Audit and Assurance Committee

Date: **16 June 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 Committee at its meeting of 8 October 2014. The purpose of this paper is note the results of the TfL gap analysis, and the establishment of a single TfL Cyber Security team.

1.2 A paper is included on Part 2 of the agenda which contains exempt supplemental information and documentation.

2 Recommendation

2.1 **The Committee is asked to note the paper.**

3 Background

3.1 This is an update to the discussion held at Committee meeting of 8 October 2014 regarding cyber security at TfL.

3.2 TfL makes great use of information technologies and automated computer systems. These systems control train movement, deliver power to the network, support time-tabling and operational planning processes, schedule work activities across our maintenance teams, manage and pay our suppliers and our people and allow them to communicate effectively. Every part of every business activity at TfL relies in some way on computerised systems and information technologies. Technology is critical to TfL operations. It is vital that we understand our vulnerabilities, prioritise our risks and begin the mitigation path.

3.3 In response to these pressures, IM established an Information Security Controls Framework (ISCF). The ISCF is a set of defined cyber security controls aligned with the SANS 20, reviewed by CPNI and Gartner.

4 Scope

4.1 Cyber security is an increasingly significant challenge. Government cyber guidance applies to transport sectors in the Critical National Infrastructure (CNI), of which TfL is part of, and is increasing in volume; Cabinet Office – Office of Cyber Security and Information Assurance, Information Commissioners Office (ICO), Regulators – DfT Land Transport Cyber Security (Rail) 2015, Centre for the Protection of National Infrastructure (CPNI) and Communications Electronics Security Group (CESG) and CERT UK.

4.2 In order to assess the appropriateness of TfL arrangements for cyber security the following actions were taken:

(a) an information security controls framework (ISCF) was created to assess maturity;

(b) the processes in IM were assessed against the ISCF;

(c) processes were scored against the Active Risk Manager (ARM);

(d) the ISCF considered the SANS 20[1] controls; and

(e) carried out a gap analysis of the ISCF with regard to processes across TfL.

5 Management of Cyber Security and Information Assurance issues

5.1 TfL's risks in the area of cyber security and information assurance are aligned with guidance from the government and the management of these risks is a strategic level risk.

5.2 The ISCF maps to the controls in HMG Security Policy Framework (SPF), SANS 20, as well as unique TfL requirements. The SPF published by HMG in 2009, and last updated in 2013, requires a "holistic" approach to security policy management.

5.3 The HMG SPF applies to Critical National Infrastructure (CNI) transport assets as identified by government. The SANS 20 has been endorsed by the Centre for the Protection of the National Infrastructure (CPNI) and the Communication Electronics Security Group (CESG).

5.4 The Information Security Controls Framework contains 29 controls. The ISCF has been reviewed by Gartner and CPNI. (Gartner is a recognised global leader in IT research, advising in cyber security). The gap analysis for addressing cyber security risks was completed against the IM risks only. The cyber security proposal will be expanded to include all disciplines in TfL upon completion of the gap analysis across the additional TfL disciplines. The gap analysis will:

(a) utilise the information security controls framework (ISCF) to ensure a repeatable, testable and traceable analysis;

(b) be the basis for the on-going cyber security proposal to define TfL risk, identify remediation steps, governance and financial investment.

6 Summary

6.1 The cyber security and information assurance analysis across TfL has been reviewed. An action plan has been created and the Audit and Assurance Committee will be updated on progress with the actions at the meeting on 8 October 2015.

List of appendices to this paper:

A paper on Part 2 of the agenda contains exempt supplemental information.

List of Background Papers:

None

Contact Officer: Steve Townsend, Chief Information Officer
Number: 020 30544130
Email: stevetownsend@tfl.gov.uk

[1] SANS 20 refers to the Critical Security Controls for cyber defence, a baseline of high-priority information security measures and controls that can be applied across an organisation in order to improve its cyber defence.