Inspection of the Compliance of HM Revenue & Customs' Law Enforcement Entities with the Government Protective Marking Scheme

Revisit

www.hmic.gov.uk

ISBN: 978-1-84987-478-6

Contents

Acronyms and Abbreviations

ACPO	Association of Chief Police Officers
BAM	Branch Assurance Manager
CD	Compact Discs
CDT	RIS-CIG Case Development Teams
CI	Criminal Investigation
DSP	Data Security Programme (HMRC)
DSSM	*Department Security Standards Manual* (HMRC: replaced by *SBCPSG*)
EMAF	Enforcement Management Assurance Framework
ESS	Estates and Support Services (HMRC)
GPMS	Government Protective Marking Scheme
HCR	Human Contact Report
HMIC	Her Majesty's Inspectorate of Constabulary
HMRC	HM Revenue and Customs
HumInt	Human Intelligence
IG	Internal Governance
IT	Information Technology
LSP	Lockable Storage Project
MPS	*Manual of Protective Security*
OPSEC	Operational Security Manager
OPSY	Operational Security Manager
RIS	Risk and Intelligence Service
RIS-CIG	Risk and Intelligence Service: Criminal Intelligence Group
SBCPSG	*S&BC Policy, Standards and Guidance*
S&BC	Security and Business Continuity (HMRC)
SI	Specialist Investigation
SMU	Source Management Units
SMS	Security Management System
SO	Senior Officer
SOCA	Serious Organised Crime Agency
SP&P	Criminal Investigation Strategy Planning and Professionalism
SPF	*Security Policy Framework* (Cabinet Office)
SPOC	Single Point of Contact
ST	Criminal Investigation Specialist Teams
UKBA	United Kingdom Border Agency

Executive Summary

Background

I. Following the loss by HM Revenue & Customs (HMRC) of two data disks containing personal details of Child Benefit recipients in early 2008, HM Inspectorate of Constabulary (HMIC) were commissioned to conduct an inspection of HMRC law enforcement entities' compliance with the Government Protective Marking Scheme (GPMS), which is the cornerstone to Government security. The resulting report was presented to the Financial Secretary to the Treasury, HMRC's Chairman, and the Director General Enforcement and Compliance, HMRC in October 2008.

II. During 2010, HMIC revisited this original inspection to assess HMRC's law enforcement entities' progress in implementing the original report's 16 recommendations and four considerations. Before the revisit commenced, the Cabinet Office reframed Government security policies, replacing the *Manual of Protective Security* with the *Security Policy Framework.* At the time of writing, however, GPMS policy remains unchanged and so the recommendations and considerations made in the original report remain apposite.

Approach to Implementing the Report

III. HMRC's law enforcement entities have not developed effective mechanisms to implement the original report's recommendations and considerations and robust governance arrangements are yet to be established. The report's findings required action across a number of directorates within HMRC's Enforcement and Compliance (E&C) line of business, but no project sponsor was appointed from within E&C (although the Director General E & C and the Director Criminal Investigation (CI) were considered as potentials). In the absence of senior management governance, the role of co-ordinating HMRC's response to the report was delegated to a CI officer.

IV. Progress in actioning the report's recommendations and considerations has been slow. Although a co-ordinator was appointed and an Action Plan devised, there was no co-ordinated management of delivery. Lead contacts (mainly from within CI) were appointed for all recommendations and considerations and some work to address the recommendations was undertaken in early 2009. However, the lead contacts were not formally asked to commence reviews of their allocated areas until the report was published in June 2009. These individuals also had a range of other responsibilities, but were neither informed of the relative priority of this work nor given deadlines for delivery. Consequently, progress against the recommendations and considerations in the original report was limited by the demands of other prioritised work. Furthermore, management of delivery was through infrequent requests for updates rather than active assurance that timely progress was being made.

V. Neither Risk and Intelligence Service Criminal Intelligence Group (RIS-CIG), nor Inland Detection appointed individuals to oversee their contributions to the recommendations or considerations, or to act as a single point of contact for the lead contacts. In the case of Inland Detection, this largely stemmed from the precursor Detection directorate not effectively communicating to the Inland Detection business stream its obligations in respect of the Report, upon the de-merger to UKBA. The lack of clear oversight of the Report within these

directorates, coupled with the fact that some lead contacts' did not engage with other directorates, has resulted in an unco-ordinated approach, with a number of recommendations and considerations not being addressed by all HMRC's law enforcement entities. It was encouraging that RIS-CIG looked to address this by developing its own bespoke Action Plan, although this did not occur until the Revisit was being conducted..

Progress against Recommendations and Considerations

VI. HMRC's law enforcement entities' compliance with GPMS remains unsatisfactory. The unco-ordinated approach to implementing the report's recommendations and considerations has resulted in slow progress. The only two recommendations that have been fully addressed were those subsumed into ongoing Departmental projects. There has been no real progress in addressing the recommendations concerning the core principles of GPMS. This is exemplified by the organisation not recognisng that there is conflicting Departmental guidance on whether all GPMS material requires physical marking, and no demonstrable engagement with law enforcement partners to develop GPMS guidance for law enforcement. Overall, HMRC law enforcement practitioners' knowledge of the aspects of GPMS addressed in the original report has not measurably improved and, unlike the CPIA definitions of sensitive and non-sensitive material, is not engrained in their culture. Concerns highlighted in the Executive Summary of the original inspection, including the misconception that sensitive material that stays within an office does not require marking, remains widespread.

VII. HMRC's progress in addressing the recommendations and considerations is outlined, through RAG scoring, in Table 1 below. Only Recommendations 10 and 15 have been fully discharged, and the issues addressed by the remaining recommendations and considerations remain extant. However, given the findings of the revisit the following recommendations have been amended to reflect the current situation:

- Recommendation 1: HM Inspector recommends that HMRC law enforcement entities adopt the policy outlined in HMRC's *Security Zone* and ensure that staff mark all protectively marked documents and data upon its creation, and rigorously assure this.

- Recommendation 2: HM Inspector recommends that HMRC's law enforcement entities actively engage with Cabinet Office, ACPO and other UK law enforcement agencies to inform and produce a consistent GPMS law enforcement policy and guidance that is both robust and achievable in the current economic landscape. It is imperative that HMRC assess the risks that non-compliance with GPMS policy and guidance would have and the resources required to comply with them.

- Recommendation 4: HM Inspector recommends that CI, RIS-CIG and Inland Detection ensure that staff mark all emails containing classified information. They should liaise with S&BC to determine whether the *Security Zone* or the *SBCPSG* Standard reflects Departmental policy and then ensure that their staff are aware of and compliant with this.

- Recommendation 5: HM Inspector recommends that HMRC's law enforcement entities instruct staff to mark appropriately all hard copy and electronic forms containing classified information upon their completion.

CI, RIS and Inland Detection should also prioritise which template forms require urgent amendment and liaise with CAM accordingly.

- Recommendation 8: HM Inspector recommends that HMRC ensure that all CI, RIS-CIG and Detection units that handle TOP SECRET and SECRET material maintain a Register for Protectively Marked Documents SECRET and TOP SECRET, and all SECRET documents including legacy material is recorded.

Further Recommendations

VIII. While the revisit focused upon HMRC's delivery against the original report's recommendations and considerations, it identified further areas of concern that warrant further recommendations:

- Recommendation 17: HM Inspector recommends that material sent outside the UK is marked in accordance with the Government International Protective Security policy.

- Recommendation 18: HM Inspector recommends that HMRC devise an urgent secure resolution to address the electronic transmission of SMU SECRET material.

IX. The Cabinet Office is currently engaged in a fundamental review of GPMS. It is imperative that HMRC proactively engage with the Cabinet Office and law enforcement partners to assist in the development of a practical, achievable marking system that addresses the security requirements of law enforcement in an age of austerity.

Table 1: Assessment of progress against the recommendations and considerations of the 2008 inspection

RECOMMENDATION / CONSIDERATION	RAG
Recommendation 1 - HM Inspector recommends that CI, RIS-CIG and Detection introduce a policy that mandates staff to mark all protectively marked documents and data upon its creation. This will obviously have implications across the whole Department	
Recommendation 2 - HM Inspector recommends that CI, RIS-CIG and Detection consult with ACPO and other UK law enforcement agencies to produce a consistent GPMS policy and guidance that is relevant to law enforcement activity	
Recommendation 3 - HM Inspector recommends that HMRC ensure that all SECRET documents produced by CI, RIS-CIG and Detection are fully compliant with GPMS	
Recommendation 4 - HM Inspector recommends that HMRC introduce mandatory requirement for all CI, RIS-CIG and Detection IT traffic to be GPMS marked before transmission	
Recommendation 5 - HM Inspector recommends that HMRC ensure that all HMRC law enforcement template stationery and forms are marked in compliance with the regulations outlined in the DSSM	
Recommendation 6 - HM Inspector recommends that the protective marking of printed documents including Day Books, Notebooks and Case Decision Logs are suffixed “when completed”	
Recommendation 7 - HM Inspector recommends that HMRC ensures all CI, RIS-CIG and Detection audio tapes and photographs are protectively marked in accordance with GPMS	
Recommendation 8 - HM Inspector recommends that HMRC ensures all CI, RIS-CIG and Detection units that handle TOP SECRET and SECRET material maintain a Register for Protectively Marked Documents SECRET and TOP SECRET	
Recommendation 9 - HM Inspector recommends that CI and RIS-CIG devise a policy, in line with the requirements of DSSM 11070, to review the markings of protectively marked assets	
Recommendation 10 - HM Inspector recommends that CI, RIS-CIG and Detection ensure that protectively marked waste is appropriately secured or shredded.	
Recommendation 11 - HM Inspector recommends that HMRC ensure operational information displayed on whiteboards is appropriately secured to reflect its GPMS status	
Recommendation 12 – HMRC make sufficient cabinets of the appropriate specifications available for all staff in CI, RIS-CIG and Detection who handle GPMS marked material and that combinations are regularly changed in accordance with instructions	
Recommendation 13 - HM Inspector recommends that HMRC make the CONFIDENTIAL infrastructure available to all staff within CI, RIS-CIG and Detection	
Recommendation 14 - HM Inspector recommends that HMRC re-evaluate the protective marking and transmission of Human Contact Reports.	
Recommendation 15 - HM Inspector recommends that HMRC, as a matter of urgency, undertake any work required to ensure that the CONFIDENTIAL infrastructure gains accreditation	
Recommendation 16 - HM Inspector recommends that HMRC introduce a structured assurance regime for GPMS compliance with corporate responsibility at a senior management level to enforce the importance of GPMS	
Consideration 1 - Consideration should be given to mandating the marking of all CI, RIS-CIG and Detection folders or files containing material that requires a GPMS marking with the same marking as the highest level of the document it holds	
Consideration 2 - Consideration should be given to locating all CI, RIS-CIG and Detection units that regularly handle CONFIDENTIAL, SECRET and TOP SECRET material in lockable offices with additional entry security systems such as privacy locks and swipe cards	
Consideration 3 - Consideration should be given to equipping all CI, RIS-CIG and Detection offices with Brent telephones in an environment where conversations cannot be overheard	
Consideration 4 - Consideration should be given to removing the requirement for the creation of CONFIDENTIAL, SECRET and TOP SECRET material to be authorised.	

