Safety and Security Panel

Date: **12 February 2025**

Item: **Enterprise Risk Update – Significant Security Incident including Cyber Security (ER04)**

This paper will be considered in public

1 Summary

1.1 This paper provides an update of Enterprise Risk 04 (ER04) – the risk of a significant security incident (including cyber security) and seeks feedback on whether it is accurately defined within the current threat environment and the preventative and corrective controls and actions in place to reduce this risk.

1.2 The risk is described as failure to prevent, identify, prepare for, respond to, and minimise impact of a significant security incident which could have major and adverse effect on us and our suppliers' operations, finances, people, customers, reputation, data and assets.

1.3 A paper is included on Part 2 of the agenda which contains supplementary information that is exempt from publication by virtue of paragraphs 3 and 7 of Schedule 12A of the Local Government Act 1972 in that it contains information relating to the financial and business affairs of TfL and information relating to any action taken or to be taken in connection with the prevention, investigation or prosecution of crime. Any discussion of that exempt information must take place after the press and public have been excluded from this meeting.

2 Recommendation

2.1 **The Panel is asked to note the paper and the exempt supplementary information on Part 2 of the agenda.**

3 Current Status

3.1 We are an operator and owner of critical national infrastructure and play a key role in the safety and security of London. We recognise that the threat from intentional criminal acts to harm Transport for London (TfL) and London is constant, evolving and increasingly significant in an unstable world. The insight from our colleagues in the Police and Security Services is that cyber crime, organised crime, sabotage, extortion, extreme violence, disorder and espionage, terrorism and the hostile actions of nation states are becoming increasingly indistinguishable. Because of the fluid and dynamic nature of the threats that we and London face, we adopt a holistic and risk-based approach to assessing and improving security. Our aim is to protect our organisation, our data and finances, our customers, our assets and our workforce from hostile and deliberate criminal actions that seek to cause harm.

3.2 We identify existing and emerging security risks and seek to reduce our vulnerability to all forms of terrorism and ideologically motivated violent crime, nation state hostile acts, extortion (through cyber-attacks), organised financial crime such as fraud and blackmail, bribery and corruption, espionage, sabotage, activism and industrial scale theft. Our systematic approach to protective security contributes to our sustainability and that of London.

3.3 Since the last update to the Audit and Assurance Committee in November 2023 we have continued to develop ER04 through a series of workshops with our internal security specialists, business lead owners and external experts' briefings on the current threat landscape. From February 2025, we will provide annual updates to the Safety and Security Panel.

3.4 ER04 has been developed to take a holistic approach to the security threats we face. ER04 defines a significant security incident as the impact on our operations, assets, customers, people, finances and reputation caused from an incident of terrorism, extortion, sabotage, espionage, activism or serious fraud and financial crime.

3.5 The scale and nature of the impact is a combination of a failure to sufficiently identify and understand the threats we face, or to recognise our vulnerabilities and seek to protect them, to deter, detect, deny, delay and defend against such criminal activity. At Level 0, the causes fall within five broad categories: terrorism, sabotage, espionage, serious financial crime (including extortion) and activism.

3.6 The key sources we draw on to understand our risk include the current national terrorism threat level, UK and London national risk register, and insight from the Police, Security Services, National Protective Security Authority and the National Cyber Security Centre.

3.7 We have in place several preventative and corrective controls and actions that we regularly review, refine and monitor progress against. We currently have 17 Security Improvement Programmes (see Appendix 1) underway across our organisation to reduce our vulnerability and better protect our customers, colleagues and organisation from criminal, malicious and hostile actions.

3.8 In September 2024, we experienced a high-impact cyber incident. We responded rapidly and a detailed investigation is ongoing, in coordination with the National Crime Agency, National Cyber Security Centre and expert partners. We have identified that some personal data was accessed and have reported that to the Information Commissioner's Office. We contacted customers at risk to offer support. An independent review is underway overseen by the Chair of the Audit and Assurance Committee and the Chair and Vice Chair of the Panel on behalf of the Board. We will address the learnings, recommendations and improvements identified from the reports of our incident response partners, as well as the independent review of the incident as appropriate, and adjust our mitigations accordingly.

3.9 Our corporate Security Governance programme has brought about greater oversight of our security risk management. Regular reporting has been established on security matters to the Executive Security Group which brings

together representatives from all business areas to enable proportionate and effective decision making.

3.10 We stay ahead of changes in legislation and regulation to strengthen our defences and to be well prepared for compliance. In the pipeline for 2025 with security implications are the updates to the Light Rail Security Programme regulations; the introduction of Martyn's Law (Terrorism Protection of Premises Bill); updates to the Network and Information Systems Regulations 2018; the Cyber Security and Resilience Bill; updates to Economic Crime and Corporate Transparency Act 2023; and the Procurement Act 2023.

3.11 We recognise that everyone at TfL has a role to play in security and we have a proactive plan to increase awareness, understanding and competence through clear and active people leadership, policy, training, briefings and communications.

3.12 ER04 provides oversight of the risk, causes, consequences and controls in place to manage it. Detail of this work is presented in the paper on Part 2 of the agenda.

List of appendices to this report:

Appendix 1: Security Improvement Programmes 2024/25

A paper containing exempt supplemental information is included on Part 2 of the agenda

List of Background Papers:

None

Contact Officer: Siwan Hayward OBE, Director of Security, Policing and Enforcement
Email: Siwan.Hayward@tfl.gov.uk

Appendix 1 – Security Improvement Programmes 2024/25

Theme	Programme	Purpose
Work together to be safe and secure	Command and Control (Resilience and Events)	Align and develop resilience activity across TfL business areas; increase our testing and exercising regime for key risk areas
	London Underground Security Programme	Create and update guidance/standards/rule book entries to provide governance to ensure compliance with government regulations
	Head Office Buildings Security	Protect head office occupants from harm and disruption
	TfL Security Risk Management – Local Security Action Plans	Identification of security vulnerabilities across all unregulated TfL areas with specialists providing recommendations for mitigation
	Bus Security Programme	Deliver the Bus Security Programme to ensure mitigation of security and crime risks
	Piers Security Programme	Improve existing pier security arrangements
Keep everyone safe when travelling	Workplace Violence and Aggression strategy	Eliminate work related violence and aggression by preventing incidents and supporting those that experience it
	Ending Violence Against Women Girls Programme	Support victims and improve safety for women and girls in public spaces
	Policing partnerships and joint crime prevention activity	Review of funded policing arrangements to reduce crime, deliver improved security outcomes and better value for money

Appendix 1 – Security Improvement Programmes 2024/25 (continued)

Theme	Programme	Purpose
Protect our Organisation	Cyber Security Improvement Programme	To improve TfL's cyber security maturity and embed a three lines of defence model
	Sensitive Information	Improvement in TfL's ability to control access to and distribution of sensitive information held in M365.
	Revenue Protection	Optimising the Revenue Operating Model to support Revenue Protection and tackle ticket fraud and reduce workplace violence and aggression linked to fare evasion. Reducing the level of fare evasion taking place across TfL network
	Counter Fraud and Corruption	To prevent and deter fraud and corruption, detect offenders, and pursue disciplinary action / criminal prosecution. To continue to make TfL a hostile environment for fraudsters.
	Infrastructure Security Working Group	Pan-TfL working group establishing consistency of approach towards the physical security of our infrastructure
	Visual Surveillance Systems	A single approach for renewals, maintenance and trials of new technology considering all operational and security related uses of CCTV
	Security Culture, Comms and Engagement	Build a culture of how we all behave and respond in a security conscious way and where customers have confidence to travel
	Security Governance	Embed security governance into the TfL value chain