APPENDIX 1 – DETAILED UPDATE ON ALL OUTSTANDING HIGH RISK AUDIT RECOMMENDATIONS
(as at 13 November 2009, for inclusion in December CGC paper)

Ref No.	**Systems for Intelligence and Detection** **- SCD Lead** *(SCD lead with DoI activity required to implement this recommendation)*	Update on 1 outstanding High Risk recommendation raised November 2007	Target date for completion
1	Data held within the Crimint+ system is not encrypted as transmitted over AWARE. This risk is fully documented within the Crimint+ Risk Management Accreditation Document Set (RMADS) and will be kept under regular review as it is accepted as a corporate risk. Recommended that: • *data encryption is considered in line with speed of data retrieval and storage.* • *the benefits of encryption should be reviewed against costs of acquiring and maintaining encryption*	Following a report presented to MPA Corporate Governance Committee in June 2009, it was agreed that the most appropriate action to address this recommendation was for DoI to undertake another IT Health-check Assessment of the CRIMINT+ system. The outcome of that Health-check, due to be completed by the end of October 2009, will be reviewed with MPA Directorate of Audit, Risk and Assurance and in the event of the risk remaining at an unacceptable level a bid for capital funding will be pursued. Update: A progress report has been submitted by DoI to the Directorate of Audit, Risk and Assurance. It details the actions DoI have put in place to mitigate risks identified in the audit report and confirms that an IT Security health check will be conducted early 2010. DARA are reviewing the report and will conduct a short review to verify that action is sufficient to address the recommendations.	Revised to February 2010

Ref No.	**Palace of Westminster** **- SO Lead** *(SO lead with HR consultation required to implement this recommendation)*	Update on the 1 outstanding High Risk recommendation raised January 2008	Target date for completion
2	*The recommendations and updates are now reported in Appendix 2, which is exempt.*		

Ref No.	**Systems supporting financial reporting follow up** **- DoI Lead**	**Update on the 1 remaining High Risk recommendation raised July 2008** **Now implemented**	**Target date for completion**
3	MetFin - Restricting access to data/programs. The DoI need to protect access to the operating system through standard System Application Products (SAP) programs, which allow users to access the operating system command line. This enables certain users to perform operating system commands from within SAP (a recognised software package for finance and procurement systems). Recommended that: • *Access to these utilities should be restricted to appropriate users in the production environment. Operating system access should be administered via the operating system itself and not from within SAP.*	Operating system access has been removed from all end user roles. Access has been restricted to only the SAP System Administrator role.	Now Complete

APPENDIX 1 – DETAILED UPDATE ON ALL OUTSTANDING HIGH RISK AUDIT RECOMMENDATIONS
(as at 13 November 2009, for inclusion in December CGC paper)

Ref No.	**Crime related property - TP Lead** *(TP lead with HR (Logistical Services) activity required to implement this recommendation)*	Update on the 1 remaining outstanding High Risk recommendations raised August 2008	Target date for completion
4	Strategic framework & culture Recommended that: *The current processes, guidelines and instructions for the management of crime property are consolidated into a strategic policy that is approved by Management Board and that:* • *Includes a performance management framework at corporate and operational level.* • *Identifies and documents the specific arrangements required for central departments and the overlap between BOCUs and central departments.* • *Documents cash handling requirements* • *Includes monitoring arrangements to ensure compliance with policies and procedures.* • *Clarifies roles and responsibilities for processing and managing property, inc. the roles of operational officers, property staff, the Crime Property Manager and SMT Lead.* • *Is supported by documented and approved corporate and local procedures*	Central Property Services have taken the corporate lead in partnership with other stakeholders. However, in order for this to succeed, the responsibility for monitoring and compliance must lie with the individual operational units. Central Property Services, via a consultation process and working closely with TP, will be revising policy and updating SOPs within the MPS Property Manual. Additional chapters around governance, compliance and audit processes will be developed to link in with the Directorate of Audit, Risk and Assurance recommendations. A team within Operation Emerald is working in partnership with Central Property Services to address the issues identified. Following consultation with the TP Finance Modernisation Team and the Payback Team, an exercise to deal with the cash handling issue commenced at the end of November 2008. The results were collated and analysed and informed the future policy on cash handling. Cash handling guidelines were issued to TP BOCUs on 5 August 09 by the TP - METAFOR Team. Work is now ongoing with other Business Groups to develop guidelines appropriate to them. Central Property Services are in the process of compiling a risk register that is expected to be completed by the target date. Central Property Services managers continue to undertake regular documented audit checks. [This recommendation has links to the high risk recommendation re crime property made in the corporate B/OCU audit conducted earlier this year. The Directorate of Resources is leading on that particular recommendation and the Quality Assurance Team in Finance Services is ensuring all relevant parties are connected - see ref no. 12 in this appendix].	December 2009

