



New Powers Against Organised and Financial Crime

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

July 2006

© Crown Copyright 2006

The text in this document (excluding the Royal Arms and departmental logos) may be reproduced free of charge in any format or medium providing that it is reproduced accurately and not used in a misleading context. The material must be acknowledged as Crown copyright and the title of the document specified.

Any enquiries relating to the copyright in this document should be addressed to The Licensing Division,
HMSO, St Clements House, 2-16 Colegate, Norwich, NR3 1BQ.
Fax: 01603 723000 or e-mail: licensing@cabinet-office.x.gsi.gov.uk

A consultation produced by the Home Office.
This information is also available on the Home Office website www.homeoffice.gov.uk

ISBN:
1-84726-005-5
978-1-84726-005-5

Contents

Foreword -----	
Introduction -----	1
How to Respond -----	2
What Will Happen Next? -----	3
Executive Summary -----	4
The Proposals -----	12
Consultation Questions -----	40
Departments and Organisations Consulted During the Development of this Paper -----	42
Consultation Co-ordinator -----	43
The Consultation Criteria -----	44
Glossary -----	45
Relevant Legislation - (with hyperlinks where available) -----	46

Foreword

Home Secretary

In March 2004 the Government in its White Paper ‘One Step Ahead, a 21st Century Strategy to Defeat Organised Crime’ (Cm6167) set out its plans for bringing a new approach to tackling organised crime, a class of crime which causes social and economic costs of upwards of £20bn to the UK each year.

We want to make the UK the least desirable place for organised criminals to operate. The White Paper set the direction and we are now beginning to see the fruits of it. The Serious Organised Crime Agency (SOCA) came into being on 1 April this year. We therefore now have a single dedicated enforcement agency responsible for tackling organised crime and reducing the harms it causes. Its approach will be intelligence-led and prioritised towards those criminal networks and markets causing the most harm.

SOCA, and the rest of the law enforcement community, also needed new tools if they were going to make the inroads required. Thus in the Serious Organised Crime and Police Act 2005 we provided the power to compel individuals to cooperate with investigators, and we established a clear regime of incentives for defendants to testify against their criminal associates. These powers are now in place and ready for use but we think that there are further measures which would make it even harder for the criminals to operate.

Good information and intelligence are essential if SOCA is to identify and target the most serious organised criminals, yet the level of data shared within government, let alone between government and the private sector, is remarkably low. This is exploited by criminals, especially those involved in fraud. This needs to change. I believe that we can do this without infringing data protection legislation or people’s rights.

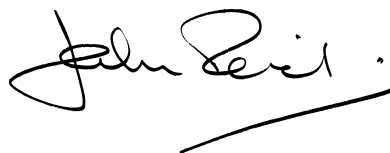
The 2004 White Paper noted that there was a gap in the criminal law for catching those involved at the edges of organised crime. We have now

developed proposals, building on Law Commission proposals, which would fill that gap.

Currently law enforcement authorities essentially have a choice between prosecution or no action when dealing with organised crime. That can be a stark and unproductive choice and we see a place for something in between – organised crime prevention orders – which could be imposed on individuals or organisation in such a way as to prevent organised criminality continuing.

The Proceeds of Crime Act 2002 introduced new powers to seize and recover criminal assets which have been strongly welcomed and have been successful. But experience has shown that there is room for improvement in how some of the provisions operate, and I believe we should make these improvements.

There can be no let up in our attack on organised criminality and this consultation document puts forward proposals which build on and complement our overall strategy. I would welcome your views on them.



Dr John Reid

Introduction

The purpose of this paper is to seek stakeholder views and to explain the proposals for new powers against those committing organised and financial crime.

The consultation is aimed at those with an interest in Criminal Justice and data sharing issues in the UK.

It is available as a printed document, and can also be downloaded from www.homeoffice.gsi.gov.uk

This consultation is being conducted in line with the Code of Practice on Written Consultation issued by the Cabinet Office. The Code Criteria are set out in Annex B of this document.

A partial Regulatory Impact Assessment is available on the Home Office website.

The aim of this paper is to generate thought and discussion of these proposals in order to receive views and comment. In order to achieve this we are specifically distributing this document to and inviting comments from:

- Law enforcement agencies
- The Judiciary
- Financial institutions and regulated bodies

The consultation is also open to Other Government Departments, interested organisations and members of the public to contribute.

The full list of those who we consulted in developing this paper can be found at Annex B.

How to Respond

The closing date for comments is 17th October 2006.

There are a variety of ways in which you can provide us with your views.

You can email us at:

Oc.consultation@homeoffice.gsi.gov.uk

Or you can write to us at:

**OC Consultation
Specialist Crime team 2
5th floor Fry building
2 Marsham Street
London
SW1P 4DF**

Additional copies of this paper are available through our website
www.homeoffice.gov.uk

Alternative Formats

You should also contact the Organised Crime Consultation Team should you require a copy of this consultation paper in any other format, e.g. Braille, Large Font, or Audio.

Responses: Confidentiality & Disclaimer

The information you send us may be passed to colleagues within the Home Office, the Government and related agencies.

Furthermore, information provided in response to this consultation, including personal information, may be published or disclosed in accordance with the access to information regimes (these are primarily the Freedom of Information Act 2000(FOIA), the Data Protection Act 1998 (DPA) and the Environmental Information Regulations 2004).

If you want the information that you provide to be treated as confidential, please be aware that, under the FOIA, there is a statutory Code of Practice with which public authorities must comply and which deals, amongst other things, with the obligations of confidence. In view of this it would be helpful if you could explain to us why you regard the information you have provided as confidential. If we receive a request for disclosure of the information we will take full account of your explanation, but we cannot give an assurance that confidentiality can be maintained in all circumstances. An automatic confidentiality disclaimer generated by your IT system will not, by itself, be regarded as binding on the Department.

Please ensure that your response is marked clearly if you wish your response and name to be kept confidential.

Confidential responses will be included in any statistical summary of numbers of comments received and views expressed.

The Department will process your personal data in accordance with the DPA – in the majority of circumstances this will mean that your personal data will not be disclosed to third parties.

Individual contributions will not be acknowledged unless specifically requested.

Representative groups are asked to give a summary of the people and organisations they represent when they respond.

Thank you for taking the time to read this document and respond.

What Will Happen Next?

The Consultation Period will end on 17th October 2006.

We expect to publish a summary of the responses received within 1 month of the closing date for this consultation, and this will be made available on the Home Office website.

Executive Summary

The White Paper 'One Step Ahead'¹ set out a radical departure in the way we tackle organised crime. It included proposals for institutional changes, new powers and the better use of existing ones, all integrated into a new strategy for tackling the problem

The fundamentals of this new approach are simple. We are turning away from defining success by the number of essentially tactical outputs like volumes of seizures, or the number of arrests or operations. Instead we want to measure our success by the extent to which we can prevent organised crime harms in the first place; to demonstrate that we have disrupted illicit markets and to change profoundly the risk / reward relationship which currently favours the criminal.

Progress Since the White Paper

The period since the White Paper has seen huge steps made to implement its vision and deliver a more effective national capability against organised crime.

Most obvious have been the institutional changes. The Serious Organised Crime and Police Act 2005 (SOCPA) established the Serious Organised Crime Agency (SOCA), which came into being on 1 April 2006. Meanwhile, major steps have been taken to improve the police response to 'level 2' (regional) organised crime, long seen as a major gap.

Improving police force capacity against 'level 2' crime has been identified as one of the three initial priorities for the new National Policing Improvement Agency (NPIA), and £10m additional funds have been provided to forces in 2006-07 and 07-08 to build regional capacity. Her Majesty's Inspectorate of Constabulary have reported on the need to improve forces' capacity in protective services, including against organised crime. The Home Secretary has made it clear that delivering this improved capacity is our priority, and discussions continue with police forces and authorities on the way ahead.

All these changes are necessary but not sufficient steps on the way to changing fundamentally the risks and rewards confronting potential organised criminals. We have been working over the past couple of years with SOCA's precursor agencies, SOCA itself and local forces to understand the business of organised crime, and to develop a strategy to change the risk reward relationship which organised criminals face.

First, we need to prevent crime opportunities, by helping victims protect themselves and working to reduce the demand for illicit products. Operations like GRAFTON, which has made significant inroads into high value theft at Heathrow are a model for 'target hardening' approaches, while Government is devising strategies to reduce both the supply of victims of people trafficking and

¹ Cm 6167

the demand for their services to mirror long standing policies to reduce the demand for illicit drugs.

Secondly, the strategy involves ensuring resources are targeted against the most serious offenders. The traditional approach to organised crime has been a series of discrete, tactical operations against members of particular criminal groups. While the operations themselves were often highly effective, intelligence information frequently became scattered in operational case files and not collected centrally, meaning that law enforcement has had disparate snapshots of criminal groups' activities, rather than a coherent ongoing picture.

The creation of SOCA has provided an unprecedented opportunity to build on operational success while also developing a fresh and comprehensive database of knowledge, putting together the jigsaw pieces from the precursor agencies. This process has identified over 1000 individuals of interest, with a core of top national targets and a wider group of associates. Many of those individuals who are now identified as top national targets have not been subject to recent law enforcement attention, and SOCA is ensuring its resources are redirected against them. This alone should deliver a sharp increase in the average impact of SOCA operations, as they are increasingly targeted on players of real national significance.

A similar process has been underway in the Metropolitan Police (MPS). The MPS' new approach to 'Organised Crime Networks' in the London area has similarly pulled together data from across the force area to give a rich picture of the criminal networks causing most harm to London.

This sort of work is enabling both SOCA and other law enforcement to maximize the impact of their effort, moving from tackling 'targets of opportunity' to a more clearly centrally directed prioritisation of targets, focusing on those causing most harm. At the same time, a new focused approach to collecting intelligence, for example through SOCA's National Intelligence Requirement (NIR), is designed to uncover progressively more significant players currently invisible to law enforcement.

Thirdly, law enforcement has been working to drive up the efficiency of its operations, to deliver more investigations and prosecutions from its existing resources.

SOCA is working closer than ever with prosecutors to ensure cooperation at an early stage in order to avoid wasted effort and improve the efficiency of case preparation. At the same time, CPS has appointed 'organised crime counsel' from the professional Bar who will personally take prosecutions and share their trial expertise with CPS caseworkers. Together, these measures are ensuring a much more tightly integrated approach from initial casework through to trial.