Progress against Recommendations and Considerations

Recommendation 1

HM Inspector recommends that CI, RIS-CIG and Detection introduce a policy that mandates staff to mark all protectively marked documents and data upon its creation. This will obviously have implications across the whole Department.

Background

1.1. At the time of the original inspection, HMRC's GPMS policy[1] stated that it would be impractical to mark all material meriting a PROTECT marking, and that only material requiring a higher classification had to be physically marked. This policy ran contrary to the principles of GPMS, then outlined in the Cabinet Office's *Manual of Protective Security* (*MPS*), which stated that all assets must be clearly and conspicuously marked, unless the nature of the asset make it impractical to do so (for example if it is military hardware). Volume of material alone did not fall within the Cabinet Office's definition of impracticality.

1.2. Since the inspection, Cabinet Office has restructured its security policies. The new *HMG Security Policy Framework (SPF)* replaced the *MPS* and sets out mandatory standards and guidance across seven security policy domains. The need for staff to mark protectively marked material is now enshrined in *SPF* Mandatory Requirement 19, which states:

> *Assets must be clearly and conspicuously marked. Where this is not practical (for example the asset is a building, computer etc) staff must still have the appropriate personnel security control and be aware of the protection and controls required.*[2]

Action Taken – Security and Business Continuity (S&BC)

1.3. Following the creation of the *SPF*, HMRC S&BC restructured its security instructions, reorganising the *DSSM* to create new *S&BC Policy, Standards and Guidance* (*SBCPSG*). Although there is an ongoing review of the *SBCPSG*'s content, there are currently inconsistencies between the various S&BC policies and guidance about the requirement to mark protectively mark material. The *HMRC Security Sub-Policy 2: Protective Marking and Asset Control* states:

> *…it is mandatory to Protectively Mark all HMRC information assets in accordance with the GPMS where it is practical to do so, unless there are exceptions, such as customer communications.*[3]

1.4. While this is slightly ambiguous and does not detail other valid exceptions, it broadly reflects the *SPF*. This is not the case, however, with the underpinning *SBCPSG* guidance, which outlines the legacy policy. This states:

> *It may not always be physically possible to mark or label an asset or it may be impractical to mark every document or piece of information.*

---

[1] As detailed in the *Departmental Security Standards Manual* (*DSSM*).
[2] Cabinet Office, *Security Policy Framework* (*Online).* Available at http://www.cabinetoffice.gov.uk/media/111428/spf.pdf
[3] HMRC Security and Business Continuity, *Security Sub-Policy 2.* Unpublished.

> *Although taxpayer information merits a PROTECT marking, it was decided it would be impractical to mark every item that required the PROTECT marking. However, you must handle ALL protectively marked assets as if they were marked, and protect them to the required level.*[4]

The guidance also gives "examples of protectively marked material that should NOT show a marking at PROTECT or RESTRICTED level."[5]

1.5. The problems of these inherent inconsistencies within the *SBCPSG* are compounded by the guidance in the HMRC *Security Zone*, launched in September 2009. Available on the HMRC Intranet, the *Security Zone* is a distillation of the key elements of the *SBCPSG* and is designed to be staff's first point of reference for details of the Department's security requirements and procedures.[6] The GPMS instructions contained within the *Security Zone* are clear, stating:

> *All information should be assessed for a protective marking, and if assessed as PROTECT or higher, then the marking should be visible. The only cases where we do not show the protective markings are communications from customers and communications sent to customers.*[7]

Although not introduced in response to the original HMIC inspection Report, the *Security Zone* is in line with Recommendation 1.

Action Taken – E&C Directorates

1.6. The *GPMS Action Plan* highlights that CI Strategy Planning and Professionalism (SP&P) was unaware of the discrepancies between *SBCPSG* 5355 and the *Security Zone*, as it states "the requirement is now covered by: HMRC Security Zone [and] SBCPSG 5315, 5325 and 5355"[8]. Before the creation of the *SBCPSG*, SP&P had planned to engage with S&BC to recommend that Departmental policy be changed in light of Recommendation 1. However, SP&P shelved this as they erroneously concluded that the new *SBCPSG* and *Security Zone* addressed the recommendation.

1.7. In January 2010, SP&P emailed all CI Branch Assurance Managers, together with contacts in RIS Standards & Security, to provide them with links to *SBCPSG* 5315, 5325 and 5325 and the *Security Zone*, requesting feedback on how this is being implemented, and how it is operating in reality. As SP&P received no responses to the email, it concluded that the directorates must be compliant.

Impact

1.8. HMRC's law enforcement entities have not fully addressed the recommendation or mitigated the underlying risks.

1.9. Even though a senior S&BC manager has informed HMIC that the *Security Zone* reflects HMRC's official line on the marking of protectively marked material, there is little awareness that all protectively marked material has to be marked. No instructions have been issued to staff by CI, RIS-CIG or Inland Detection to mark

---

[4] HMRC Security and Business Continuity, *SBCPG5355 – Guidance – Protective Marking System: Protectively Marked Assets Working With: How to Show a Protective Marking*. Unpublished.
5 HMRC Security and Business Continuity, *SBCPSG5325 - Guidance: Protective Marking System: Protectively Marked Assets Working With: Choosing the Correct Level of Marking.* Unpublished.
[6] The S&BC Intranet still continues to provide links to the more comprehensive *SBCPSGs,* as well as the *Security Zone*.
[7] HMRC, *Security Zone.* Unpublished.
[8] HMRC, *HMRC (HMIC) GPMS Action Plan*. Unpublished.

all material that requires a protective marking; and no local guidance, instruction or policy detailing this requirement has been developed. The extent of the confusion over this fundamental aspect of GPMS is exemplified by the fact that, during the revisit, senior security co-ordinators in two of the three directorates that constitute HMRC's law enforcement entities were unaware of the policy that all PROTECT material has to be marked.

1.10. In the absence of clear guidance, there is a widespread misunderstanding among staff in HMRC's law enforcement entities about the need to mark all protectively marked material. In one location, staff stated that they only mark the small volumes of CONFIDENTIAL or SECRET material they produce, as they believed RESTRICTED material did not require marking. In three other locations, staff are under the misapprehension that only material leaving their office requires marking and therefore do not mark most of their material. Both these interpretations are incorrect: GPMS applies to all protectively marked material, irrespective of where it is located (including designated secure areas).

1.11. HMRC's law enforcement entities' approach to marking daybooks and notebooks provides examples of the continuing non-compliance with GPMS. New versions of notebooks containing pre-printed markings have been produced, however, these have, understandably, not being issued until stocks of the pre-existing unmarked have been exhausted. In the interim, staff should manually mark pages containing protectively marked material, however this remains very much the exception. Unlike notebooks, daybooks are pre-printed RESTRICTED. This does not exempt staff from their duty to evaluate the sensitivity of the information they enter into these documents, but such an evaluation is not being routinely undertaken.

1.12. Within CI, most operational staff accept that they do not routinely mark documents. They evaluate case material as either sensitive or non-sensitive, in accordance with CPIA requirements, but they do not generally conduct a similar evaluation to determine the appropriate GPMS marking. This is, in part, due to a widely held view that material that will be presented in court or otherwise enter the public domain should not be GPMS marked.[9] Consequently, aside from those template forms that contain a pre-printed marking or choice of markings and some isolated examples of good practice, the overwhelming majority of CI case material remains unmarked. This is clearly not compliant with the requirements outlined in either the *Security Zone* or the *SPF*. Even though material may enter the public domain at some point, it still should be marked earlier in its lifecycle if it meets the protective marking criteria. Such documents need to be reviewed and reclassified appropriately at points when the sensitivity of the document changes.

1.13. With the exception of the Intelligence Management Unit, staff across the RIS-CIG offices also do not routinely protectively mark non-templated material. The majority of papers forming or informing CDT intelligence packages and handwritten CONFIDENTIAL Source Management Unit (SMU) material do not contain a GPMS marking.[10] Similar non-compliance was evident among Inland Detection documents.

Updated Recommendation 1
HM Inspector recommends that HMRC law enforcement entities adopt the policy outlined in HMRC's *Security Zone*, ensure that staff mark all protectively marked documents and data upon its creation, and rigorously assure this.

[9] This issue is discussed at Recommendation 2: see paragraph 2.7 below.
[10] Including the handwritten notes of calls with sources.

1.14. Under GPMS principles, staff are also required to protectively mark material coming into their possession from outside HM Government that has been previously marked to indicate sensitivity. CI case files and RIS intelligence packages include large numbers of such documents, including bank statements. None of those examined during the revisit was marked. Similarly, the CI SMS implies that case officers mark documents seized during investigations. Again, there is no evidence that such activity is actually taking place. Many CI and RIS staff feel that marking such material would be inappropriate, as it could potentially constitute evidence. The issue of how evidential exhibits should be handled in order to meet the requirements of GPMS while not physically changing the evidence should be addressed through the creation of consistent policy on how GPMS should be applied within UK law enforcement.

Recommendation 2

HM Inspector recommends that CI, RIS-CIG and Detection consult with ACPO and other UK law enforcement agencies to produce a consistent GPMS policy and guidance that is relevant to law enforcement activity.