Ref No.	**Health and Safety legislation implementation - HR Lead**	Update on the 1 remaining outstanding High Risk recommendations raised January 2009	Target date for completion
5	At present the MPS Accident reporting system MetAIR does not provide the MPS with the means to provide data, which can assist in decision making at a corporate and local level. The need for a fit for purpose accident monitoring and reporting system is increased by the introduction of the MPA/MPS annual assurance process for health and safety. Recommended that: • *A review is carried out of the information requirements for the accident report system and that the MetAIR system is either upgraded or replaced.*	The existing MetAIR system will be replaced as part of the Transforming HR Project. The replacement MetAIR system under the THR project is integral to the THR IT solution. Therefore the delay in THR go live will directly affect the delivery of the MetAIR replacement. There is no scope to bring forward the use of the new MetAIR system prior to the revised THR go live; a date for which has yet to be formally determined.	Date to be determined

APPENDIX 1 – DETAILED UPDATE ON ALL OUTSTANDING HIGH RISK AUDIT RECOMMENDATIONS
(as at 13 November 2009, for inclusion in December CGC paper)

Ref No.	**Diplomatic Protection Group - SO Lead**	Update on the 1 outstanding High Risk recommendation raised February 2009, now implemented from MPS perspective	Target date for completion
6	The Home Office is reviewing the Dedicated Security Post (DSP) funding arrangements aiming to change them for the 2009/10 bidding process and the MPA Treasurer is involved in the process. Recommended that : - *The MPA Treasurer continues to monitor progress on DSP under funding and reports the latest position to the MPA Counter-Terrorism and Protection Services Sub-Committee*	MPA Members (as appropriate) and the Home Office up to ministerial level are aware of the situation and are continuing to consider the under funding of DSP and the risks to which the MPS is exposed. A report will be submitted to the September 2009 Counter-Terrorism and Protective Services Sub-Committee to update progress to date. The MPA Treasurer will continue to monitor progress with all appropriate bodies and report as appropriate. A response from the Home Secretary was received on 26 June 2009, and following internal MPS discussions ACSO and the MPA Chief Executive met with Home Office officials on 18 August 2009. It was agreed at the meeting that: - Home Office will write to MPS/MPA regarding proposals for reform of RAVEC (Royal and VIP Executive Committee) - Home Office OSCT (Office for Security and Counter Terrorism) has prioritised funding the current year DSP inflation shortfall out of anticipated under spends in other budgets, however not confident of covering inflation in 2010/11 in current financial climate - Home Office view is that DSP Grant is a contribution to costs but it will look at setting a 'floor' to the level of contribution. - Home Office to await the review by National Co-ordinator Ports Policing (John Donlan) into DSP posts allocated to Ports before considering what to do with any identified savings. A further response has recently (early November) been received from the Home Secretary indicating that the Home Office need to do some further work on the options for reform of the DSP grant mechanism itself and that both the MPS and MPA have made constructive suggestions about this. The Home Secretary is sympathetic to the MPS request to have additional funds in this financial year to cover the shortfall in inflation provision on the existing grant. The Home Office will continue its dialogue with the MPS and MPA to come up with proposals to improve the present MPS mechanism.	No further action for MPS Recommendation is for MPA Treasurer to progress