At trial, organised crime cases have traditionally been bedevilled by the complexity of the case and the burdens of disclosure. Recent rulings in the House of Lords have helpfully clarified the position on disclosure, and clearer practice directions and a new disclosure manual should help reduce unnecessary burdens and improve the efficiency of the trial process.

The new powers in SOCPA help too, notably the 'disclosure notices' which enable prosecutors to require subjects to produce documents and answer questions on them, and the new provisions putting Queen's Evidence on a statutory footing.

Fourthly, we are looking to ensure that penalties have the maximum possible impact on preventing future harm from organised criminals. In particular, Government is reviewing the working of the asset recovery process with a view to delivering a further step change in performance to the point that asset recovery begins to impact on the criminal economy as a whole as well as on individual criminals.

SOCA's new approach to 'lifetime management' of organised crime offenders is beginning to take shape, with plans, for example, to impose tailored licence conditions on organised crime offenders after release from prison and to apply to courts to impose the new Financial Reporting Orders established in SOCPA to monitor convicted criminals' finances.

Finally, the vision in the White Paper put considerable stress on alternative ways to disrupt organised crime in addition to prosecution. As well as being a powerful disruption tool in its own right, successful prosecutions have major advantages for increasing public confidence in the law. But it remains an output serving our ultimate objective, which is to prevent crime happening in the first place.

SOCA has begun the process of ensuring all known foreign organised criminals and their associates subject to immigration control have their details entered on the Warnings Index, enabling us to prevent them receiving visas to visit the UK, and we are working with the Association of Chief Police Officers (ACPO) to improve police use of the same facility. The Assets Recovery Agency's mix of cases has moved from a predominance of failed prosecution referrals to an increasing number of cases where the Agency is able to use its civil recovery and tax powers against those individuals who have never been prosecuted. This is particularly the case in Northern Ireland.

International cooperation is also continuing to play a major role, with SOCA successfully integrating the separate liaison officer networks previously controlled by HM Customs and Excise and the National Criminal Intelligence Service, and working on key strategic relationships with major overseas partners.

Gaps Remaining

There is no doubt that SOCPA and other recent initiatives have considerably improved the range of tools at agencies' disposal against serious and organised crime. Work with SOCA's precursor agencies, SOCA itself and law enforcement more generally has, however, suggested that some continuing gaps in our capability remain. Some of these were already highlighted in the White Paper, others have emerged while fleshing out with law enforcement the details of our new approach.

Knowledge and Data Sharing

Every single aspect of this new effort against organised crime depends on a considerable improvement in the quality and use of our information about the threat. Improved knowledge is SOCA's key strategic priority.

SOCA has radically overhauled the intelligence it inherited from the precursor agencies and is building a data set much more fit for purpose. The IMPACT programme for police forces is similarly putting in place a mechanism for sharing information across force intelligence databases. Underlying all this, and as anticipated in the White Paper, improved guidance has gone out on the sharing of law enforcement information, with a Code of Practice on the Management of Police Information issued earlier in 2006, and SOCA issuing in 2005 its own Statement of Information Management Practice setting out how it would use the specific gateways provided in SOCPA.

While this progress is welcome, to make a real impact, law enforcement needs to use a lot more than the information at its own disposal. It has become increasingly clear from discussions with our stakeholders that data sharing with other parts of the public sector is highly patchy, while sharing across the public-private divide is rarely even attempted.

Meanwhile, pilot exercises in the identity fraud arena and within SOCA are throwing up striking examples of what can be done when public and private data is shared, with particular potential to reduce financial crime, money laundering and fraud. Pilot exercises within the insurance industry and analysis of fraud against the tax credit system are just two areas where closer scrutiny has revealed a much greater organised fraud component in what had previously been thought to be simple volume fraud.

Whenever problems with data sharing crop up, the assumption is often that there are problems with the Data Protection Act 1998 (DPA). In practice, we have found no evidence that the Act places genuine obstacles in the way of sensible and proportionate data sharing. Excessive caution about the Act's provisions are a problem, as is the common fear that disclosure will have repercussions.

A more significant problem we have identified is with public sector bodies and departments whose underlying powers do, or are perceived to, set unnecessary limits on data sharing within the public sector and beyond.

This paper sets out some simple and practical steps for improved data sharing, which we believe could make a considerable impact against financial crime, fraud and money laundering. Our proposals reflect similar findings being identified in the Fraud Review, as well as the Lander review of the Suspicious Activity Report (SAR) regime and the wider work across Government to develop a common strategy on data sharing across the public sector.

We believe that Government agencies should commit to:

- The public sector sharing information internally and with the private sector where this is potentially in the public domain anyway and would be

helpful in preventing crime - for example the names and details of deceased persons

- Putting a mechanism in place to enable the public sector to share information with themselves and with the private sector on suspected frauds. A strong vehicle for delivering this in the short term would be for departments and public agencies to become members of *CIFAS – the UK's Fraud Prevention Service*. This is likely to require legislation to amend the vires of a number of agencies, notably again HMRC, DWP and DVLA
- Suspicious Activity Reports coming into SOCA being routinely matched against data in a range of other departments' databases, notably HMRC, DWP, DVLA and the Passport Service in order to develop the intelligence value of the reports and identify reports with a particularly strong indication of crime
- The Audit Commission's National Fraud Initiative, which matches data across a range of public sector bodies to identify fraud against audited bodies, being put on a specific statutory footing, and its scope expanded
- Law enforcement and the public sector being able to engage in targeted and proportionate data mining of public and private sector databases to identify cases where the information supplied for different purposes is so incongruous that there is a strong suspicion of criminal activity. These exercises will need to be carefully structured to ensure they get the balance right between the needs of law enforcement and the privacy of the individual, and we will discuss approaches with the Information Commissioner

The implementation of these proposals will need careful management to maintain a proper balance between respecting privacy rights, while ensuring that publicly held data can be properly used to prevent crime, as the public has every right to expect. Nothing that we are proposing is likely to pose DPA problems, but it is important that processes across the public sector are adjusted to ensure that the public are aware when passing information to Government of the legitimate purposes to which it will be used, while Government is also examining ways of ensuring data is protected against misuse.

Streamlining Investigations and Prosecutions: Filling Gaps in the Criminal Law

As has already been discussed, there is a whole range of measures in place to improve the efficiency of investigations, prosecutions and trials. But we have been conscious for some time of possible gaps in the criminal law as it impacts on organised crime. The White Paper committed us in particular to reviewing the law of conspiracy, while the Law Commission has separately been considering the law around encouraging and assisting crime.

The Law Commission has now reported with proposals on encouraging and assisting crime². We welcome these proposals, and are considering adopting them while looking at how they can be extended to deal more effectively with those on the periphery of organised crime through special targeted provisions.

Maximising the Impact of Penalties: Asset Recovery

We have also been looking at some important, if essentially technical, changes to the Proceeds of Crime Act 2002 (POCA). These would enable us, for example, to enable financial investigators who are police staff to exercise more of the powers under POCA, to contract out the enforcement of confiscation orders, and to examine what improvements might be necessary to the 'consent regime' in POCA.

Other Disruption Tools to Prevent Crime: Serious Crime Prevention Orders

The new strategy against organised crime goes beyond the traditional focus on law enforcement operations. SOCA and other law enforcement are increasingly interested in alternative tools which can prevent crime from happening in the first place, rather than simply dealing with the offenders afterwards.

Working with SOCA, police and other law enforcement agencies, it has been striking to see how many fewer levers law enforcement has against these sort of criminals than, say, white collar criminals or lower level anti social behaviour, or the sort of powers that regulators often have against businesses in their sectors. At present, law enforcement basically has the option of prosecution or nothing.

This presents law enforcement with real problems in coming to grips with a sort of crime which in addition to being highly harmful and requiring long and complex investigations, also has many of the characteristics of a business and may depend on a range of facilitators with varying degrees of culpability in the underlying criminality.

We propose a new type of civil orders, capable of being imposed against individuals or organisations, covering a wide range of potential prohibitions or requirements. The court would work to a civil standard of proof, with the court having to be satisfied that the proposed measures are necessary and proportionate to reducing the threat from organised crime, taking into account the human rights of all those potentially affected. Breach of the order would be a criminal offence

We can see three basic areas where these orders would come in useful.

² Inchoate Liability for Assisting and Encouraging Crime: July 2006
http://www.lawcom.gov.uk/assisting_crime.htm

Prevention orders against known criminal individuals would be designed to impose conditions which should make carrying out crime more difficult; for example imposing restrictions on travel or limiting the use of communications to phone numbers which had been notified in advance. Even if these restrictions failed in their primary aim to deter continuing criminal activity, they would either force the subject to change his way of working, leaving himself open to easier law enforcement scrutiny, or in the case of a stubborn refusal to follow the order's provisions at all, the subject would become vulnerable to breach proceedings.

These sort of orders might be used in cases where there was a strong weight of evidence but either not enough for a prosecution, prosecution was planned but additional measures were urgently needed to prevent harms in the interim, prosecution had been ruled not appropriate on public interest grounds, or the evidence of criminal activity could not be prosecuted (eg because it took place overseas). These sorts of orders could be imposed to prevent criminal activity in the first place, but they might also constitute an alternative disposal for those individuals at the fringe of major cases who were not targeted for prosecution, but from whom specific assurances of future good behaviour are needed, or for individuals preparing to agree a deal under the Queen's Evidence provisions in SOCPA.

At least as important as orders against individuals, however, is the idea of orders against companies or other organisations facilitating organised crime. Businesses in particularly sensitive areas are already subject to regulation to protect the public, and the Hampton review of regulation has noted and encouraged an increasing trend away from onerous blanket regulation towards a more risk based approach. Organised crime obviously does not make up an easily identifiable sector of the economy. These orders hold out the prospect of a new kind of regulatory regime, flexible and risk based, imposing no burdens at all on legitimate companies but a proportionate and highly targeted burden on specific organisations for which there is already good evidence of complicity in criminal activity.

Orders could restrict businesses' activities in certain areas or with certain customers, or permit certain lines of business only in return for transparency about customers - for example, a company making concealed compartments supposedly to enable drivers to hide their valuables, but which in practice have been used to conceal drugs. Making the compartments is not in itself illegal, but an order could impose a requirement on the business to notify law enforcement of the details of all such compartments which have been fitted and the details of the customers.

