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:	11
Date:	3 March 2016
Subject:	Information Security – Departmental 'Health Check' for the BTPA
Sponsor:	Chief Executive
For:	Decision

1. Purpose of Paper

1.1 This paper presents the draft 2015/16 'Health Check' relating to Compliance with HM Government's Security Policy Framework ahead of its submission to the Department for Transport (DfT) on 30 April 2016. The proposed submission is attached as Appendix A. The submission from the BTP will be separately considered by the Audit & Risk Committee later in the year, since theirs follows 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 and best practice 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 report on compliance to the Cabinet Office. Changes to the form of reporting have been introduced, and the new Departmental Security Health Check (DSHC) has replaced the Security Risk Management Overview (SRMO) of previous years. The BTPA has been asked to submit the Health Check 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. A summary of SPF Mandatory Requirements can be found at the end of this report.

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.

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 This year, the DfT have placed an additional requirement for the document to be counter-signed by a Chief Information Security Officer. This is a change from previous years, and the responsibilities of this role has never been defined. The BTPA has discussed this issue with the DfT as there is no indication that this area of work might need to be resourced differently in the

future. The BTPA has provided explanation of this position it its answer to Question 4(a).

3.3 The Audit and Risk Committee is now asked to review the draft Health Check 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

3.4 Summary of progress in relation to areas for development identified in 2013/14:-

3.2.1 Assurance that delivery partners handle personal data in compliance with Information Assurance Standard No. 6 (MR11) – Two third parties have been identified as being delivery partners for the purposes of Information Management: our pensions managers (RPMI) and the payroll software (Midland HR). In 2014/15, the BTPA sought assurance of their compliance against IAS6 and this was received in time for the submission deadline in March 2015. This year, suppliers have been asked to fill a questionnaire, and this is expected to be completed before the 30 April 2016 deadline.

3.2.2 Police Service Network (PNN Replacement) – The migration to a new Police Security Network was identified a key risk in previous years as the national project overseeing the migration was facing a challenging deadline. The BTP have confirmed that implementation of PSN in currently in progress.

3.2.3 New Government Security Classifications Policy (GSC) – Initially tipped to be introduced alongside PSN in October 2014, the adoption of the new Security Classifications system by the Police Service has been deferred on a number of occasions. It is understood that the National Police Chiefs' Council have decoded to adopt the new System with effect from 1 April 2016. The BTPA – alongside the BTP – will need to ensure all staff are familiarised with new classifications system.

Looking ahead

3.5 Summary of issues identified in the Health Check, and which the Audit & Risk Committee is asked to note are as follows:-

3.2.1 Physical Security / Responding to Security Incidents (MR16 – MR20) & Personnel Security (MR13 – MR15) **-** Following the confirmation BTPA will remain in the offices at the Forum (November 2015), the BTPA is carrying a review of arrangements concerning physical security as well as access to information by temporary and permanent members of staff (particularly looking at permissions to access files on the G:\ Drive).

3.2.2 Review of Policies (MR10) – An outstanding action concerns the review of all IM policy documents at the Authority, and this will be conducted once the Police Service moves to a new Security Classification system. The National Police Chiefs' Council confirmed at its meeting in January 2016 the adoption of the new security markings on 1 April 2016.

4 Recommendation

It is recommended that the Audit & Risk Committee:-

4.1 Note the content of the draft Departmental Health Check 2014/15 for the British Transport Police Authority; and

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

Summary of SPF Mandatory Requirements

The twenty measures below are from tier three of the Cabinet Office Security Policy Framework (SPF). For more detail on the requirements that fall under each MR please refer to the SPF. Your assurance in Section E should cover all requirements under each measure.

