Government Response
to the
Magee Review of Criminality Information

Cm 7511

Government Response to the Magee Review of Criminality Information

Presented to Parliament
by the Secretary of State for the Home Department
by Command of Her Majesty

December 2008

Cm 7511 £13.50

ISBN: 978 0 10 175112 4

GOVERNMENT RESPONSE TO THE REVIEW OF CRIMINALITY INFORMATION BY SIR IAN MAGEE

Introduction by the Home Secretary

As a Government, we recognise that one of our most fundamental responsibilities is the protection of the public. We are grateful to Sir Ian Magee for his Review which highlights the importance of criminality information in fulfilling this responsibility. We agree with him that the organisations through which this responsibility is discharged constitute a "Public Protection Network" (PPN) which depends to a significant extent for its effectiveness on the flow and availability of criminality information.

We have already made progress on a number of fronts that help to reduce the risks to public protection. For example:

- The Association of Chief Police Officers (ACPO) has created a Central Criminal Records Office which is providing a focal point for several agencies involved in Multi Agency Public Protection. Work is already under way with data exchanges between ACPO through this office to the UK Border Agency, Prison Service, the Criminal Records Bureau and the Independent Safeguarding Authority
- The establishment of a UK Central Authority for the Exchange of Criminal Records by the police, has enabled the exchange of criminal conviction information between EU member states and the three jurisdictions of the UK
- The National Policing Improvement Agency is delivering a co-ordinated approach to meeting the information needs of the police service
- The National Offender Management Service brings together the work of prisons and probation and opens the way to more integrated information handling
- The creation of the UK Border Agency enables a focus on information needs related to securing our borders and controlling immigration
- The setting up of organisations like the Criminal Records Bureau, the Independent Safeguarding Authority and the Child Exploitation and Online Protection Centre strengthens the information framework for protecting children and other vulnerable groups
- The various criminal justice organisations are now linking together much more effectively in terms of information handling through the introduction of the National and Local Criminal Justice Boards
- The Multi-Agency Public Protection Arrangements are boosting local collaboration to protect the public against violent and sexual offenders

We plan to build on these achievements by capitalising on opportunities to further improve our business processes. These need not involve doing fundamentally new things with high price tags, such as building new IT systems. But rather, factoring the principles of the Magee agenda into existing, or planned, programmes of work which Ministers are committed to delivering. For example:

- Work to support the deportation of EEA nationals in appropriate circumstances
- The developing Identity Management Strategy
- Training commitments for staff in public protection organisations following recent Reviews incorporating data security and data sharing

It is important to remember that the ultimate purpose of all these endeavours is public protection. So we need to keep that focus which can drive all the individuals and organisations involved to improve their performance around managing criminality information. Everyone needs to recognise how the tasks for which they are responsible contribute to protecting the public and how that contribution forms part of the broader Public Protection Network.
Leaders throughout the PPN need to spell out the importance of criminality information and why capturing and handling it properly is so vital to public protection. They must take steps to ensure that staff are properly trained, including in how to ensure that information is shared where necessary for public protection in a timely and secure way. Data protection is fundamental to Government's ability to share information. But it is important to remember that we are protecting and securing information as one aspect of protecting the public.

I agree with the Review that independent challenge is essential to implementation of this important agenda. With this in mind, we intend to appoint an Independent Advisor (supported by a small internal secretariat). The Independent Advisor will focus on maintaining pressure on agencies to take actions forward and act as a champion to help advance public understanding and debate about the policy issues and associated dilemmas. A key priority for the Advisor will be to advise on how public protection agencies and services can work together across boundaries to improve, and make best use of, the information they collect to tackle crime.

Implementing the recommendations in this Review is not just about solving the problems of managing criminality information experienced yesterday and today. It is also about ensuring, as far as possible, that similar problems do not occur in the future. This will be achieved by helping to bring about long-term change to how departments, agencies and services operate – both within their own organisations and across organisational boundaries. It is important therefore to recognise that this will take time, but also to have a clear idea of what success will look like in the short term. Work has already started to establish robust Ministerial governance and by the end of January 2009 we will have agreed a strategic direction for criminality information management. Alongside these structures, we will have started the recruitment process for the Independent Advisor by early 2009. We will have provided new guidance on managing risks across the whole PPN by April 2009 and by the middle of next year we will have implemented a number of the practical steps to improve and bring more rigour to our business processes. By September 2009 we will have enhanced the training for staff on managing criminality information.

Ultimately this is all about ensuring that frontline staff have access to the information they need, when they need it, to make difficult decisions relevant to public protection. Our response to Sir Ian's Review is an important aspect of meeting that challenge.

The Rt Hon Jacqui Smith, MP
Secretary of State for the Home Department

Contents

Overview

1. This is the Government's Response to Sir Ian Magee's Review of Criminality Information. We welcome the Review and are grateful to Sir Ian for his thorough analysis and important recommendations. This Response, and the attached Action Plan, set out how we intend to use those recommendations to improve the handling of criminality information in support of public protection.

Genesis of the Review

2. Following an inquiry early in 2007 into the handling of notifications by other European countries of criminal convictions relating to UK citizens, the Home Secretary asked Sir Ian Magee to examine and recommend necessary improvements for recording and sharing information about criminality within the UK and between the UK and other countries in the interests of public protection. The definition of public protection in the Review is: "the safeguarding from harm of our communities and individuals within them"; and the definition of criminality information is: "any information which is, or may be, relevant to the prevention, investigation, prosecution, or penalising of crime".

3. The Terms of Reference for the Review were to:

   - scope the problem and assess what is broken and where the deficiencies lie

   - 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

Lessons from the Review

4. The Review highlights the need for agreement across Government departments, agencies and services on a clear strategic direction for the management and use of criminality information both domestically and internationally. There also needs to be effective governance to clarify responsibilities for the management of criminality information and help us address risks around information handling and security before they turn into immediate problems. Data sharing and data protection are not conflicting objectives. We must be positive in helping to strike an appropriate balance between them.

5. As is clear from the Review, public protection relies on a whole range of organisations across Government and agencies working together effectively – what Sir Ian refers to as the Public Protection Network

(PPN). There is already a huge amount of good practice, but much more can, and will, be done. We will vigorously support the breaking down of silo working across the PPN. For example, by seeking to ensure that risks are managed across the Network and the broader needs of public protection are considered when decisions are made about major investments in technology.

What difference does it make to the public?

6. Implementing the recommendations from this Review will have real and positive impacts on the public, building on action we have already taken to share criminality information to tackle crime and protect the public; for example, helping to ensure that:

   - Those who are in jobs looking after children and vulnerable adults have been properly vetted based on all the necessary information
   - Applicants for UK Visas have their fingerprints checked against criminal records held on the Police National Computer and where there is a match UK Border Agency staff are provided with the criminal history so those who are prolific offenders or otherwise raise public protection concerns can be denied entry
   - The risk of a prisoner being released from prison when they may be wanted by the police on other matters is reduced
   - UK nationals who have committed sex offences abroad can be identified via exchange of criminal records and therefore on their return to the UK can be managed in the community via the Multi-Agency Public Protection Arrangements (MAPPA)
   - Foreign nationals who pose a risk to the public are prioritised for removal from the UK
   - Police are able to check EU nationals' previous criminal records meaning that they will not be able to hide their past and the courts can make appropriate bail and sentencing decisions
   - We continue to develop our processes so that public protection organisations properly capture, securely store and appropriately use and share criminality information

Summary of the Recommendations

7. The Review of Criminality Information produced a package of recommendations covering nine key areas. This package includes a mix of high level strategic recommendations to bring about systemic change to how we manage criminality information in the future, and pragmatic early steps that can be taken to improve some front line business processes.

8. It is suggested that a **strategic direction** for criminality information management and oversight should be established across the PPN with clear goals, performance assessment and an improvement agenda which adheres to key principles.

9. The **governance** recommendations look to support coherence within the strategic direction and its core principles. They are based around a Ministerial group (chaired by the Home Secretary) to take overall responsibility, a Home Office led implementation team, an independent Commission to champion efficient and appropriate information management and the existing agencies and Departments which will lead on delivery.

10. On **leadership** the Review emphasises the importance of leaders at all levels demonstrating awareness of the importance of information management, with a clear link to improving the capture of accurate data and ensuring appropriate sharing.

11. There are some practical recommendations around **risk management.** These include relevant departments and organisations giving explicit consideration to the potential impact of their decisions on risks to public protection as a whole. And the development of mechanisms within each organisation to enable escalation of significant front line risks to public protection.

12. On **investment** the focus is on ensuring a much more joined up approach across the PPN. In particular, Investment Boards in the various public protection organisations should take much more account of wider public protection priorities in making funding decisions.

13. In relation to **technology,** a full review of IT systems as they relate to criminality information management is recommended. Priority should be given to enhancing IT integration and to programmes that increase information sharing. An assessment process should be used to help ensure the effectiveness of IT developments and a new emphasis put on engaging with suppliers to make sure they understand cross-cutting requirements. There is also the need for greater clarity around governance of, and access to, the Police National Computer (PNC), and where possible, the implementation of the remaining recommendations from the Bichard Inquiry should be expedited.

14. The Review recognised the added complexity of operating in the **international dimension,** and makes a number of recommendations for improvement. In particular:

    - The development of a strategic direction for the UK on international exchange of criminality information so that all concerned are clear about what the UK requires
    - A set of initiatives to ensure improved UK use of international mechanisms for exchanging criminality information

- A more joined-up approach to engaging with international proposals on the management of criminality information, with full involvement from international experts, senior policy makers and relevant delivery organisations

15. Looking to **the future** the Review suggests that the proposed independent Commission should undertake horizon scanning on a regular basis. Picking up on current public concerns, it recommends that Ministers should lead a public debate about the DNA database and the use of biometrics more widely.

16. A number of recommendations impinge directly on work **at the front line.** They cover three specific business areas on which the Review team carried out detailed work: release from custody, foreign national prisoners and vetting and barring.

17. The details of all these recommendations, and the action the Government proposes to take, are set out in the **Responses to Specific Recommendations** section**.**

Opportunities and Challenges for Government

18. The recommendations made in the Review share a collective goal of making better use of criminality information to reduce the risks to public protection. They identify both a number of specific opportunities to do this at the frontline and a number of steps to ensure that full advantage is taken of the opportunities that exist throughout the PPN.

19. Capitalising on these opportunities will often not be about doing fundamentally new things, but about collectively (across the PPN) managing and sharing the available information to better protect the public. It also provides an opportunity to rationalise current data sharing processes, further reduce silo working and to create an environment where frontline staff are encouraged to share criminality data (where it is appropriate and proportionate to do so within proper safeguards) for the benefit of public protection. The Government acknowledges that this will not be without its challenges, but we believe that by working together to implement the Review's recommendations much good can be achieved.