With many of these businesses straddling the legitimate and illegitimate economy, there should be a good prospect of these orders succeeding in prompting many businesses to leave the criminal field, faced with the restrictions and the reputational risk which these orders would impose. If the businesses continued to be complicit in organised crime, the restrictions imposed should make them more vulnerable to law enforcement action.

Finally, we would see the orders as enabling law enforcement to apply to the courts to have companies or other organisations restructured, or to require

individuals to divest themselves of interest in certain assets if measures of these sort were considered proportionate to reduce the harm done by serious crime, taking into account the rights of all those affected.

Conclusion

Together, we see these proposals as marking a significant shift in the balance of power between organised crime and the public. We would welcome views, particularly on the questions set out in annex A.

The Proposals

CHAPTER 1: DATA SHARING

In his April 2002 foreword to the PIU report 'Privacy and Data Sharing: The Way Forward for Public Services', the Prime Minister set out a clear framework for the way in which public bodies should use data

“there is great potential to make better use of personal information to deliver benefits to individuals and society, including through increased data sharing. But these benefits will only be realized if people trust the way that public services handle their personal data.

The Government strongly supports the twin objectives...of encouraging better use of personal data to deliver improved public services and safeguarding personal privacy”.

Clearly the public want data sharing to be necessary and proportionate, with particularly confidential material like medical records rightly expected to be treated with special care. But for the majority of data, studies show that the public is most prepared to accept data sharing when this is in order to prevent or detect crime. Too often, however, we are failing to make proper use of the material which is available.

The current blocks to sharing data can frustrate the public, which does not expect to have to give the same information to large numbers of different arms of Government. This frustration turns to concern when there is evidence that a lack of confidence in our powers to share data is leaving the public vulnerable to fraud and other crime.

The Prime Minister has established a cabinet committee MISC31 to develop the Government's strategy on data-sharing across the public sector. The Government is looking to address legislative, cultural and institutional barriers to data sharing where that sharing will deliver greater choice and personalisation in public services; protect vulnerable individuals and groups or increase the individual's personal security through combating international terrorism and crime.

We also, however, need to ensure that data is shared within a framework that properly protects individuals' rights and with enhanced protection to guard against its abuse. To the latter end, the Department of Constitutional Affairs (DCA) is giving serious consideration to the possibility of increasing the penalties available to the courts for those found guilty of offences under section 55 of the DPA.

At the same time, the Information Commissioner is beginning to work on basic principles of data sharing and considering the possibility of high level codes governing data sharing in various key areas. This holds out the prospect of putting the sharing of data for key aims like crime prevention on a much clearer and surer footing than hitherto.

Recent work on emerging fraud threats in both the public and private sector are bringing home that organised crime is likely to have a much larger role in fraud than previously realised. Pilot studies in data matching have revealed previously undetected fraud rings in the insurance industry, for example. Similar techniques have revealed links between different Suspicious Activity Reports submitted by the regulated sector to SOCA. Getting the data sharing regime right is therefore going to play a vital role in the fight against organised crime, as well the wider effort against financial crime and fraud.

Encouraging data sharing has been on the agenda of a series of groups looking at different aspects of crime; including the Fraud Review and the Identity Fraud Steering Committee, while it has also been identified as an important tool needed to address emerging threats like tax credit fraud.

There is a common perception in both the public and the private sector that data sharing is made almost impossible by the Data Protection Act. In reality, data protection will not create insuperable barriers to legitimate, proportionate data sharing – and it is difficult to see why this misperception has gained such common currency among policy makers and front line staff. Much more frequently, any real problems lie with departments' and agencies' statutory vires to share information.

Government is looking at the wider issue of vires to share information in the public interest. All too frequently, government departments would do better not to legislate at all on data sharing. Common law or implied statutory powers have proved time and time again to provide a more flexible solution than specific gateways, which risk getting out of date as data processing moves on and new bodies appear on the scene. Even where legislation proves necessary, it is still possible to rely on implied powers within that legislation, rather than including specific gateways, which can have the effect of creating uncertainty in the minds of front line staff in any situations where no explicit gateways exist.

In the meantime, fraudsters are clearly taking advantage of the fact that the lack of routine data sharing means all too often that the left hand in the public sector does not know what the right hand is doing, and contradictory information can be submitted to a range of different agencies without it being picked up.

This paper sets out some specific initiatives which we believe will be needed to deliver greater public protection from crime. As significantly, it sets out some general ideas on the sort of data sharing which the Government believes is likely to be necessary and proportionate for the prevention of crime, and commits the public sector to act to make this possible. Some of this new data sharing might require legislative changes; in particular changes to the vires of agencies whose data sharing is governed by statutory provisions. Much should be achievable simply through a more robust approach to the use of existing powers, though there may also be a need to make secondary legislation under the DPA.

At this Green Paper stage, as one would expect, the operational feasibility of our proposals require further testing: the implementation of projects involving large scale data manipulation is complex and challenging. Learning from recent experience, SOCA, Home Office and other delivery bodies will work to best practice set out by the Office of Government Commerce as they move to implementation. We shall also need to ensure that there is sufficient capacity within the Home Office family's overall programme portfolio to deliver these policies as their feasibility is tested and the operational system requirements become better understood.

1.1 Identity Fraud / Deceased Persons Fraud

As financial transactions are completed ever more quickly and the financial sector becomes more diverse, so criminals have a growing opportunity to make a quick profit if they are able to come up even temporarily with a plausible false identity.

In the longer term, this problem should be largely addressed by the ID cards programme. In the meantime, we ought at least to be able to put a stop to one of the fastest growing problems of recent years, the use of deceased persons' identities.

CIFAS- *the UKs Fraud Prevention Service* have estimated that deceased persons fraud is now costing its 250 members, mainly in the financial services industry, up to £300m annually, as identity fraudsters submit applications in the name of individuals they know have recently died.

While fraud is likely to be one of the main reasons to take on the identity of a dead person, the practice might also be concealing money laundering or a range of other serious crimes. SOCA recently matched its Suspicious Activity Report database and identified over 300 reports on subjects whose names appeared in the database of deceased children.

Credit reference agencies seek to get information on the names of the deceased as quickly as possible, but this can take many months. The Government already has this information, however. The UK's three Registrars General have the information from death certificates, and this is passed to the Department of Work and Pensions (DWP), which matches the names of the deceased to addresses and NI numbers, enabling them to cancel any benefit or pension payments being made.

Until recently, neither the Registrars General nor DWP felt they had the statutory power to share this information more widely, however, leaving the financial sector vulnerable to continuing fraudulent claims. The Home Office have inserted a clause into the Police and Justice Bill, currently before Parliament, to allow for the timely supply of death registration information from the Registrars General for England and Wales and for Northern Ireland to law enforcement or other organisations specified by order for use in preventing, detecting investigating or prosecution of offences such as fraud. Scotland proposes to have similar arrangements in place once the Local Electoral

Administration and Registration Services (Scotland) Bill receives Royal Assent in a few weeks' time.

The Registrars General will be working with the credit reference agencies and other interested partners to finalise the practicalities of passing this information on once the statutory powers are in place. We will also be reviewing whether the information available to the Registrars General will be sufficient to prevent all the related fraud, or whether there is also a case for access to further information in the public sector, for example DWP data which has matched the deceased persons records to NI numbers and addresses.

1.2 Sharing Information on Fraudsters

Preventing fraud and financial crime is clearly better than tackling it once it has happened. One of the most basic ways of self protection is to share information on frauds which have been attempted or committed to ensure other agencies can be on the look out for the same fraud. Very little if any such sharing takes place routinely within the public sector.

Things are rather better in the private sector. As long ago as the 1980s, the credit industry became increasingly concerned about fraud losses they were suffering and the poor arrangements in place for sharing information on them. As the financial sector liberalised and the number of players increased, fraudsters could commit the same frauds in a short period on a whole range of institutions, maximising criminal profit while minimising the risk of detection.

As a result, the industry set up CIFAS (the UK's Fraud Prevention Service) as a non profit making body to facilitate matching of reported frauds. Member bodies were originally drawn only from the credit industry, but this has expanded to include other types of members as well. Members pay a subscription, are obliged to report all cases of suspected fraud to CIFAS. The CIFAS database includes personal and address data for these suspected fraud cases. Members check the database when processing new applications, say, for loans or credit cards. They may also check existing customers.

When the check reveals a match, members are not allowed to take the existence of a match as the sole ground for refusing an application, but are required to undertake further checks and if necessary carry out a fraud investigation. In 2005, members reported savings of £682m as a result of the CIFAS database, a huge return on the £2.4m pa which CIFAS costs to operate.

The current information sharing process through CIFAS has been discussed at length with the Information Commissioner. There are a number of grounds for legitimate processing including customer consent. Customers are also made aware of the possible use to which information about them can be put. The sharing can also rely on the exemption in section 29 of the DPA.

The threshold for inclusion on the CIFAS database is that sufficient evidence must exist for a report to have been made to the police.

There is currently no parallel to this sort of information sharing within the public sector, and extremely limited evidence of information sharing on individual frauds, although FIN-NET provides a forum for members across Government Departments, law enforcement and regulatory bodies to raise enquiries on frauds and financial crime.

One possible approach to addressing the problem of sharing suspicions of fraudulent activity would be for public sector bodies to become members of CIFAS. A successful pilot exercise of public sector agencies submitting data to CIFAS suggested that a high proportion of address data (on average 31% but as high as 40% for some agencies) matched addresses already identified as suspect by the CIFAS database.

On this basis, government departments and agencies would, like current CIFAS members, be able to flag the applicant for services as having possible increased risk associated with him. It would not automatically stop access to services or payments, but should trigger increased due diligence. Given the scale of total payments made by the public sector, there is likely to be scope for many tens of millions of pounds of savings to be generated over time, in return for membership fees which are typically capped at around £100,000 per organisation.

There should not be any DPA difficulties with the public sector joining CIFAS and sharing data of this sort. Public sector bodies should be able to rely on conditions 5 and 6 in Schedule 2 DPA to share data for fraud prevention. Even in those circumstances involving sensitive data (such as criminal convictions or allegations of crime) in most cases the current DPA conditions should suffice. Where they do not, it would be possible to make further Orders under the DPA (for example under schedule 3) to ensure that the sharing and processing could take place. In addition, public sector bodies should be able to rely on the DPA exemption in section 29 for data sharing for crime prevention purposes or on other provisions in the same legislation.