Ref No.	**Royalty & Specialist Protection - SO Lead**	Update on the 1 outstanding High Risk recommendation raised March 2009, now implemented from MPS perspective	Target date for completion
7	The Home Office is reviewing the Dedicated Security Post (DSP) funding arrangements aiming to change them for the 2009/10 bidding process and the MPA Treasurer is involved in the process. Recommended that : - *The MPA Treasurer continues to monitor progress on DSP under funding and reports the latest position to the MPA Counter-Terrorism and Protection Services Sub-Committee.*	- Please see wording of Diplomatic Protection Group above - high risk recommendations are identical.	No further action for MPS Recommendation is for MPA Treasurer to progress

APPENDIX 1 – DETAILED UPDATE ON ALL OUTSTANDING HIGH RISK AUDIT RECOMMENDATIONS
(as at 13 November 2009, for inclusion in December CGC paper)

Ref No.	**Security vetting and clearance - SO Lead**	Update on the 2 outstanding High Risk recommendations raised March 2009	Target date for completion
8	Approval for the creation of a new centralised Vetting Unit has been given following agreement between ACSO and ACSC. Recommended that: *Senior Management in the new unit develops a strategy for approval by Management Board that* • *Supports National and Corporate Policy.* • *Includes clearly defined roles and responsibilities;* • *Sets out governance arrangements including the remit of the Departmental Vetting Officer;* • *Contains a requirement for designated Business Group Vetting Officers to identify the levels of clearance required for key posts within their BGs and to document clearly the rationale;* • *Sets out monitoring and review activities;* • *Is supported by appropriate, documented and approved corporate and local procedures;* • *Includes a requirement for KPIs to be set and monitored.*	MPS Vetting Policy is closely aligned to ACPO National Vetting Policy (NVP) and Home Office Circular 54/2003. These documents are currently under review. Publication of v3 NVP will allow the MPS to carry out a full review of its policies. No publication date is currently available. The management and staffing structure will be agreed prior to amalgamation and reviewed within 6 months MPS Vetting Board, under Professional Standards Strategic Committee, was created in 2004. The relationship between MPS Vetting Board, MetSec Board and PSSC is unclear. Governance will be reviewed in discussion with the Chairs of each Committee/Board and published once agreed. NSVU currently update MetHR when MPS staff have been vetted and are working through back record converting.	
	Units within SCD and SO are both responsible for different aspects of the vetting system and both maintain separate stand alone IT systems. To improve control over record keeping it is recommended that: • *Each BG Vetting Officer maintains details of non MPS staff clearance requests submitted to the central vetting unit* • *An independent central list of all non-MPS personnel is established by a designated individual in liaison with each Business Group* • *The vetting unit compares a sample of individuals on this list against the access logs and their database of non MPS staff who have been security cleared;* • *A central database is maintained showing the security clearance status of all MPS staff and contractors.*	SCD26 Vetting Unit in agreement with HR Recruitment update MetHR with MSC and 10 year renewal results. Warrantor could be required to facilitate this purpose. However, MetHR is the ideal location for a central database of all cleared persons but is only used for MPS employees not NPP. To achieve this will require HR directorate to direct that NPP are placed on MetHR or a link between Warrantor, or a replacement database, and MetHR. It was agreed between MPS and MPA that Commander Simon Pountain (SCD) would lead a review of MPS vetting, to include implementation of the Directorate of Audit, Risk and Assurance recommendations. SO15 and SCD26 together with DPS are assisting the Commander with this piece of work. With full support from each Business area concerned this review is expected to be completed by December 2009. In October 2009 Management Board agreed that the two vetting units in SO and SCD should remain separate at present in order that the good performance in each could be maintained. There is a decision pending from ACPO as to whether the MPS will conduct part of the National Security Vetting process on behalf of the police service. Once this decision is made the MPS will be in a position to revisit the decision of where vetting should sit. This was presented to SOP at its November meeting.	December 2009 (Please note - DARA has agreed to conduct the follow up audit in February 2010)