20. Sir Ian's Review cannot, and should not, be considered in isolation. There is a vast amount of change already going on across the PPN in relation to future IT infrastructure and reworking of business processes. We will seek to ensure that these planned developments incorporate the spirit of Sir Ian's recommendations, and thereby contribute to reducing the risks to public protection. Examples include the implementation of the remaining Bichard recommendations, the recent Green Paper *From the Neighbourhood to the National: Policing our Communities Together*, the Public Service Agreement to *Make Communities Safer* and the Home Office *Tackling Violent Crime* Action Plan which all share a common element with the Magee agenda – to provide PPN staff (in these cases,

mainly police officers) with the right information, at the right time, to help them make the best decision possible. Likewise with planned changes across the EU, with new mechanisms for criminality information exchange coming on line over the next few years such as implementation of the Prüm agreement (allowing comparison of DNA and fingerprint data on a hit/no hit basis and exchange of vehicle ownership information) and the intended connection to the SIS II database (allowing police officers checking the Police National Computer to have access to alerts placed by other EU countries in relation to missing or wanted persons, stolen vehicles and passports and other similar information). Further afield we have also established a number of other information sharing mechanisms, many on a more ad hoc basis and with many negotiations on-going.

21. Where exchange mechanisms are already in place we accept that there is a clear need to rationalise the processes so that frontline staff have a better understanding of what information they are able to access and share, and how to do that. The key aim has got to be to enable frontline staff making public protection decisions to have access to the information they require to make those decisions promptly and easily. They should be able to obtain it by going to one, or at most two, points of contact. When developing new data streams we need to make sure that they fit into existing mechanisms and that we avoid further diversification wherever possible.

22. Awareness training across all staff involved in the PPN will be a key challenge and priority. We aim to identify opportunities for adapting existing courses (which are already scheduled and funded) to include training on criminality information management and sharing, so that it becomes part of mainstream training.

23. In implementing the recommendations we must have regard to the vast range of organisations which make up the public protection network. Across the UK there are 52 police forces involved and other agencies such as the UK Border Agency and National Offender Management Service (NOMS) which have a more national or regional remit and whose regional boundaries are not co-terminus with those of the police forces and other agencies. Also across the UK there are different legal and criminal records systems in place in England and Wales, Scotland and Northern Ireland. Responsibility for these is devolved in Scotland and, though reserved in Northern Ireland, is the responsibility of the Northern Ireland Office and not the Home Office. This needs to be borne in mind when formulating policy both within the UK and at international level. This problem becomes exacerbated as we begin to factor in the different systems in place in the other EU countries and practice becomes more diverse still as we look further out across the world. We are already engaging fully with colleagues in the devolved administrations. In Scotland's case, while they will not join the formal UK Government Response to the Review, they will work alongside us and consider

whether and, if so, how they wish to take the recommendations forward in Scotland.

24. There will therefore be a challenge in terms of getting an agreed UK or EU position and in ensuring that initiatives considered at national and international level make sense and will work at local level. Such initiatives must be easy for frontline staff to understand and use and must not involve disproportionate costs for the organisations having to implement them.

25. We recognise that just by accepting recommendations we are not immediately reducing the risks to public protection and indeed we are aware that the risks can only be reduced, not eliminated. Action is needed to implement the recommendations and in order to do that, new processes and mechanisms must be embedded across Departments, agencies and services. As the Review recognises, achieving fully collaborative and productive working across the whole territory of public protection will not be easy and so we need to be realistic about the time that will be required to make significant progress in some areas - particularly on the international front, and in putting in place new information systems.

26. The complexity of the different criminal records and vetting and barring information held by different countries means that the negotiation of new international data sharing arrangements takes time. Additional data flows will also need to be funded and so an overall risk based approach will be needed to ensure that priority flows are initiated and funded first and that opportunities for rationalisation and realising savings are identified early on. A clear idea of the way forward and what the overall system might ideally look like some years ahead will also need to be factored in to the design of any new information systems if maximum benefits are to be obtained. International negotiations will also need to take account of the views of the devolved administrations and their ability to fund and carry through the policies agreed.

Cost of Implementation

27. The Government accepts the principles behind all of the recommendations and we have already started work to implement those which will support the future development of this work, for example we have committed the necessary funding to establish the implementation team and new governance arrangements. These recommendations are shown in this response as **accepted**. Other recommendations, shown as **accepted in principle**, will be subject to detailed consideration of the business implications. This consideration will include looking at the balance of costs, risks, identifying any potential savings or efficiencies and conducting full cost benefit analyses of the potential options to deliver the outcomes set out in the Review. This further work will be undertaken in the coming months but, in any event, will be completed by the end of December 2009. Many recommendations will not involve new

or discrete action as work is already under way for which funding has already been agreed. However implementation may require use of some of this funding to be prioritised in different ways to that currently envisaged.

28. Careful planning will therefore be required to ensure that maximum benefit can be obtained through existing streams of work. Opportunities to increase the benefits realised from new IT programmes will need to be identified early on to ensure that they are included at the design stage as funding is unlikely to be available for bespoke changes later on. Good interagency co-operation will also be required to identify where resources or costs might be shared.

Steps to implement the Magee agenda

29. Work on scoping and implementing many of the recommendations is already under way. Key early steps are:

- Leaders will make their own statements of intent to emphasise to their staff the importance of management of criminality information by **December 2008**

- A strategic direction for the improvement of criminality information management will be agreed across Government by the National Criminal Justice Board (NCJB) in **January 2009**

- We will also agree a strategy across the public protection network for the international exchange of criminality information by the **end of January 2009**. This will include reaching a common agreement on what criminality information we require and for what purposes and will enable us to identify priority areas for opening up new channels for exchange. This will help us towards our goal of obtaining information relating to foreign nationals that will allow us to carry out employment vetting and barring, properly deal with in the courts those who commit offences here and to remove those who present a significant risk to the public

- We will seek to lead the way in Europe on exchanging criminality information. We are already beginning a pilot for the secure electronic exchange of this information with other EU Member States and we will look for other ways that we can speed up the transfer of data so that frontline PPN staff dealing with EU nationals have the information they need to make decisions relating to protection of the public

- We will appoint an Independent Advisor to advise how public protection organisations can work together across boundaries to improve, and make best use of, the information they collect to tackle crime. Further, the Independent Advisor will challenge the organisations in the PPN if they have not taken action to implement Magee recommendations

- We will enhance procedures so that there is a much stronger focus on identifying criminality information-related risks to public protection and managing them in partnership across the PPN. Guidance will be provided to public protection organisations by April 2009

- We will work with the organisations across the PPN to enhance training for staff at all levels to ensure it gives a real focus to the importance of criminality information management by September 2009

- We will complete the work to deliver against the key outstanding recommendations from the Bichard Inquiry which bite on the effective use and sharing of criminality information

- We are implementing the changes we have already identified to business processes to assist frontline staff in their day-to-day work protecting the public, for example, by:

    - Making better use of information technology to improve the safety and efficiency of immigration removal centres
    - Delivering new guidance to employers and voluntary organisations on how to make best use of criminality information in their recruitment practices to reduce the risk of an employee or volunteer causing harm to children or vulnerable adults, especially where job applicants have spent time abroad

- We will review information systems to identify opportunities for changes to business processes, particularly where tactical IT fixes are needed, and to ensure that there is a programme of continuous improvement

Checking on Progress

30. Sir Ian Magee will return to review the Government’s progress in **Spring 2009.** Progress reports will be provided every six months to the senior Ministerial group.

Responses to Specific Recommendations

Strategic Direction

Recommendation 1: Agreeing the Direction

By January 2009, the Government should agree, across Departments, a strategic direction for the improvement of criminality information across the Public Protection Network (PPN), which includes prioritised immediate objectives for improvement. The strategic direction should articulate clear goals for the role of criminality information in supporting public protection and be based on an objective assessment of performance against those goals.

Accepted

31. The Home Office is working with organisations across the PPN to agree a draft strategic direction for consideration by Ministers by January 2009.

32. The **ultimate outcome** for the strategic direction will be to reduce the risks to public protection by improving the prevention, investigation, prosecution and penalising of crime and thus impact positively on:

    - Crime reduction
    - Public confidence in protection from crime
    - Efficient use of resources

33. However, in more immediate terms the concept of the strategic direction will be based on improving the effectiveness of criminality information in supporting and facilitating effective decisions relevant to public protection. In developing a strategic direction, we have a **vision** of an environment in which all those making such decisions have all the criminality information they reasonably need, when they need it and in the form they need it. In such an environment access would be straightforward, effective and secure. Proportionate and timely sharing of information would be the foundation for an effective set of systems which delivered criminality information requirements across the PPN.

34. The strategic direction will be based on enabling principles which will need to be applied if these goals are to be achieved, but will need to drive a prioritised set of **immediate objectives for improvement.** These objectives will flow from an ongoing analysis of the extent to which current arrangements already apply the enabling principles referred to above. For business and technical processes, this analysis will need to take place at both the macro level (for example, the proposed review of PPN information systems referred to in recommendation 19) and micro level (for example, the type of frontline work referred to in recommendations 26-29). This analysis will also need to be applied to

what might be described as the ‘infrastructure’ issues around risk, investment and training.

35. It will not be sufficient for analysis to confine itself to the demands and requirements of the world as it exists now. Identifying priorities will also need to allow for developments in the business and policy environment within which the PPN is operating and broader environmental trends in society and technology. The strategic direction will need to recognise this.

36. Fundamental to the successful implementation of the strategy will be public confidence in the way data are handled and shared by bodies in the PPN. In developing the strategic direction, the Government will seek to ensure that principles of proportionality and necessity apply, and that the public can gain a clear understanding of how personal information will be handled and shared by bodies in the PPN. The Government believes it is vital that the public be assured that their data, while used increasingly effectively for public protection purposes, will be treated in full compliance with data protection rules and individual privacy rights.

37. While some objectives will be inherited from existing work (including from the Magee Review and the Bichard Inquiry), new ones will be constantly emerging from the process of analysis referred to above. Some aspects of that process will be carried forward centrally, but much of the work will effectively be led from within individual parts of the PPN.

38. Ownership of specific sets of analysis work and improvement objectives will need to be allocated to particular levels of governance, with the Ministerial structures taking responsibility for the top-level improvement agenda.

39. In support of this, a clear set of relationships will need to be established between the central governance structures dealing with criminality information and the various relevant structures in all the component organisations making up the PPN.

Governance and Delivery

Recommendation 2: Establishing a delivery team

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 with cross departmental staffing. This unit should be substantially in place by September 2008.

Accepted

40. The Criminality Information Unit (CIU) was established on 1 August 2008 in the Home Office. Staff have been recruited from the various Departments and agencies involved in the PPN (including UKBA, NOMS and the Office for Criminal Justice Reform) or seconded from the services via ACPO and the Serious and Organised Crime Agency (SOCA). The CIU has worked with stakeholders across the PPN to initiate implementation and the Criminality Information Steering Group (CISG), consisting of senior officials from across the PPN, was established to help produce this Response and Action Plan. CIU will continue to work with stakeholders at various levels within the relevant agencies to support implementation.

