Audit and Assurance Committee

Date: **8 December 2015**

Item: **Cyber Security Update**

This paper will be considered in public

1 Summary

1.1 This paper provides an update to the report on cyber security presented to the meeting of 16 June 2015.

1.2 A paper is included on Part 2 of the agenda which contains exempt supplemental information and documentation. Subject to the decision of the Committee, this paper is exempt and is therefore not for publication to the public or press by virtue of paragraph 7 of Schedule 12A of the Local Government Act 1972 in that it contains information relating to action which might be taken in relation to prevention, investigation or prosecution of a crime.

2 Recommendation

2.1 **That the Committee is asked to note the paper and the related supplemental information on Part 2 of the agenda.**

3 Background

3.1 TfL makes extensive use of information technologies and automated computer systems. These systems hold personal data, control train movement, deliver power to the network, support time-tabling and operational planning processes, schedule maintenance work, manage and pay our suppliers and our people and allow us to communicate effectively. Every part of every business activity at TfL relies in some way on computerised systems and information technologies.

3.2 The cyber security capability within TfL has continued to mature since the last paper.

(a) **Cyber Security Monitoring and Incident response** – We scrutinise network performance for indicators of potential points of compromise. We continue to build our team of cyber security analysts to maintain awareness of the status of our network, respond to incidents and carry out investigations.

(b) **Cyber Security Threat Analysis** – In coordination with government authorities, we monitor local, national and international cyber security threats, and translate information received into actionable intelligence relevant to TfL's operations.

(c) **Cyber Security Policy Development** – We actively take into account regulatory and technical developments in cyber security. The policy will be aligned with the Centre for the Protection of National Infrastructure's (CPNI)

10 Steps to Cyber Security[1]. This policy team also oversees the TfL Cyber Security Awareness programme for employees – Protect Our Brand, Protect Your Brand.

(d) **Cyber Security Compliance** – Policy deployment is only as effective as the implementation of the policy. The compliance effort focuses on the technical implementation of cyber security policy.

(e) **Cyber Security Project Support** – This effort supports programme managers across TfL to ensure cyber security requirements are considered and applied in project development.

3.3 **Next Steps** – Continue to mature cyber security competency at TfL and a further update will be provided to a future meeting.

List of appendices to this paper:

Exempt supplemental information is included in a paper on Part 2 of the agenda.

List of Background Papers:

CPNI 10 Steps to Cyber Security

TfL Cyber Security Awareness programme for employees – Protect Our Brand, Protect Your Brand.

Contact Officer: Steve Townsend, Chief Information Officer
Number: 020 3054 4130
Email: SteveTownsend@tfl.gov.uk

[1] CPNI, GCHQ, BIS and Cabinet Office have published an updated '10 Steps to Cyber Security' showing businesses the practical steps they can take to improve the security of their networks and the information carried on them.