It is essential that we put proper safeguards in place if public sector bodies are to move to sharing information on suspected frauds with each other and with the private sector. In addition to having the statutory vires, we also need to look at processes for dealing with clients to ensure they are properly notified of the use that may be made of the information they supply, and to ensure that information is accurate and protected from misuse. Preliminary discussions with the Information Commissioner suggest that codes of practice could be a useful way of agreeing procedures for public sector data sharing of this sort, giving public sector organisations the confidence to act, and the public the confidence that reasonable safeguards are in place.

Legally, we expect the main obstacle to progress to be departments and agencies' statutory vires, which may in some cases prevent data sharing with the private sector. If the CIFAS route were to be followed, we would also need to consider an order under schedule 3 DPA to enable CIFAS to process sensitive personal data received from the public sector.

The mechanics of a public-private database of this sort need to be agreed, as there are several options available, of which CIFAS is one which could be useful in the short term. There is potential for a lot more functionality than exists at present, however. In particular, law enforcement needs to have full access to any central database of frauds. All the intelligence suggests that relatively small scale white collar frauds often help fund more serious crime. Crimes on the CIFAS database which have never been reported to the police could provide valuable new lines of enquiry for law enforcement teams working on, for example, terrorism or organised crime. Ensuring law enforcement has access to the CIFAS database, perhaps ultimately through the new IMPACT portal, will be vital.

Long term solutions to the problem of reporting fraud and of being able to use that information to detect crime are also essential. The Fraud Review has been looking into precisely this, and is exploring ways by which both individual and business victims are able to report frauds more easily to the police in future, and what systems need to be put in place to deliver this. The Fraud Review will argue that greater use should be made of fraud reports to provide services and information which will help businesses and government generate a better response to the problem of fraud and how to ensure a link through to the necessary law enforcement response. These proposals and links will be explored further in the Review, which reports later this summer.

Any system for sharing information on frauds needs to be part of a wider strategy to tackle fraud; after all, once they are identified, they should if possible be investigated and the criminality behind them stopped. This means not only being able to warn and alert contributors, but having a link to law enforcement too. This is particularly important with organised fraud networks.

For this consultation, we are proposing

- That anyone accessing public services should expect that service providers can check on their entitlement to that benefit for fraud prevention purposes
- That anyone suspected on the balance of probability of committing fraud against the public sector should face the prospect of having data concerning them shared with other public and private sector bodies to help protect these bodies against future frauds. All public sector bodies, but particularly key providers of benefits and services like HMRC, DWP, DLVA, the Identity and Passport Service and local authorities should ensure their vires are adjusted if this is necessary to enable this sharing to take place
- We will discuss with the Information Commissioner the option of a code of practice to set out the basis on which such information sharing should take place
- Taking account of the recommendations of the Fraud Review, we will discuss with interested parties the best vehicle for data sharing of this sort, and how to increase the level of functionality we can draw on, so that the best use is made of the information available.

Q1. Should public sector information on suspected fraudsters be shared more widely within the public sector and with the private sector to prevent and detect fraud? What sort of safeguards would you expect to see? What do you believe the most appropriate vehicle for data-sharing would be?

1.3 Data Matching to Prevent Fraud: The National Fraud Initiative

One of the thorniest areas for data sharing is the extent to which bulk matching of data is permissible in order to prevent or detect fraud. Despite the existence of numerous DPA routes enabling data to be shared, many agencies believe that the data subject's consent is also required, at least in general terms. This is a misunderstanding. As far as data sharing within Government is concerned, consent is not required. If vires to share exist, consent is not needed; where vires do not exist, consent will not be a substitute, as it is not possible to consent to an ultra vires action.

The public sector should be moving towards a general expectation that anyone applying for payments or other benefits from the public sector can expect to have the details in their application checked against relevant databases to ensure entitlement and prevent fraud. This presumption should exist in all but the most exceptional circumstances where there are compelling public interest reasons why individuals' data should not be matched. It is important that people's expectations are managed appropriately and that they are notified that their data may be used for fraud prevention purposes.

This expectation would merely replicate for payments from the public sector the sort of terms and conditions which anyone would expect from a bank or credit institution, which will make careful checks through their own records and probably credit reference agencies to confirm the applicant is who they claim to be, that the details submitted are accurate and that they do not have outstanding creditors.

There is no question that doubts about data sharing are leading us to miss major opportunities to prevent and detect crime at present. For example, the Audit Commission's National Fraud Initiative (see below) matches pension fund data to identify beneficiaries who have died. This matching process also reveals housing benefit claimants who are fraudulently not disclosing their pension income, but this information is not being routinely acted on.

There is also thought to be a considerable amount of housing benefit fraud on the part of owner occupiers who are claiming to be renting. Trials of data with one leading financial company has revealed that matching is likely to produce considerable savings to the public, as well as identifying fraudulent customers who the financial sector will not want to deal with and financial sector staff involved in frauds. Again, there are continuing discussions about how

consent might be obtained from mortgage customers to make this permissible.

Once misconceptions about consent have been dispelled, there is considerable potential to make inroads into the fraud problem through bulk data matching. This is the process of taking datasets which may contain multiple bits of data (for example employment records) and, literally, matching them with other sets of data (eg pension records). The Audit Commission's National Fraud Initiative is a prime example of how matching similar data can prevent fraud. Simply uncovering matches in fields which should be incompatible provides strong suspicion of fraud for further investigation (for example claimants who claim housing benefits on the grounds of having no income while also appearing on payroll records).

The National Fraud Initiative has run every two years since 1998. The data sharing is based on a statutory duty to share information with the Audit Commission for the purposes of the NFI and is subject to the Code of Data Matching Practice 2006, developed in consultation with the Information Commissioner's Office. Together, these ensure compliance with DPA. The NFI uses data matching techniques to tackle a broad range of fraud risks by the public sector, such as widespread non declaration of income by benefit claimants, council tenancy and right to buy abuse and employment fraud by failed asylum seekers and UK visa overstayers. The value of fraud and overpayments detected by the 1300 bodies taking part in the NFI in 2004/05 exceeded £111m, a 33% increase over the previous exercise. The ratio of savings identified to NFI costs is estimated at over 100:1.

The frauds detected are often extremely simple, and rely once again on fraudsters' confidence that information given to one public body will not be checked against the records of another. Thus NFI is picking up applicants for housing benefit in one authority who claim to have no income but are actually employed by a neighbouring authority or health trust. Public sector employees have been found who are holding down more than one job with overlapping shift patterns, or being employed by one public sector body while on paid sick or compassionate leave from another. The NFI has helped private pension funds to identify numerous beneficiaries who have died.

The NFI is far from the only tool currently being used, but it is unique in its reach. Already however the scope of the initiative is reaching the boundaries of the formal remit of the Audit Commission as auditor of local government and NHS bodies.

Contracting out and institutional changes have also moved parts of the local government sector outside the Commission's remit, for example housing associations, contracted out local authority staff and NHS Foundation Trusts. As such, the benefits the NFI can offer to local government (eg detecting fraudulent tenants and payroll frauds) are no longer automatically available to these bodies.

Accordingly, the Commission has proposed a specific new power to conduct the type of exercise envisaged; a power to conduct matching exercises and to disclose matches as relevant for follow up action to all participating bodies in both the public and private sector. We will also need to ensure that

participating bodies all have the power to receive and use the data from the Commission. It will need to include a power to charge a reasonable fee to bodies which are not currently within the Audit Commission's audit regime in order to cover costs. We are also working with Northern Ireland and Scotland to see what legislation would be needed to enable similar data matching across borders.

Q2. Should the scope of the National Fraud Initiative be expanded and placed on a statutory footing in order to increase its capacity to detect fraud within the public sector?

1.4 Data Matching Against Money Laundering and Serious Crime: Suspicious Activity Reports

SOCA has from the very start been determined to identify opportunities for new ways of tackling organised crime, with making better use of data a high priority. SOCA has both gateways for sharing information, and in the Suspicious Activity Report system an under-used and highly powerful potential source of information.

Under the Proceeds of Crime Act and related legislation on terrorist financing, the regulated sector is required to submit Suspicious Activity Reports (SARs) to SOCA where there are reasonable grounds for suspicion that money laundering has occurred or is in prospect, or an offence under sections 15 to 18 of the Terrorism Act 2000 has been committed.

The reporting system has recently been reviewed by Sir Stephen Lander. The key conclusion of this review was that the reports are a potentially invaluable resource and could be used much better. One of the key ways this could happen is through better information sharing.

SARs represent a prima facie basis for suspicion of crime, and provisional SOCA analysis of SARs suggests that the underlying suspicion of criminal activity is likely to be well founded in at least 40% of reports made. Prioritising the reports for action and developing the information they contain is, however, a substantial challenge given the very large numbers submitted (over 200,000 per annum). Depending on the underlying facts behind the report, there could be a range of possible responses. Some might justify full scale criminal investigation themselves, others might lead to valuable further leads, and many are likely to justify further investigation on tax or asset recovery grounds.

In the past, incoming SARs were checked only against NCIS's ELMER database of past reports, and against NCIS's own internal intelligence database, while other organisations seconded staff to work in the financial team to identify and pass on SARs likely to be of interest to them.

SOCA is currently working to develop an IT approach which will enable SARs to be checked periodically against a series of relevant non-law enforcement

databases containing information that could have a bearing on crime. The main ones are those concerned with direct and indirect taxes, with records of births, marriages and deaths, with benefit and state pension payments, with the issuing of passports and with driver and vehicle licensing.

SOCA has already piloted a data matching exercise with a sample of some 10,000 SARs. While the process involves some work to cleanse data and ensure material from different databases is converted to a compatible format, it does not normally require additional IT investment or changes to existing systems. The pilot study came up with some striking findings, including 25% of SARs matching records on the CIFAS database, and around 1% matching records in DWP.

These matches potentially enable SOCA and its partners to identify and prioritise those reports which, in addition to the original suspicion, concern subjects who are, for example, unknown to the tax authorities, in receipt of benefits or using what appears to be a false identity. As well as vital criminal leads, this should cast light on a number of cases where other agencies will want to take action, for example withdrawal of benefits or tax action, and SOCA will need to discuss with other agencies possible burden sharing.

The logistics and practicality of this sort of data matching are highly challenging, with different protocols for recording data often meaning manual checking is required. Government agencies are looking amongst other things at the scope for standardising the way information is recorded in order to facilitate exercises of this nature. SOCA will work with partner agencies to see how these problems can be addressed, and any IT solution would clearly need to be carefully designed with a robust business case, but the potential for real added value to SARs is obvious.

