroud	Chief Executive, NPIA
Alastair Noble	Sex Offender Policy, Interpersonal Violence Team, HO
Sir David Normington	Permanent Secretary
XXXXXXX XXXXXX	Director of Law, Security & International, OSCT
John O'Brien	Programme Director, Vetting & Barring Scheme, ISA
Grant Oliver	Head of G8 & Wider World Unit, International Directorate, HO
Sir Hugh Orde	Chief Constable, PSNI
John Palmer	Head of Local Government Policy, Welsh Assembly
Dr Kok-Fu Pang	Programme Manager for Biometrics, HO
Robin Pape	Deputy CIO and Head of Strategy, OCIO, HO
Kate Paradine	Senior Doctrine Developer, NPIA
Colin Parker	Establishment Drugs Co-ordinator, HMP Wandsworth
Curtis Parkyn	Enforcement Projects, London Local Criminal Justice Board
Chetan Patel	Home Office Reform Programme, HO
Lindsey Patterson	Justice and Home Affairs, Joint Office of the UK Law Societies in Brussels
Bill Peace	Deputy Director , SOCA
Angela Pearce	Head of Criminal Casework Directorate, UKBA

Kate Pearce	Head of the National Analysts' Working Group, NPIA
Roger Pearce	PINS Users, MPS
Clive Peckover	(formerly) Nationality Identification Programme Manager, UKBA
Angela Perfect	Head of Returns Group Documentation Unit, UKBA
William Perrin	Deputy Director of Strategy & Policy, Cabinet Office
Nick Perry	Director General, Policing and Security, Northern Ireland Office
Bernard Petit	International Relations Division, SCCOPOL
Tony Plunkett	Head of Operational Policy, Strategy Directorate, IPS
Chris Potter	Mental Health Policy Lead, Public Protection Unit, NOMS
Nick Poyntz	Head of Victims and Witness Unit, OCJR
Emma Provan	Assistant to the National Member, Eurojust
Steve Przybylski	Assistant Director of Business Development, CPS
Gary Pugh	Director of Forensic Services, MPS
Jeanette Pugh	Director of Safeguarding, DCSF
Matthew Pyne	UKCA Casework, PPOD, HO
Dr Malcolm Ramsey	Health & Offender Partnership, Dangerous Severe Personality Disorder Programme Unit, NOMS
Vijay Rangarajan	Counsellor (Justice and Home Affairs), UKREP
Paul Regan	Head of Police Finance Team, HO
Marek Rejman-Greene	Senior Biometrics Adviser, HO
Owain Richards	Portfolio Holder on Violent & Sex Offenders, ACPO
Steven Rimmer	(formerly) Director of Strategy, Modernisation & Performance, MPS
Craig Robb	Thomas / Walport Data Sharing Review, MoJ
Allan Robinson	Business Analyst, CRB
Lorraine Rogerson	Director of Policy & Head of Profession, UKBA
Jenny Rowe	Chief Executive, Supreme Court (formerly at the Attorney General's Office)
Ellie Roy	Chief Executive, YJB
Justin Russell	(formerly) Special Advisor to Home Secretary, HO
Tim Rymer	Head of JBOC, UKBA