APPENDIX 1 – DETAILED UPDATE ON ALL OUTSTANDING HIGH RISK AUDIT RECOMMENDATIONS
(as at 13 November 2009, for inclusion in December CGC paper)

Ref No.	**Building security - Physical and Technical Guards - SO Lead**	Update on the 6 outstanding High Risk recommendations raised March 2009 - All now Implemented	Target Date for Completion
9	This audit covered building security including contractor provided guarding across MPS and the MPA building. It reviewed and evaluated the adequacy and effectiveness of systems established by management. Recommendations are aimed at introducing effective controls or improving those currently in place. Recommended that: • *Management Board level directives are issued regularly to ensure MPS wide compliance for building security policy and procedures* • *The Critical Buildings List and supporting records are approved and signed off by Assistant Commissioner, Chair of the Resilience and Business Continuity Board* • *The appropriateness of the Critical Building List is monitored and reviewed by the Resilience and Business Continuity Board and any decisions documented and approved at AC level* • *The risks of large scale access of both cleared and un-cleared individuals is considered and how the risks can be managed effectively across the MPS estate, inc means of access* • *Only MPS security cleared individuals with MPS passes are allowed access to MPS premises* • *Uncleared contractors and visitors should only be given escorted access as appropriate and locations where they are required to visit are given prior warning, inc providing all relevant details*	A Working Group was formed earlier this year. There are 25 recommendations in total raised in this audit report. A report has now been approved by OCU commander SO6 and the proposals it contains embedded in Security Operating Procedures (SOPs) fully implemented at the end of September 2009. OCU commander, SO6 has now given her opinion that the recommendations of the MPA Audit have been implemented and the intentions of the audit have been appropriately considered by the working group against current standard operating procedures and practices and agreed. Particularly significant is the involvement of Management Board Directives driving building security compliance. The Director of Information, in her capacity as chair of the METSEC Programme Board, has recently written to all Management Board members, Senior Designated Officers and all Building Security Officers reminding them of their mandatory responsibilities under MPS policy 'Security of the Metropolitan Police Estate' and specifically relating to completion of the physical security log.	Complete

APPENDIX 1 – DETAILED UPDATE ON ALL OUTSTANDING HIGH RISK AUDIT RECOMMENDATIONS
(as at 13 November 2009, for inclusion in December CGC paper)

Ref No.	**Systems for Custody records & procedures - TP Lead**	Update on the 1 outstanding High Risk recommendation raised April 2009 - Now implemented	**Target date for completion**
10	Recommended that: TP Emerald Custody Directorate ensure that BOCU SMTs are fully aware of the requirements of PACE Code C regarding the following: • *The custody officer recording the level of observation required for a detainee within the NSPIS Custody application;* • *The adherence to the guidelines on the frequency of visits to check a detainee's condition;* • *The recording of visits to a detainee's cell in the detention log at the time of the visit and not as part of a subsequent visit;* • *Local Custody Managers review NSPIS Custody application detention logs to ensure the detainee observation guidelines are complied with and that the results of the review are recorded.*	A memorandum has been sent to BOCU commanders to ensure that they and their staff are fully aware of the requirements in PACE Code C and the Custody SOP about these issues. This includes the care plan (PACE Code C, para. 3.8-3.10 and Custody SOP para.4.18) and the guidance on constant supervision issued in May 2007 (this will be incorporated into version 4 of the Custody SOP). These issues are already addressed in some depth on all custody related courses, in particular the Safer Detention Learning Programme undertaken by sergeants prior to performing the role of Custody Officer. It has also been included in the recently trialled course for sergeants with more than 10 years' service and in the gaoler training package being developed by NCALT. The Custody Directorate has already taken action to emphasise the importance of these issues including placing posters of the detainees checklist the '4Rs' (Rouseability, Response to questions, Response to commands and Remember) on each cell door in every custody suite. Cell checks and PACE Code C, Annex H compliance will form a specific theme of inspections by the Custody Directorate during 2009. The Custody Directorate recommends custody managers have a checking regime of custody records. The system used at Merton BOCU has been identified as good practice and circulated to all other BOCU Custody Managers.	Now Complete

