1. BACKGROUND

The Immigration, Asylum and Nationality Act (the IAN Act) 2006 created new passenger, crew, service and freight data acquisition powers for the police, and extended and enhanced the powers of the then Border and Immigration Agency and HMRC to require this type of data in advance of arrival. It also introduced a duty requiring that this information be shared between the border agencies.

These powers enhance the border agencies’ ability to establish, in advance of travel, the level of threat posed by an individual or freight movement and tailor the appropriate operational response. This is a key component of an intelligence-led risk-based approach to border control.

The Code of Practice details how information will be shared between the border agencies under section 36 IAN Act 2006 and the safeguards to be implemented with regard to such sharing. It also aims to provide reassurance and confidence in respect of how personal data will be used and stored.

This preliminary review of the Code of Practice has been undertaken by representatives of the border agencies and included consultation with the Information Commissioner’s Office. This review takes account of: operational or technical developments; further evidence based assessments of the data requirements; changes to procedures; and ensuring that adequate safeguards are in place to protect data of the individual. A further in depth review of data sharing and operation of the Code of Practice will take place once e-Borders operations transfer to the National Border Targeting Centre.
2. INTRODUCTION

2.1 Scope of the Code
The Code of Practice covers data shared under S36 IAN Act 2006 as implemented by the duty to share order (S.I. 2008, No. 539) which includes a range of joint working arrangements, including e-Borders. This review examines the operational sharing of passenger, crew and service data between the border agencies and whether operational processes follow the key principles set out in the Code of Practice.

2.2 Project Semaphore

Project Semaphore was launched in 2004 as a pilot project aiming to “de-risk” the development and delivery of the e-Borders solution. It was a cross cutting initiative co-ordinated by the Home Office in partnership with the key border control and law enforcement agencies: Border and Immigration Agency, HM Revenue & Customs, the police service and UKvisas.

The Semaphore system processes advance passenger information provided by carriers on journeys to and from the UK. This information is screened against watchlists in the Joint Border Operations Centre (JBOC). Where a match is identified an alert is issued to the appropriate agency.

In addition to checking advance passenger information against watchlists, Semaphore is also receiving reservation data for analysis against profiles. This enables the identification of potentially high risk individuals from information contained in carrier reservations data. A match does not mean that someone is a criminal or even a suspect, only that there is a case for further investigation.

Project Semaphore initially targeted six million passenger movements a year travelling on a number of international air routes to and from the UK. After a successful first year the Project was granted additional funding to increase the capability of the system. From one carrier and two routes at the outset, Project Semaphore now receives data from 105 air and sea carriers on passengers travelling to and from 185 non-UK departure points. On 31 March 2008 Semaphore moved from the developmental project phase into business as usual mode.

Information on passenger movement is also captured by the Freight Targeting System (FTS) operated by HMRC.

2.3 Transition to e-Borders
On 14 November 2007 a contract was awarded to Trusted Borders to deliver the e-Borders Programme. The early stages of deployment of e-Borders have seen responsibility for managing the Semaphore system pass to Trusted
Borders who will continue to support it until their own system is rolled out. From 1 June 2008 management of the JBOC was taken over by the newly formed Intelligence and National Operations Directorate of the UK Border Agency.

2.4 UK Border Agency

In April 2008 the UK Border Agency was launched as a shadow agency of the Home Office. Shadow status is a transitional period of operation before operating as a full executive agency. The Agency brings together the work previously carried out by the Border and Immigration Agency, Customs detection work at the border from Her Majesty’s Revenue and Customs (HMRC) and UKvisas.

Acting as a single agency has brought greater integration to the work of the separate border agencies. Within the Joint Border Operations Centre (JBOC) Immigration and HMRC officers work closely together to identify high risk travellers.

2.5 Legislative Position

The power for police and Immigration Officers to request passenger, crew and service data from carriers is set out in detail in the Immigration and Police (Passenger, Crew and Service Information) Order 2008 (S.I. 2008, No. 5). The order specifies the broad range of travel related data that can be required in relation to aircraft, ships and trains arriving in and leaving the UK. Information obtained under this order falls under S36 IAN Act 2006 as implemented by the duty to share order (S.I. 2008, No. 539), and falls within the scope of the Code of Practice.

Due in part to the creation of the UK Border Agency, and the desire to avoid setting up short-term working practices during the merging process, the S.I. 2008/5 powers have not been used to collect data to date. Both within and outside of e-Borders data is still being obtained under legacy arrangements, with information supplied voluntarily by carriers. Arrangements are currently being made to request data under the new powers for the first time.

The new powers will allow us to formally set out the data that we require from carriers, allowing clear communication of the level of detail and timing of data transmission required. Using the new powers will also mean the data is formally covered by the safeguards set out in the code of practice.
3. WORK TO DATE

3.1 Data Collection
Between 1 March and 30 September 2008 the Semaphore system has collected Travel Document Information (TDI) data for 20,917,798 passenger movements and Passenger Name Record (PNR) data for 7,013,690 passenger movements (including duplication).

