British Transport Police Authority

The Forum
5th Floor North
74-80 Camden Street
London NW1 0EG

T: 020 7383 0259
F: 020 7383 2655

www.btpa.police.uk

Report to: Audit Committee

Agenda item: 8

Date: 4 March 2014

Subject: Security Policy Framework (SPF) Compliance – Authority Annual Assessment

Sponsor: Authority Chief Executive

For: Decision

1. Purpose of Paper

1.1 This paper presents the draft 2013/14 Annual Assessment relating to Compliance with HM Government's Security Policy Framework ahead of its submission to the Department for Transport (DfT) on 28 March 2014. The proposed submission is attached as Appendix A. The submission from the BTP will be considered by the Audit & Risk Committee at its meeting in May, since these follow a different process.

2. Background

2.1 The UK Government processes huge volumes of sensitive information (and personal data to matters of national security) and manages assets and services that are critical to public safety and the UK's way of life. It must guard against a range of threats including negligent behaviours, criminality, terrorism and espionage, as well as natural hazards such as flooding. The Government's risk management process is set out in the **Security Policy Framework (SPF),** a document which describes the standards, best practice guidelines and approaches that are required to protect Government assets (people, information and infrastructure). It focuses on the outcomes that are required to achieve a proportionate and risk-managed approach to security that enables government business to function effectively, safely and securely.

2.2 Government departments and agencies are responsible for carrying out internal reviews (at least annually) of protective security and the management of information risks across their organisation, including any delivery partners and / or suppliers with whom they exchange information to deliver services on their behalf. Departments and agencies are required to submit an **Annual Assessment Report** to the Cabinet Office – via the Department for Transport (Dft), the Authority's sponsor – indicating any key areas of concern or non-compliance with the SPF.

2.3 The SPF describes the security controls to be applied to UK Government assets. These are set out in the so-called SPF **'Mandatory Requirements'**, of which there are 20. The areas covered in these mandatory requirements are broad, and range from staff vetting, to handling of information assets, to physical security measures.

2.4 To support the mandatory requirements of the SPF, the National Technical Authority for Information Assurance publishes the **Information Assurance Standard No. 6** (known as 'IA6'), a document which sets out a range of minimum measures to protect personal data and manage information risk which must be implemented by the Departments and Agencies. Compliance with SPF cannot be claimed unless adherence to the Standards can be demonstrated.

2.5 Changes are expected to the reporting process in the future, as the DfT is seeking to roll out a web-based solution to capture information from its agencies. Whilst there were initial indications this would be introduced for the Authority in 2014, a decision has been taken to delay this until next year.

3. Summary of BTPA's Submission

3.1 The submission to the DfT needs to be signed by the Authority's Chief Executive, who fulfils the role of Senior Information Risk Owner

(SIRO). As a SIRO, he is required to be familiar with information risks and their mitigations, including information risk assessment methodology.

3.2 The Audit and Risk Committee is now asked to review the draft submission to take account of the expectation (engrained in the SPF) that an element of independent challenge should be applied in whole or in part to the reporting process.

SPF Compliance 2013/14

3.3 Summary of progress in relation to areas for development identified in 2012/13:-

3.2.1 **Assurance that delivery partners handle personal data in compliance with Information Assurance Standard No. 6 (MR11)** – A request to our pensions management (RPMI) and payroll software (Midland HR) contractors has been made to seek assurance of compliance against IAS6. This is yet to be received, at the time of writing and is expected before the 28 March deadline.

3.2.2 **Advanced Training (MR3)** – The Authority's and the Force's SIROs completed advanced training in mid-2013. Refresher training will be identified for Information Asset Owners (IAOs), to take account of new Government Security Classification Policy (GSC).

3.2.3 **Internal Assurance procedures (MR3)** – Information Management is now a standing item at Authority SMT meetings. Assurance and Reporting processes being reviewed to coincide with launch of new reporting system implemented by DfT (date not yet confirmed by DfT. It is now anticipated that this will be rolled out in 2015).

3.2.4 **Assessing the requirement for additional protective security measures when the Government Response level rises (MR19 and MR20)** – A discussion has taken place with BTP. The

Authority will follow guidance that is issued by Special Branch to understand the implications which a potential increase in the threat level would have on Information Security. Given the diverse circumstances which may trigger a variation in the threat level, it may not always be possible to pre-determine the specific measures which would have to be put in place to respond to such events.

3.3 Also attached to this report are the updated **Information Asset Register** (which forms part of the submission) and the latest **Information Management Risk Register**, which is submitted to the Audit & Risk Committee for information.

4 Recommendation

It is recommended that the Audit & Risk Committee:-

4.1 Note the content of the draft SPF Compliance - 2013/14 Annual Assessment Report for the British Transport Police Authority; and

4.2 Authorise the Chief Executive to submit the finalised report to the DfT.