Recommendation 3: Ministerial oversight and independent challenge

To develop a shared agenda for continuous improvement of the recording and sharing of criminality information across the PPN, clear ownership and accountability is needed. Sir Ian recommends that this is achieved by establishing a Home Secretary-chaired Ministerial group with external challenge and advice from a Commission for Public Protection Information.

Accepted

41. The Government is committed to leading the improvement agenda recommended by the Review. The Home Secretary will chair a Ministerial group based around the National Criminal Justice Board (NCJB) on a quarterly basis to consider criminality information issues. Other Ministers with an interest in the criminality information agenda, notably the Secretaries of State for Health and for Children, Schools and Families, will be invited to participate in these meetings. Additionally a group of junior Ministers from across Government will be established to provide a more detailed focus on the issues raised in the Review and advise the senior forum as necessary.

42. The Review identified both strengths and weaknesses of the NCJB becoming the principal Ministerial group. Since then the NCJB has re-focused its role to concentrate on problem solving and improving its links with operational delivery. It is also developing stronger governance arrangements to ensure coherence and effectiveness in criminal justice

system (CJS) delivery, for example, strengthening arrangements on technology investments. We believe this change in focus now makes it an ideal forum for Ministers to resolve the specific problems on management and use of criminality information to support public protection. Additionally, the support of a junior Ministerial group will allow detailed criminality information issues to be considered, and provide a route through which problems may be escalated as necessary. Together, these two Ministerial groups will provide the strong leadership required to drive the improvement agenda on criminality information.

43. The Government also agrees that independent challenge is essential to implementation of this important agenda. With this in mind, we intend to appoint an Independent Advisor (supported by a small internal secretariat). The key functions for this Advisor will be in line with the core responsibilities set out in the Review and will focus on maintaining pressure on agencies to take actions forward and acting as a champion to help advance public understanding and debate about the policy issues and associated dilemmas. A key priority for the Advisor will be to advise on how public protection agencies and services can work together across boundaries to improve, and make best use of, the information they collect to tackle crime.

44. The costs of supporting the implementation team and the new governance arrangements will be met from within existing budgetary constraints.

Leadership

Recommendation 4: Leadership at all levels

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.

Accepted

45. The Government agrees that strong leadership and accountability is needed to ensure that management and use of criminality information improves so helping to reduce the risks to public protection. This applies to leaders at all levels, from Ministers, heads of the PPN organisations, through to supervisors of frontline staff. These leaders must recognise the importance of better management of criminality information and ensure that staff better understand the need to share good quality information with partners in an appropriate and proportionate way. We acknowledge the complexity of the environment in which PPN staff share criminality information, and training should be provided to help staff to understand the relevance and priority of data to be shared.

46. This headline recommendation on leadership is spelled out in more detail in the three recommendations which follow. Details of work under way and planned for the future are set out below and in the Action Plan. The costs of implementing the leadership recommendations (staff and leaders' time plus some new training materials) will fall mainly to the organisations within the PPN, although some support will be provided by the CIU (for example, provision of best practice advice).

Recommendation 5: Statement of intent by leaders

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*

Accepted

47. The introduction to this response has been agreed across Government and constitutes the top level statement of intent recommended by Sir Ian. Senior leaders within the individual organisations making up the PPN will be building on this by making their own statements. These will be

consistent with the message from Ministers but tailored to the circumstances and issues facing their own staff.

Recommendation 6: Training in information management

The importance of information management should be explicitly included in leadership training and development programmes such as the Police Strategic Command Course, the Professional Skills for Government framework and other equivalent programmes before September 2009.

Accepted in principle

48. The inclusion of material highlighting the importance of criminality information, and promoting good management thereof, in the curricula of key leadership and development courses is key to raising the profile of this important issue for future leaders. The Government believes that material on information management must also be included in all induction programmes and basic training courses on offer to staff within the PPN, as well as management development programmes for leaders at all levels. This is complementary to the requirements for training on data security and handling for all staff accessing protected personal data as set out in two recent reviews on Data Handling[1] and Data Sharing[2] and is part of a wider programme to improve the management of information across Government. This training is crucial to embedding good practice on data handling into frontline processes for the future. Discussions are already under way with PPN organisations and external training providers. CIU plans to produce best practice guidance on including the importance of criminality information management in relevant programmes in Spring 2009 and to provide support to training providers in adapting programmes before September 2009.

Recommendation 7: Assessing the impact of training

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.*

[1] Cabinet Office 'Data Handling Procedures in Government: Final Report', published in June 2008

[2] Dr Mark Walport and Richard Thomas 'Data Sharing Review', published July 2008

Accepted in principle

49. It is in the interests of best practice that organisations assess and evaluate the training programmes and controls they have in place in relation to criminality data capture and information sharing.

50. All staff must know what is expected of them and in particular must understand how to record and share criminality information securely and appropriately. Education and training for all staff is a key component in this and so an assessment of current training and a training needs analysis should be conducted highlighting good practices and successes and learning from past experience.

51. Whilst the provision of the necessary tools and processes for staff is of course important, it should be recognised that this is an extremely wide ranging recommendation and may have different implications for each department, agency and service. Given the vast landscape covered by the PPN, it may not be possible to undertake one large assessment, or peer review exercise, and an agreed and proportionate assessment will need to be carried out. Where possible there should be reuse of existing technology and adoption of good practice from across the PPN. This links with other recommendations, in particular “Investment” and “At the Front Line”.

Risk Management

Recommendation 8: Identifying risk

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 9: Mechanisms to escalate risk

Each agency within the PPN should institute by January 2009 a regular mechanism to enable escalation of significant frontline 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 10: Sharing risk intelligence

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.

Accepted recommendations 8, 9 and 10, in principle

52. There are significant interdependencies between these three recommendations. Senior leads for risk management have already been identified within each of the key PPN departments and organisations. The CIU will continue to work with these leads to identify existing good practice and use it as the basis for developing clear and concise guidance on the effective management of public protection risks across the PPN. Effective risk management arrangements outside the PPN, including in the private sector, will also be examined as part of this process.

53. A central focus of the guidance will be on how to identify information-related risks to public protection and assess their potential impact, particularly where those risks extend beyond one organisation to other parts of the PPN. It will also cover the importance of recognising when risks need to be escalated up the management line and of establishing clear and well-understood mechanisms to do so. It will stress the need to integrate the management of public protection risks into broader risk management and to establish clear reporting mechanisms. There will be an emphasis on communicating risks to other organisations and

engaging with them about how to manage and mitigate risks which run across more than one area of the PPN. The target is to provide the guidance by April 2009 and then to support the relevant departments and organisations in applying it and embedding it within their work. A review of its use and effectiveness will be undertaken in autumn 2009.

54. The Independent Advisor (see response to recommendation 3) will need access to key organisations' risk registers in order to be sighted on and able to oversee those risks considered to be most critical.

55. In developing guidance on managing risk in this context it will be important to keep in mind the comments Sir Ronnie Flanagan made in his recent Review of Policing. He emphasised the need to take a proportionate approach to risk, recognising that risks can be managed, but not entirely eliminated. This theme is as applicable to addressing risks across the PPN as it is when dealing with risks concentrated within policing.

56. The CIU will incur costs in terms of developing, disseminating and supporting the application of the guidance on managing information-related risks to public protection across the PPN. These are containable within allocated Home Office budgets. Associated training costs for the relevant departments and organisations are referred to under recommendation 12. Other costs for the departments and organisations in terms of improving and joining up their approaches to risk will need to be absorbed within existing budgets. Real additional costs should be negligible because this is essentially about building on existing management, business and communications structures to recognise and address risks more effectively.

Recommendation 11: Assessing the effectiveness of risk management

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.

Accepted

57. The CIU will co-ordinate implementation, with identified inspection leads linked to each key department and organisation within the PPN to drive delivery.

58. Work has already been undertaken to determine which bodies need to be engaged within supporting delivery of this recommendation. These include independent inspectorates (such as Her Majesty's Inspectorate of Constabulary), internal teams carrying out inspection and review

functions within organisations and possibly bodies with a broader review function such as the National Audit Office.

59. CIU will work with lead players in each of these bodies to examine the extent to which their existing inspection arrangements already include an assessment of the effectiveness of risk identification and management. We will seek out good practice both on this critical inspection function and the way in which its outputs are fed back to senior management to prompt improvements. Based on that best practice CIU will develop standard procedures, promulgate them to the relevant inspection organisations/teams and support those bodies in embedding them in their work.

60. A full review of how the new and improved procedures are working will be carried out in the early part of 2010. However, throughout the course of implementing this recommendation regular progress reports will be provided to the Ministerial structures to check that everything is on track to meet Sir Ian's intention.

61. The costs of developing standardised arrangements around the inspection of information-related risk management will be met from the CIU budget. The expectation is that any cost of developing and enhancing existing procedures in line with this best practice should be borne by the inspection and review bodies concerned. In many cases this will be an evolution of systems which are already in place or partly in place and so costs should be negligible.

Recommendation 12: Training in risk management

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.

Accepted in principle

62. The CIU will co-ordinate implementation, in liaison with those responsible for training and risk management in each of the key departments and organisations.

63. There is a close link between this recommendation and recommendation 7. That recommendation requires leaders to undertake an assessment of training and this will need to focus on training on relevant aspects of risk management. This assessment should be completed by May 2009 and the requirement in recommendation 7 for leaders to commit to delivering improved training etc should be met by July 2009, including an appropriate reference to risk management training. Depending on what the assessment of the current position reveals, an improvement programme will need to be developed across the relevant departments

and organisations, but the scale and duration cannot be determined at this stage. It may be possible to integrate these improvements into more general strengthening of training on the management of criminality information which is likely to flow from the Magee work.

64. The costs of co-ordinating the work of agency leaders in assessing the current position will be met from the CIU budget. The costs of delivering enhanced training (much of which is likely to relate to the effective implementation of recommendations 8, 9 and 10) cannot be quantified at this point. There should be significant scope to absorb them by adapting and extending existing training arrangements where necessary.

Investment

Recommendation 13: Public protection in funding decisions

Investment Boards in the various public protection organisations should always take account of wider public protection priorities in making funding decisions. Sir Ian was 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. He recommends that the consideration of wider public protection benefit is embedded in that process.

Accepted

65. There is a close connection between this recommendation and recommendation 22 which suggests that all IT developments in the sphere of criminality information should pass through an initial assessment process. The CIU will allow for this linkage in co-ordinating implementation of both recommendations.

