Audit and Assurance Committee

Date: **7 December 2012**

Item 10: **Annual Report on Personal Data Disclosed by TfL to the Police and Other Law Enforcement Agencies**

This paper will be considered in public

1 Summary

1.1 To report to the Audit and Assurance Committee on the operation of TfL's policy on the Disclosure of Personal Data to the Police and other Law Enforcement Agencies.

2 Recommendation

2.1 **The Committee is asked to note this report.**

3 Background

3.1 The policy on the disclosure of personal data to the police and other Law Enforcement Agencies was approved by the TfL Board on 7 December 2006. The Board asked for a high level report on the operation of the policy to be provided to the Audit Committee on an annual basis.

3.2 TfL holds a range of information about its customers and employees and, in disclosing personal details to the police and other statutory law enforcement bodies without the subject's consent, exercises the exemption under section 29 of the Data Protection Act (DPA) 1998, for crime prevention and detection purposes.

3.3 TfL receives detailed requests from the police and other law enforcement bodies[1] for information on customers and TfL employees. In accordance with the agreed policy, TfL considers all such requests and releases personal data where it is lawful to do so and is consistent with the Mayor's Transport Strategy and its associated powers. Disclosure of such data is managed by the Community Safety, Enforcement and Policing Directorate (CSEP) in Surface Transport.

3.4 Information Governance (IG), part of General Counsel, has responsibility for overseeing compliance with the policy.

[1] Includes national security and other agencies with a statutory role in crime prevention and detection.

4 Operation of the policy

4.1 IG advises on the implementation of the policy and its compliance with current legislation and best practice.

4.2 The operation of the policy in the context of the day to day processes, procedures and auditing of disclosures to the police is managed by the Crime and anti-social behaviour Investigation Team (CIT) within CSEP in Surface Transport. This team deals with requests for personal data made to TfL by the police and other Statutory Law Enforcement Agencies (SLEAs) with the following exceptions:

(a) police requests for access to information, including CCTV images, held by London Underground Limited (LUL). These requests are processed directly by LUL, or the British Transport Police (BTP) on its behalf; and

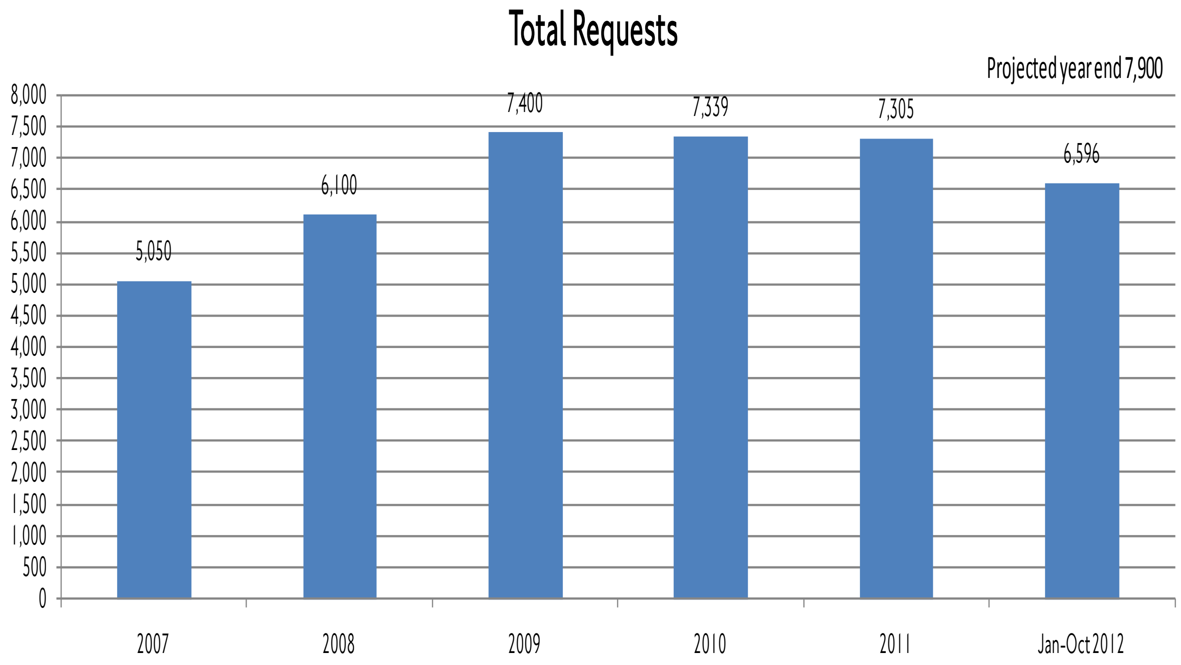
(b) police requests for information on licensed drivers, for licensing decisions, held by the London Taxi and Private Hire Directorate (LTPH) and for investigating allegations of sexual offences and other serious crimes. These requests are processed directly by LTPH. Victoria Coach Station, Bus operations, Road Network Compliance and London River Services also deal with their own requests like TPH. They follow TfL procedures and are trained and audited by CSEP.