Ruth Sanger	Head of Local Government Performance Team, Welsh Assembly
Hannah Saunders	(formerly) Programme Director, 101: Single non-emergency number, HO
Tom Saunders	Director, Home Office IT, HO
John Scott	Head of Offender Assessment & Management Unit, NPS
John Scullion	(formerly) Director of Finance, CRB
Kathy Seal	Manager of Loughborough Centre, AIT
Jackie Sear	Head of Criminal Records Team, PPPU, HO
Jonathan Sedgwick	Deputy Chief Executive, UKBA
Louise Selby	Peart / Joseph Working Group Lead, OCJR
Nigel Shackleford	Head of Caseworking, Mental Health Unit, NOMS
Alan Shaw	Head of Human Rights & Assistance Policy Team Assistance Group, FCO
Gabrielle Shaw	Head of International and Relations, CEOP
Kevin Sheehan	Director of Operations, IPS
Brian Shelby	Office of the National Co-ordinator of Special Branch, JBOC, UKBA
Professor Jonathan Shepherd	Professor of Oral and Maxillofacial Surgery, University of Wales
Edwina Sherwood	Manager, Optimum Process Model, CPS
John Simmons	Head of RDS, NOMS
Alexander Slater	Management Consultant, Accenture
Jonathan Slater	Chief Executive, OCJR
James Slessor	Management Consultant, Accenture
Claire Smith	IPS Pilot and e-Bulk, CRB
David Smith	Deputy Commissioner, ICO
David Smith	UK Interpol Desk, SOCA
Nick Smith	Assistant Director, Government and Legal, SIA
Linda-Claire Smith	Performance Support Manager, HO
Steve Southgate	Assistant Governor, Rehabilitation HMPS Holloway
Elwyn Soutter	Inspector, Border Force Directorate, UKBA Northern Ireland
Michael Spurr	Director of Operations, HMPS

Paul Stephenson	Deputy Commissioner, MPS
Mark Stocker	Client Principle, Hewlett Packard
Peter Storr	Director, International Directorate, HO
Andrew Stott	Deputy CIO, Cabinet Office
John Suffolk	Government CIO, Cabinet Office
Isabel Sutcliffe	Project Manager, London Local Criminal Justice Board
Brian Sutherland	Deputy Head of Information Systems, Scottish Prison Service
Martin Sutherland	Managing Director, Government Division, Detica
Peter Swift	Deputy Director, Safeguarding Vulnerable Groups Act Implementation Division, DCSF
John Swords	Lawyer, Legal Adviser's Branch, HO
Fenella Tayler	Acting Head of JCU, HO
David Thomas	Deputy Governor, HM Prison Camp Hill
Richard Thomas	Information Commissioner, ICO
Brian Thompson	Observation Planning, PSNI
Jo Thompson	Head of Post Release Policy, NOMS
Inspector Sam Thompson	Businesses Liaison Unit (IDENT1, PNC), PSNI
Sara Thornton	Chief Constable, Thames Valley Police
Steve Tippell	Head of Drug Strategy Unit, HO
Peter Todd	Assistant Inspector of Constabulary, HMIC
Nick Tofiluk	Head of IMPACT programme, NPIA
Rolf Toolin	Deputy Director of Enforcement, UKBA
Vic Towell	Assistant Inspector of Constabulary, HMIC
Anthony Townsin	International Data Exchange Co-ordinator, HMRC
Mark Tutton	Detective Sergeant, Hampshire Constabulary
Jessica Tuzin	Cross Government Identity Management Programme, IPS (on secondment from Ernst & Young)
Kathryn Tyson	Mental Health Policy, DoE
Mark Uden	Head of Security Systems & Information Management, HMPS
Sir David Varney	Prime Minister's Adviser on Public Service Transformation, Cabinet Office

Annette Vernon	CIO, HO
John Wailing	Chief Technical Officer, OCIO
Jane Walman	Court Manager, Woking Magistrate's Court
Dr Mark Walport	Director, Wellcome Trust
Kevin Walsh	Head of Youth Courts Team, NOMS
Malcolm Ward	Quality Assurance and Safeguarding Manager, Southwark Children's Services
Rob Ward	Listings Officer, Oxford Crown Court
Neil Ward	Chief Executive (Interim), HMCS
Tracey Warren	Regional Senior Finance Officer, HMCS
Rachel Warren	Risk Manager, OCJR
Tony Watson	Head of Operational Policy Unit, NOMS
Stephen Webb	Head of Organised & Financial Crime Unit, HO
Hans Wejman	Head of Kew Approved Premises, NPS
Phil Wheatley	Director General, NOMS
Julian White	Technical Architect, SIS Programme
Stephen Whitefield	Strategy & Delivery Team, Violent Crime Unit, HO
Darren Whiteford	Policy Officer, HMCS
Lyn Whiting	York Students In Schools, University of York
Paul Wiles	Chief Scientific Advisor, HO
Steve Wilkes	Head of Policy & Legal Compliance, IMPACT Programme, NPIA
Aled Williams	Deputy to the National Member, Eurojust
Rt Hon Michael Wills MP	Minister of State, MoJ
Chief Constable Peter Wilson	Previous President, ACPOS
Karl Wissgott	Head of PNC Services, NPIA
David Wood	Head of Criminality & Detention Group, UKBA
Jim Woodman	HR Business Change Manager, Isle of Wight Prison Cluster, HMPS
Joe Woods	Offender Management Implementation Manager, NOMS
Stephen Wooler	HM Chief Inspector, CPS
Ed Wozniak	Head of Performance Information and Measurement Services, Scottish Prison Service