66. The CIU will engage with the Investment Boards and similar structures in each of the key organisations and test the extent to which their established procedures already consider the broader public protection dimension in deciding around funding. Drawing from those discussions, CIU will develop concise process advice to boards aimed at ensuring they are all sufficiently outward looking. In parallel with that CIU will engage with the Office for Government Commerce (OGC) to ensure that their work to develop the Gateway process for programmes and projects takes sufficient account of the need to see the bigger public protection picture. Any move in the direction of a hard ‘go/no go’ gate should include this consideration of public protection issues as one of the determining factors.

Recommendation 14: Joined up investment

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

Accepted

67. The CIU will liaise with key organisations to understand the extent to which they already connect with their relevant counterparts in reaching investment decisions relevant to other parts of the PPN. This will include any work they already do through established inter-agency structures. Based on that, CIU will work with them to develop a process for ensuring these connections are adequate and effective in individual cases and then support them in applying that process.

68. Linked to that process, and building on existing mechanisms, there will need to be a set of effective responses to resolve blockages to implementation arising from funding issues which are unresolved between organisations. Ultimately the NCJB may need to be involved in addressing the most difficult problems.

69. Once again, CIU will cover costs of developing the response and lead organisations will need to absorb the costs of changes to their own procedures.

International Dimension

70. 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 and beyond. But, as the Review recognises, 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.

71. Progress is being made. For example, since the Review, the UK Central Authority for Exchange of Criminal Records (UKCA – ECR), situated in the ACPO Criminal Records Office (ACRO), has been running roadshows to increase the awareness of police forces throughout the UK of its work in exchanging criminal record information with other EU Member States. Those forces are now making regular use of this arrangement, to obtain convictions from across the EU. However, whilst we would want to create a greater impetus behind these arrangements, it must be acknowledged that roughly half of the other EU Member States are not yet engaging with the framework arrangements and therefore it may be some time before we fully have processes in place which can systematically check EU nationals as they enter into the criminal justice system.

Recommendation 15: International data flows

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 PPN*
- *The development of options for the future structure and governance of international criminality information exchange*

Accepted in principle

72. The Government will bring forward an agreed strategy in January 2009 on the international exchange of criminality information. This strategy will take account of the key elements identified in the Review but the scope of the strategy and the speed of implementation will be subject to sufficient funding being made available.

73. In relation to the EU, probable priorities will be increasing frontline staff awareness of the information already available to them in relation to EU nationals, the improved sharing of electronic information and the prioritisation of agreements on the sharing of criminality information for immigration and employment vetting and barring purposes (both at an EU and bilateral level). Outside the EU, a risk based approach will be taken to identifying those countries which need to be a priority for information exchange.

74. The strategy will also focus on how the channels for information exchange can be rationalised and ensure that future proposals fit within existing systems rather than adding to them. It will also seek to ensure coherent governance and accountability mechanisms (see recommendation 17 below).

75. In developing the strategy, the Government will need to consider carefully the potential costs of increasing the flow down existing channels and those of developing new flows of information. We will also need to consider the likely impact on those countries receiving requests from us and whether we might expect them to also be making more requests of us. The cost of specific training for staff in the key delivery organisations on these issues is likely to be high and careful thought will need to be given to integrating such training into existing training packages.

Recommendation 16: International 'champions'

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

Accepted

76. The Government accepts the rationale behind this recommendation and CIU will maintain a network of contacts within the Whitehall departments, the devolved administrations, and senior national level nominees of the key delivery organisations. However, it is likely to be impractical to maintain a wider network of contacts at a more local level within these organisations as personnel are likely to move or change responsibilities on a regular basis. Instead it will be the responsibility of the senior level nominee to maintain a network of contacts at a more local level within their organisation. For example, ACPO might nominate a senior representative at national level but they might maintain a network of contacts at a working level in each force, supported by ACRO. CIU is working with ACPO to develop terms of reference for the national level representative and for the force level contacts. This model will then be rolled out across other delivery partners in the PPN.

Recommendation 17: International collaboration

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 which would be affected or required to put them into effect. The agreed position should be re-visited periodically, as negotiations progress.

Accepted

77. The Government accepts this proposal and considers its aims are best achieved by improving and strengthening existing mechanisms where possible. This will both reduce duplication and keep support costs to a minimum.

78. Ministerial oversight of specific international data sharing and protection initiatives will be achieved through appropriate Cabinet Committees – these may include the National Criminal Justice Board as well as, for example, the Committee on National Security, International Relations and Development (Europe).

79. A Senior Official International Data Group will be established to take responsibility for ongoing oversight and dispute resolution for international data sharing and protection matters. Membership will be drawn from senior officials and senior representatives from Whitehall departments, the devolved administrations and operational delivery bodies with significant interests in international data sharing and data protection matters. This group will consider issues beyond the confines of criminality information. As such it will be chaired by the Ministry of Justice, the department with lead responsibility for data protection and data sharing matters generally. However, when considering matters relating to criminality information, senior Home Office officials and operational actors will be intimately involved in identifying priorities and leading discussions.

80. Beneath this group, a number of working-level groups will be revitalised and redesigned. In particular, there will be a standing Public Protection, Law Enforcement and Immigration Data Sub-Group, chaired jointly by the Home Office and the Ministry of Justice, again with a core membership of relevant Whitehall departments, the devolved administrations and operational delivery bodies. While lead departments will take responsibility for negotiating specific initiatives, the Sub-Group will be charged with promoting understanding of the wider picture of activity in the international data sharing and protection area as it relates to criminality information. It will work to ensure consistency of UK negotiating positions on specific international initiatives, and alignment with the domestic UK data sharing and protection agenda.

81. The CIU will work closely with the secretariat to these groups to ensure appropriate international expert and delivery organisation representation. In doing so, it will draw on its network of contacts in the PPN brought together under recommendation 16.

82. In order to ensure a joined-up UK approach to international and domestic information sharing, the CIU will work with the secretariat to these groups to help ensure information about developments surrounding the international exchange of criminality information is regularly made available to those groups leading the domestic agenda.

83. Additionally, the Home Office/MoJ chaired Judicial Co-operation Forum (JCF) has agreed to meet early in 2009 to look specifically at improving implementation of agreements reached in Europe.

Recommendation 18: Employee checks

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.

Accepted

84. Subject to reaching agreement with Jersey, Guernsey and the Isle of Man (“the Islands”) the Government accepts this recommendation and will seek to bring them into the UK disclosure regime. The exact mechanism for doing that and whether it is with the Criminal Records Bureau (CRB), Disclosure Scotland or Access Northern Ireland has yet to be determined. Given the relatively low level of expected checks, the costs are expected to be minimal and can be met within existing funding. This will enable the authorities of the Islands to conduct criminal record checks on people working with children and vulnerable adults who have moved to the Islands from the United Kingdom, filling a current gap in public protection. The CRB and Disclosure Scotland already obtain criminal records information from the Islands in relation to people from the Islands who are employed in such positions in the UK.

85. The authorities of the Islands will also be asked to be part of the network of organisations and governance structures suggested in recommendations 16 and 17, so that they can consider at an early stage whether they wish to be party to new policy initiatives in relation to international criminality information exchange.

Technology

Recommendation 19: Review of systems

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.

Accepted (Review)

86. The Government recognises that, to drive this improvement agenda forward, maintaining a coherent understanding of the IT that supports the PPN is fundamental to effectively managing the information that these systems are designed to process. We, therefore, agree that a PPN-wide review is required to test the PPN infrastructure for information management issues and identify opportunities for improvement. Selection of an appropriate level of detail will be essential, with an emphasis on identification of issues to be addressed based on information requirements at key decision points, rather than system mapping for its own sake.

87. The review can draw upon several components that have already been progressed across many areas of the PPN, for example, existing mapping and transformation initiatives within the Home Office, Office for Criminal Justice Reform (OCJR) and National Policing Improvement Agency (NPIA), as well as the quick fixes that have already been identified by the Review, as discussed under Recommendation 20.

88. OCJR is reviewing opportunities to improve criminal justice information flows affecting public protection. Examples include improving the hand over of information between the youth and adult sectors of the CJS, and better sharing of offender risk and intervention information with local authorities and third sector support providers when an offender returns to the community. OCJR is now assessing the costs, benefits and possible trade-offs of various options and will present an initial analysis to the CJS Business Change Board, (which sits below the NCJB), in early 2009.

89. CIU aims to initiate the review early in 2009 and it will take several months to complete. It will focus on high priority information management issues, confirm adequate coverage of these issues across the PPN and, where relevant, identify links to underlying technology. Review costs will be accommodated within CIU's budget, with CIOs contributing support from their own resources.

90. The Government accepts in principle that it will undertake the programme of work which results from the review. The outcome of the review will be a prioritised list of potential opportunities across the PPN, and for ongoing use, a high level summary of all identified issues and

initiatives across the PPN which will inform the programme of continuous improvement referred to in the section on strategic direction. This will include an analysis of the potential costs of the options as well as identification of any savings that might arise. The primary audience of this review and the related cost benefit analyses will be the Business Change Board.

Recommendation 20: Simple tactical fixes

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

Accepted in principle

91. Government Departments and agency CIOs have already begun a series of tactical efforts to improve the contribution of technology to protecting the public. Tactical improvements are arising in two areas. Firstly, several key tactical fixes were suggested through the 'At the Front-Line' section of the Review and are in the process of deeper investigation before being implemented. Secondly, other improvements are already being implemented based on the CIOs' own agendas. Examples of initiatives being developed to improve information sharing and integration across the PPN include:

- Improved **Home Office approach to handling of dependencies** for all IT changes across the Home Office group
- **CPS/Police two-way exchange** is looking to provide the ability for CPS to return information directly into the Police Case Management Systems and further improve end to end case management
- **Courts/Police Electronic File** seeks to eliminate the paper based filing system
- **Virtual Courts** are being piloted
- **Home Office Watchlist Risk Analysis** has identified several tactical and process improvement opportunities, along with a strategic recommendation to reuse the e-Borders watchlist service
- **Prisons roll out of NOMIS** - The full roll out of the National Offender Management Information System (NOMIS) to prisons will provide a strong platform to enable fingerprints to be taken and stored in a common standard format which can then be used to confirm identity with partner agencies such as the police and UK Border Agency (UKBA)
- **CRB/UKBA** piloting a data matching process when checking criminal records as part of employment vetting to help identify whether the applicant has a right to work in the UK

92. In addition, and as already highlighted in the Review, the ongoing 'Wiring up the Youth Justice System' initiatives offer strong examples of how to achieve rapid, low cost IT improvements via targeted efforts to connect key sources and users of information.

93. In order to provide a holistic view across the PPN, CIU will support the CIOs by co-ordinating all tactical efforts in line with the review work described in recommendation 19, as follows:

- Undertake a tactical process across the PPN to collate all current initiatives and tactical fixes that can be delivered within the next 12 months to improve information management
- Conduct a brief due diligence process based on the initiatives identified to ensure that any actions have a positive effect on the whole PPN before prioritising and producing an action plan to deliver them in an integrated manner
- Detail the lessons learned and best practices that can be extracted from these initiatives to support further joining up across the PPN in the longer term

Recommendation 21: IT Inter-operability

Building on the governance, processes, standards and architectures that will flow from Sir Ian's 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 22: Making the most of existing IT

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 Sir Ian's first Investment recommendation. This process should explicitly address use and reuse of IT capacity, making the maximum use of existing technology.