4.3 Since May 2012, CSEP has also taken responsibility for responding directly to requests from non-police bodies that have a statutory role in crime prevention and detection (for example, local authorities, HM Revenue and Customs, Serious Organised Crime Agency (SOCA). These requests were previously dealt with by IG. To ensure consistency of approach, IG continues to provide specialist advice to all areas of TfL on the disclosure of personal data to third parties.

5 Overview of requests and disclosures

5.1 Chart 1 below shows the volume of all police and SLEA data requests made to CSEP since 2007 (for full year January - December) and a comparison to the period covering 1January 2012 to 31 October 2012 (inclusive) when there were 6,596 data requests made to CSEP. The forecast for January - December 2012 is estimated at 7,900, which equates to 500-600 more requests received than in the previous three years.

Chart 1: Breakdown of request (by volume) from 2007 – October 2012



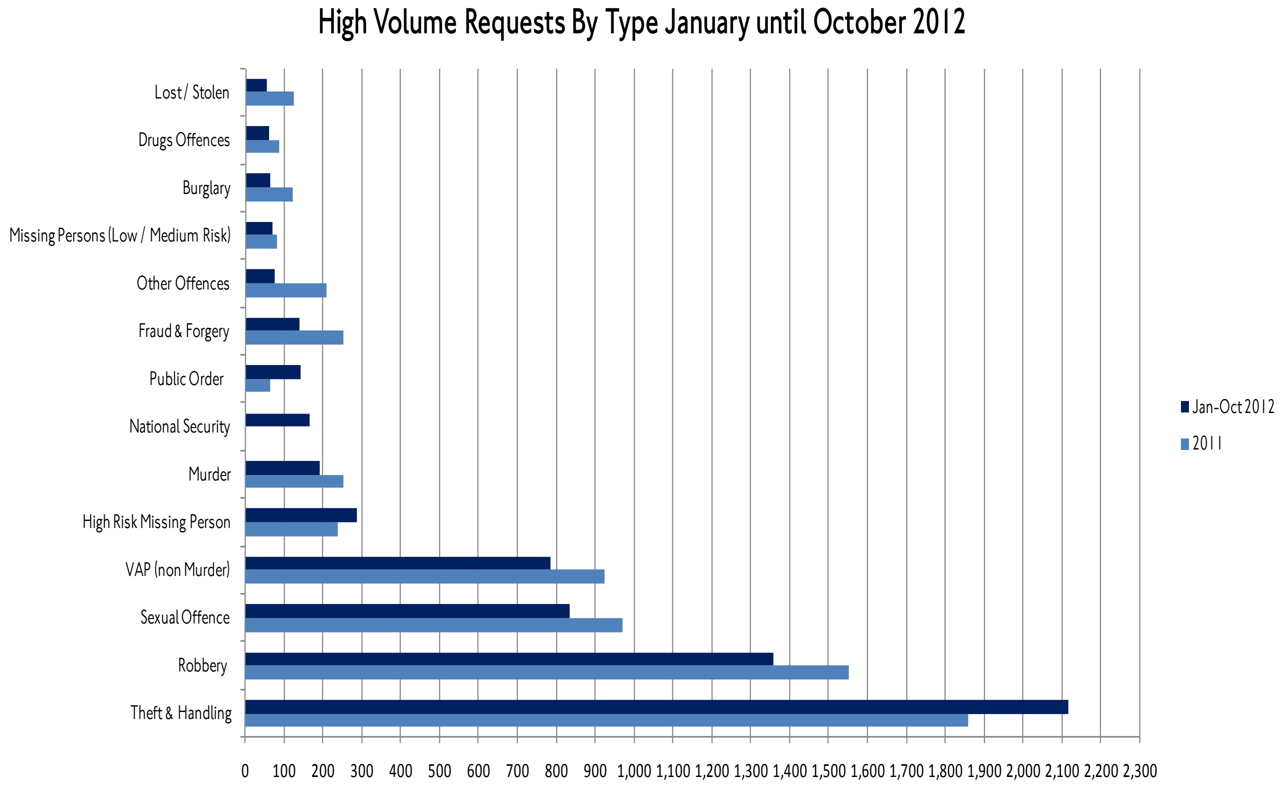
5.2 The Metropolitan Police Service (MPS) account for the majority of requests made to CSEP. Table 1 shows a breakdown of data requests by the requesting agency (by percentage).