Additionally the FTS has collected the TDI data on 4,388,020 tourist movements and 4,172,546 freight movements.

3.2 Achievements so far
Since inception access to JBOC data has supported over 2,500 arrests by police and made significant contributions to the crime and counter terrorism intelligence systems.

Between 2 March and 30 September 2008 JBOC issued over 8,000 alerts to ports which resulted in over 750 arrests. Successes include:

- 5 arrests for murder
- 2 arrests for kidnap
- 4 arrests for rape and 17 for sexual offences
- 272,540 cigarettes seized
- 5 arrests and over 250 interventions for immigration offences

Using FTS activities at the border between 1 March 2008 and 30 September 2008 have yielded the following results:

<table>
<thead>
<tr>
<th>Class Type</th>
<th>Quantity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class A Drugs</td>
<td>399.5 Kg</td>
</tr>
<tr>
<td>Class B/C Drugs</td>
<td>3536.6 Kg</td>
</tr>
<tr>
<td>Cigarettes</td>
<td>99,990,492</td>
</tr>
<tr>
<td>Tobacco</td>
<td>4251.5 Kg</td>
</tr>
<tr>
<td>Alcohol</td>
<td>468207 L</td>
</tr>
<tr>
<td>Clandestines</td>
<td>23</td>
</tr>
</tbody>
</table>

In addition, joint working with Immigration has provided numerous successes in identifying vehicles associated with non payment of civil penalty fines, with 86 vehicles identified, 48 intercepted and 22 detained.

The following results were achieved by Special Branch in one month alone using shared data:
- 32 suspicious movements generated
- 18 Schedule 7 Terrorism Act exams
- 1 exam leading to arrest for fraud
- 3 arrests referred to Port of Dover Police
- 15 intelligence reports generated
- 12 referrals to HMRC for drugs and other smuggling
4. OPERATIONAL AND TECHNICAL DEVELOPMENTS

All of the border agencies feel that current sharing procedures are working properly with minimal need for improvement.

The current e-Borders system configuration limits UK Border Agency user access rights along the lines of previous legislation. Work is currently underway to amend access rights to fully utilise the data acquisition power provided by the Immigration and Police (Passenger, Crew and Service Information) Order 2008 and gain wider access to OPI data.

FTS has been upgraded. The latest version provides users with improved functionality which includes advanced analytics and data matching capabilities. It also allows for the submission of shipping manifests in a format that is potentially compatible with E-borders. This has the potential to provide the agencies with improved data on passenger and freight movements.

4.1 Lessons Learned

HMRC and Immigration agreed a number of processes and safeguards for sharing information in line with the Code of Practice. These remain in place and so far have not identified any additional issues.

Within the police, experience of utilising the JBOC product has led to police developing guidelines for police use of the e-Borders system and data and the type of offence for which it will be used. Access will be limited and for serious offences and those circulated as wanted only.
5. SAFEGUARDS

The code sets out in Section 4 the key data protection principles governing the sharing of information under Section 36 of the IAN Act 2006. The principles set out in the code are being adhered to, and we have processes in place that ensure the data available is proportional to both role and agency. Data is collected and stored in accordance with data protection principles and system availability is restricted and all system actions are fully audited.

5.1 Information Storage
The Code indicates that data should be kept in an active database for a maximum of five years, with flexibility to allow access to older data on a case-by-case basis for a further five years maximum. This principle is being adhered to and at present all travel data processed to date is stored in the Semaphore historical database as none of the information has reached the date for transfer to the inactive database or for destruction. This currently totals over 70 million records.

5.2 Authorised Access
In accordance with the standards set out in the code of practice data access is subject to strict control in secure buildings. All staff members are vetted and cleared to Security Check standard and have individual system user accounts and passwords. Access to systems is controlled according to the individual’s role and all systems are fully audited.

5.3 Training and guidance
Within JBOC there is a week long induction for all operational staff which includes training on data protection principles and appropriate data usage. At the FTS Hub, HMRC, Special Branch and Immigration receive training on the use of the systems and attend HMRC data security workshops.

5.4 Monitoring and Auditing
JBOC managers frequently monitor processes and a record of outcomes of such checks is retained. 1758 checks were made over the period 1 March 2008 to 28 October 2008.

HMRC Enforcement Systems Management Team has responsibility for auditing and monitoring FTS usage. Local management checks are also in place.

No occurrences of misuse of data have been detected.
5.5 Subject access requests
Subject access requests are still currently handled by the separate agencies. No requests for personal information obtained through e-Borders have been received by HMRC or the police.

JBOC has requested this information from the Data Protection Unit based in Lunar House, Croydon.