Accept recommendations 21 and 22, in principle

94. The CIU and CJS CIOs Forum will work together to ensure consistent governance for all ongoing and future initiatives. Initial work has already commenced within each Department through the commitment of CIOs to include Review priorities within the existing project governance infrastructures. Examples of progress include:

- Current work by OCJR to strengthen the governance structures to improve coherence and effectiveness of technology investments across the CJS. CIOs will play a key role in this process

- Implementation of the Home Office's Information, Systems and Technology Strategy (2008-09) will improve the management of information, technology and suppliers through its Next Generation IST Transformation and Information Assurance Programmes. The Home Office's Office of Chief Information Officer (OCIO) also participates in project governance for all major Home Office programmes as a matter of course

95. Together, both governance efforts will support a co-ordinated approach to both the Review and broader Government ambitions around shared services and the Operational Efficiency Programme.

96. Linked to these processes, CIOs will be working together to maximise the overall performance of information management across the full PPN so that any future developments:

- Build on the governance, processes, standards and architectures consistent with the Review
- Facilitate improved information sharing and increase IT integration and inter-operability
- Consider the use and reuse of existing IT capacity
- Address the potential for duplication, inter-operability issues and overlaps between systems

97. All decisions around integration or inter-operability of IT systems will be based on questions of long term operational need and other key issues such as getting the right balance between information sharing and data protection. The Government is committed to conducting privacy impact assessments for any new IT projects.

98. The IT investment process will also ensure that these key questions are asked for all IT investments. The Home Office Group Investment Board already fulfils this role, to a degree, as will the CJS Funding Approval Authority, once constituted. Where necessary, the CIU will offer support to this investment decision process by providing clarity around the extent to which proposed initiatives do, or do not, meet the information needs of the PPN. It will be supported in this by both the investment recommendations 13 and 14 and the overview of PPN information systems and flows provided in response to recommendation 19. It will also be able to build on the OGC work referred to in the response to recommendation 13 and the principles included in the IT Strategy for Government which is being developed by the Cabinet Office.

Recommendation 23: Engaging with suppliers

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 PPN, and to encourage their active help and expertise in making suggestions as to how re-usability can be achieved, instead of building fresh systems.

Accepted in principle

99. In common with many institutions across the public and private sector, members of the PPN have outsourced large areas of their business to IT suppliers. Many contracts are successful within themselves but the requirement to seek separate contracts in support of competition has in some cases introduced artificial boundaries between the information management activities of different agencies and directorates.

100. OCIO (Home Office), OCJR and the Ministry of Justice have each realised the importance of taking more strategic ownership horizontally across their lines of business, as per the recommendations of the Government CIO. Use can be made of the building blocks already established within the departments such as OCIO (Home Office), CJ IT (Ministry of Justice), Information Systems Improvement Strategy (ISIS) programme (NPIA) and the MoJ IT Supplier Sourcing Strategy. As these programmes are rolled out and provide future direction, they should ensure that they maintain the PPN perspective.

101. The responses to recommendations 19-22 will provide valuable inputs into a process of engagement with the current IT suppliers to identify improved ways of working. The proposed CJS Commercial Authority will address recommendation 23 through the development of cross CJS commercial frameworks for core services and also focussed alignment across initially MoJ, and then other Government Departments, for use of suitable framework contractual frameworks. Active engagement of suppliers will be embedded within the frameworks and they will be required to build in their help and consideration on re-usability.

102. At this stage, the incremental costs associated with this effort are minimal. Relevant future costs are likely to include business transformation efforts required to accommodate new supplier arrangements and will be offset by benefits from multi-year improvements to these major contracts.

Recommendation 24: Governance of the Police National Computer

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.*

Accepted in principle

103. Good progress is already being made around PNC governance. The National Police Databases Board (NPDB) has been established under NPIA auspices and with a senior ACPO chair. It provides oversight and responsibility for a range of key police databases, including the PNC and includes representatives from the Home Office, OCJR, the Association of Police Authorities and other partner organisations. For the first time it offers top-level co-ordination of the various strands of operational and policy work which underpin the effective operation of the PNC. The arrangements for access to the PNC are relevant to the developing remit of NPDB and this creates a clear opportunity to review these arrangements in the light of the Review and ensure they are appropriate, proportionate and effective. The head of CIU is a member of the NPDB and will press for further clarity around PNC governance and strengthened approaches to determining access.

104. A detailed study has already demonstrated that it is feasible to share data between the PNC and the PSNI/Causeway system in Northern Ireland. The NPIA, PSNI and Causeway staff have endorsed the approach emerging from the study, which would make use of available commercial products and reuse the well-established PNC Phoenix Force Interface. Funding discussions between the key players will continue, with a view to securing agreement. However, resolution of this long-running issue will need to be brokered at a senior level and perhaps between Ministers. It could provide an early test of the effectiveness of the evolving governance arrangements following the Review.

Recommendation 25: Delivering Bichard recommendations

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

Accepted

105. Oversight of progress on the outstanding Bichard Inquiry recommendations is being integrated into the Magee implementation programme and will be supported by the Magee governance structures. CIU has already contacted all the Senior Responsible Owners (SROs)

for the remaining recommendations, obtained progress reports and has discussed the position with them further, where necessary. The CIU will participate in all the key governance structures relating to these recommendations, such as the IMPACT Programme Board and the Bichard 7 Project Board. Ministers have been made aware of any substantial concerns about progress and will press SROs to expedite timetables as Sir Ian recommends.

106. As progress on delivery of the Bichard recommendations was last reported to Parliament in May 2007, we are incorporating our latest report on outstanding Bichard Projects and Programmes in the response to this recommendation and in the attached Action Plan. Future Bichard reporting will continue to be integrated into progress reports on the criminality information agenda flowing from this Review. Looking across the set of relevant Bichard recommendations, current progress is positive but mixed.

107. The improvements to both the technical and business processes around police information management which will flow from the IMPACT Programme will be a crucial part of the strategic direction which will emerge from the Magee work. The Police National Database (PND) will achieve a new level of integration for police data at a national level and the Management of Police Information (MOPI) framework is driving the adoption of consistent good practice in the way police officers and staff handle criminality information. The Programme is on-track to start delivering PND capabilities during 2010. It is extremely unlikely that it will be possible to bring this forward; implementation of the database, the necessary business change and data preparation are all complex processes that cannot be shortened. Three consortia were selected to participate in detailed contractual negotiations. Those negotiations were due to finish in September this year but it became clear that the best long-term benefits would be secured through an eight week extension of that process. The negotiations have now been completed and all three consortia have been invited to submit final tenders by early January. Whilst this means that an award of contract is now scheduled for March 2009, this extension was beneficial to ensure that the best solution is obtained for the money available and to allow optimal arrangements to be agreed for delivering what the police service needs. Deployment of PND is still expected to commence in 2010.

108. Contractual and procurement constraints also apply to the introduction of the Independent Safeguarding Authority, which has begun its work to underpin the staged transition from the existing barring schemes to the new service. This is also on track, but we must ensure these national arrangements which improve the safeguarding of children and vulnerable adults are in place by autumn 2009.

109. Most of the other improvements to employment vetting procedures advocated by Sir Michael Bichard have been fully delivered. Of those that remain, improvements include strengthening identity verification in

relation to those applying for CRB checks using fingerprint data within the identification process and extending the set of databases to which CRB has access for vetting purposes.

110. The Bichard recommendation which calls for improved arrangements for the checking of people from overseas who want to work with children and vulnerable adults remains very challenging and progress has been limited to a number of initiatives. Getting other countries to participate in such arrangements has been particularly difficult and there are also issues concerning the quality and availability of many overseas records even where they are willing to do so. However, the Home Office is working up a more targeted approach which might allow us to obtain European criminal conviction data for employment vetting purposes. There needs to be some testing of the possible approach before Ministers are presented with high level options in January 2009. The agreed approach being developed on the international strategy will help to take this work forward.

111. A link between the Magistrates' Courts and the Police National Computer**,** to enable automatic transmission of court results, is now in place in two areas. The linking up of the computer systems was more complex than originally thought and this delayed roll-out earlier this year, as planned. However, the project is now entering its final phase, with full deployment of a technical solution due to be achieved during 2009.

112. The outstanding Bichard recommendations generally have established funding streams. However, there are emerging pressures around the costs of exchanging conviction and other criminality information with other countries and these are still being quantified as part of the work described above.

113. Further detail on progress with each of the outstanding Bichard recommendations is in the Action Plan at the end of this document.

At the Frontline

114. There are four recommendations that focus on finding practical ways of improving the management and use of criminality information to ensure that frontline staff make best use of information when making decisions that affect public protection. These relate to improving the capture, storage and access, sharing, analysis and actioning of criminality information.

115. A number of actions have been identified in the Review to improve the quality and timeliness of criminality information available to frontline staff. They cover three specific business areas; foreign national prisoners, vetting and barring and release from custody. These have been prioritised on the basis of risk to the public and early practical steps towards delivery are summarised below.

116. Progress has been made to deliver some of the remaining actions, and plans for the delivery of others are currently being agreed across the PPN.

Recommendation 26: Confirming offender identity

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.

Accepted in principle

117. Government departments and agencies across the PPN are in the process of developing a Crime and Justice Identity Management Strategy. The strategy, which will be completed by March 2009, will aim to develop a consistent approach to the establishment and use of identity.

118. **Early practical steps:** *UKBA to ensure that both pre and post sentence, all individuals who cannot prove UK nationality and who meet minimum sentencing and non-EEA (i.e. 12 month) criteria are referred for consideration by Criminal Casework Directorate (CCD), with CCD verifying and applying nationality criteria for deportation eligibility.*

119. As a priority, UKBA and the Prison Service are working together to ensure that foreign national prisoners are identified and their status checked earlier in the criminal justice process. This will help to ensure that those individuals eligible for deportation can be quickly and efficiently removed at the end of their sentences. In addition, CIU is investigating whether there are ways this can be done earlier e.g. at the point of arrest.

120. UKBA will pilot new information sharing processes to ensure that all prisoners will have their nationality checked, where possible against

trusted data sources. Prisoners whose nationality remains in doubt will be referred to UKBA to verify nationality if possible. This pilot is being led by UKBA and is due to be completed by the end of January 2009. A full review of costs, benefits and success will be carried out at the end of the pilot.