MR no.	**Security Policy 1. Governance and security approaches**
MR1	Departments and Agencies must establish an appropriate security organisation (suitably staffed and trained) with clear lines of responsibility and accountability at all levels of the organisation. This must include a Board-level lead with authority to influence investment decisions and agree the organisation's overall approach to security.
MR2	Departments and Agencies must: * Adopt a holistic risk management approach covering all areas of protective security across their organisation. * Develop their own security policies, tailoring the standards and guidelines set out in this framework to the particular business needs, threat profile and risk appetite of their organisation and its delivery partners.
MR3	Departments and Agencies must ensure that all staff are aware of Departmental security policies and understand their personal responsibilities for safeguarding assets and the potential consequences of breaching security rules.
MR4	Departments and Agencies must have robust and well tested policies, procedures and management arrangements in place to respond to, investigate and recover from security incidents or other disruptions to core business.
MR5	Departments and Agencies must have an effective system of assurance in place to satisfy their Accounting Officer / Head of Department and Management Board that the organisation's security arrangements are fit for purpose, that information risks are appropriately managed, and that any significant control weaknesses are explicitly acknowledged and regularly reviewed.
	Security Policy 2. Security of Information
MR6	Departments and Agencies must have an information security policy setting out how they and any delivery partners and suppliers will protect any information assets they hold, store or process (including electronic and paper formats and online services) to prevent unauthorised access, disclosure or loss. The policies and procedures must be regularly reviewed to ensure currency.
MR7	Departments and Agencies must ensure that information assets are valued, handled, shared and protected in line with the standards and procedures set out in the Government Protective Marking System (including any special handling arrangements) and the associated technical guidance supporting this framework.

MR8	All ICT systems that handle, store and process protectively marked information or business critical data, or that are interconnected to cross-government networks or services (e.g. the Public Services Network, PSN), must undergo a formal risk assessment to identify and understand relevant technical risks; and must undergo a proportionate accreditation process to ensure that the risks to the confidentiality, integrity and availability of the data, system and/or service are properly managed.
MR9	Departments and Agencies must put in place an appropriate range of technical controls for all ICT systems, proportionate to the value, importance and sensitivity of the information held and the requirements of any interconnected systems.
MR10	Departments and Agencies must implement appropriate procedural controls for all ICT (or paper-based) systems or services to prevent unauthorised access and modification, or misuse by authorised users.
MR11	Departments and Agencies must ensure that the security arrangements among their wider family of delivery partners and third party suppliers are appropriate to the information concerned and the level of risk to the parent organisation. This must include appropriate governance and management arrangements to manage risk, monitor compliance and respond effectively to any incidents. Any site where third party suppliers manage assets at SECRET or above must be accredited to List X standards.
MR12	Departments and Agencies must have clear policies and processes for reporting, managing and resolving Information Security Breaches and ICT security incidents.
	Security Policy 3. Personnel Security
MR13	Departments must ensure that personnel security risks are effectively managed by applying rigorous recruitment controls, and a proportionate and robust personnel security regime that determines what other checks (e.g. national security vetting) and ongoing personnel security controls should be applied.
MR14	Departments and Agencies must have in place an appropriate level of ongoing personnel security management, including formal reviews of national security vetting clearances, and arrangements for vetted staff to report changes in circumstances that might be relevant to their suitability to hold a security clearance.
MR15	Departments must make provision for an internal appeals process for existing employees wishing to challenge National Security Vetting decisions and inform Cabinet Office Government Security Secretariat should an individual initiate a legal challenge against a National Security Vetting decision.
	Security Policy 4. Physical security and counter- terrorism
MR16	Departments and Agencies must undertake regular security risk assessments for all sites in their estate and put in place appropriate physical security controls to prevent, detect and respond to security incidents.

MR17	Departments and Agencies must implement appropriate internal security controls to ensure that critical, sensitive or protectively marked assets are protected against both surreptitious and forced attack, and are only available to those with a genuine ‘need to know’. Physical security measures must be proportionate to level of threat, integrated with other protective security controls, and applied on the basis of the ‘defence in depth’ principle.
MR18	Departments and Agencies must put in place appropriate physical security controls to prevent unauthorised access to their estate, reduce the vulnerability of establishments to terrorism or other physical attacks, and facilitate a quick and effective response to security incidents. Selected controls must be proportionate to the level of threat, appropriate to the needs of the business and based on the ‘defence in depth’ principle.
MR19	Departments and Agencies must ensure that all establishments in their estate put in place effective and well tested arrangements to respond to physical security incidents, including appropriate contingency plans and the ability to immediately implement additional security controls following a rise in the Government Response Level.
MR20	Departments and Agencies must be resilient in the face of physical security incidents, including terrorist attacks, applying identified security measures, and implementing incident management contingency arrangements and plans with immediate effect following a change to the Government Response Level.