Ref No.	**IS/IT Access & Usage - DoI Lead**	Update on the 1 outstanding High Risk recommendation raised April 09	Target date for completion
11	Recommended that: • *The DoI develop a strategy for delivering security awareness training to ensure all users are aware of their roles and responsibilities for accessing and using MPS assets, data and information.* • *Delivering security awareness should be monitored to correlate against improvements in security.*	There are currently a number of initiatives in place e.g. 'Computers and You'. Information compliance is undertaking a review of current training deliverables to establish whether a gap exists and to make recommendations to the METSEC Board. If necessary, a business case will be developed for consideration by the MPS Training Board. Update: The review is complete. Findings are being collated and will be presented to the METSEC Board at the end of November.	Revised to November 2009

APPENDIX 1 – DETAILED UPDATE ON ALL OUTSTANDING HIGH RISK AUDIT RECOMMENDATIONS
(as at 13 November 2009, for inclusion in December CGC paper)

Ref No.	**B/OCU - Corporate Issues - DoR Lead**	Update on the 2 outstanding High Risk recommendations raised April 2009	Target date for completion
12	This audit highlighted corporate issues identified as part of the B/OCU audit programme for the attention of relevant systems owners. Recommended that: *On Police Overtime:* • *The limitations of MetDuties in respect of overtime recording and authorising are highlighted and addressed.* • *An efficient, effective and consistent interim solution is identified and guidance issued to B/OCUs.* • *Corporate guidance in respect of Working Time Directive (WTD) rules is published to increase B/OCU awareness* *On Crime Property:* • *A strategic framework is established that includes the creation of an operational system owner and the development of KPIs and performance monitoring* • *The Crime Property System (TOAST) and accompanying records and activities are reviewed and revised, where appropriate, to ensure that they meet current MPS needs and address key system risks* • *The impact of NSPIS on the crime property system is assessed and the current weaknesses are addressed before the system is rolled out to other B/OCUs* • *Any system interdependencies are identified and that consideration is given to developing a corporate integrated property management system*	Finance Services and HR are working closely with the Directorate of Audit, Risk and Assurance in devising action plans to improve local arrangements for controlling and authorising overtime payments at B/OCU level. The F&R Modernisation Programme has more clearly defined the role and responsibilities of local Finance and Resource Managers in this area and improved guidance developed in the form of Finance and Resource Manuals which complement the guidance contained within the Police Overtime Manual. The ongoing clustering of F&R staff within Business Groups will also assist in developing and disseminating best practice for monitoring and controlling Police overtime. The new version of CARM, CARM 3 will be rolled out Q1 2010 as a part of the METTime 2 Programme. CARM 3 includes an electronic booking on and off system which will remove the need for any duty state/overtime sheet/variations sheet or excel workbook. The rules engine in CARM has been enhanced to cover all police overtime rules. That should remove issues around inconsistency in the application of the rules and will aid compliance. CARM 3 also contains a sophisticated and thorough overtime approval process starting when the officer books on and off, ending with submission for payment to Logica. Whilst there is no direct link between WTD and overtime worked HR is working on developing a relevant message on WTD to B/OCUs. The high risk recommendation relating to Crime Property is being progressed by Criminal Exhibit Services (formerly known as Central Property Services). The original planned replacement for the Crime Property System (TOAST) was to be the development of METAFOR. DoI informed Management Board on 16 November 2009 that METAFOR was to be formally closed down which will be subject to a further report to Management Board and the MPA. DoI is working with business groups on options for meeting the current business needs. Finance Services are involved in the development of NSPIS with regard to the financial aspects of crime property management and this work will contribute towards the ongoing management of this risk. [This recommendation has links to the high risk recommendation re crime related property made in an audit on that subject in 2008. TP Emerald team is leading on this particular recommendation and the Quality Assurance Team in Finance Services is ensuring all relevant parties are connected - see ref no. 4 in this appendix]	March 2010 April 2011

)