121. Funding for the Pilot will be found from existing UKBA resource. The main benefits are dependent on the pilot being successful and funding for full delivery but these in principle are:

- Clearer understanding of the nationality of prisoners
- More efficient decision making regarding removal of foreign nationals
- Reduced risk of harm to the public as a result of removing foreign national offenders

Recommendation 27: Access to information

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

Accepted in principle

122. **Early practical steps:** *All police forces to implement prisoner location and release information solutions.*

123. Work is under way to reduce the risk of offenders being released from prison into society when they are wanted by the police on other matters. The police and the Prison Service have made significant progress on this with offender location information accessed and interpreted locally in a number of forces. The main benefit is:

- Reduced risk of harm to the public as a result of returning to custody those offenders that are wanted by the police on other matters

124. A longer term solution is being considered which would make this information available nationally but it will be dependent on central funding.

Recommendation 28: Systematic approaches to information sharing

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

Accepted in principle

125. The Crime and Justice Identity Management Strategy will also seek to improve information sharing across the PPN by linking relevant personal data to an identity accessible by all agencies.

126. **Early practical steps:** *Determinations from tribunals of foreign national prisoner appeals should be passed on promptly to caseworkers in UKBA CCD, Prisons, Probation and Immigration Removal Centres (IRCs).*

127. A bail hotline has been set up which ensures that CCD caseworkers receive immigration bail determinations within a few hours and went live on 1 October 2008. Arrangements have also been made for appeal rights exhausted cases to be notified quickly to caseworkers. Delivery was completed on 20 October 2008.

128. It is anticipated that there will be no additional costs as the work will be absorbed within existing resources. The main benefits are:

- Reduced cost per removal of foreign national offenders by reducing the time spent in immigration detention after appeal rights have been exhausted
- Reduced risk of harm to the public by promptly triggering offender management procedures for foreign national offenders released into the UK on bail
- Speed up the removal of foreign national prisoners whose appeal rights have been exhausted

129. **Early practical steps:** *UKBA to consider bringing together and providing a more integrated information system to improve the interface between UKBA Detainee Escorting and Population Management Unit (DEPMU), IRCs, CCD and Asylum and Immigration Tribunal to facilitate better information access and more effective oversight and management of processes.*

130. Work has been completed in defining an operating model for the immigration removals estate. Further activity is under way in UKBA to analyse and understand the full business requirements associated with this action and to consider appropriate solutions for delivery that are not currently met by existing initiatives.

131. Funding for user requirements analysis work will be provided from existing UKBA resources. Additional costs incurred through delivery and support of existing or future technology will be identified as part of the initial analysis work. The main benefits are:

- Increased efficiency and safety in the management of foreign national offenders held in immigration detention
- Increased capacity for removals per bed in the immigration detention estate

132. The benefits above must be supported, where appropriate, by investment in improved technology to enable information sharing. Providing the additional technical solutions will depend on securing sufficient funding.

Recommendation 29: Clear frameworks for frontline staff

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.

Accepted in principle

133. **Early practical steps:** *Independent Safeguarding Authority (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. These standards to be incorporated into relevant employer guidance (e.g. Department for Children, Schools and Families) and existing employer inspection regimes (eg Ofsted).*

134. Vetting and barring stakeholders have agreed that there should be core guidance for employers on best practice in the use and sharing of criminality information. The Home Office Vetting and Safeguarding Policy Unit, in conjunction with other government departments, is leading this work. Guidance will be developed to be sector specific where this is appropriate.

135. By synchronising this change in conjunction with delivery of the ISA it is anticipated that there will be no additional costs for delivery. The benefits are:

- An increase in public protection through employers systematically making better use of available criminality information
- A reduction in effort expended by government and employers in writing consistent guidance on the use of criminality information by having a single core guidance owner
- Sharing of good practice in the use of criminality information by employers

136. Delivery of benefits is dependent on effective agreement and communication of the guidance by the ISA and CRB such that employers

build risk based decision making into their employment processes. As criminality convictions from overseas become available to employers through longer term initiatives, the processes put in place now will be ready to benefit from that information.

137. **Early practical steps:** *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*.

138. Work is under way to ensure that the complex health needs of those managed by the criminal justice system are included in statutory government mechanisms for providing appropriate healthcare as a part of a more comprehensive approach to resettlement.

139. The cost of identifying appropriate interventions is anticipated to be covered in the current implementation of new statutory processes in this area. The costs of delivering these interventions lie with health service providers. The main benefits are:

- A more comprehensive approach to reducing re-offending by ensuring that health needs of offenders are met as part of their overall needs for successful resettlement.
- Reduced costs of handling re-offenders for organisations in the PPN
- More appropriate care for a section of society with particularly complex health and social care needs

140. The success of this work is dependent on an acknowledgement by senior healthcare leaders (i.e. Primary Care Trust Chief Executives and their equivalents) that the needs of those involved with the criminal justice system are something to be dealt with specifically, as meeting them provides a benefit to society over and above the benefit achieved directly for these individuals.

Other identified frontline actions

141. The assumption is that for the remaining actions the costs will be included in existing business as usual or are not significant. However, work on these together with the benefits to be derived and any interdependencies are currently being developed in consultation with stakeholders across the PPN.

The Future

Recommendation 30: Scanning the horizon

Horizon scanning should be undertaken (on a regular basis) by the proposed independent Commission for Public Protection Information. (This links with the Governance recommendations).

Accepted

142. The Government accepts that horizon scanning will be crucial to continuous improvement in how we manage and use criminality information. Without it, in future we might experience similar problems to that set out in Sir Ian's Review. Horizon scanning to inform improvements in the way frontline staff manage and use information to tackle crime will be a key role of the independent Advisor (see response to recommendation 3).

Recommendation 31: Leading the debate on biometric data

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

Accepted

143. The Government welcomes this recommendation and believes that it is both timely and helpful to examine these issues in detail. Ministers are proposing to publish a White Paper which will look at the application of forensic science in the criminal justice system and will include an assessment of the proportionality of the current approach. The paper will have a significant, but not exclusive, focus on DNA. However, the Government will consider the judgement by the European Court in the cases of S and Marper which is expected in early December, before making that assessment.

ction Plan

Recommendations	Status	Benefits	Progress	Key Milestones
Section 1 – Strategic Direction				
Recommendation 1. *By January 2009 the Government should agree, across departments, a strategic direction for the improvement of criminality information across the Public Protection Network (PPN), with prioritised immediate objectives for improvement.*	**Accepted**	Benefits in terms of prioritising criminality information management. Will provide greater efficiency and effectiveness of spend across the PPN. Scope to quantify benefits will only emerge as planning and delivery work goes forward.	Concept of, and approach to, strategic direction agreed.	**By December 2008:** Further stakeholder engagement and development of a strategic direction. **By January 2009:** Ministers consider and sign off the strategic direction.
Section 2 – Governance and Delivery				
Recommendation 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.*	**Accepted**	Unit focused on the Magee agenda working with stakeholders across the PPN to facilitate resolution of problems in current business processes and identify other areas where improvement is needed.	The Criminality Information Unit (CIU) based in the Home Office was established on 01 August 2008. CIU is working with key partners to take forward the Magee agenda.	**By December 2008:** Publication of Government response.

Recommendations	Status	Benefits	Progress	Key Milestones
Recommendation 3. *The work of the agencies and Unit should be governed by a Home Secretary-chaired Ministerial group with external challenge and advice from a Commission for Public Protection Information.*	**Accepted**	Benefits in terms of continued focus and ownership of the criminality information agenda. Will lead to improved prioritisation, co-ordination and decision-making. Independent scrutiny will assist in expediting decisions on bottlenecks to delivery.	It has been agreed that the National Criminal Justice Board (with its membership suitably extended for this purpose) will act as the senior Ministerial group. It will be supported by a Home Office - chaired junior Ministerial group. Ministers have agreed that external challenge and advice will come from a single Independent Advisor.	**By Jan 2009:** Ministerial governance established. **By early 2009:** Recruitment process for Independent Advisor started.
Section 3 – Leadership				
Recommendation 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.*	**Accepted**	Benefits are in terms of prioritising criminality information management. Benefits will feed through into improved data quality and availability and therefore better decision making at all levels around public protection. May have dividends in terms of efficiency. Scope to quantify benefits will only emerge as planning and delivery work goes forward.	Means by which specified awareness can be demonstrated have been identified; e.g. allocating clear leadership roles, giving clear messages to staff, including issues on board and other agendas, in job descriptions, in training and development programmes, in inspection, review and risk management arrangements etc.	**By March 2009:** In liaison with the relevant organisations, develop guidance on how to demonstrate awareness. **By April 2009:** Agree guidance with Senior Business Forum. **By October 2009:** Report to Senior Business Forum on extent to which specific action is being taken to demonstrate awareness.
Recommendation 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*	**Accepted**	Clear commitment at leadership level will reinforce focus on criminality information management.	Approach to the statements of intent agreed by cross-Government steering group.	**By December 2008:** Ministerial statement of intent incorporated as introduction to Government response. Senior leaders within PPN organisations make tailored statements of intent for their own organisations.

Recommendations	Status	Benefits	Progress	Key Milestones
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 6. *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*.	**Accepted in principle**	Benefits realised will be in terms of: • improved focus on and prioritisation of criminality information management • improved data quality and availability • better decision making around public protection	Relevant training and development programmes identified.	**By February 2009:** Develop best practice guidance around how to include importance of information management in relevant programmes. **By May 2009:** Finalise guidance with those responsible for relevant programmes and agree how their programmes need to be developed to take account of it. **By August 2009:** Support those responsible in adapting programmes as necessary.
Recommendation 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*	**Accepted in principle**	A consistent and supportive set of tools and processes to support criminality information handling across the PPN.	Work has begun on developing a process for carrying out assessment.	**By January 2009:** With leaders develop a process for carrying out assessment. **By June 2008:** Senior Business Forum to review outputs from assessment process. **By July 2009:** Based on the outcome of the assessment, leaders make a public

Recommendations	Status	Benefits	Progress	Key Milestones
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*				commitment to delivering the necessary facilities and support for staff to improve capacity and confidence in criminality information.
Section 4 – Risk and Risk Management				
Recommendation 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).*	**Accepted in principle**	Improved handling and identification of risks will enhance public protection and support the effective allocation of resources.	Senior leads for risk management within key organisations identified. Work to draw out existing good practice is under way.	**By March 2009:** Taking account of existing good practice, develop central guidance on how to: • identify • assess the potential impact of • escalate where necessary • manage (in conjunction with other agencies where necessary) • report on risks to public protection. **By April 2009:** Provide relevant

Recommendations	Status	Benefits	Progress	Key Milestones
Recommendation 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.*	**Accepted in principle**	See recommendation 8.	See recommendation 8.	audiences with the guidance and seek their commitment to its application, offering support and advice where necessary **By September 2009:** Review application and effectiveness of guidance and report back to Senior business forum
Recommendation 10. *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.*	**Accepted in principle**	See recommendation 8.	See recommendation 8.	
Recommendation 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.*	**Accepted**	Inclusion in inspection frameworks will help to ensure risk management standards are maintained.	Relevant inspection and review bodies identified. Review of existing inspection arrangements has begun.	**By May 2009:** Taking account of existing good practice, develop standardised arrangements for: • assessing/inspecting the effectiveness of risk identification and management • feeding the outputs back to appropriate levels of management **By August 2009:** Provide relevant inspection bodies with

Recommendations	Status	Benefits	Progress	Key Milestones
				the procedures and seek commitment to their application, offering support and advice where necessary. **Once Ministerial structures established:** Ministerial structures to receive regular reports and to ensure that roles are acted upon and that the agreed approach to inspection is fully established across all PPN organisations.
Recommendation 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.*	**Accepted in principle**	Training will ensure managers at all levels are focused on risk issues.	Relevant leaders are being identified and a process for assessing current provision is being developed.	**By May 2009:** Linked to recommendation 7, agency heads/leaders to complete process of assessing the adequacy of training in risk assessment and management. **By July 2009:** Agency heads/leaders to include training in risk assessment and management in commitment to delivering necessary facilities and support for staff.
Section 5 – Investment				
Recommendation 13. *Investment Boards in the various public protection organisations should always take account of wider public protection priorities in making funding decisions. Sir Ian was encouraged by*	**Accepted**	Investment will be more efficient in supporting public protection across the board.	Initial engagement with Investment Boards and similar structures to examine their existing procedures.	**By February 2009:** Complete examination of existing procedures. **By May 2009:** Complete process advice to Boards and agree with Senior Business Forum.

