Audit and Assurance Committee

Date: **8 March 2016**

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 8 December 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 Subject to the decision of the Committee, this paper is exempt and is therefore not for publication to the public or press by virtue of paragraph 7 of Schedule 12A of the Local Government Act 1972 in that it contains information relating to action which might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 provided on Part 2 of the agenda.**

3 Background

3.1 We make extensive use of information technologies and automated computer systems. We completed a risk assessment of our cyber security in 2015 and this is an update to our actions.

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

(a) **Cyber Security Risk Management** – We have identified cyber security as a risk on the pan TfL risk register. We have developed proportionate controls against cyber risk and are working with relevant stakeholders to implement.

(b) **Cyber Security Policy Development** – We actively take into account government direction and technical developments in cyber security. Our cyber security policies will be aligned with the Centre for the Protection of National Infrastructure's (CPNI) 10 Steps to Cyber Security.

(c) **Cyber Security Procurement Instructions -** We have developed procurement language that supports cyber security principles throughout the lifecycle of the contracting process.

(d) **Cyber Security Awareness –** We have developed a cyber security awareness work stream with the objective to raise cyber security attentiveness across TfL.

(e) **Next Steps** – Continue to mature cyber security competency at TfL. A further update will be provided at 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 0020
Email: SteveTownsend@tfl.gov.uk

Contact Officer: Michele Hanson, Chief Information Security Officer
Number: 020 3054 0020
Email: MicheleHanson@tfl.gov.uk