Jo Wright	Vice President, Global Capability Practices, BT
Eric Young	Head of Implementation Team for MOPI , NPIA
Focus Group	Focus Group, Cambridgeshire Police Federation
Focus Group	Focus Group, Lancashire Police Federation
Focus Group	Focus Group, Metropolitan Police Federation
Focus Group	Focus Group, North Yorkshire Police Federation
Staff Meeting	Staff Meeting, Criminal Casework Directorate, UKBA
Staff Meeting	Staff Meeting, Detainee Escorting & Population Management Unit, UKBA
Staff Meeting	Staff Meeting, Heathrow Intelligence Unit, UKBA
Staff Meeting	Staff Meeting, Colnbrook Immigration Removal Centre, UKBA
Staff Meeting	Staff Meeting, Asylum & Immigration Tribunal, UKBA
Staff Meeting	Staff Meeting, HM Prison Wandsworth, HMPS
Staff Meeting	Staff Meeting, Isle of White Prison Cluster, HMPS
Staff Meeting	Staff Meeting, Mental Health Policy, DoH
Staff Meeting	Staff Meeting, London Probation Service

Annex G: List of documents reviewed

General criminal justice

- Cutting Crime: A New Partnership 2008-11 – Home Office, July 2007
- Re-balancing the criminal justice system – Home Office, July 2006
- Cutting Crime, Delivering Justice – A Strategic Plan for Criminal Justice 2004–08
- Criminal Justice System Business Plan 2007-08
- Joining up justice – an introduction to criminal justice IT
- CJIT introductory material
- Bichard Enquiry Recommendations Fourth Progress Report – Home Office May 2007
- The Use of Forensic Science in Volume Crime Investigations – Home Office Online 43 / 05
- Office for National Statistics, Social Trends, 2007
- Department of Transport, Transport Analysis Guidance, Values of Time & Operating Costs, February 2007
- Home Office Risk Management Policy & Guidance
- Multi-Agency Public Protection Arrangements Annual Reports 2006 – 2007

General Information Management

- Cross-Government Information Sharing Vision Statement, September 2006
- Review of the Barriers to Information Sharing Within the Public Sector – Ministry of Justice
- Home Office Information, Systems and Technology Strategy 2007-08: Volume 1 & 2
- Framework Code of Practice for Sharing Personal Information – Information Commissioner's Office
- Population Data Paper – Business Assurance Workstream (2007), ISA
- PNC Quality & Timeliness 2nd Report, HMIC, April 2002

Police

- National Community Safety Plan 2006-09
- Information Systems Strategy for the Police Service (ISS4PS)
- Her Majesty's Inspectorate of Constabulary Business Plan 2007-08
- Criminal Justice Inspectorates' Joint Inspection Business Plan 2007-08
- National Policing Improvement Agency Business Plan 2007-08
- Serious Organised Crime Agency Annual Plan 2007-08
- Forensic Science Service Report 2005-07
- Report of the Review of the Police Information Technology Organisation, Home Office, February 2005
- Global DNA Database Inquiry – Interpol
- The Review of Policing by Sir Ronnie Flanagan – Interim report
- The Review of Policing by Sir Ronnie Flanagan
- HMIC Raising the Standard
- Retention Guidelines for Nominal Records on the Police National Computer
- Police Grant Report 2007 / 08, ROCI Team Interviews & Analysis
- Home Office Statistical Bulletin, Arrests for Recorded Crime, E&W 2004
- Draft National Policing Improvement Agency Business Plan 2008-11