Recommendations	Status	Benefits	Progress	Key Milestones
work being done to create an assessment process at inception for new projects and programmes, particularly where there is a substantial IT component. He recommends that the consideration of wider public protection benefit is embedded in that process.				**By December 2009:** Support relevant Boards in embedding process advice in their procedures.
Recommendation 14. *The Implementation Team should facilitate mechanisms to ensure better joined up approaches to investment across the PPN. This should include unblocking problems quickly to prevent delays in implementing solutions to improve the flow of criminality information.*	**Accepted**	Less scope for investment issues to impede progress on criminality information improvements.	Initial liaison with key organisations around extent to which they connect with counterparts on investment issues.	**By February 2009:** Complete examination of existing arrangements. **By May 2009:** Complete development of process for ensuring adequate connections and agree with Senior Business Forum, including a default process for resolving funding blockages. **By December 2009:** Support organisations in embedding and utilising improved processes.
Section 6 – International Dimension				
Recommendation 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*	**Accepted in principle**	The agreed approach will ensure a more coherent negotiating position with other countries, ensuring all the criminality information exchange requirements are identified and there is a single approach to each country rather than several organisations approaching	Stakeholder Workshop held on 26th November 2008 to discuss implementation of the international recommendations.	**By January 2009:** Agreed UK approach to international exchange of criminality information agreed.

Recommendations	Status	Benefits	Progress	Key Milestones
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 PPN.* • *The development of options for the future structure and governance of international criminality information exchange.*		them for different reasons. Rationalising the channels for data flow will make procedures easier to understand for frontline staff in PPN organisations and for foreign officials. It will be easier for PPN officials to know what information is available to them.		
Recommendation 16. *Police forces, individually and collectively, and other PPN organisations should nominate a lead official for international criminality information issues and the resulting network should be maintained by the Implementation Team.*	**Accepted**	CIU will have a central point of contact in each PPN organisation which will help them gain clearance and input for new policy initiatives. The wider network of contacts within the PPN organisations will raise awareness of international criminality information issues and allow input on how new initiatives will impact on the ground.		**By December 2008:** Write to PPN organisations asking for national level nominees as their lead official on international criminality information issues and asking them to co-ordinate a network within their own organisation. **By January 2009:** PPN international contacts are fed into the development of new policy as required.

Recommendations	Status	Benefits	Progress	Key Milestones
Recommendation 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 which would be affected or required to put them into effect. The agreed position should be re-visited periodically, as negotiations progress.*	**Accepted**	A more joined up approach to policy development will ensure that practical implementation and cost issues will be fully taken into account as policy develops and that delivery organisations have the chance to feed into policy development and are fully ready for the implementation phase.	Ministry of Justice have put forward suggestions for the use of the International Data Group.	**By December 2008:** Agree MoJ approach to use of International Data Group for this purpose **By January 2009:** All new policy initiatives are evaluated under the new arrangements.
Recommendation 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.*	**Accepted**	Joining the UK disclosure arrangements will plug a gap in the public protection arrangements whereby the Crown Dependencies are not currently able to request a criminal record check in relation to UK residents who go to the Islands to work with children and vulnerable adults.		**By December 2008:** Obtain agreement from Guernsey, Jersey and Isle of Man on how to proceed.
Section 7 – Technology				
Recommendation 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*	**Review accepted**	Input to an improved and integrated approach to developing information systems and supporting IT relevant to public protection.	Review work completed to date has been identified within • Home Office OCIO • Home Office NGISTT programme • OCJR Information Flows Review • CJIT Programme Initial interviews with CIOs across the	**By end February 2009:** • Based on the review work to date, identify areas or interfaces that have not been covered. • Map major information needs by volume and cost of crime impact across the PPN to identify breaks or

Recommendations	Status	Benefits	Progress	Key Milestones
where appropriate, to address any duplications, inter-operability issues and overlaps.			PPN have been carried out and a detailed delivery plan is in the process of being produced	inefficiencies. • Assess the impact of each break upon the efficiency or effectiveness of the PPN **By end May 2009:** Produce a prioritised list of initiatives based on an assessment of their cost, feasibility and impact
Recommendation 20. *Each CIO should consider as a matter of urgency giving effect to any simple tactical IT fixes that will support Sir Ian's recommendations elsewhere on improving criminality information management.*	**Accepted in principle**	Specific and targeted improvements to information systems.	Based on the recommendations made in the Review, progress has already been made on a number of initiatives. Of these, the two most dependent on technology are: • Prisoner Location System • UKBA estate management system	**By end February 2009:** Identify the initiatives currently under way across the PPN to improve the flow of criminality information and those planned in the immediate short term Continue with the work currently under way to deliver short term solutions **By end 2009:** Complete delivery of the tactical IT fixes and move into benefits tracking
Recommendation 21. *Building on the governance, processes, standards and architectures that will flow from Sir Ian's 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.*	**Accepted in principle**	IT systems in support of criminality information management will be more efficient, integrated and cost-effective.	The Cabinet Office is publishing a Government IT Strategy Draft governance structures are currently being produced in co-ordination with PPN leaders and this review	**Ongoing:** Deliver the PPN initiatives plan as identified and set out from Recommendation 19 **By Spring 2009:** Establish the IT governance and support element within the overall PPN governance structure **By Summer 2009:** Strengthen/ create the IT leadership role across the PPN

Recommendations	Status	Benefits	Progress	Key Milestones
Recommendation 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 Sir Ian's first Investment recommendation. This process should explicitly address use and reuse of IT capacity, making the maximum use of existing technology.*	**Accepted in principle**			Ensure all CIOs are aligned and bought into the Government IT strategy issued by the Cabinet Office **By Autumn 2009:** Produce a comprehensive IT development policy for the PPN, addressing: • Process/Data standards • Information sharing • Reuse of existing infrastructure • Support for inter-operability and elimination of duplication/ overlaps
Recommendation 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 PPN, and to encourage their active help and expertise in making suggestions as to how re-usability can be achieved, instead of building fresh systems.*	**Accepted in principle**	IT developments will be more focussed on the requirements of the PPN as a whole.	IT supplier base lining and sourcing work has already begun in the MoJ and Home Office	**By Spring 2009:** Produce a draft set of PPN IT supplier policy guidelines **By Summer 2009:** Work with the CIOs and practitioners across the PPN to produce an IT supplier guideline document to ensure that they: • comply with the policy set out as a result of Recommendations 21 and 22 • actively look across the whole PPN portfolio **By Autumn 2009:** Implement a PPN wide IT supplier sourcing strategy to help reduce development and delivery costs and increase solution effectiveness

Recommendations	Status	Benefits	Progress	Key Milestones
Recommendation 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.*	**Accepted in principle**	Uncertainties around governance of, and access to, the PNC will be removed. Visibility of criminality information from Northern Ireland will be improved.	National Police Databases Board established under NPIA auspices, with an ACPO chair. Technical feasibility of sharing data between PNC and PSNI/Causeway system in Northern Ireland has been established.	**By January 2009:** Clear agreement to be reached between all parties on how the improved links between the PNC and Northern Ireland should be funded. **By March 2009:** CIU to complete review of revised PNC governance arrangements, including procedures for considering and granting access to PNC.
Recommendation 25. *25: The SRO* [senior responsible owners] *for the remaining Bichard Recommendations should urgently re-consider the timetables for implementation with a view to expediting them. Sir Ian expects to see greater progress when he revisits these issues in early 2009, and in particular to see that the court resulting recommendation will be fully implemented by April 2009.* ('BR' references below are to the Bichard Inquiry Report Recommendations 2004.)	**Accepted**	Implementation of the remaining Bichard recommendations will further improve information management capabilities and underpin wider public protection and safeguarding arrangements.	Letters dispatched to Bichard SROs on 30 September 2008 and monitoring and review of progress on-going. All 31 Bichard recommendations accepted by (then) Home Secretary on 22 June 2004, on behalf of Government. 22 of 31 Bichard recommendations now substantially delivered, although full implementation in some cases is lengthy; work on-going to deliver nine outstanding Bichard Recommendations (as below). The Government remains committed to full implementation of all the Bichard recommendations – delivery milestones set out below.	**By April 2009:** Review of the scope to expedite outstanding recommendations.

Recommendations	Status	Benefits	Progress	Key Milestones
BR 1 - *A national IT system for E&W to support police intelligence should be introduced as a matter of urgency*		Improved police intelligence capabilities nationally and efficiency savings (non-cashable) for police service, in support of policing priorities.	Large and complex programme of work, now well advanced; procurement phase, involving three short-listed consortia, nearing conclusion with award of contract anticipated by March 2009. Roll-out and deployment of Phase 1 across the police service (sharing of intelligence and other information currently held on local systems) on track to commence in 2010 (target date). No scope to bring forward milestones due to the contractual timetable/ procurement considerations and required business change within forces.	**By 2010:** Deployment of PND will commence (Phase 1) - intelligence capabilities across the police service. **By 2010:** Compliance by all forces with the Management of Police Information Code of Practice.
BR 4 - *Investment should be made available by Government to secure the PNC's medium and long term future, given its importance to intelligence led policing and the criminal justice system as a whole.*		Long term arrangements for the national repository of police information/ intelligence.	Medium term future already secured. How best to secure the long term future is under consideration and subject to funding being available in the next CSR period.	**By 2014:** Anticipated deployment of PND Phase 2 – subject to CSR position/ Ministerial agreement.
BR7 - *Transfer of responsibility for inputting court results to PNC should be reaffirmed and accelerated ahead of 2006 target. At worst that deadline must be met.*		Improved public protection through the provision of better quality and timelines of data on PNC and reduced administrative burden on the police service.	Roll-out of the links between Magistrates' Courts and the Police National Computer has been achieved in 2 early adopter areas, with a third 'going live' shortly. A further version of the solution will be rolled out in the New Year, after which the phased deployment to remaining areas will begin. Changes to the Crown Court systems will be introduced early next year, with the link between Crown Courts and the Police National Computer are being introduced from the Spring**.**	**During 2009:** Full deployment of a technical solution to automate transmission of at least 80% of court results direct to PNC.