Table 1: Data requests by requesting agency

SLEA	No of requests	Percentage %
MPS	5,618	85
British Transport Police	488	7
Other police forces	182	3
National Security	120	2
Non-police bodies that have a statutory role in crime prevention and detection	85	>1
City of London Police	44	<1

5.3 Chart 2 illustrates the breakdown of data requests by crime/incident type. The table only shows the crimes/incidents where we have received 50 or more requests from 1 January to 31 October 2012 (inclusive).

Chart 2: Data request by crime type



5.4 Examples of the types of investigations supported and the outcome of the use of Oyster data can be found in Appendix 1.

6 Overview of recent improvements

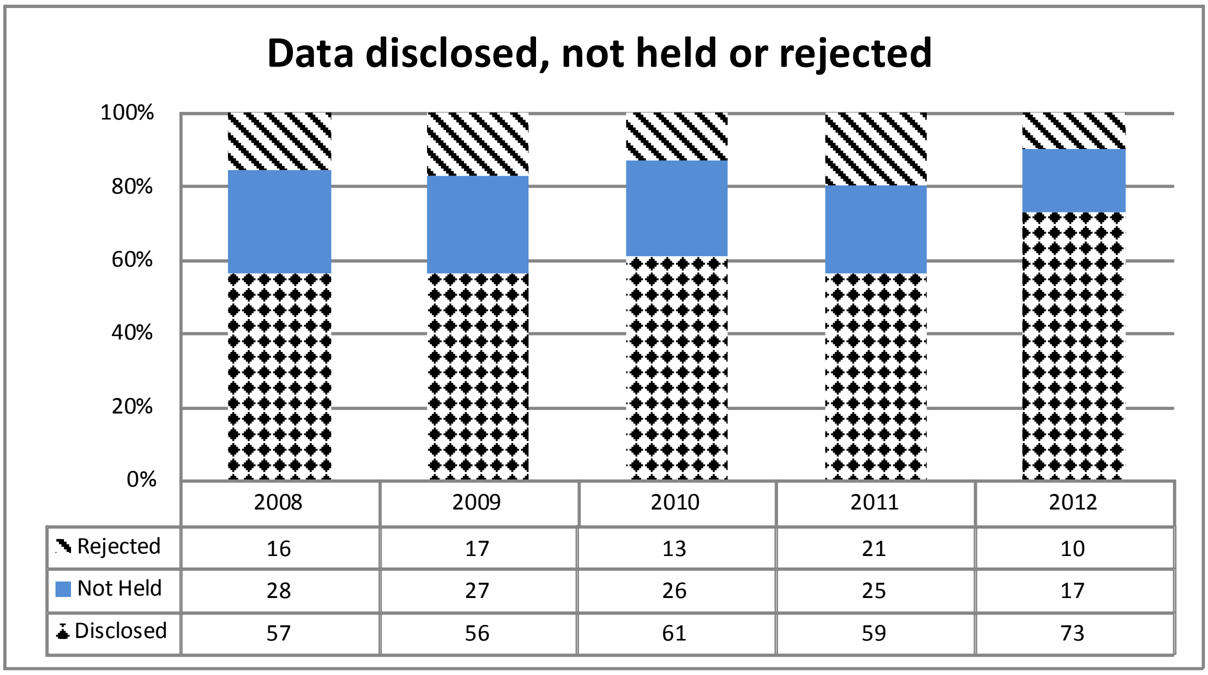
6.1 CSEP continually reviews how best to manage current and projected levels of demand. In 2011, guidance was issued to the SLEAs and this was updated and comprehensive guidance placed on their intranet sources.

6.2 The purpose of the guidance is to provide clear advice on how data requests should be made and, once received by TfL, how they will be categorised. It supports the TfL policy on disclosure and provides a uniform and structured approach. This allows the police to be clear on the type of data requests that will be considered. Requests are dealt with on a case by case basis but are categorised into one of three tiers when they are received, determining if and how they will be dealt with. This ensures that any disclosures are lawful, necessary and proportionate. The guidance on the three tiers can be found at Appendix 2.

6.3 As a result, CSEP has seen a marked increase in the proportion of requests which result in a disclosure. This means fewer requests are rejected on the grounds that they are not clear or appropriate, leading to more crime investigations being supported through the use of Oyster card and other personal data held by TfL.

