Audit and Assurance Committee

Date: **11 October 2016**

Item: **Cyber Security Update**

This paper will be considered in public

1 Summary

1.1 This paper provides a status update to our cyber security programme.

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 Subject to the decision of the Committee, this paper is exempt and is therefore not for publication to the public or press by virtue of paragraph 7 of Schedule 12A of the Local Government Act 1972 in that it contains information relating to action which might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. To protect our systems from the cyber security threat we have established a central cyber security team and a central set of policies and controls.

3.2 Our focus on cyber security includes:

(a) **Cyber Security Risk Management** – We have identified cyber security as a risk on the strategic TfL risk register. We have developed 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 and technical controls are 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 Incident Response** – We operate a cyber security incident response capability 24 hours a day and 7 days a week.

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

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:

None

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