Background

2.1 The original inspection highlighted the subjective nature of the law enforcement definitions of GPMS classifications. There was no specific guidance on how HMRC staff should interpret them, and this mirrored a lack of consistency across UK law enforcement as a whole. Furthermore, it outlined the lack of both HMRC and consistent UK guidance on other specific GPMS issues, including on how uplifted evidence should be marked and how the aggregation of protectively marked law enforcement material, such as case papers or intelligence files, affects the marking of the totality of these assets.[11]

Action Taken

2.2 HMRC has made very slow progress in addressing this recommendation. SP&P committed in June 2009 to contact the Association of Chief Police Offices (ACPO), Serious Organised Crime Agency (SOCA) and the United Kingdom Border Agency (UKBA). By September 2009, CI were still determining whether a specific Law Enforcement policy was realistic and were reviewing suitable opportunities for liaison with ACPO, SOCA and UKBA. There is no evidence that this work was prioritised. SP&P did not send its first preliminary emails to contacts in these agencies until December 2009. By the time the revisit commenced:

- SOCA had responded, supporting the introduction of a consistent GPMS interpretation across law enforcement, providing a copy of their GPMS guidance and offering to contribute further to the process if required;
- The email sent to ACPO had been forwarded to the National Police Improvement Agency;
- No response from UKBA had been received; and
- SP&P had not decided whether the review process should be conducted through meetings, or via email.

Subsequently, at time of writing, the NPIA confirmed that they will participate in the review but there is no evidence that any formal discussions to devise standard guidance has commenced.

2.3 In the absence of a quick resolution to this issue, no interim solution has been sought. Even though S&BC confirmed to HMIC that directorates are permitted to devise supplementary GPMS guidance that builds upon Departmental policies, CI security managers and SP&P are opposed to doing this.

2.4 SP&P have approached neither RIS-CIG nor Inland Detection to contribute to this recommendation, and neither RIS-CIG nor Inland Detection have produced any bespoke guidance for their staff.

[11] HMIC (June 2009) *Inspection of HM Revenue & Customs The Compliance of HM Revenue & Customs' Law Enforcement Entities with the Government Protective Marking Scheme*, pp.10–13.

Impact

2.5 HMRC's law enforcement entities have not fully addressed the recommendation. None of the concerns highlighted in the original report that underpin Recommendation 2 has been resolved,[12] and there remains a lack of consistent GPMS guidance across UK law enforcement agencies.

2.6 No guidance has been produced in HMRC to assist staff in interpreting the subjective law enforcement definitions of GPMS classifications. The production of the *Security Zone* has also inadvertently increased inconsistencies, as its definitions differ from those in the *SPF* and those in the *SBCPSG* (see Annex B).

2.7 Under the *Security Zone's* definitions, the only difference between RESTRICTED and CONFIDENTIAL material is that the latter relates to serious crime. A robust interpretation of serious crime, using the definition enshrined in the Serious Crime Act 2007, would mean that all material that could hinder any HMRC investigations or make any HMRC offences easier to commit would be CONFIDENTIAL. Although the original inspection report highlighted this issue, HMRC's law enforcement entities have not recognised or actively considered this and have therefore made no decision as to whether this interpretation is appropriate. In actuality, staff across RIS-CIG, CI and Inland Detection are generally not aware of the law enforcement definitions of GPMS and do not routinely assess the law enforcement operational impact of their material to determine a GPMS marking. Instead, CI and CDT officers generally use CPIA definitions, deeming that SENSITIVE material equates to CONFIDENTIAL. In IMU, only papers that relate to high profile individuals are deemed CONFIDENTIAL, irrespective of the nature of the allegation.

2.8 At the time of writing, the Cabinet Office has recently commenced a fundamental review of GPMS, which will include consultation with key stakeholders.

Updated Recommendation 2

HMIC recommends that HMRC's law enforcement entities actively engage with S&BC, ACPO and other UK law enforcement agencies to inform the development of consistent GPMS law enforcement policy and guidance that is both robust and achievable in the current economic landscape. It is imperative that HMRC assess the risks that non-compliance with GPMS policy and guidance would have and the resources required to comply with them.

[12] See above, paragraph 2.1.

Recommendation 3

HM Inspector recommends that HMRC ensure that all SECRET documents produced by CI, RIS-CIG and Detection are fully compliant with GPMS.

Background

3.1. The original inspection identified that very few SECRET documents contained the full details of the author, title and name of the originating office, as required by the *DSSM*.[13]

Action Taken – S&BC

3.2. The requirements outlined in the *DSSM* remain apposite and now form part of the *SBCPSG* 5355, which instructs staff to:

> *Indicate on every [SECRET or TOP SECRET] document, it's [sic] author, title, name of the originating office, reference or copy number and date of publication. Give a serial number to any documents issued in a series. Number each page of the document. Number each annex of a document in a separate series to the main text.*[14]

Neither the *Security Zone* nor the *Data Security* booklet include reference to these requirements.

Action Taken – CI

3.3. According to the *GPMS Action Plan*, HMRC has addressed this recommendation through assurance activity undertaken by CI Specialist Teams, OpSecs and through the Enforcement Management Assurance Framework.[15] There is no evidence that the requirements contained in *SBCPSG* 5355 have been disseminated to BAMs or other CI staff, and they are not outlined in the *Enforcement Handbook*.

Action Taken – RIS-CIG

3.4. In November 2009 a memo sent by RIS Standards and Security to a CIG Grade 6 outlined that there was no standard procedure for the handling and registering of TOP SECRET/SECRET material within CIG. It concluded that "there is a need to urgently remedy this situation as soon as possible in order to comply with HMIC recommendations [3 and 8]," and outlined five recommendations to address these shortcomings. The first of these focused on the importance of disseminating departmental guidance to staff and called for an email to be sent to all RIS Grade 7s reminding staff of the existing guidance in relation to the handling of SECRET/TOP SECRET material. The associated Implementation Plan indicated that this recommendation would be addressed urgently, stating that the email would be issued by 30 November 2009.[16] It also outlined that Standards and Security would compile a schedule of CIG teams that handle SECRET / TOP

[13] HM Inspectorate of Constabulary (June 2009), p.14.
[14] HMRC Security and Business Continuity *SBCPG5355 – Guidance – Protective Marking System: Protectively Marked Assets Working With: How to Show a Protective Marking*. Unpublished.
[15] EMAF is outlined below: see Recommendation 16.
[16] Implementation Plan in relation to RIS-CIG compliance with SECRET/TOP SECRET Handling Procedures: RESTRICTED.

SECRET material by 15 December 2010 , through liaison with RIS managers and that an assurance report would be completed by 31 March 2010.

3.5. By the time the revisit commenced, none of the required actions outlined in the November 2009 memo had been actioned. According to the latest version of the Implementation Plan (dated May 2010), the email to Grade 7s is not expected to be sent until 30 June 2010. This constitutes a delay of seven months. Equally, the dates for the completion of the schedule of teams that handle SECRET / TOP SECRET material and the assurance report have been put back to 30 July 2010 and 21 December 2010 respectively.

3.6. In 2009, independent of the RIS-CIG Implementation Plan, the SMU Operational Security Manager (OPSEY) undertook an assurance of how SMUs store, mark and transmit SECRET material. However, CHIS-OPS management have not disseminated the *SBCPSG* 5355 requirements to SMU staff, or included reference to them within the SMU Standard Operating Procedures.

Impact

3.7. HMRC has not fully addressed this recommendation or mitigated its inherent risks. Given RIS's delay in disseminating details of the requirements to staff and the omission of this guidance from both Departmental publications and directorate instructions, it is unsurprising that they were not widely known even among staff who create SECRET documents. During the revisit, HMIC examined a sample of SECRET documents recently produced by three SMUs, none of which included all the requisite information.

3.8. HMIC has been unable to identify the range of other RIS-CIG units that create SECRET documents, since there is still no definitive list of these.[17] Similarly, no SECRET documents originating from either CI or Inland Detection were available during the revisit. Consequently, it has not been possible to assess the compliance of SECRET documents outside SMUs.

3.9. It is also apparent that not all SECRET material is marked accordingly. In two of the SMUs visited, a number of documents capable of revealing the true identity of CHIS were not marked SECRET. Although staff are treating these documents as SECRET, all documents assessed as SECRET should be marked as such.

17 HMIC are aware that FCLOs create limited SECRET material overseas. This has not been examined during the Revisit.

Recommendation 4

HM Inspector recommends that HMRC introduce mandatory requirement for all CI, RIS-CIG and Detection IT traffic to be GPMS marked before transmission.

Background

4.1. The original HMIC inspection identified that staff in HMRC's law enforcement entities were not routinely protectively marking emails produced on the restricted network that contained classified material.

Action Taken

4.2. An S&BC manager was appointed lead contact for Recommendation 4 in early 2009. Prior to this, and not directly in response to HMIC's recommendation, S&BC included guidance on the marking of emails in the *SBCPSG* (and latterly in the *Security Zone*). The two sets of guidance differ, however, on where the marking should be placed on the email.

4.3. In September 2009, the lead contact suggested to SP&P that, as Departmental guidance was in place, the responsibility for addressing the recommendation now falls into the business areas to mandate the application of guidance in the way that best meets their needs. This has not occurred. CI, RIS-CIG and Inland Detection have not ensured that staff across the business streams are aware of the requirement to mark emails, in the way suggested by the lead contact. Although there is evidence that managers in some discrete business areas have informed their staff of the requirement (as has happened in Internal Governance and the International Mutual Assurance Team), this message has not been successfully delivered to all practitioners across the three business streams.

4.4. Before the original inspection, S&BC had examined the potential of introducing a software solution to automate the marking of emails produced on the Restricted network. This work has continued. In October 2009, S&BC highlighted that SOCA utilise such a software solution. However, in response to requests from S&BC and SP&P, both the Data Security Programme and Central Compliance Enforcement and Compliance (E&C) Finance confirmed that there are no available funds to implement a similar system across either HMRC or E&C.

