Inspection of HM Revenue & Customs

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

HMI Denis O'Connor

Denis O'Connor CBE QPM
HM INSPECTOR OF CONSTABULARY
Ground floor, Allington Towers, 19 Allington Street, London, SW1E 5EB
Tel: 0207 035 5713 Fax: 0207 035 5184 Mobile: 07901 716197
Email: Denis.O'Connor@homeoffice.gsi.gov.uk

Rt Hon Stephen Timms MP
Financial Secretary to the Treasury
HM Treasury
1 Horse Guards Road
LONDON SW1A 2HQ

15th October 2008

Dear Minister

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

Please find attached a copy of my inspection report relating to the compliance of the Criminal Investigation Directorate, the Risk and Intelligence Service Criminal Investigation Group and the Detection Directorate of HM Revenue & Customs (HMRC) with the Government Protective Marking Scheme (GPMS). The report raises sensitive issues, which may require the drafting of a redacted version for publication and these matters will be considered by HMRC legal advisers.

In response to the loss of data relating to child benefit recipients in November 2007 the Government commissioned Kieran Poynter to investigate security processes and procedures for data handling within HMRC. In addition, the Cabinet Secretary was charged with conducting a review to ensure that all Government departments and agencies reviewed their security procedures in relation to the storage and use of data. As the GPMS underpins the protective marking and control of material across Government it was considered that an inspection of the law enforcement entities of HMRC in this regard would complement and add-value to the efforts to improve security.

HMRC fully co-operated with the inspection team and showed a deep resolve to address any security shortcomings that were identified. Although the inspection focused upon the law enforcement elements certain issues were identified that affected the wider department. A fundamental one related to the adoption of a baseline marking of PROTECT whereby HMRC chose not to protectively mark material at that level. This was contrary to the Cabinet Office Manual of Protective Security. The Security and Business Continuity directorate of HMRC acknowledged this and agreed that they would seek to take steps to address the situation despite the potential implications caused by the bulk of material that they handled.

As the Criminal Investigation (CI) Directorate were familiar with handling sensitive material their security in this regard was, in general, to a satisfactory standard and in those areas that dealt with STRAP material a robust assurance regime was in place. A

lack of suitable storage facilities for protectively marked material by CI operational teams was identified as requiring urgent attention as was the inadequate physical security at certain of their offices however these are primarily estate issues.

The inspection noted that there needed to be a more consistent approach to GPMS policy and guidance across UK law enforcement particularly in the area of serious and organised crime investigation and to that end it was recommended that HMRC discuss the issue with ACPO and others.

I am pleased to note that HMRC have already taken steps to address a number of issues raised in the inspection following the submission of the draft report. This includes the CONFIDENTIAL IT infrastructure which, at the time of inspection, was not accredited and thereby potentially undermined the credibility of HMRC criminal justice activity. Interim accreditation has since been obtained and remedial work undertaken with the aim of full accreditation as soon as possible.

I am forwarding a copy of the final report to Mike Clasper, HMRC Chairman and to Mike Eland, HMRC Director-General Enforcement & Compliance.

Yours sincerely,

Denis O'Connor
HM Inspector of Constabulary

HM Treasury, 1 Horse Guards Road, London, SW1A 2HQ

Denis O'Connor CBE QPM
HM Inspector of Constabulary
Allington Towers
London
SW1E 5EB

8 **December 2008**

Dear Mr O'Connor

HMIC Inspection into the compliance of HM Revenue & Customs' law enforcement entities with the Government Protective Marking Scheme

Thank you for your letter of 15 October 2008 together with a copy of your report *The compliance of HM Revenue & Customs' law enforcement entities with the Government Protective Marking Scheme.*

I am pleased to say that HMRC accepts your recommendations and as you note in your letter, had already begun to address some of the issues raised, whilst your report was in draft. HMRC now has a plan through which all recommendations will be addressed and implemented.

I am copying this letter to Mike Clasper, the HMRC Chairman, and to Mike Eland, HMRC Director-General of Enforcement and Compliance.