Prosecution

- CPS Annual Report 2006-07
- CPS Business Plan 2007-08

Courts

- HM Courts Service Annual Report 2006-07
- HM Courts Service Business Plan 2007-08
- Ministry of Justice Sentencing Statistics 2006 (England & Wales)

Prisons

- Prison Service Annual Report 2007
- Prison Service Business and Corporate Plan 2007-08
- Her Majesty's Inspectorate of Prisons Business Plan 2007-08
- NOMS Business Plan 2007-08 (in draft)
- Ministry of Justice Story of the Prison Population 1995-2007 (2008-0362)
- Forum for Preventing Deaths in Custody, Annual Report 2006 / 07
- Parole Board Annual Report & Accounts 2006 / 07

Probation / supervision / monitoring

- National Probation Service Annual Report 2006-07
- Her Majesty's Inspectorate of Probation Plan 2007-08
- Her Majesty's Inspectorate of Probation Annual Report 2006-07
- Ministry of Justice update: End of Custody Licence Releases and Recalls 1 to 29 February 2008, England & Wales

Youth Justice

- Youth Justice Board Annual Report 2006-07
- Youth Justice Board Corporate and Business Plan 2004 / 5-2006 / 7

Immigration

- Borders and Immigration Agency Business Plan 2007-08
- Securing the UK Border – Home Office, March 2007
- Health: Tackling Alcohol Related Violence in City Centres – Emergency Medical Journal 2006
- Control of Immigration Statistics United Kingdom, 2005
- Home Office Statistical Bulletin Aug 2007 – Asylum Statistics, UK 2006

Identification

- Home Office Strategic Action Plan for the National Identity Scheme
- Home Office Identity Management Strategy
- Identity and Passport Service Business Plan 2007-08
- Identity Management Risk Modelling – Home Office / Identity & Passport Service, March 2007
- Identity Service Proposition – A joint venture between IPS and CRB

Safeguarding Vulnerable Groups / Employment Vetting

- CRB Five Year Strategy and Business Plan 2006-07
- Fourth Progress Report on the Bichard Inquiry Recommendations
- Bichard Implementation Programme – Lessons Learned
- Review of the Protection of Children from Sex Offenders – Home Office
- Child Exploitation and Online Protection Centre, Strategic Overview 2006–07
- Child Exploitation and Online Protection Centre, Business Plan 2007-08
- CRB Business Plan 2007 / 2008
- CRB Identity Authentication Pilot
- DfES Safeguarding Children and Safer Recruitment in Education
- NHS Employment Check Standards
- Ofsted – Safeguarding Children – An evaluation of procedures for checking staff appointed by schools
- CEOP Business Plan 2007 / 2008
- NSPCC Report: Protecting Children from Sexual Abuse in Europe: Safer Recruitment of Workers in a Border Free Europe

European / International

- Report of Amroliwala Inquiry into Home Office handling of notifications of overseas convictions
- Report by the Home Office on progress in clearing the overseas convictions backlog
- Foreign national prisoners: a follow-up report by Her Majesty's Chief Inspector of Prisons
- House of Commons Home Affairs Committee – Justice and Home Affairs Issues at European Union Level
- A review of the failure of the Immigration & Nationality Directorate to consider some foreign national prisoners for deportation
- Obtaining Criminal Record Histories from European Union Member States – The UK Central Authority for the Exchange of Criminal Records
- European Security Review 2007

Scotland

- Scottish Criminal Records Office Annual Plan 2006-07
- Scottish Criminal Records Office Corporate Plan 2006-–09
- Report of Her Majesty's Chief Inspector of Constabulary for Scotland 2005-06
- Her Majesty's Inspectorate of Constabulary for Scotland – Corporate Plan 2006-09

Northern Ireland

- Police Service of Northern Ireland Chief Constable's Annual Report 2006-07

ISBN-978-1-84726-656-9

HO_01033_G