4.5. S&BC has subsequently re-examined the issue, albeit because of a different driver: Security and Design Authority tasked S&BC with examining HMRC's requirements for secure email. This review recommended a drop-down menu for GPMS markings. At the time of writing, S&BC are set to present their findings to key internal stakeholders to see whether they can secure funding and HMIC are encouraged by this development

Impact

4.6. HMRC has not fully addressed this recommendation or mitigated its inherent risks. Although S&BC has introduced a requirement to mark emails, this is not widely known nor routinely adhered to by practitioners in RIS-CIG, CI and Inland Detection. Although some staff have started to protectively mark the emails they send on the Restricted network, this is sporadic and there is, in general, a low level of adherence to the requirement. In all but one of the revisit locations, staff either

conceded that they do not mark emails, or the audit found that less than half the sample of emails requiring a protective marking were marked.

4.7. Among the minority of staff who do mark emails, there appears to be low levels of knowledge of and adherence to the *Security Zone* instruction that they should place markings at the top of emails.

Updated Recommendation 4

HMIC recommends that CI, RIS-CIG and Inland Detection ensure that staff mark all emails containing classified information. They should liaise with S&BC to determine whether the *Security Zone* or the *SBCPSG* standard reflects Departmental policy and then ensure that their staff are aware of and compliant with this.

Recommendation 5

HM Inspector recommends that HMRC ensure that all HMRC law enforcement template stationery and forms are marked in compliance with the regulations outlined in the DSSM.

Background

5.1. The original inspection identified that HMRC corporate stationery was locked to prevent staff from editing the headers and footers, and thus such documents could not to be protectively marked electronically.[18] It also illustrated that although some commonly used template forms were marked, these represented a minority of the template forms used across HMRC's law enforcement entities.[19]

Action Taken – Stationery

5.2. From March 2009, CI SP&P actively sought to address the first aspect of this recommendation. It identified that by making the stationery templates available on the SEES system, a drop-down list of protective markings could be included. As with the Ministry of Justice's letterhead form identified in the original inspection,[20] this solution would require staff to select a protective marking, or indicate that the document should not be protectively marked, in order for a document to be created. Considerable work was progressed over the following months to develop this system and to ensure that all corporate stationery used by CI, SI, Detection and RIS was included. This work is commendable, however, it was put on hold in September 2009 when it became apparent that large numbers of CI and CIG staff who use the CONFIDENTIAL IT infrastructure are unable to access the SEES system. SP&P has considered other possibilities, including saving a range of stationery templates with different protective markings on the shared drives: however, at the time of writing none of these had been implemented.

Action Taken – Forms

5.3. While CI SP&P has focused its attention on the stationery aspect of Recommendation 5, by the time the revisit commenced no discernable action had been undertaken to address the non-compliance of template forms. Subsequently, SP&P (in liaison with RIS-CIG) has compiled a list of 492 form templates available on the *Enforcement Handbook* and passed this to CAM, which has been tasked with updating the forms and adding protective markings. Due to funding and resource constraints, CAM is unable to update all the forms as a one-off project and is therefore, resources permitting, looking to work through them during 2010/11.

5.4. The current progress with this aspect of Recommendation 5 raises a number of concerns:

- CI SP&P has not sought to evaluate the relative potential impact that the omission of GPMS marking would have on different *Enforcement Handbook* forms. In the absence of such an evaluation, no form has been prioritised from a security impact perspective. Instead, CAM has been left to determine its workflow, prioritising those forms that require amending following operational

[18] See HMIC (June 2009), para 3.4.
[19] See HMIC (June 2009), para 3.6–3.7.
[20] See HMIC (June 2009), para 3.4.

changes, those printed forms that reach stock reprint levels, and those that feature on its cyclical review of material. It has also determined that it would not be cost effective to destroy existing stock. Consequently, a frequently used form, which would contain RESTRICTED or CONFIDENTIAL information when complete but is currently unmarked, would not necessarily be subject to review before a less impactive form.

- It is currently unclear whether a standard marking will be applied to all the forms. In April 2010, CAM confirmed that it would review the forms in liaison with the form owners on a case-by-case basis and would not undertake a blanket approach to applying the protective markings. However, SP&P has subsequently sought to ensure that the marking is generic across all the forms and have proposed marking all the forms "RESTRICTED / CONFIDENTIAL (when completed)". This kind of universal solution is inappropriate. It does not constitute an active determination of the sensitivity of the information that (a) is contained within the pre-printed text in each template form or (b) would be included once each form is completed. For example, some forms relating to certain intelligence or investigative techniques would when completed always require a CONFIDENTIAL marking, whereas information in others may be classified as "not protectively marked", "PROTECT" or "SECRET".

- SP&P has only tasked CAM to amend those template forms available in the *Enforcement Handbook*. This does not constitute the totality of forms used by staff across HMRC's law enforcement entities. Neither CI nor RIS-CIG has instructed staff to ensure that the plethora of bespoke, locally produced template forms are marked. There is also no evidence either that SP&P has liaised with Inland Detection to obtain details of their commonly used forms, or that Inland Detection has proactively sought to address this issue.

- No interim solution has been developed. Staff have not been instructed to manually mark printed forms or editable electronic forms during the period preceding the completion of CAM's update programme.

Action Taken – Impact

5.5. Although SP&P has attempted to implement Recommendation 5, at time of writing, this has yet to improve compliance.

5.6. Staff are still unable to add a protective marking to electronic corporate stationery. Moreover, at the time of writing, CAM had not amended the GPMS markings on any of the template forms contained in the *Enforcement Handbook*. Therefore, the varying levels of GPMS adherence of such forms that was identified in the original inspection continues. During the revisit, it was also apparent that a similar picture exists across the bespoke local forms used in the units visited.

Updated Recommendation 5

HMIC recommends that HMRC's law enforcement entities instruct staff to appropriately mark, upon completion, all hard copy and electronic forms containing classified information. CI, RIS and Inland Detection should also prioritise which template forms require urgent amendment and liaise with CAM accordingly.

Recommendation 6

HM Inspector recommends that the protective marking of printed documents including Day Books, Notebooks and Case Decision Logs are suffixed "when completed".

Action Taken

6.1. CI SP&P has actively sought to address Recommendation 6. In June 2009, it provided HMRC's CAM with a proposed design for a **notebook** cover that includes GPMS markings. Progress was slow during the following months, due to CAM's heavy workload and subsequent negotiations between CI and CAM on the precise wording of the printed markings and aesthetic design of the document. However, a final version was agreed in November 2009, and then printed and supplied to HMRC's stores facility by early 2010. This new notebook contains the following on its front cover:

6.2. SP&P has subsequently realised that this text does not comply with this recommendation, as blank versions of this Notebook carry a default RESTRICTED marking. To address this, SP&P has redesigned the notebook again. Once existing stocks are exhausted they will be replaced with a new version that states 'RESTRICTED / CONFIDENTIAL (when completed)' at the top and bottom of every page.

6.3. SP&P has also commenced work on producing a new version of the HMRC **Case Decision Log** (CDL). By March 2010, following constructive consultation with stakeholders, SP&P had provided CAM with a revised CDL design. This design contained the GPMS marking shown at Paragraph 6.1, but was subsequently revised, in advance of any copies being produced, to include 'RESTRICTED / CONFIDENTIAL (when completed)' at the top and bottom of every page. At time of writing, this design has been signed off and the new CDLs are due to be printed in late Summer 2010, at which point any blank 'old style' CDLs will be destroyed.

6.4. Before the revisit, progress had not been made to amend the **daybooks** in accordance with Recommendation 6, however, at the time of writing, a new version of the daybook, that states 'RESTRICTED / CONFIDENTIAL (when completed)' at the top and bottom of every page, has been agreed between CAM and SP&P and is awaiting senior manager approval.

6.5. While SP&P focused on revising the format of daybook, notebooks and CDLs, no interim solution was considered that could ensure the suffix was added to the printed documents currently in use.

Impact

6.6. Progress has been made in addressing this recommendation, and the latest versions of the daybooks, notebooks and the CDL are compliant with this.

Recommendation 7

HM Inspector recommends that HMRC ensures all CI, RIS-CIG and Detection audio tapes and photographs are protectively marked in accordance with GPMS.

Action Taken

7.1. The form used to request photographic printing from CI Specialist Teams (ST) Photographic Unit has been amended since the original inspection and now requires the customer to indicate which protective marking should be applied to the prints. SP&P determined that this amendment fully addressed the photographic element of Recommendation 7.

7.2. CI SP&P has made some progress in taking forward the second part of this recommendation. It determined that adding a protective marking to the standard printed tape label template would be cost prohibitive. Consequently, work has been focused on amending the seal applied to master copies of tapes. SP&P liaised with stakeholders in RIS-CIG, CI, Detection and CAM to achieve this and a revised seal including the header "Delete as Applicable RESTRICTED / CONFIDENTIAL" was sent for printing in late 2009. SP&P has accordingly closed this aspect of Recommendation 7.

Impact

7.3. Although some progress has been made, the risks that underpin the original recommendation remain.

7.4. Despite the amendment to the form, staff in CI ST Photographic Unit still do not apply markings to photographs and have not been made aware of this requirement. Furthermore, CI and RIS-CIG are generally unaware of the need to consider marking photographs or any associated electronic media, whether produced by the Photographic Unit or elsewhere. Of the material examined, a small number of documents which include photographic images (such as target sheets) are marked. However, systemic non-compliance with the requirement to mark actual photographs or CDs containing photographs continues.

7.5. The action taken in respect of the marking of audio tapes is only a partial solution: the new marked seal is only applied to the master copies of tapes and working copies remain unmarked. Furthermore, the new template seal had not been issued to the operational teams seen during the revisit. Although it is acceptable for existing stocks to be exhausted rather than replaced, no interim measure to mitigate the risk (such as mandating staff to manually mark tapes) had been implemented.

Recommendation 8

HM Inspector recommends that HMRC ensure all CI, RIS-CIG and Detection units that handle TOP SECRET and SECRET material maintain a Register for Protectively Marked Documents SECRET and TOP SECRET.

Action Taken

8.1. Since the original inspection, CI ST has revised its pre-existing Register for Protectively Marked Documents SECRET and TOP SECRET. Subsequently, as part of an assurance undertaken in early 2009, it reminded staff who had signed for OMEGA SECRET material of their obligation to maintain a register and issued them with a template register. It also now conducts six-monthly inspections of its register and those used by its customers as part of its regular assurance programme.