There has traditionally been considerable nervousness about this sort of data sharing, with some agencies believing that only individual 'case by case' requests can be made under the legislation. We believe however that targeted exercises of data sharing can themselves be considered on a case by case basis, without requiring agencies to look at every item of data separately. Moreover, in the case of SARs, each report has already undergone an individual assessment in the reporting institution, which by filing the report has expressed a suspicion of criminal activity. As such, data matching should be possible under the existing DPA exemptions allowing information to be shared for the prevention or detection of crime, with the matching exercise merely building on the existing individual suspicion.

SOCA and key public sector partners will work to develop data matching of SARs, and to develop an agreed protocol enabling the match results to be passed on and actioned.

Q3. We would welcome your views on SOCA matching Suspicious Activity Reports received from the regulated sector against a range of public sector databases.

1.5 Data Matching / Mining to Identify Suspicious Profiles

Data matching and mining can be interpreted in different ways in different circumstances. For the purposes of this paper, we see data matching as taking two separate data sets with comparable information (ie both contain the same types of information, for example names) and cross referencing them to produce matches. These data sets would typically be for mutually exclusive purposes which can reveal where entitlements are being incorrectly granted, eg when the same name appears in connection with pension payments and a list of deceased persons.

Data mining, on the other hand, uses more advanced software to analyse data in a number of ways. It can be used within data sets to expose fraud, and is particularly useful when there are many variables within a data set, or the sheer volume of data means that automated analysis is necessary. For example, banks use software to identify unusual spending patterns on bank accounts, despite having millions of transactions every day, and possibly hundreds on each account.

We believe there may be greater scope for law enforcement to adopt this process of 'profiling' in order to check across a range of datasets to identify suspicious patterns of activity.

As technology advances, and ever more information is stored electronically, there is a huge opportunity to use these sort of techniques, which hold out the opportunity to protect the public by picking up patterns and trends in criminal activity which might not be spotted when data is looked at individually. Equally, however, the very bulk of information out there imposes a particular duty to make sure our use of data is proportionate, and also that law enforcement would be capable of using the information it gathers.

A good example of the sort of 'profiling' work we would like to see more of is an exercise carried out a few years ago by HM Customs and Excise. Parallel checks were made on VAT and excise databases with information from the licensing trade and information on building dimensions from Land Registry.

This exercise outlined a number of businesses which were submitting records which all looked reasonable enough in their own terms, but when put together came up with a picture which was highly suspicious. In a large number of cases, turnover was being reported which would have been physically impossible given the size of the premises, providing a strong suspicion of money laundering activity.

SOCA is reviewing all the main datasets in existence around the public and private sector to identify similar opportunities for unveiling suspicious activity. But there remains at present a lot of confusion among law enforcement and public bodies about when this sort of data mining is allowed, and the HMCE pilot exercise has not subsequently been repeated despite the striking findings it uncovered.

Many public bodies fear that this sort of exercise will be seen as a fishing expedition. Some believe the DPA require a reasonable suspicion of crime on a case by case basis for every bit of data matching and sharing if it is to benefit from the exemption in section 29 DPA. We would question this analysis, however, and believe a robust case can be made for data mining in relation to entire data sets in appropriate circumstances.

Having identified, in partnership with SOCA and other law enforcement agencies, priority areas for mining, we intend to work with the Information Commissioner with a view to producing guidance on the circumstances in which this sort of exercise can take place, perhaps building on the principles set out in the Code of Data Matching produced by the NFI. Such guidance should provide assurances for agencies with relevant databases in both the public and private sector about the circumstances in which this sort of exercise can safely be run, while giving the public the confidence that due safeguards are in place.

There are a number of obvious safeguards which will be needed. First, any such exercise will need to work to clear parameters designed to uncover suspicious behaviour. Secondly, the exercises need to be proportionate to the harm they are seeking to prevent, and to the level of effort which law enforcement will need to be able to devote to acting on their findings. In practice, we would expect them to be short term and targeted exercises, rather than ongoing processes which could swamp law enforcement with data.

Data holders may need to have been notified of the prospect of this sort of exercise. We will need to consider whether personal data need be anonymised until suspicious matches are identified, and if any other safeguards are needed.

There is no reason why reasonable safeguards necessary to comply with the provisions of DPA, and indeed with most people's sense of what is fair and proper, should stand in the way of a common sense tool for identifying suspicious activity which might otherwise go entirely undetected.

Q4. We would welcome your views on what you would regard as appropriate and targeted data mining of public and private sector databases to detect and prevent criminal activity, and what the appropriate safeguards for such exercises should be.

CHAPTER 2: THE CRIMINAL LAW

2.1 Streamlining Investigations and Prosecutions: Filling Gaps in the Criminal Law

The exercise of the legal tools provided by SOCPA and the Proceeds of Crime Act 2002 is expected to have a considerable impact in terms of bringing organised criminals to justice, but there is more that could be done. As organised crime becomes more sophisticated, it is important to ensure that the criminal law remains capable of dealing with it.

We are conscious of possible gaps in the criminal law as it applies to those who encourage and assist offences. This is particularly important in relation to organised crime where the relationships between those involved in offences are more complex and key players often go to great lengths to distance themselves from the actual commission of offences they have encouraged or assisted. The 2004 White Paper highlighted a concern that the current law does not always provide a practical means of addressing peripheral involvement in serious crime and committed to review the law of conspiracy.

Separately, the Law Commission (for England and Wales) has been considering the law around inchoate and secondary liability for encouraging and assisting crime. The Law Commission has this month reported in respect of inchoate liability for encouraging and assisting crime. It is expected that a further report on secondary liability for encouraging and assisting crime will be published later this year. The Law Commission's Report and draft Bill are available at http://www.lawcom.gov.uk/assisting_crime.htm

The Law Commission report recommends new statutory inchoate offences of encouraging or assisting a criminal act with intent, or encouraging or assisting a criminal act believing that an offence will be committed. Their proposals also provide for the situation whereby a person provides encouragement or assistance believing that one of a number of different offences will be committed, but without knowledge of exactly which one. These offences would close a gap at common law whereby it is an offence to encourage, but not to assist, another person to commit an offence which does not go on to take place.

The issue of inchoate liability for those who encourage or assist crime is particularly important when tackling organised crime. Increasingly, SOCA and the police are able to identify acts of assistance or encouragement to an offence before the offence itself takes place but currently, where the act is of assistance, they have to wait until the principal offence is committed or attempted before taking action against the person who provided assistance. By contrast, if the act is of encouragement, the police would be able to charge incitement. It has been argued that a general offence capturing acts of encouragement or assistance would be a useful way of disrupting crime, particularly organised crime.

The Government is very grateful to the Law Commission for the thorough and painstaking work they have done in this very complex area of the criminal law

and welcomes the recommendations in their report. It believes that the Law Commission proposals, if implemented, would help strengthen the criminal law and will be studying the detail carefully over the next few months. However, the Government would welcome views on specific elements of the proposals.

2.2 Clause 2: The Requirement for D to “Believe” that an Offence “Will” be Committed

Under Clause 2(1) of the Law Commission’s draft Bill, a person who has provided assistance or encouragement (referred to in the Report, Draft Bill and hereafter as “D”) can be liable if he does an act which is capable of encouraging or assisting another person to do a criminal act in relation to a principal offence he believes will be committed. Similarly, under Clause 2(2) D would be liable where his conduct has the capacity to provide another person with encouragement or assistance in relation to a range of possible principal offences, and D believes that one of the offences in that range will be committed (with his encouragement or assistance) but he is unclear which offence it will be.

The Law Commission argues that because the Bill deals with inchoate offences, it is necessary to ensure the offences do not have too wide a reach, particularly in relation to the Clause 2 offences where it is not D’s purpose that an offence be committed, rather he is indifferent as to whether it is committed.

The Government agrees that it is important to ensure that these offences are carefully drafted in order to ensure that liability is not extended too far, but we also need to ensure that those who could be said to have a reasonable degree of belief that an offence was likely to take place, and that their act would provide assistance or encouragement, could not escape prosecution by arguing that they were not absolutely certain that the offence would take place.

The Government believes therefore that it might be necessary to lower the threshold for this offence to cover those who might be able to claim not to have the degree of certainty implied in saying that they believed something would happen but who are nevertheless in a position where they know it is highly likely that it will or have strong suspicion that this will be the case.

The decision as to what level of belief should be required for this offence will need to be carefully thought through. The aim of the offence is to ensure that it can be used where there is evidence that D had a good degree of knowledge or suspicion that an offence would take place but was not 100% certain. It is not the intention to widen criminal liability to every person who has some idea that their acts could assist others to commit offences. As such we would welcome views as to what level of belief should be required for liability to arise.

Q5. Should Clause 2 be restricted to those who believe that an offence will take place or should this be widened?

2.3 Encouraging and Assisting Serious Organised Crime

The Law Commission proposals impose liability on a person who provides assistance or encouragement either intending that a particular offence be committed, or believing that a particular offence, or one of a number of specific offences, will be committed. The physical element of the proposal is that D does an act capable of encouraging or assisting a criminal act.

However there are circumstances in which a person provides assistance or encouragement to criminal acts generally without knowledge or intention that the conduct will contribute in any way to the commission of specific criminal offences. There are also circumstances where the assistance is indirect or peripheral and may not be considered capable of encouraging or assisting a criminal act itself. This is a particular problem in relation to organised crime as the assistance or encouragement can often be to wider activity underpinning the criminal network rather than specific offences. Such activities would include, for example, the maintenance of the legitimate activities of a “front” business or providing facilities for meeting or storage facilities can indirectly assist others in the preparation or planning of serious criminal activity.

The Government’s view is where there is sufficient evidence to show that D does something for a person (X) whom they knew or suspected to be involved in serious organised crime and that D believes or suspects their own actions could encourage or assist the criminal activities, D should be guilty of an offence.

An example of how this offence could be used would be where D provides a property, which he fits with security features, for X. D knows or suspects X is a criminal involved in drug trafficking, blackmail or other serious offences typically committed by organised groups. While D has no idea what offence X might be planning in this property he knows or suspects that the property will be used by X in his “criminal activities”. The assistance would not need to be linked to the planned commission of a specific criminal offence or of one of a list of offences, (unlike the offence set out in Clause 2 of the Law Commission’s proposals). Rather it would derive from D’s knowledge or suspicion about X’s involvement in serious crime of a particular type, coupled with his knowledge or suspicion that his assistance would directly or indirectly support X’s criminal activities.