6.4 The following chart shows these increases since 2008.

Chart 3: Breakdown of data requested to data disclosed



	2008	2009	2010	2011	2012
▨ Rejected	16	17	13	21	10
🟦 Not Held	28	27	26	25	17
▩ Disclosed	57	56	61	59	73

6.5 The chart shows that over the past year, with the introduction of the tier process, the police have become more efficient in making requests for data resulting in fewer rejections (due to lack of clarity or not meeting our policy or priorities) or where data is simply not available to disclose.

6.6 Alongside these efficiency benefits, CSEP have also overseen improvements in the time taken for disclosures. The speed of data disclosure can be vital to police investigations and quicker disclosures have demonstrably led to bringing offenders to justice sooner than they normally would. This can have the further positive outcome of preventing any further crimes being committed by that offender against our staff, passengers or infrastructure.

6.7 The average time taken for a request to be disclosed in 2011 was 7.5 days; in 2012 this decreased to 4.8 days. Some requests are complex and can take further liaison with the police, to ensure that data which is necessary for the investigation is released.

6.8 Of greater significance is the fact that in 2011, 44 per cent of requests were turned around within 1 day of receipt, but in 2012 this rate stands at over 52 per cent.

6.9 Despite an increase in the number of requests received there has also been an increase in certain types of requests, such as passenger lists which take longer to process due to the analysis of data. In most cases CCTV may have to be viewed with the OIC and checked against Oyster data.

6.10 Throughout this period the CSEP CIT have achieved these improvements without increasing staff capacity. The team continues to oversee three civilian members of the MPS Transport Data Retrieval Team and one member of British Transport Police (BTP) staff who are on attachment to the team and assist in the processing of requests for Oyster card data.

6.11 In the previous report it was highlighted that there was to be a move away from faxed or paper based requests. CSEP has now developed a way to deal with the secure transfer of data through electronic means. As part of this process, staff are using Criminal Justice Secure eMail (CJSM), which has been developed to provide a secure way for criminal justice agencies and practitioners to exchange emails with each other. It can now be reported that approximately 60 per cent of all Oyster requests are electronic, and other areas of Surface Transport have had this method of data transfer rolled out to them post-Games.

6.12 Data disclosures by the team in CSEP are regularly audited internally to ensure that all work is carried out in accordance with TfL policy and the principles of the Data Protection Act.

6.13 Overarching 'Information Sharing Protocols' (and a number of subsidiary procedures) with the MPS, City of London Police (CoLP) and the BTP have been concluded and implemented. A similar agreement is also being finalised with SOCA. These agreements streamline the process for entering into arrangements for the regular sharing of information with the police while ensuring that all relevant legal and operational requirements are satisfied.

6.14 TfL continues the bulk transfer of data (but not images) collected by Congestion Charging Automatic Number Plate Recognition (ANPR) cameras to the MPS, solely for the purpose of safeguarding national security. The Home Secretary has certified that it is necessary that this transfer (and the associated processing of this data by the MPS, other police forces and national security agencies) be exempted from a number of provisions of the DPA, in order to safeguard national security.

6.15 The Mayor made a manifesto commitment to make the data collected by Congestion Charging's ANPR cameras available to the MPS for use in crime prevention and detection (in addition to its existing use for national security purposes). This commitment is currently being taken forward, with the joint development by TfL and the MPS of the legal framework that will enable implementation.

7 Conclusions on the effectiveness of TfL disclosures

7.1 Through the transfer of data, TfL is making a prominent contribution to the safety and security of London's transport infrastructure and its passengers by enabling Police partners and other SLEAs to access data they consider to be necessary to their efforts to investigate, prevent and detect crime on the TfL network and threats to national security and crime.

7.2 Further performance improvements can be realised as the police improve their understanding about what Oyster data can do and what they can lawfully request. There will be a focused drive in 2013 to make further improvements in a number of areas of data disclosure performance.

7.3 Future changes in ticket technology do pose challenges for this work but discussions are ongoing within TfL to ensure the impact is minimal. In time these developments may in fact result in many data improvements, which will contribute further to police investigations.

List of appendices to this report:

1 Feedback and case studies
2 Guiding definitions and working principles on the disclosure of personal data to the Police and other SLEAs

List of Background Papers:

None

Contact: Steve Burton, Director, Community Safety, Enforcement and Policing, Surface Transport.
Number: 020 3054 0755
Email: Steve.Burton@tfl.gov.uk

Appendix 1

Feedback and case studies of data disclosed

The Crime and anti-social behaviour Investigation Team (CIT) within CSEP have been instrumental in helping Law Enforcement Agencies identify and apprehend subjects who have committed serious crimes on and off the TfL network through the analysis of Oyster data and Congestion charging data. Through the data held we have aided the victims and assisted in apprehending suspects.