8.2. The SP&P lead contact for Recommendation 8 highlighted that the ST assurance would not capture SECRET material produced by other CI teams or received from other sources. To resolve this, a consultation was conducted with potential recipients of such material across the directorate. OPSECs and BAMs were reminded of the requirements under *SBCPSG* to review and register SECRET and TOP SECRET material.

8.3. RIS has also made progress in respect of this recommendation. In June 2009, CI SP&P contacted a RIS Deputy Director to inform them that the HMIC report had highlighted as an area of concern the lack of SMU SECRET registers. Commendably, within three weeks NSU issued a Dissemination to all SMU staff, instructing them to create and maintain a register with immediate effect.[21]

8.4. The November 2009 memo, which outlined recommendations to improve CIG's compliance with SECRET/TOP SECRET handling procedures,[22] also specifically highlighted the need to introduce registers.

Impact/Areas for improvement

8.5. Although SMUs have introduced registers, the NSU Dissemination does not state whether these should include legacy SECRET material that predates the registers' inception, consequently, none of the pre-existing SECRET documents has been retrospectively registered in any of the SMUs visited. As SMUs do not destroy any such documents, large quantities of SECRET material held by SMUs remain unregistered.

8.6. Further shortcomings were identified in two of the three SMUs visited. As previously stated,[23] the revisit identified that not all SECRET material is physically being marked SECRET. These 'unmarked SECRET documents' are not being included in the registers. Moreover, the register in one of the SMUs was not being properly maintained and did not list all recently created documents marked SECRET.

8.7. While the NSU Dissemination states that documents leaving an SMU manager's control have to be signed out in the register, it does not detail procedures relating

[21] NSU Dissemination 05/09 (08 July 2009). *GMPS Markings – Registers for Secret and Top Secret Material.* Unpublished.
[22] See above, para 3.5.
[23] See above, para 3.10.

to SECRET material received from third parties or transferred electronically. Consequently, not all electronic movements of SECRET material are registered.

8.8. As mentioned above at Recommendation 3, the delay in reminding staff across CIG of the current guidance in relation to the handling of SECRET / TOP SECRET material, including the requirement to register such material, is unfortunate. The production of a schedule of RIS teams that handle SECRET material has also been delayed. This is now not expected to be completed until 30 July 2010 – over seven months after its original target completion date. In its absence, RIS-CIG are still unable to ensure that its SECRET material is registered appropriately.

Updated Recommendation 8
HM Inspector recommends that HMRC ensure all CI, RIS-CIG and Detection units that handle TOP SECRET and SECRET material maintain a Register for Protectively Marked Documents SECRET and TOP SECRET, and that all SECRET documents (including legacy material) is recorded.

Recommendation 9

HM Inspector recommends that CI and RIS-CIG devise a policy, in line with the requirements of DSSM 11070, to review the markings of protectively marked assets.

Background

9.1. At the time of the original inspection, *DSSM* 11070 outlined the requirement for staff to review the markings of protectively marked assets. This is now encapsulated in *SBCPSG* 1590, which states: "[t]he originator must determine the level of protective marking and review that marking throughout the life of the asset."[24] *SBCPSG* 5435 complements this, stating "… you should review the protectively marked information you hold (whether on paper, electronically etc) to check if the marking is still appropriate." [25]

Action Taken

9.2. The *GPMS Action Plan* states that CI reviews the conformance with this recommendation as part of the EMAF BAM assurance and that, once developed, RIS-CIG's SMART Programme will encompass such assurances. It also suggests that an annual review of the GPMS markings could be undertaken. There is, however, no evidence that this annual assurance occurs.

9.3. There is no evidence of any other activity being undertaken by CI, RIS-CIG or Inland Detection to address Recommendation 9.

Impact

9.4. HMRC has not addressed this recommendation or mitigated its inherent risks. Action is required to ensure that staff are informed of their responsibilities.

9.5. There is no evidence that staff have been reminded of their responsibilities to review markings and the staff interviewed stated that periodic reviews do not occur.

9.6. Of the units subject to the revisit, the only evidence of GPMS markings being revised and removed was witnessed in the UK-based component of the Overseas Liaison Officer network.[26] Material passed from this unit is declassified before being passed to overseas agencies. This is in breach of the guidance contained within the Government-wide International Protective Security Policy, which explicitly states that all protectively marked material given to other jurisdictions has to retain any protective markings.

Additional Recommendation 17

HM Inspector recommends that material sent outside the UK is marked in accordance to Government International Protective Security policy.

One unit visited during the revisit had undertaken such a process and had stamped all papers contained in SECRET folders SECRET, including those

[24] HMRC Security and Business Continuity, *SBCPSG Standard 1590 - Protective Marking System: Information Labelling and Handling.* Unpublished.
[25] HMRC Security and Business Continuity, *SBCPSG5345 - Guidance: Protective Marking System: Protectively Marked Assets Working With: Control of Protectively Marked Assets.* Unpublished.
[26] This does not include the CI Specialist Teams, which at the time of the original inspection had already introduced a process to conduct such reviews. See HMIC (June 2009), p.20

pre-marked with lower classifications. This, however, had only occurred after the unit had been informed that its documents would be examined by HMIC. Elsewhere, the inspection team saw no examples of such reviews occurring.

9.7. A periodic assurance review of compliance with the requirement to review protectively marked material (such as EMAF) would not adequately address this recommendation. Instead, it is imperative that staff who create and handle marked documents actively look to revise these markings appropriately. HMI recommends that clear guidance should be produced and disseminated to staff to assist them in identifying when documents should be reviewed. .

Recommendation 10

HM Inspector recommends that CI, RIS CIG and Detection ensure that protectively marked waste is appropriately secured or shredded.

Action Taken

10.1. In direct response to the recommendations made in the Poynter Review, HMRC's Estates and Support Services (ESS) introduced a new policy for the disposal of protectively marked waste across HMRC in early 2009. This requires staff to place RESTRICTED waste in new lockable bins, which is then shredded on site by an external contractor. The policy retains the requirement for CONFIDENTIAL material to be shredded using crosscut shredders. The new policy has been disseminated to staff, and is articulated in the *Security Zone* and in the new version of the *Data Security* booklet.

10.2. The CI Data Guardian and SP&P sought to ensure that the new policy met the Directorate's requirements, discussing and resolving concerns with ESS before instructing staff to adopt the new procedures. By June 2009, these procedures had been rolled out across the CI estate and the *GPMS Action Plan* had been updated to show that Recommendation 10 had been "completed".

10.3. In October 2009, in response to a request from SP&P, CI BAMS provided an assurance that their branches were compliant with Recommendation 10 and that the new policy is not presenting any problems. Ongoing monitoring of the procedure is also included within CI's EMAF and is integrated into SP&P's programme of out-of-hours security sweeps.

10.4. The new service for disposal of protectively marked waste also encompasses the RIS-CIG and Inland Detection estates. There is no evidence that SP&P liaised with either business area in respect of this recommendation, or undertook any other specific action in response to it.

Impact

10.5. Encouraging progress has been made to address the recommendation. The introduction of the new waste disposal policy appears to have significantly reduced the practice of using unsecured containers to dispose of protectively marked material. During the revisit, it was apparent that staff are aware of the new policy in respect of RESTRICTED material – stating they adhere to, or exceed its requirements[27] – and no inappropriate disposal of such material was witnessed. It should be noted, however, that the revisit did not include detailed out-of-hours inspections of offices and therefore it is not possible to determine the precise level of compliance with this recommendation, although no evidence was seen of security breaches in this area.

[27] In some offices, local policies have been devised that require staff to shred all protectively marked material.

Recommendation 11

HM Inspector recommends that HMRC ensure operational information displayed on whiteboards is appropriately secured to reflect its GPMS status.

Action Taken

11.1. CI SP&P have actively sought to address this issue; and according to the *GPMS Action Plan*, this recommendation has been closed.[28] In June 2009, SP&P contacted all OPSYs and BAMS across CI, RIS and SI, informing them of the recommendation and directing them to remove details of official vehicles and other sensitive information from whiteboards. The *Enforcement Handbook* was amended accordingly and the out-of-hours security sweep template was changed to include testing of compliance with this recommendation.

11.2. The SI OPSEC also informed staff of the new procedures. An Inland Detection Operational Security Report issued to all staff in April 2010 recommended "where information is displayed in a shared office, or where there is any likelihood of unknown persons having access to the office, it should be limited to what is in the public domain….".[29]

Impact

11.3. Encouraging progress has been made to address this recommendation, although some issues remain unresolved.

11.4. It would appear that the action taken by SP&P has addressed the risks in CI. None of the whiteboards in the CI offices visited during the revisit contained any sensitive material and there was also no evidence of non-compliance within SI. However, SI should consider revising the Operational Security Report's recommendation. To fully comply with the 'need to know' principle, protectively marked material should only be openly displayed where every individual who can view it has a valid requirement to do so.

11.5. Although RIS OPSYs and BAMs were informed of this recommendation and CIG officers have access to the *Enforcement Handbook*, adherence across RIS-CIG remains sporadic. This was demonstrated in the revisit, where sensitive material, including a criminal network chart and details of the UKBA cutter fleet's active deployments, was openly displayed in two RIS-CIG offices.

[28] See HMRC, *HMRC (HMIC) GPMS Action Plan*. Unpublished.
[29] HMRC, *SI Inland Detection Operational Security Report 06/10: Office Display of Sensitive Material*. Unpublished.

Recommendation 12

HM Inspector recommends that HMRC make sufficient cabinets of the appropriate specifications available for all staff in CI, RIS-CIG and Detection who handle GPMS marked material and that combinations are regularly changed in accordance with instructions.

Action Taken

12.1 In 2009, the cross-HMRC Data Security Programme (DSP) and ESS funded a Lockable Storage Project (LSP) to address problems with secure storage across the Department. CI SP&P actively engaged with this Project. In October 2009, CI SP&P conducted an assurance of secure storage across the Directorate estate and provided DSP with a collated schedule detailing CI's cabinet, lock and key requirements. A further assurance was undertaken in May 2010 when DSP was issued with details of outstanding and additional requirements. SP&P intend to review new requirements and work with DSP to monitor delivery on a quarterly basis.