The offence would be aimed at those who assist or encourage organised criminals involved in, for example, the organised crime lifestyle offences set out in Schedule 2 of POCA: drug trafficking, money laundering, people trafficking, arms trafficking, counterfeiting, intellectual property theft, blackmail and organising prostitution.

An offence of this nature would need to be carefully formulated as it would impose liability for acts that may be legitimate and do not relate directly to specific criminal offences. However preliminary discussions with prosecutors suggest an offence of this type would be useful to ensure those involved on the fringes of organised crime and on whom it largely depends cannot escape prosecution.

In particular the Government will give careful consideration to:

- the degree of knowledge required by D;
- the offences that X would need to be involved in for this offence to apply;
- how to define the physical element of this offence; the indirect assistance of “criminal activities”; and
- the level of penalty available.

The Government would welcome comments as to whether such an offence should be created, and if so, how such an offence should be formulated.

Q6. Is the Government right to consider extending liability to those who indirectly encourage or assist a person (X) where they suspect this encouragement or assistance will aid X’s criminal activities (as against specific criminal offences)?

2.4 Conclusion

The Government believes that changes to the law are needed to allow law enforcement agencies to deal more effectively with the threat of organised crime. The Law Commission’s proposals form an excellent starting point for looking at the best way to achieve this, and offences suggested above build on this in relation to organised crime. They will target those on the periphery of organised crime who are difficult to prosecute under the existing legal framework. In addition, these offences, coupled with the powers provided by the Serious Organised Crime and Police Act and the Proceeds of Crime Act, should also lead to a greater number of convictions for some of the “major players” as some of those on the periphery should be persuaded to testify against their bosses in return for discounted sentences. Tackling organised crime is a high priority and the Government would welcome an informed debate on the proposals for doing this by better criminal offences as outlined above.

CHAPTER 3: ORGANISED CRIME PREVENTION ORDERS

Transforming the quality of information at law enforcement's disposal and strengthening the criminal law and the effectiveness of its sanctions will help tilt the risk/reward balance for organised criminals.

This is in itself an important result. But the ultimate outcome we are looking for is not results in the criminal justice system, but preventing crime from happening in the first place.

In tackling organised crime, law enforcement is all too often faced with the choice of prosecution or no action. We have been working with law enforcement to identify possible new tools which could help prevent crime, examining in particular the sort of range available to agencies dealing with fraud and regulators.

The widest range of such tools, covering administrative, civil and criminal remedies, tends to rest in the hands of some of the newer agencies like the Financial Services Authority (FSA). This wide range of potential disposals gives considerable flexibility and arguably increases the likelihood of voluntary settlement with those subjected to investigation. The purpose of the disposals includes preventing future harms and redressing past ones.

This approach reflects a general trend in regulation, exemplified in the Hampton Review, which stressed the importance of a risk based approach, targeting the more invasive regulatory tools in the areas where breaches are most likely.

In a parallel process, successive Governments over recent years have introduced a new category of civil orders against individuals for harm or crime prevention purposes. There are a range of such orders, covering areas like anti-social behaviour, sexual offences, restraining orders and football banning orders. As Lord Steyn has noted³

“the unifying element is.. the use of a civil remedy of an injunction to prohibit conduct considered to be utterly unacceptable, with a remedy of criminal penalties in the event of disobedience”.

Probably best known, section 1 of the Crime and Disorder Act 1998 introduced Anti Social Behaviour Orders. These can be obtained against subjects when the court believes

(1)(a) That the person has acted... in an anti-social manner, that is to say, in a manner that caused or was likely to cause harassment, alarm or distress to one or more persons not of the same household as himself; and

(1)(b) That such an order is necessary to protect relevant persons from further anti-social acts by him.

³ R (McCann) v Manchester Crown Court (2003)

As civil orders, civil rules apply, notably a different regime for disclosing material to the defence and greater use of 'hearsay' evidence. For example, professional witnesses like police officers or council officials are able to testify to anti social behaviour in cases where neighbours or other members of the public are too intimidated to do so.

In practice, since the McCann judgement, the threshold of evidence required to satisfy the condition in section 1(1)(a) is not far off the criminal standard, while the condition in (1)(b) is a matter for the judgement of the court.

Preceding the ASBO legislation by almost 10 years are the Football Banning Orders under the Football (Spectators) Act 1989. Of particular importance here are the ability here to ban foreign travel where there is a threat of trouble from football hooliganism. Another notable category of orders are Disqualification Orders under the Criminal Justice and Court Services Act 2000, which prohibit persons from working with children.

These orders constitute a significant toolkit of approaches for those involved with tackling anti social behaviour and certain sorts of serious crime. In comparison, the armoury available to those tackling organised crime is relatively bare.

SOCA and police forces are developing a range of regulatory and other responses to make organised crime more difficult to commit. The powers in POCA and the new Financial Reporting Orders in SOCPA have considerable potential for disrupting convicted criminals' ongoing criminal finances. SOCA is working hard with colleagues in the National Offender Management Service (NOMS) and the Immigration and Nationality Directorate (IND) to ensure full use is made of existing probation and immigration powers to target organised criminals who are on licence or potentially liable to immigration action.

In addition, some police forces have developed approaches to using other administrative powers (eg planning, health and safety) against organised crime groups, working in partnership with local authorities and other regulators. But these approaches tend to be piecemeal and rely heavily on individual relationships. The use of such powers must obviously fall within the normal framework for action, if interventions are not to be seen as simple harassment.

Moreover, these powers all have weaknesses. They are overwhelmingly focused on individual offenders. Most can only be used against offenders who have been convicted and only apply to the period of their sentence. Immigration powers obviously only apply to those who are subject to immigration control.

3.1 The Case for a Serious Crime Prevention Order

We therefore believe there remains a gap which we believe could be filled by a new civil order, the "Serious Crime Prevention Order". The purpose of the order would not be punitive, but to impose binding conditions to prevent individuals or organisations facilitating serious crime, backed by criminal penalties for breach.

This would be a civil order, and given the range of potential restrictions, would probably need to be made in the High Court. Orders should be appealable to the Court of Appeal.

The courts would be able to impose an order if they believe on the balance of probability that the subject

- Has acted in a way which facilitated or was likely to facilitate the commissioning of serious crime
- That the terms of the order are necessary and proportionate to prevent such harms in future.

This order could be imposed following a contested hearing, or the terms could be agreed between the subject and prosecution and the order validated by the court. We would envisage the courts having the option of publicising, or not, the existence of orders, depending on the circumstances of the case.

It will ultimately be for the courts, as a public authority under the Human Rights Act to decide if this test is met, and if the restrictions being applied for are compatible with human rights obligations. Most significant will be the need to ensure proportionality, particularly in cases where the degree of complicity in crime is unclear, and in cases where an order could cut across the interests of third parties.

3.2 The Relationship Between Civil Orders and Prosecution

We are proposing limiting the power to apply for these civil orders to designated prosecutors in the three main prosecution agencies (CPS, RCPO and SFO). There are a number of reasons for this. First, it reflects the likely legal complexity of these orders. Secondly, it matches the position of other key new powers against serious and organised crime, like the disclosure notices in SOCPA. Thirdly and probably most significantly, it reflects the need for a conscious and careful choice between prosecution or the civil route, and to ensure that the response chosen is proportionate in the way it balances the rights of those potentially affected.

As the name suggests, the fundamental purpose of these orders is preventative. As with other disposals available to agencies like the FSA, those deciding whether to prosecute or pursue a civil order will need to decide which disposal is most likely to reduce harm in the long run, while taking due account of the public interest in prosecutions.

For ASBOs, the underlying behaviour justifying the order does not itself need to be criminal, so prosecution is not necessarily an option. This is much less likely to be the case for organised crime, particularly if action is taken to address the various problems with the law around conspiracy, promoting and encouraging crime. There may still be cases where a prevention order can have clear harm reduction benefits while the illegality of the underlying behaviour is borderline (eg case study D below).

Where the underlying behaviour is criminal, the prosecuting authorities will obviously need to consider carefully whether prosecution or civil orders are the appropriate way forward. We can envisage circumstances in which civil orders could play a role where prosecution *is not feasible*, *alongside* prosecution or as *an alternative* to prosecution.

In the first category would fall cases where there is sufficient evidence to justify an order to a civil standard, but insufficient for a conviction. This may be because of the absolute quantity of evidence, or because some of it is in a form not admissible in a criminal proceeding but which can be used in civil cases (eg certain types of hearsay evidence).

Law enforcement might also have evidence of crimes committed overseas which cannot be prosecuted in the UK, or the subject of an order might have been released after conviction overseas in circumstances where we would expect them in the UK to be subject to strict licence conditions – the prevention order would enable us to put such controls in place.

Secondly, orders could be an additional option in the run up to a criminal prosecution, imposed to restrict the harm the subject can do while the case is being prepared, in cases where the subject is aware of law enforcement interest already. The orders might be used *alongside* prosecution, for example as part of a deal to turn Queen's Evidence, ensuring that the QE subject is bound to conditions of good behaviour. One option might also be to enable the courts to impose an order as part of a disposal after conviction, over and above the standard licensing conditions, although this would obviously have implications for the licensing system.

There are also, however, likely to be cases where orders are an appropriate tool as an *alternative* to prosecution. In practice, law enforcement and prosecutors need to make difficult decisions around putting cases together for court. The courts have reasonable practical and case management reasons for objecting to over-large trials. But in the case of organised crime investigations, there may be significant numbers of individuals at the fringes who cannot be pursued in the main trial, and for whom a separate trial is not thought worthwhile. Such individuals' role might have been marginal and not warrant a prosecution, but an order might be sufficient to deter future criminal activity.

At present, this sort of case essentially leaves law enforcement with a choice between prosecution or no action, and the risk remains that these essentially peripheral players can step up to leadership in the organised crime group once the principals have been convicted. A preventative order disrupting future criminal activity by these currently minor players could play an important role in preventing them taking over the organisation in the leaders' absence.

An important consideration will be the degree of knowledge of those who are subject to the order, or whose interests will be affected by it. Clearly this will be an important consideration both for the prosecution in deciding whether to apply for the order, and for the court in deciding whether it would be proportionate to make it.

3.3 What Sort of Conditions?

For a civil order not to be considered criminal, and thus attract the additional protections of article 6 ECHR, the conditions attached must be designed to prevent harm, not be punitive.