Recommendations	Status	Benefits	Progress	Key Milestones
BR19 - *New arrangements should be introduced requiring those who wish to work with children or vulnerable adults to be registered. This register would confirm that there is no known reason why an individual should not work with these client groups*		The Vetting and Barring Scheme will put in place robust arrangements to ensure unsuitable persons are prevented from working with children/ vulnerable adults.	Phased implementation of ISA. Vetting and Barring Scheme launch under way. ISA has been advising DCSF/ DH Ministers on new barring cases from March 2008; work to launch VBS remains on track for 'go-live' for new applications to the Scheme by October 2009, although limited or no scope to revise delivery milestones due to the complicated contractual timetable/ procurement arrangements.	**By January 2009:** ISA take over decision-making on new cases. **October 2009:** Launch of the Vetting and Barring Scheme by the Independent Safeguarding Authority and go-live for new applications.
BR 21 - *All posts that involve working with children and vulnerable adults should be subject to the Enhanced Disclosure regime.*		Establishing the necessary legal provisions to underpin the VBS operation.	Following earlier changes to requirements of the ED regime, secondary legislative provisions are being brought forward under the launch of the VBS and are on schedule to be in place at 'Go Live' (October 2009).	**By October 2009:** Completion of the second tranche of legislative changes to securing further amendments to Rehabilitation of Offenders Act, brought in under the VBS launch.
BR 23 & 25 - *CRB/ Registered Bodies should be able to check passports/ driving licences presented as proof of identity against IPS/ DVLA databases/ Fingerprints should be used as a means of verifying identity.*		More rigorous identity checks.	The CRB has issued revised guidance to all Registered Bodies and participated in joint work with IPS; future progress has been subsumed into the longer-term work under the HO Identity Management Strategy Programme.	Further progress substantially linked to HO ID Management Programme.
BR30 - *Proposals should be brought forward as soon as possible to improve the checking of people from overseas who want to work with children or vulnerable adults.*		Improved vetting checks drawing on wider pool of relevant data.	EU States: UK Central Authority (UK-ECR) established to handle all requests for conviction data and participation in EU initiatives on-going. Non-EU States: HO leading project work to establish scope for reciprocal arrangements for exchange of data, focusing initially on Australia.	**By January 2009**: Following discussions across the Home Office a more targeted approach to the obtaining of European criminal conviction data for employment vetting purposes has been agreed. This will be tested and advice sent to Ministers setting out high level options.

Recommendations	Status	Benefits	Progress	Key Milestones
BR 31 - As a priority, legislation should be brought forward to enable the CRB to access additional databases for vetting purposes.		Improved vetting checks drawing on wider pool of relevant data.	Following establishment of a legislative gateway, the CRB has access to relevant data in all UK Forces, inc. Police Service Northern Ireland, Service Police Crime Bureau (for Army, Navy & Air Force data), Ministry of Defence Police and SOCA. The CRB work is on-going with CEOP, HMRC, Isle of Man and the Channel Islands.	**Ongoing**: As new criminality data sources are identified the CRB will continue to extend its access to stakeholder intelligence data for vetting purposes.
Section 8 – At the Frontline				
Recommendation 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.*	**Accepted in principle**	Clearer understanding of the nationality of prisoners. More efficient decision making regarding removal of foreign nationals. Reduced risk of harm to the public as a result of removing foreign national offenders.	Government departments and agencies across the PPN are in the process of developing a Crime and Justice Identity Management Strategy. The strategy, which will be completed by March 2009, will aim to develop a consistent approach to the establishment and use of identity. **Early practical steps:** UKBA to ensure that both pre and post sentence, all individuals who cannot prove UK nationality and who meet minimum sentencing and non-EEA (i.e. 12 month) criteria are referred for consideration by CCD, with CCD verifying and applying nationality criteria for deportation eligibility. As a priority, UKBA and the Prison Service are working together to ensure that foreign national prisoners are identified and their status checked earlier in the criminal justice process. This will help to ensure that those individuals eligible for deportation can be quickly and efficiently removed at the end of their sentences.	**By January 2009:** Pilot new information sharing processes to check foreign national prisoners completed. **By March 2009:** Crime and Justice Identity Management Strategy completed.

Recommendations	Status	Benefits	Progress	Key Milestones
			CIU is investigating whether there are ways this can be done earlier. UKBA will pilot new information sharing processes to ensure that all prisoners will have their nationality checked, where possible against trusted data sources. Prisoners whose nationality remains in doubt will be referred to UKBA to verify nationality if possible. This pilot is due to be completed by the end of January 2009. A full review of costs, benefits and success will be carried out at the end of the pilot.	
Recommendation 27. *Clear accountability and standard procedures should be developed to manage storage and access to all key PPN information.*	**Accepted in principle**	Reduced risk of harm to the public as a result of returning to custody those offenders that are wanted by the police on other matters.	**Early practical steps:** All police forces to implement prisoner location and release information solutions Work is under way to reduce the risk of offenders being released from prison into society when they are wanted by the police on other matters. The Police and Prison Services have made significant progress on this with offender location information accessed and interpreted locally in a number of forces. A longer term solution is being considered which would make this information available nationally but it will be dependent on central funding.	**By December 2009:** Ensure that all Police Forces are making use of offender location and release information for the benefit of public protection.

Recommendations	Status	Benefits	Progress	Key Milestones
Recommendation 28. *Where information sharing is both necessary and proportionate to support effective public protection, arrangements should be systematic, proactive and accountability clear.*	**Accepted in principle**	Reduced cost per removal of foreign national offenders by reducing the time spent in immigration detention after appeal rights have been exhausted. Reduced risk of harm to the public by promptly triggering offender management procedures for foreign national offenders released into the UK on bail. Speed up the removal of foreign national prisoners whose appeal rights have been exhausted.	The Crime and Justice Identity Management Strategy will also seek to improve information sharing across the PPN by linking relevant personal data to an identity accessible by all agencies. **Early practical steps:** Determinations from tribunals of foreign national prisoner appeals should be passed on promptly to caseworkers in UKBA CCD, Prisons, Probation and IRCs. A bail hotline has been set up which ensures that CCD caseworkers receive immigration bail determinations within a few hours and went live on 1 October 2008. Arrangements have been made for appeal rights exhausted cases to be notified quickly to caseworkers. Delivery was completed on 20 October 2008.	
		Increased efficiency and safety in the management of foreign national offenders held in immigration detention. Increased capacity for removals per bed in the immigration detention estate.	**Early practical steps:** UKBA to consider bringing together and providing a more integrated information system to improve the interface between DEPMU, IRCs, CCD and AIT to facilitate better information access and more effective oversight and management of processes. Work has been completed in defining an operating model for the immigration removals estate. Further activity is under way in UKBA to analyse and understand	**By March 2009:** Agree full list of information requirements for management of the immigration removal estate. **By July 2009:** Identify whether these requirements will be met by wider UKBA initiatives or need to be met by those responsible for managing the immigration removal estate.

Recommendations	Status	Benefits	Progress	Key Milestones
			the full business requirements associated with this action and to consider appropriate solutions for delivery that are not currently met by existing initiatives.	
Recommendation 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.*	**Accepted in principle**	An increase in public protection through employers systematically making better use of available criminality information. A reduction in effort expended by government and employers in righting guidance on the use of criminality information by having a single core guidance owner. Sharing of good practice in the use of criminality information by employers.	**Early practical steps:** 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. These standards to be incorporated into relevant employer guidance (for example Department for Children, Schools and Families) and existing employer inspection regimes (e.g. Ofsted). Vetting and barring stakeholders have agreed that there should be core guidance for employers on best practice in the use and sharing of criminality information. The Home Office Vetting and Safeguarding Policy Unit, in conjunction with other government departments, is leading this work.	**January 2009:** Issued employment guidance for the use of criminality information following consultation with stakeholders. Release to be co-ordinated with roll-out of new guidance (and hence employer action required) being produced for the Vetting and Barring Scheme.

Recommendations	Status	Benefits	Progress	Key Milestones
		A more comprehensive approach to reducing re-offending by ensuring that health needs of offenders are met as part of their overall needs for successful resettlement. Reduced costs of handling re-offenders for organisations in the PPN. More appropriate care for a section of society with particularly complex health and social care needs.	**Early practical steps:** 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. Health and public protection practitioner workshops identified key ways to improve the relationship between these groups for the overall benefit of public protection.	**By March 2009:** Assess available health and public protection information sources to inform provision of healthcare for those managed by the Criminal Justice System.
Section 9 – The Future				
Recommendation 30. *Horizon scanning should be undertaken (on a regular basis) by the proposed independent Commission for Public Protection information. (This links with the Governance recommendations).*	**Accepted**	Issues identified before they become problems.	This is linked to recommendation 3 and is being considered alongside it.	**By February 2009:** CIU to establish interim function. **By October 2009:** Full horizon scanning function to be in place under auspices of independent Advisor.
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.*	**Accepted**	Improved foundations for developing work around biometric information.	Initial discussions about feasibility of using the proposed forensic science White Paper as a helpful vehicle.	**By Spring 2009:** Determine how the debate will be carried forward, taking account of developments in relation to the White Paper.

Printed in the UK by The Stationery Office Limited
on behalf of the Controller of Her Majesty's Stationery Office
ID5984242 12/08 414571 19585

TSO
information & publishing solutions

Published by TSO (The Stationery Office) and available from:

Online
www.tsoshop.co.uk

Mail, Telephone, Fax & E-mail
TSO
PO Box 29, Norwich NR3 1GN
General enquiries: 0870 600 5522
Order through the Parliamentary Hotline *Lo-call* 0845 7 023474
Fax orders: 0870 600 5533
Email: customer.services@tso.co.uk
Textphone: 0870 240 3701

TSO Shops
16 Arthur Street, Belfast BT1 4GD
028 9023 8451 Fax 028 9023 5401
71 Lothian Road, Edinburgh EH3 9AZ
0870 606 5566 Fax 0870 606 5588

The Parliamentary Bookshop
12 Bridge Street, Parliament Square
London SW1A 2JX

ISBN 978-0-10-175112-4