12.3 SP&P identified that poor housekeeping in operational branches prevents the optimum use of the Directorate's secure storage, and has reminded CI staff of the need to dispatch legacy material to remote storage.

12.4 Before the revisit, RIS-CIG had not actively addressed Recommendation 12. However, in May 2010, RIS Standards and Security tasked CIG team leaders to assure compliance with the recommendation and confirm that sufficient lockable storage was available for their staff. Such assurances were received from all but two teams, and in both these cases business cases had been submitted for additional facilities.

Impact

12.5 Encouraging progress has been made in addressing the recommendation. Through SP&P's involvement with the LSP in 2009/10, CI has received more than 100 lockable cabinets. Most of the offices visited during the revisit appeared to have sufficient storage, and all the SECRET and CONFIDENTIAL material viewed in SMUs was secured in approved security containers, in accordance with the requirements outlined in the *SBCPSG*.

12.6 Compliance is still not universal, however. The delivery of most locks and keys requested by CI has been delayed. In the interim, some protectively marked material – both RESTRICTED and CONFIDENTIAL – continues to be stored in unlockable 'privacy cupboards' (that are only authorised to hold material classified as RESTRICTED or below[30]) and security containers. In at least one location, legacy case material continues to be stored in cardboard boxes in the corridor.

12.7 Most CI case material and CDT papers are stored in 'privacy' cupboards. Clearly, if documents were marked according to a robust definition of CONFIDENTIAL (such as that outlined in the *Security Zone*[31]) these storage arrangements would be inadequate. Even under the status quo, not all the relatively small volumes of CONFIDENTIAL marked material is stored in approved security containers. Staff

[30] The Internal Governance office in Slough remains the exception to this, with all material stored in security cabinets.
[31] See above, Recommendation 2.

are not universally aware that such material should not be locked in 'privacy cupboards'. There is also confusion about what constitutes an approved security container, and neither the *SBCPSG* nor *Security Zone* contain a definition. Consequently, there remain instances where CONFIDENTIAL material is filed alongside other related case papers or within case development packages and stored in privacy cupboards.

12.8 HMRC's law enforcement entities should ensure that staff follow storage and housekeeping policies, where suitable facilities allow. However, the acquisition of additional or higher specification storage is largely dependent upon securing resources from other areas of the Department. Currently, DSP have no funds to provide the items requested in May 2010 and there is no guarantee that any such funding will be secured. Stakeholders in the Department – including S&BC, ESS, DSP, CI, CIG and Inland Detection – need to urgently evaluate whether compliance with this element of GPMS is achievable, given the current economic climate; and if not, how risks can be mitigated in other ways.

Recommendation 13

HM Inspector recommends that HMRC make the CONFIDENTIAL infrastructure available to all staff within CI, RIS-CIG and Detection.

Background

13.1. The original inspection highlighted that the CONFIDENTIAL IT infrastructure's limited footprint across HMRC's law enforcement directorates had resulted in security breaches occurring, with CONFIDENTIAL material being created, sent and received on the RESTRICTED network. It also raised concerns that some staff who did not have access to the CONFIDENTIAL infrastructure were knowingly under-classifying material as RESTRICTED in order to meet the requirements of their IT platform.[32]

Action Taken

13.2. In respect of this recommendation, the *GPMS Action Plan* simply states "implementing this recommendation would be a huge undertaking and prohibitively expensive [and therefore] no further action [is required] at this time". However, this does not reflect the totality of work undertaken in HMRC to address the issues with the CONFIDENTIAL Infrastructure since 2009.

13.3. The ongoing HMRC IT Spectrum Project is tasked with delivering upgrades to the CONFIDENTIAL infrastructure and achieving connectivity to the XGSI network. During periods of the Project's lifecycle, a moratorium was imposed on the creation of additional CONFIDENTIAL accounts. However, by the time the revisit was undertaken this embargo had been lifted and the CONFIDENTIAL infrastructure had been installed in a further six sites across the CI and CIG estates.

13.4. Other ongoing CI projects also contributed to increasing the proportion of HMRC's law enforcement staff who can access the CONFIDENTIAL infrastructure. The original inspection makes specific mention of CI direct tax investigation teams who could only access the RESTRICTED network.[33] The CI Accommodation Consolidation Programme has resulted in many of these teams being relocated to offices with access to the infrastructure, and the move to multi-functional investigation teams has further reduced the number of teams that have no access to it.

Impact

13.5. Activity undertaken by HMRC has partially mitigated the problems that underpinned Recommendation 13. However, patches of non-compliance remain.

13.6. As a result of the Spectrum Project and the changes to CI's estate and investigation team model, the CONFIDENTIAL infrastructure is currently more widely available across CI and CIG than during the 2008 Inspection. Moreover, since the demerger to UKBA, the Detection units that were highlighted in the 2008 Inspection as creating, sending and receiving CONFIDENTIAL material on the restricted network no longer fall within the ambit of HMRC's law enforcement entities.

[32] HMIC (July 2009), p.26
[33] HMIC (July 2009), para 5.4.

13.7. Although all the units that handle CONFIDENTIAL material and that were visited in the revisit have some degree of access to the CONFIDENTIAL infrastructure, this is not the case across the entirety of HMRC's law enforcement entities. One CI office has been informed that there are insufficient funds to install the CONFIDENTIAL infrastructure into the building. Consequently, inevitable security breaches occur, such as the completion of CONFIDENTIAL marked template documents on RESTRICTED, and the inevitable under-classification of documents that should be CONFIDENTIAL.

13.8. Another IT issue has been identified during the revisit. It has become apparent that SMUs are creating and transmitting small quantities of SECRET material on the CONFIDENTIAL infrastructure, which is not accredited to hold such material. CHIS-OPS management have highlighted their concerns about the current situation to the RIS Data Guardian and have proposed that either a bespoke SECRET network is developed, or, in the short term, authorisation is sought for them to encrypt the material and transmit it on the CONFIDENTIAL infrastructure. At present, such authorisation has not yet been secured, and is being considered by RIS senior managers. Given the inherent duty of care issue that would arise from this material being compromised, it is imperative that this issue is resolved urgently.

Additional Recommendation 18
HM Inspector recommends that HMRC devise an urgent secure resolution to address the electronic transmission of SMU SECRET material.

Recommendation 14

HM Inspector recommends that HMRC re-evaluate the protective marking and transmission of Human Contact Reports.

Background

14.1 The original inspection outlined how HMRC's Human Contact Reports (HCRs), which contain details of members of the public who pass information to HMRC (HumInts) as well as details of the person accused of criminality, are classified as RESTRICTED and are transmitted within the Department on the standard IT network. As Covert Human Intelligence Sources' (CHIS) true identity is classified as SECRET, and as some HumInts may be later authorised as CHIS, the report highlighted that "there is an argument that HCRs should be classified at least at CONFIDENTIAL level."[34]

Action Taken

14.2 RIS-CIG CHIS-OPS management took the lead on addressing this recommendation. In June 2009, they emailed CIG management and informed them that if they accepted the recommendation and made HCRs CONFIDENTIAL, all HMRC staff would have to be given access to the CONFIDENTIAL IT infrastructure and be security cleared to SC level. It was also highlighted that providing CONFIDENTIAL infrastructure solely to the SPOCs who email HCRs to the National HumInt Centre would not resolve the issue, as the transmission of the HCR to the SPOC would still be on a RESTRICTED network. CIG management determined that this email constitutes the re-evaluation of the security marking required by the recommendation, and therefore the co-ordinator of the *GPMS Action Plan* was informed that :

> *HMRC have re-evaluated the protective marking and transmission of Human Contact Reports. HMRC will not be implementing this recommendation due to financial / IT infrastructure issues i.e. HMRC needs the HumInt system to be available to the widest possible number of HMRC staff to make it effective.*[35]

The recommendation was also added to the RIS Issues Register, outlining an aspiration to move all HumInt / HCR activity to the CONFIDENTIAL infrastructure for RIS/HMRC.

14.3 During the revisit, CHIS-OPS management confirmed their position. They stated that although HCRs would benefit from being classed as CONFIDENTIAL, as they hold true identity material, there is no IT infrastructure in place to allow the recommendation to be implemented; that it would be cost prohibitive to extend the CONFIDENTIAL infrastructure to all staff; and that transmitting the material in hard copy would incur delays and additional costs and would be less secure than transmitting it over the RESTRICTED IT network. They also highlighted the importance of ensuring that the HumInt system is utilised by the whole Department, and the consequent CPIA and duty of care risks that would incur if access was limited.

[34] HMIC (July 2009), p.26.
[35] HMRC, *HMRC (HMIC) GPMS Action Plan.* Unpublished.

Impact

14.4 The decision not to mark the HCRs CONFIDENTIAL was based on CHIS-OPS management's views of what the resourcing impact would be. There has been no documented, thorough assessment of the impact that the inadvertent loss or interception of an HCR would have on the HumInt, or whether the current RESTRICTED marking is the most appropriate of the following:

RESTRICTED	**cause substantial distress to individuals;**
CONFIDENTIAL	**prejudice individual security or liberty;**
SECRET	**threaten life directly.**

However, the expressed view that "HCRs would benefit from being classed as CONFIDENTIAL" indicates that there is an awareness of the inappropriateness of the current marking.

14.5 CHIS-OPS management conducted no consultation with internal stakeholders (such as CHIS-Ops practitioners, S&BC or RIS Security and Standards) to discuss their views on the appropriate classification. Equally, no other Government department or law enforcement body was consulted to identify other possible solutions to transmitting large volumes of CONFIDENTIAL material. There was also no evaluation of:

- the risks of staff handling and securing printed HCRs in accordance with RESTRICTED rather than CONFIDENTIAL requirements;
- whether separating the HumInt's and accused's details onto separate documents would reduce the requisite classification;
- whether encrypting or password protecting the HCR would mitigate the impact;
- whether, in reality, the approved method of transmitting CONFIDENTIAL material through track and trace would be less secure than emailing them over the RESTRICTED network.