Within these constraints, the sort of conditions imposed under ASBOs are extremely varied and the legislation provides almost unlimited discretion. The most common conditions include exclusion zones, curfews, bans on associating with named individuals and prohibitions on specific anti-social behaviour. ASBO conditions are prohibitive, they are not used to require certain courses of conduct.

In the case of terrorist control orders, Parliament chose to specify in broad terms the sort of conditions which could be imposed (section 1(4) of the Prevention of Terrorism Act 2005). The conditions possible under terrorist control orders include requirements to behave in certain ways as well as prohibitions; an additional power we are keen should apply to these orders too.

Given the acquisitive nature of organised crime, it is particularly important to be clear that the court could impose particular restrictions on the subject's financial dealings, including for example requiring them only to use notified financial instruments (credit cards, bank accounts) and restrictions on the amount of cash they are permitted to carry.

We are also keen to ensure the orders include a power either compulsorily to purchase businesses or property or otherwise to require individuals to divest ownership of certain possessions which have been used to facilitate serious crime.

Q7. The Government would welcome views on the kinds of conditions that might be attached to an organised crime prevention order.

3.4 Standard of Proof

Standards of proof vary for the various civil orders on the statute book. In the case of terrorist control orders, the basis is 'reasonable suspicion'. For ASBOs, while the orders are civil, the legislation referred to 'proof', and the *McCann* judgement has ultimately imposed a standard not far from the criminal one.

We believe these varying standards usefully reflect the different levels of threat posed to society by terrorism and anti-social behaviour. In the case of organised crime, the potential harms are somewhere between, and we would envisage stating on the face of the legislation that to impose an order the courts should be satisfied on the balance of probability that the test is met.

PREVENTION ORDERS AGAINST INDIVIDUALS: CASE STUDIES

<p>Case Study A</p> <p>F is an associate of a known criminal group. While working at a call centre, F was involved in the compromise of customer data and identity theft, leading to fraud of several hundreds of thousand pounds. F left the job mid way through disciplinary hearings, and a report was made to the police. Information has suggested that F has subsequently left another financial company at short notice and is believed to be applying for jobs at further organisations, possibly under false identities. The police, supported by the financial sector, apply for an order prohibiting F from working anywhere in the financial sector, and requiring him to keep them informed of his employment status. This interference with F's rights would be proportionate to the legitimate aim of preventing crime.</p>	<p>Case Study B</p> <p>Subject R has prior convictions for money laundering in England, and for drug trafficking in another EU country. R is not currently removable from the UK. Law enforcement has source intelligence that R has continued his drug trafficking business in association with a known London criminal group C. R organises consignments face to face by travelling to a third country, S, known to be a major transit country for drug consignments to the UK.</p> <p>Law enforcement will want to apply for a civil order preventing R from travelling to S, or associating with known members of group C, or using forms of communication (eg mobile phones) the details of which have not previously been notified to the authorities. The order can draw on the pattern of known behaviour from past convictions and the evidence of R's current activity.</p>
<p>Case Study C</p> <p>D has recently been identified as a leading Missing Trader Intracommunity (MTIC) fraudster, laundering the proceeds through an offshore financial centre. An urgent investigation has been launched by HMRC. The case is likely to take over a year to get to trial, and in the meantime D is thought to be linked to a number of ongoing fraudulent companies. HMRC applies in the interim for a control order, prohibiting D, his wife and a list of known associates from being involved in certain industry sectors, from benefiting from VAT refunds, requiring all business activity to be notified to HMRC in advance, and requiring all overseas travel to be notified in advance, with travel to a series of named countries with major offshore financial centres prohibited altogether.</p>	
<p>Case Study D</p> <p>R runs a business inviting people to participate in bogus 'competitions' in return for personal details. In practice, the prizes offered are almost worthless, and there is no commercial rationale for the operation. The sole purpose of the mailshots are to identify likely future candidates for advanced fee fraud. These frauds are either carried out by R, or he sells on his mailing lists. Law enforcement applies for a prevention order prohibiting R from engaging in any activity involving large scale mailshots.</p>	

3.5 Prevention Orders Against Organisations

A unique feature of the orders we are proposing is that they should be capable of being imposed not only on individuals but also on organisations, for example companies or voluntary associations.

The range of possible restrictions would be broad, depending upon what is necessary and proportionate in each case. They might include restrictions on how the enterprise carries out its business, it could require the removal of certain directors or office holders, or in extreme circumstances it could require the dissolution of an entity altogether. We also believe the court should be able to authorise the compulsory purchase of property or assets where this is necessary to prevent serious crime, and in the most serious cases to impose new office holders or a court ordered administrator at the entity's own expense. All the restrictions would, of course, have to be proportionate to the harm they were seeking to prevent.

These sort of orders reflect recent trends in regulation of sensitive sectors. Government requires various sectors of the economy to be regulated where there is a pressing public interest in this, an interest which will often include the prevention of crime, but will also extend to consumer protection, public health and avoidance of systemic risks.

Organised crime operates in a highly flexible manner. For some criminal activities (for example money laundering), particular sectors are especially vulnerable and are hence regulated. But many activities necessary to facilitate crime take place in sectors which are currently unregulated, and imposing regulation on them simply in order to catch the tiny minority of operators who are engaged in serious crime risks being disproportionate.

These orders therefore would amount to a highly targeted imposition of controls, restrictions and obligations on entities which are already known to be supporting crime. In addition, however, these orders would enable the authorities to tackle the root cause of the problem where there is criminal infiltration of a particular entity. Any number of prosecutions cannot stop this infiltration where those convicted are simply replaced in the suborned organisation.

Some of these powers exist elsewhere in certain circumstances already, and the court making the order might be given access to powers elsewhere exercisable by regulators or the secretary of state (for example the Secretary of State's power in the Companies Act to wind up companies when it is in the public interest).

These orders against organisations draw on US experience on Civil RICO (Racketeer Influenced and Corrupt Organisations). Civil RICO is an exceptionally broad power. USC §1964(a) sets out procedures for orders

"including, but not limited to: ordering any person to divest himself of any interest, direct or indirect, in any enterprise; imposing reasonable restrictions on the future activities or investments of any person...or

ordering dissolution or reorganisation of any enterprise, making due provision for the rights of innocent persons"

From 1970, the Teamsters Union had had over 340 officers convicted for mafia related crimes, but these prosecutions altered nothing in the mafia domination of parts of the union, as convicted individuals were simply replaced. Only when civil measures began to be taken to introduce court ordered administrators into particularly corrupt 'locals' (union branches) did the threat of mafia influence begin to be tackled effectively.

PREVENTION ORDERS AGAINST ORGANISATIONS: CASE STUDIES

<p>Case Study 1: Drug Trafficking</p> <p>Company G runs a small coachbuilding business making horseboxes, and also has a couple of trucks carrying exports from the UK. On at least one occasion, a horsebox manufactured by company G has been found to be carrying drugs in a concealed compartment, which company G claims it built in order to enable the drive to hide valuables. Police also investigate the trucking business. Rather than returning to the UK with empty trailers the company's trucks typically carry a 'backload'. Sometimes these are prearranged and have a clear audit trail, but a disproportionate number of these loads are arranged at short notice with very little paper work. The police apply for a suppression order requiring company G to notify them of the names of any clients for whom they have built concealed compartments, and the compartments' location, and requiring company G to carry only backloads with a proper audit trail and which are notified to law enforcement at the point of entry to the UK. This notice is publicised, and is designed to destroy company G's attractiveness as a logistics supplier to the drugs trade. To the extent to which G trades legitimately, however, the regulatory burden is negligible.</p>	<p>Case study 2: Money Laundering</p> <p>X is a money service bureau (MSB). While complying with the requirements under the MSB licensing regime, it makes a disproportionate number of payments to S, known to be a major transit country for the supply of drugs to the UK. Several of these are linked to known drugs transactions. X has not made any Suspicious Activity Reports to SOCA as required under POCA, but there is not yet sufficient evidence in any case to justify a prosecution under the POCA offences. Law enforcement apply for an order imposing enhanced due diligence checks on payments which X makes to S, identification requirements for payments over a fixed amount to a further group of high risk destination countries and again monitors compliance through 'mystery shopping'. This should enable either money laundering activity to be curbed or a case to be built up for prosecution under POCA.</p>
---	--

Case study 3: vehicle ringing

L owns a breakers' yard, which has been in his family for many years, and which he claims to have sub let to D and W. Over a period of 5 years, both D and W are convicted of vehicle ringing and imprisoned. E is put in charge. Police believe D, W and E are all employees of L, but there is insufficient evidence to prove this, and nor is it easy to prove that the yard itself constitutes the proceeds of crime and is hence liable for civil recovery under POCA. The location of the yard makes surveillance almost impossible. Police apply for a compulsory purchase order, forcing L to relocate the business, and demand enhanced reporting of which vehicles are processed through the business in future in order to improve the prospects of identifying future ringing.

Q8. The Government would welcome views on the types of situation where an organised crime prevention order may prove useful and proportionate in preventing organised criminality.

3.6 Rights of Third Parties

The sort of restrictions envisaged in these orders would undoubtedly impact on various convention rights, mainly article 8 (privacy and family life) and article 1 of the 1st protocol (interference with property). To be justified, such restrictions need to be based on provisions set out in law, proportionate and necessary for various aims, one of which is the prevention of crime.

An important feature for the courts will be ensuring that the restrictions that orders impose are proportionate to the harm prevention purpose. In particular, we would expect the courts to want to have before them evidence as to the steps which have been taken to secure a voluntary agreement before an application for an order is made. In addition, it will be important that the courts are made aware of the possible impact of orders on the rights of third parties. We are considering whether this would require including something on the face of the legislation requiring the courts to take due account of the rights of third parties (as in the US legislation on Civil RICO cited above), or whether this is already implicit in the regime imposed by the Human Rights Act. A simpler alternative might be for the legislation or rules of court to state explicitly that the authority applying for the order should draw to the court's attention relevant facts about the possible interests of third parties.

Q9. Should the prosecution be required (whether by legislation or court rule) specifically to draw the court's attention to relevant facts about the impact of potential orders upon the interests of third parties?

CHAPTER 4: PROCEEDS OF CRIME

The new powers introduced in the Proceeds of Crime Act 2002 to take the profit out of crime been strongly welcomed by police and other law enforcement agencies. They have also been a great success. Over £230million has been recouped from criminals over the last 3 years, with annual asset recovery performance doubling over the same period.