In September 2012, a member of the CIT received a commendation from the Assistant Commissioner of the Metropolitan Police Service for her work on a particular case, which resulted in a long prison sentence for the perpetrator.

However, over the last year the CIT have had positive feedback on some cases they have assisted with. The examples below show the range of enquiries they are involved in:

1. In November 2012, a police officer attended the offices at Palestra at 10.30am, with the CCTV from a bus where a passenger was the victim of a sexual offence. A passenger list had been run, and from viewing the CCTV and analysing the data from Oyster the suspect was identified. The police contacted the CIT at 2.30pm the same day to confirm that the suspect was on the Sex Offenders register. The speedy assistance provided meant that the police were able to obtain sufficient information to make an arrest and potentially prevent any further offences.

2. In a similar case, the CIT identified a suspect for an offence from Oyster data in April 2011. It was only in July 2012 that the CIT were notified that the offender received six months imprisonment, suspended for 24 months and an 18 month supervision requirement. This shows that cases can take a considerable time to get to court, making feedback a challenge.

In addition, the CIT receive numerous requests for statements every month from police for use in court on data previously released.

Appendix 2

Transport for London

Guiding definitions and working principles on the disclosure of personal data to the Police and other Statutory Law Enforcement Agencies

Effective from October 2011

Policy on disclosure

It is TfL's policy to disclose Personal Data it holds to the police and other SLEAs, primarily to address policing, national security and law enforcement issues providing that disclosure complies with the relevant law and that such disclosures are both necessary and proportionate.

The Data Protection and Disclosures Team (DPDT) within the Community Safety, Enforcement and Policing directorate (CSEP) of Transport for London are one of the main areas of the organisation who are responsible for the disclosure of data to the Police and other Statutory Law Enforcement Agencies.

TfL data may be released to third parties, subject to meeting certain conditions under the Data Protection Act (DPA) for purposes such as;

- The prevention, investigation and / or detection of crime;
- The apprehension and / or prosecution of offenders;
- Public and employee safety

This guidance note has been prepared to provide guidance on how data requests will be categorised. It is subordinate to the TfL Policy on the disclosure of personal data to the police and other Statutory Law Enforcement Agencies.

Working practice

In support of the TfL policy on disclosure a uniform and structured approach has been introduced to provide the DPDT and police with clarity on the type of data requests that will be considered.

All requests are dealt with on a case by case basis and will be categorised into one of these tiers when they are received. This will determine if and how they are dealt with.

Tier 1: *All requests for information for the prevention and detection of crime and the apprehension of offenders for* ***crimes committed on / connected to TfL services and facilities.***
Note: These can be all crime types from dip thefts to serious crimes of assault and murder. Information will only be disclosed if the request meets DPA requirements.

Tier 2: *All requests for information for the prevention and detection of crime and the apprehension of offenders for **serious crimes committed off / un-connected to TfL services and facilities***

Note: As these requests are for the disclosure of data relating to incident off the TfL services or facilities, they will be considered on a case by case basis. Requests may be considered for serious crimes **only** and subject to the request meeting the requirements of DPA.

Requests which are likely to be considered under Tier 2 include, but are not limited to: National Security, Murder, Serious Sexual Offences, Robbery, All Weapons Offences, Threat to Life, Unexplained Death and High Risk Missing Person

Tier 3: *All requests for information where either:*

(a) no crime has actually been committed or there are no substantial grounds to suggest that it is likely that a crime will be committed;

*(b) in relation to **crimes committed off / un-connected to TfL services and facilities that are not considered as 'serious', as those defined under Tier 2.***

Note: Requests will **not be** processed that fall within tier 3.

Contact

For further information please contact:

Keith Waghorn
Crime and ASB Investigation Manager

Transport for London
Community Safety, Enforcement and Policing Directorate
9th Floor, Palestra
London SE1 8NJ

Phone: 0203 054 3191
Mobile: 07747 767256
email: keith.waghorn@tfl.gov.uk

Notes:

- *If a data request relates to a deceased person, the DPA does not apply and so there are no legal parameters around the amount of data you can release. However, the information supplied must be proportionate in relation to the data requirements, i.e. to identify the person for the purpose of informing relatives or for identification for the police or be in the public interest.*
- *TfL Services are defined as services overseen by TfL such as Bus, Tube, Overground rail, Tram, DLR, Cycle Hire Scheme, Congestion Charging Services.*
- *TfL Facilities are defined as Bus Stops, Shelters or Stations, London Underground / LOROL / Tram / DLR Stations or Ticket Offices and Piers.*