14.6 By tacitly recognising the inappropriateness of the current marking, CHIS-OPS management has, in effect, accepted the risk. However, there is no evidence that either the Director RIS or Director General E&C, as the heads of the business stream that holds the risk, have been involved in this decision. It is not featured on the RIS Risk Register or E&C Risk Register and is not subject to any form of structured risk management. There is also no evidence that the Departmental Security Officer has been informed of the decision, even though any decision to breach S&BC policy has to be signed off at that level.

14.7 After SP&P were informed of CHIS-OPS's approach, the recommendation was removed from the RIS Issues Register. There is no evidence of any work being conducted to realise the quoted aspiration of making the HumInt process CONFIDENTIAL.

14.8 HMIC recognises that HMRC is unable to instigate highly resource intensive solutions to this issue (such as expanding the CONFIDENTIAL infrastructure to all staff), and also recognises that in order to fulfil its CPIA obligations all staff need access to the HumInt system. However, given the serious consequences

that could result from the compromise of a HumInt identity, it is imperative that all possible solutions to the secure transmission of this material are explored, even if this requires the re-design of the HumInt system. If there truly is no solution to overcome the problem and the current procedure is continued, this risk must be owned, accepted and actively managed at the appropriate level, and HumInts advised of that risk.

Recommendation 15

HM Inspector recommends that HMRC, as a matter of urgency, undertake any work required to ensure that the CONFIDENTIAL infrastructure gains accreditation.

Action Taken

15.1. One stream of the Spectrum Project focuses on gaining internal accreditation for the CONFIDENTIAL infrastructure. Through working to address the issues highlighted in S&BC's *CONFIDENTIAL Infrastructure Remedial Action Plan*, interim accreditation has been obtained and is extant until September 2010. The plan is that external accreditation standards for XGSI connectivity will be achieved by this time and a submission for full internal accreditation will accompany connection to the XGSI network. If there is any slippage in these timings, the Spectrum Project Team is able to seek an extension to the interim accreditation from S&BC.

Impact

15.2. The effective action undertaken by the Spectrum Project Team has ensured that the CONFIDENTIAL infrastructure has gained and maintained interim accreditation.

Recommendation 16

HM Inspector recommends that HMRC introduce a structured assurance regime for GPMS compliance with corporate responsibility at a senior management level to enforce the importance of GPMS.

Action Taken

16.1 S&BC were charged with lead responsibility for actioning this recommendation. However, due to resourcing cuts within the Directorate, the planned S&BC Assurance Programme was suspended. In the long term S&BC look to reinstate this, but wholesale assurance does not currently feature in the S&BC Business Plan. In the absence of central assurance, responsibility for security assurance rests with individual directorates and Internal Audit.

16.2 The Poynter Review recommended that HMRC introduce a corporate approach to risk management of security. A new corporate governance and assurance structure at EXCOM level down has been developed. This is designed to address all security risks, with a line of sight from the top to the bottom of the organisation. GPMS is implicit rather than explicit within this new structure. The importance of GPMS has not been specifically championed from a senior management level in the way that other security issues have been. The new structure is predicated upon each directorate's Security Management System, which outline the policies, procedures and controls through which the directorate manages its security risks. These feed into the directorate's Statement of Internal Controls and then into risk registers for each business (such as E&C). These are in turn managed by the Corporate Risk Champions and the EXCOM-led Corporate Risk Management Group.

16.3 This high-level governance structure has been in development since, but not in response to, the original inspection. However, the assurance activity that underpins it at a directorate level is largely unchanged since 2008. Within E&C, each directorate's Enforcement Management Assurance Framework (EMAF), discussed in the 2008 report, remains the primary assurance tool. Through EMAF, managers and BAMs RAG score a wide range of specified risks, to determine the frequency of assurance that each require. Even if a particular risk is scored "Green", the Framework still mandates six-monthly assurances. Therefore GPMS assurance (which features as a minimum control measures to address EMAF's specified 'Data Security' consolidated risk) should, in theory, be undertaken by all of HMRC's law enforcement entities at least twice a year.

16.4 RIS-CIG are currently developing an electronic assurance system (SMART). This will mandate staff to conduct compulsory assurances to underpin EMAF, and create a searchable record to inform managers and RIS Security and Standards of the assurances that have been completed and any that are outstanding.

16.5 Within CI, there are further assurance mechanisms. BAMs conduct bespoke assurance activity on the highest EMAF risks, and on specific topics highlighted by local management. SP&P continue to conduct security audits across the estate. While these do not specifically focus upon the actual marking of material, their remit does cover some GPMS-related issues, such as compliance with storage, clear desk, whiteboard and waste disposal policies. Similar assurances are not conducted within RIS-CIG. There are also the local assurance mechanisms in place within CHIS-OPS and CI ST (mentioned above, Paragraphs 8.1 and 3.6).

Impact

16.6 As is outlined elsewhere in this report, HMRC's law enforcement entities' compliance with the requirement to protectively mark material in accordance with GPMS has not materially improved since the original inspection. It is clear, therefore, that the assurance measures in place, especially around the physical marking of assets, are not uniformly effective. In some CI branches, actions to 'assure' the application of GPMS are limited to ensuring staff have received security training and guidance; in others, EMAF assurance is in hiatus. Furthermore, no specific national BAM assurances of GPMS have taken place since the original report. In RIS-CIG, there is no evidence that local management are effectively assuring the EMAF Data Security risk.

16.7 The paucity of assurance is in large part due to the importance of GPMS not being effectively communicated to staff. Moreover, given the lack of clear guidance on how (or even if) documents should be protectively marked,[36] many staff and managers tasked with conducting assurance lack knowledge of the standards against which such assurances should be benchmarked. It is impossible for effective assurance to be undertaken until this is resolved.

[36] See above, Recommendations 1 and 2.

Consideration 1

Consideration should be given to mandating the marking of all CI, RIS-CIG and Detection folders or files containing material that requires a GPMS marking with the same marking as the highest level of the document it holds.

Background

C1.1. At the time of the original inspection, the Cabinet Office GPMS guidance did not mandate the marking of folders and files containing protectively marked material. This was addressed with the introduction of the *SPF*, which states that "a file, or group of protectively marked assets, must carry the protective marking of the highest marked document or asset contained within it".[37]

Action Taken

C1.2. The lack of consistency across HMRC's security instructions that is discussed above[38] is also evident in respect of this requirement. While the *Security Zone* reflects the new *SPF* policy stating that "a file or compilation of documents must be protectively marked to at least the level of the most sensitive documents it contains"[39], the *SBCPSG* only mentions this specifically in relation to SECRET and TOP SECRET material.[40]

C1.3. Within HMRC's law enforcement entities, there is no evidence that any proactive activity has been undertaken to address Consideration 1. Although a member of CI SP&P was appointed lead contact for this consideration in December 2008, they remained unaware of this responsibility until the issue was raised by HMIC during the revisit. Subsequently, CI SP&P has determined that the issue falls outside this person's work area and has conferred responsibility for leading on this consideration to the CI Data Guardian.

C1.4. Similarly, RIS-CIG had not looked to address Consideration 1 until midway through the revisit, when RIS Standards and Security management simply tasked a member of staff to examine what the Departmental policy states. There is also no evidence of Inland Detection seeking to address this consideration.

Impact

C1.5. HMRC's law enforcement entities remain systemically non-compliant with the requirements to mark folders. This is unsurprising, given the inconsistent instruction contained within the Departmental guidance and the lack of activity undertaken by HMRC's law enforcement entities in this regard. There were isolated patches of good practice witnessed during the revisit. For example, one unit, upon being informed that they were to be examined as part of the revisit, introduced a folder-marking policy and marked all relevant folders prior to HMIC's arrival. However, with the exception of this team and one SMU that appropriately marks the folders containing its SECRET material, no marked folders were seen in any of the locations visited.[41]

---

[37] Cabinet Office, *Security Policy Framework* (*Online).* Available at http://www.cabinetoffice.gov.uk/media/111428/spf.pdf.
[38] See above, Recommendations 1 and 2.
[39] HMRC, *Security Zone.* Unpublished.
[40] HMRC Security and Business Continuity, *SBCPSG 5405: Guidance: Protective Marking System: Protectively Marked Assets Working With: Registering and Filing Documents.* Unpublished.
[41] As the Containers National Intelligence Unit has been disbanded and the Revisit did not examine either its successor or the National Source Unit, it is unclear whether the good practice that was highlighted in these locations during the original inspection is being continued.

Consideration 2

Consideration should be given to locating all CI, RIS-CIG and Detection units that regularly handle CONFIDENTIAL, SECRET and TOP SECRET material in lockable offices with additional entry security systems such as privacy locks and swipe-cards.

Action Taken

C2.1. In respect of this consideration, the *GPMS Action Plan* largely replicates the entry for Recommendation 12, stating that "*agreed accommodation standards are already in place. All CI sites are in access controlled areas and have sufficient lockable storage, property stores and more secure cabinets for material confidential and above*".[42] The CI *Accommodation Specifications* state that CI office areas should be controlled by proximity readers, which provide individuals with limited access to designated areas.[43]

C2.2. Since the original report, the CI estate has been consolidated. Although not in a direct result of this consideration, the consolidation process resulted in a number of teams based in offices that lacked electronic locks being relocated to accommodation that met the CI Accommodation Standards.

C2.3. SP&P states that following the CI Accommodation Consolidation Project, Custom House London is the only location where some CI offices are not secured by swipe-cards or privacy locks. SP&P had sought to address this, asking ESS in 2009 whether such locks could be installed. This proved unachievable because building regulations prohibit changes to the fabric of listed buildings, such as Custom House, and because of health and safety considerations. As there is no capacity within the other building in the CI London estate, CI has been unable to relocate staff. Instead, SP&P states that the security risk is managed through exterior building security, measures to secure visitor access, the presence of security guards and adherence to the clear desk policy.

C2.4. In October 2009, SP&P asked CI BAMS to provide assurances that their branches were compliant with this consideration, and no non-compliance was reported.