4.1 Proposed New Measures

Operational experience of the legislation over the last three years has shown areas where it might be improved. We are seeking ways to further improve the enforcement of confiscation orders, potentially by merging the confiscation and enforcement hearings so that findings of fact as to assets that the defendant owns can be made. This would remove the sometimes lengthy litigation on this point that follows a confiscation hearing.

We are also considering new provisions to enable us to contract out the enforcement of confiscation orders and examining the scope for the statutory cancellation of old orders that are deemed unenforceable or very difficult to enforce. There are cases where confiscation debt remains and should be collected but collection is highly unlikely (for example, the order was based on hidden assets, the defendant has absconded or died, or all available enforcement methods have been exhausted).

The extension of certain powers previously the reserve of police and HM Revenue & Customs officers, namely investigation and restraint powers, has been a success. There are 19 bodies and agencies, including trading standards officers, Serious Fraud Officers and immigration officers with such powers.

We are considering extending all powers that are currently limited to the police and HM Revenue and Customs officers to all financial investigators. This includes

- executing search and seizure warrants,
- seizing property subject to a restraint order to prevent its removal from the UK and
- searching for and seizing cash suspected of being criminally tainted.

Financial investigators are becoming more independent from police in their work and therefore to give them the full range of powers would be beneficial. The extension of such powers has precedent in the Police Reform Act 2002 which allows chief constables to designate police staff to have access to certain powers of a constable under the Police and Criminal Evidence Act 1984.

Q10. We would welcome your views on new measures to merge confiscation and enforcement hearings, to contract out enforcement of confiscation orders, to cancel orders which cannot be enforced, and to extend certain search and seizure powers to all financial investigators.

4.2 Money Laundering

Depriving criminals of their illicit assets also means strengthening our defences against money laundering. The Proceeds of Crime Act strengthened UK's anti-money laundering controls and made it much harder for criminals to launder their proceeds.

The Act updated, expanded and unified the money laundering offences, and removes the distinction between drug and non-drug money laundering.

The Government made some amendments to the money laundering provisions in POCA in the Serious Organised Crime & Police Act 2005. These sought to respond to concerns about aspects of the legislation which had been highlighted by the regulated sector. The purpose of the amendments was to:

- reduce some of the burden on the regulated sector in complying with the requirements to report money laundering
- respond to other concerns about the legislation which industry had raised, and
- improve the effectiveness of the money laundering reporting system

One of these amendments concerned the method by which suspicious activity is reported to SOCA. An earlier chapter has outlined the potential value that could be extracted from SARs through improved data-mining and data-matching. However, the success of these approaches is dependent on SOCA being able to access and manipulate the data effectively using technology, which is affected by the form and manner in which it is submitted by reporters. The debate around the introduction of a prescribed form has recently been outlined in the Lander Review. SOCA is now consulting stakeholders on the best way forward. This may involve additional amendments to POCA.

Another SOCPA amendment to (Section 103) concerned the consent provisions in POCA. This issue was also considered in the Lander Review of the Suspicious Activity Reports regime. Following the Review's launch, SOCA has started consultation with stakeholders to define an approach that will retain the law enforcement value of the consent regime while limiting burdens on industry. This includes not only administrative and technological changes, but also possible further amendments to POCA, taking into account that any changes would have to be consistent with EU Money Laundering Directives.

SOCA is working to implement the recommendations of the Lander Review. Part of the increased dialogue with stakeholders will be ongoing consultation about how to continue driving improvements in the use of POCA.

Q11. We welcome views and comments on further amending and improving the consent provisions in the Proceeds of Crime Act 2002 in a way which a) maintains the existing benefits to law enforcement agencies in terms of seizing and restraining suspect assets and disrupting criminal activity and b) enables the reporting sectors in industry to suspend transactions or activity with a client without making him/her suspicious.

Annex A:

Consultation Questions

Chapter 1: Data-Sharing

Q1. Should public sector information on suspected fraudsters be shared more widely within the public sector and with the private sector to prevent and detect fraud? What sort of safeguards would you expect to see? What do you believe the most appropriate vehicle for data-sharing would be?

Q2. Should the scope of the National Fraud Initiative be expanded and placed on a statutory footing in order to increase its capacity to detect fraud within the public sector?

Q3. We would welcome your views on SOCA matching Suspicious Activity Reports received from the regulated sector against a range of public sector databases.

Q4. We would welcome your views on what you would regard as appropriate and targeted data mining of public and private sector databases to detect and prevent criminal activity, and what the appropriate safeguards for such exercises should be.

Chapter 2: The Criminal Law

Q5. Should Clause 2 be restricted to those who believe that an offence will take place or should this be widened?

Q6. Is the Government right to consider extending liability to those who indirectly encourage or assist a person (X) where they suspect this encouragement or assistance will aid X's criminal activities (as against specific criminal offences)?

Chapter 3: Organised Crime Prevention Orders

Q7. The Government would welcome views on the kinds of conditions that might be attached to an organised crime prevention order.

Q8. The Government would welcome views on the types of situation where an organised crime prevention order may prove useful and proportionate in preventing organised criminality.

Q9. Should the prosecution be required (whether by legislation or court rule) specifically to draw the court's attention to relevant facts about the impact of potential orders upon the interests of third parties?

Chapter 4: Proceeds of Crime

Q10. We would welcome your views on new measures to merge confiscation and enforcement hearings, to contract out enforcement of confiscation orders, to cancel orders which cannot be enforced, and to extend certain search and seizure powers to all financial investigators.

Q11. We welcome views and comments on further amending and improving the consent provisions in the Proceeds of Crime Act 2002 in a way which a) maintains the existing benefits to law enforcement agencies in terms of seizing and restraining suspect assets and disrupting criminal activity and b) enables the reporting sectors in industry to suspend transactions or activity with a client without making him/her suspicious.

Annex B:

Departments and Organisations Consulted During the Development of this Paper

Attorney General's Office
Audit Commission
Department for Communities and Local Government
Department for Constitutional Affairs
Department for Education and Skills
Department for Health
Department for Work and Pensions
Financial Services Authority
GCHQ (Government Communications Headquarters)
Her Majesty's Customs and Excise
Her Majesty's Treasury
Scottish Executive
Serious Fraud Office

Annex C:

Consultation Co-ordinator

If you have any complaints or comments specifically about the consultation process only, you should contact the Home Office consultation co-ordinator Christopher Brain by email at: Christopher.Brain@homeoffice.gsi.gov.uk

Alternatively, you may wish to write to:

Christopher Brain
Consultation Co-ordinator
Performance and Delivery Unit
Home Office
3rd Floor Seacole
2 Marsham Street
London
SW1P 4DF

Annex D:

The Consultation Criteria

This consultation follows the Cabinet Office Code of Practice on Consultation - the criteria for which are set below.

The six consultation criteria

1. Consult widely throughout the process, allowing a minimum of 12 weeks for written consultation at least once during the development of the policy.
2. Be clear about what your proposals are, who may be affected, what questions are being asked and the timescale for responses.
3. Ensure that your consultation is clear, concise and widely accessible.
4. Give feedback regarding the responses received and how the consultation process influenced the policy.
5. Monitor your department's effectiveness at consultation, including through the use of a designated consultation co-ordinator.
6. Ensure your consultation follows better regulation best practice, including carrying out a Regulatory Impact Assessment if appropriate.

The full code of practice is available at:

www.cabinet-office.gov.uk/regulation/Consultation

Annex E:

Glossary

ACPO	Association of Chief Police Officers
ARA	Asset Recovery Agency
CIFAS	UK's Fraud Prevention Service
CPS	Crown Prosecution Service
DCA	Department for Constitutional Affairs
DVLA	Driver and Vehicle Licensing Agency
DWP	Department for Work and Pensions
FIN-NET	Financial Crime Information Network
Fraud review	Interdepartmental review into the detection, investigation and prosecution of fraud.
FSA	Financial Services Authority
Hampton review	Treasury led review of regulatory inspections and enforcement, final report published on 16 March 2005.
HMCE	HM Customs and Excise
HMIC	HM Inspector of Constabulary
HMRC	HM Revenue and Customs
ICO	Information Commissioner's Office
IMPACT	IMPACT programme is designed to deliver a national system to support police intelligence.
IND	Immigration and Nationality Directorate
Lander review	Review of Suspicious Activity reports regime led by Sir Stephen Lander, published March 2006
MISC31	Cabinet committee created to develop the Government's strategy on data-sharing across the public sector
MPS	Metropolitan Police Service
MTIC	Missing Trader Intra Community
NCIS	National Criminal Intelligence Service
NCIS ELMER	National Criminal Intelligence Service database for Suspicious Activity Reports
NFI	National Fraud Initiative (run by Audit Commission)
NI	National Insurance (number)
NIR	National Intelligence Requirement- drawn up by SOCA for law enforcement agencies.
NOMS	National Offender Management Service
NPIA	National Police Improvement Agency
Operation Grafton	Met Police led operation to tackle high value organised crime around Heathrow airport.
PIU report	Cabinet Office Performance and Innovation unit published a report on privacy and data sharing on 11 April 2002
SAR	Suspicious Activity Report
SFO	Serious Fraud Office
SOCA	Serious and Organised Crime Agency
VAT	Value Added Tax

Annex F:

Relevant Legislation - (with hyperlinks where available)

Anti-terrorism, Crime and Security Act 2001

<http://www.opsi.gov.uk/ACTS/acts2001/20010024.htm>

Crime and Disorder Act 1998

<http://www.opsi.gov.uk/acts/acts1998/19980037.htm>

Criminal Justice and Court Services Act 2000

<http://www.opsi.gov.uk/acts/acts2000/20000043.htm>

Data Protection Act 1998

<http://www.opsi.gov.uk/ACTS/acts1998/19980029.htm>

Football (Spectators) Act 1989

http://www.opsi.gov.uk/acts/acts1989/Ukpga_19890037_en_1.htm

Freedom of Information Act 2000

<http://www.opsi.gov.uk/ACTS/acts2000/20000036.htm>

Police and Criminal Evidence Act 1984

Police Reform Act 2002

<http://www.opsi.gov.uk/acts/acts2002/20020030.htm>

Proceeds of Crime Act 2002

<http://www.opsi.gov.uk/acts/acts2002/20020029.htm>

The Serious Organised Crime and Police Act 2005

<http://www.opsi.gov.uk/ACTS/acts2005/20050015.htm>

Terrorism Act 2000

<http://www.opsi.gov.uk/Acts/acts2000/20000011.htm>