C2.5. Within RIS, Standards and Security has focused its attention on addressing security concerns at the HMRC building in Gravesend. Two reviews of this building's security have been commissioned by RIS Standards and Security and undertaken during the last year. Both highlight serious concerns with the physical security of accommodation, especially at the SMU. Although the SMU offices are secured with keypad locks, the door does not meet requirements. The reviews also outline that the SMU is located on the ground floor – a practice highlighted as a concern in the original inspection report, and against ACPO advice. The reports also deemed that the SMU had inadequate perimeter security and required considerable upgrades to the alarm systems, walls and windows to raise the security of the offices to an acceptable level. Given the scale of the upgrades required, the latest review recommends that the SMU is moved to currently unoccupied first floor offices within the building. At the time of writing, RIS Standards and Security are still in negotiations with ESS to progress this issue. In

[42] HMRC, *HMRC (HMIC) GPMS Action Plan*. Unpublished.
[43] CI Accommodation Standards.

the interim, some CONFIDENTIAL and SECRET SMU documents have been relocated to other, more secure RIS sites.

Impact

C2.6. The three CI teams visited during the revisit are located in offices with either swipecard or privacy lock access, and as far as HMIC is aware, Custom House London remains the only building where some CI offices are not secured in this way. CI SP&P are encouraged to periodically re-evaluate whether changes in staffing at other London offices could facilitate the relocation of CI staff from Custom House London to more appropriate accommodation.

C2.7. With the exception of the International SMU, which is located in Custom House London, all the RIS-CIG offices visited during the revisit met the requirements outlined in the consideration. RIS has been proactive in looking to address the Gravesend issues and has understandably prioritised action there. Given limited resources, physical security issues at other parts of the CIG estate (such as Manchester SMU's ground floor location) are not being actively addressed until the Gravesend issues are resolved.

Consideration 3

Consideration should be given to equipping all CI, RIS-CIG and Detection offices with Brent telephones in an environment where conversations cannot be overheard.

Action Taken

C3.1. As with Recommendation 12 and Consideration 2, the *GPMS Action Plan* infers that the pre-existing CI Accommodation Standards address Consideration 3. It states that agreed accommodation standards are already in place and that "all CI sites are in access controlled zones and have Brent phones securely housed".[44] According to the Accommodation Standards, Brents are located in secure communications rooms such as managers' offices.

C3.2. In October 2009, CI SP&P asked CI BAMS to provide an assurance that their branches were compliant with this consideration. These were duly supplied. This request aside, there is no evidence that any further action has been taken by SP&P in respect of Consideration 3.

C3.3. Within RIS, a report from CESG (the national technical authority for information assurance) precipitated an internal inspection of encrypted telephony and IT across the RIS estate. This focused on whether the Directorate complied with the CESG and the Cryto-Custodian's requirements for the standard of building, pass and staff security in Brent sites. Although it did not specifically examine whether calls could be overheard, it did identify two locations where this was possible.

C3.4. Inland Detection do not currently make any calls they consider, under their understanding of the GPMS definitions, to be CONFIDENTIAL. Therefore, they do not have any Brent telephony, and are not actively looking to acquire it.

Impact

C3.5. Brent telephony is still not located in all RIS-CIG or CI offices in places where conversations cannot be overheard.

C3.6. Until recently, all CI operational offices were equipped with Brents. The UKBA de-merger, however, has resulted in the Brent in one CI office becoming a UKBA asset. While CI officers are still permitted to use it, CI does not therefore currently have its own secure telephony in this location.

C3.7. The original report highlighted that some SMUs lack direct access to Brents. This remains apposite, as three SMUs still lack secure telecoms. In two of these locations, staff are able to use Brents in the co-located CI offices. In the third, the handlers and controllers have no access to Brents, although the team SO, located remotely, does have such equipment. Despite the CI Accommodation Standards and the assurances provided by CI BAMS that the Directorate is compliant with this consideration, issues remain about the citing of Brents. Many of CI's Brents are located in managers' offices, in line with the CI Accommodation Standard. However, in one CI office visited, additional Brents were also located in the team's open-plan accommodation, where calls could be overheard. This was also the case in the RIS-CIG Case Development Teams (CDT) and one of the three SMUs

[44] HMRC, *HMRC (HMIC) GPMS Action Plan*. Unpublished.

examined. Even though such calls can only be heard by other members of the team, they do not necessarily need to hear this information. By definition, therefore, this situation cannot fully comply with the ‘need to know’ principle that underpins GPMS.

Consideration 4

Consideration should be given to removing the requirement for the creation of CONFIDENTIAL, SECRET and TOP SECRET material to be authorised.

Background

C4.1. At the time of the original inspection, HMRC's DSSM stated that the production of CONFIDENTIAL material had to be authorised by a Higher Officer or above, whereas SECRET and TOP SECRET material required at least Senior Officer (SO) authorisation.

Action Taken – S&BC

C4.2. The requirement previously outlined in the DSSM has been retained in HMRC's new *SBCPSG*.[45] S&BC senior management feel that this guidance remains valid, as it keeps SO and Grade 7 managers across HMRC aware of the CONFIDENTIAL and SECRET material produced by their teams, thus enabling them to ensure requisite procedures, storage and assurances are in place to manage this. S&BC managers also claim that it acts as a safeguard against staff over and under marking documents.

Action Taken – Law Enforcement Directorates

C4.3. In response to this consideration, CI concluded that authorising the creation of material marked CONFIDENTIAL or higher "serves little or no benefit"[46] for the Directorate. Consequently, in December 2009, SP&P indirectly contacted S&BC management, through the S&BC Helpdesk, asking for the requirement to be removed. In response, in January 2010, S&BC emailed SP&P, outlined the reasons for authorisation, and stated:

> *this approach…is designed for the entire HMRC Department. However, it is guidance, not a standard and should you want to document alternative guidance containing an alternative rationale for your directorate that would be acceptable.*[47]

C4.4. There is no evidence that CI SP&P has actively pursued this issue since January 2010, or effectively outlined to S&BC the scale of the impact this would have within law enforcement entities. Because of CI's lead in addressing this consideration, neither RIS-CIG nor Inland Detection has taken any action in respect of it.

C4.5. During the revisit, S&BC senior managers reiterated to HMIC that CI and HMRC's other law enforcement entities are entitled to derogate from this guidance. Once they recognised the volume of CONFIDENTIAL material produced in some CI and RIS-CIG units, an S&BC senior manager acknowledged the problems that the guidance would pose to them and stated they would contact CI and RIS to discuss the issue. It is unclear whether this has occurred.

[45] HMRC, Security and Business Continuity *SBCPSG5325 – Guidance: Protective Marking System: Protectively Marked Assets Working With: Choosing the Correct Level of Marking.* Unpublished.
[46] HMRC, *HMRC GPMS Report (by HMIC) Action Plan.* Unpublished.
[47] *ibid.*.

Impact

C4.6. HMIC recognises the benefit of maintaining the policy for most staff across the wider HMRC who rarely, if ever, are required to create CONFIDENTIAL, SECRET or TOP SECRET material. It is disappointing, however, that local guidance has not been devised in CI and RIS-CIG, as per the consideration.

Appendix

2008 Report Recommendations and Considerations

Recommendation 1
HM Inspector recommends that CI, RIS-CIG and Detection introduce a policy that mandates staff to mark all protectively marked documents and data upon its creation. This will obviously have implications across the whole Department

Recommendation 2
HM Inspector recommends that CI, RIS-CIG and Detection consult with ACPO and other UK law enforcement agencies to produce a consistent GPMS policy and guidance that is relevant to law enforcement activity

Recommendation 3
HM Inspector recommends that HMRC ensure that all SECRET documents produced by CI, RIS-CIG and Detection are fully compliant with GPMS

Recommendation 4
HM Inspector recommends that HMRC introduce mandatory requirement for all CI, RIS-CIG and Detection IT traffic to be GPMS marked before transmission

Recommendation 5
HM Inspector recommends that HMRC ensure that all HMRC law enforcement template stationery and forms are marked in compliance with the regulations outlined in the DSSM

Recommendation 6
HM Inspector recommends that the protective marking of printed documents including Day Books, Notebooks and Case Decision Logs are suffixed “when completed”

Recommendation 7
HM Inspector recommends that HMRC ensures all CI, RIS-CIG and Detection audio tapes and photographs are protectively marked in accordance with GPMS

Recommendation 8
HM Inspector recommends that HMRC ensures all CI, RIS-CIG and Detection units that handle TOP SECRET and SECRET material maintain a Register for Protectively Marked Documents SECRET and TOP SECRET

Recommendation 9
HM Inspector recommends that CI and RIS-CIG devise a policy, in line with the requirements of DSSM 11070, to review the markings of protectively marked assets

Recommendation 10
HM Inspector recommends that CI, RIS-CIG and Detection ensure that protectively marked waste is appropriately secured or shredded.

Recommendation 11
HM Inspector recommends that HMRC ensure operational information displayed on whiteboards is appropriately secured to reflect its GPMS status

Recommendation 12
HMRC make sufficient cabinets of the appropriate specifications available for all staff in CI, RIS-CIG and Detection who handle GPMS marked material and that combinations are regularly changed in accordance with instructions

Recommendation 13
HM Inspector recommends that HMRC make the CONFIDENTIAL infrastructure available to all staff within CI, RIS-CIG and Detection

Recommendation 14
HM Inspector recommends that HMRC re-evaluate the protective marking and transmission of Human Contact Reports.

Recommendation 15
HM Inspector recommends that HMRC, as a matter of urgency, undertake any work required to ensure that the CONFIDENTIAL infrastructure gains accreditation

Recommendation 16
HM Inspector recommends that HMRC introduce a structured assurance regime for GPMS compliance with corporate responsibility at a senior management level to enforce the importance of GPMS

Consideration 1
Consideration should be given to mandating the marking of all CI, RIS-CIG and Detection folders or files containing material that requires a GPMS marking with the same marking as the highest level of the document it holds

Consideration 2
Consideration should be given to locating all CI, RIS-CIG and Detection units that regularly handle CONFIDENTIAL, SECRET and TOP SECRET material in lockable offices with additional entry security systems such as privacy locks and swipe cards

Consideration 3
Consideration should be given to equipping all CI, RIS-CIG and Detection offices with Brent telephones in an environment where conversations cannot be overheard

Consideration 4
Consideration should be given to removing the requirement for the creation of CONFIDENTIAL, SECRET and TOP SECRET material to be authorised.