Yours sincerely,
Stephen Timms

RT HON STEPHEN TIMMS

Contents

Executive Summary

I As organised crime has become more sophisticated, particularly in terms of identity fraud, there is increasing concern about the vulnerability of personal data. This was brought into sharp focus, in October 2007, by HM Revenue & Customs' (HMRC) loss of two disks containing personal details of 25 million child benefit recipients. In response to this, the Government commissioned security reviews of procedures for handling personal data, both across HMRC and wider Government.

II Following further highly publicised data losses by other Government Departments, HMRC commissioned HMIC to conduct an inspection of the Department's law enforcement entities' compliance with the Government Protective Marking Scheme (GPMS); recognising that this would be valuable in informing its re-evaluation of data security procedures.

III The GPMS, which is derived from the Manual of Protective Security (MPS) produced by the Cabinet Office, is considered to be the bedrock on which security standards across Government are set in relation to information, personnel, IT and communication security[1]. GPMS creates a mandatory baseline control for sensitive assets, which includes the marking of such material in order that it may receive the appropriate level of protection. Government Departments and Agencies must develop their own security policies, tailored to their own business needs, and based upon the minimum standards laid down in the MPS. Within HMRC, the responsibility for security policy lies with Security & Business Continuity (S&BC), who produce the Departmental Security Standards Manual (DSSM).

IV The inspection highlights a fundamental shortcoming in the interpretation by HMRC of the GPMS. HMRC has created a policy that sets a baseline protective marking for sensitive documentary and other assets. Through this, HMRC only stipulate the physical marking of an asset if its sensitivity requires a protective mark above the baseline. This policy is based upon the Department's consideration that it would be impractical to mark all the sensitive material it handles. This creates a situation whereby three levels of material are unmarked, which seriously undermines the core principle of GPMS: that sensitive material requires protection and should be conspicuously marked. Conversely, although some material is afforded a degree of data security on the basis that it is classified as Sensitive, under the Criminal Procedure and Investigations Act 1996 (CPIA) definitions; this does not correlate with the GPMS.

V As a result of the data loss, HMRC have initiated an ambitious training programme on data security. However, this has been hampered by outdated guidance in the DSSM. Furthermore, the training continues to perpetuate a fundamental misconception that sensitive material that remains within an office does not require protective marking.

VI It is also evident that there is a lack of clear guidance to assist HMRC's law enforcement officers with their assessment of GPMS classifications. This has consequently led to an inconsistent application of the GPMS markings across and within CI, Risk & Intelligence Service - Criminal Intelligence Group (RIS-CIG) and Detection. This situation reflects wider inconsistencies of interpretation across the UK law enforcement sector. Consultation is required between law enforcement agencies and departments to facilitate the development of holistic GPMS definitions and guidance to ensure a commonality of application across law enforcement.

VII In addition to the concerns around HMRC's policy and guidance, the inspection has also highlighted problems with the Department's infrastructure. The limited availability of secure storage, encrypted telephony and CONFIDENTIAL IT networks significantly impacts on HMRC's law enforcement entities' compliance with the GPMS.

VIII There is no effective management regime to ensure compliance with the GPMS. In addition to the establishment of a credible, robust management assurance framework for the GPMS, it is also essential that senior management enforce the importance of GPMS so compliance becomes embedded in the culture and the working practices of staff.

IX Although this inspection has a law enforcement focus, HMRC may wish, where applicable, to translate the points raised into a wider context. Given the potential challenges involved, it is considered impractical to retrospectively apply protective marking procedures. However, with the spotlight on security across Government it is vital that the significance of GPMS is fully understood and a regime established to implement and develop it. The risk of not doing so could have severe repercussions, affecting both the reputation of HMRC and Government integrity.

X This inspection has found that HMRC's law enforcement entities' compliance with GPMS is poor. Commendably, since the data loss, it has made significant efforts to address data security. Furthermore, during the inspection, no evidence was found of staff breaching the requirements for the transmission of hard copy protectively marked material. The challenge for the Department now is to apply the same rigour and determination to improve overall GPMS compliance.

Recommendations

HMIC recommends that:

1 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;

[1] Subsequently, the MPS has been updated by HMG Security Policy Framework, published by the Cabinet Office in December 2008.

2 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;

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

4 HMRC introduce mandatory requirement for all CI, RIS-CIG and Detection IT traffic to be GPMS marked before transmission;

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

6 HMRC ensures the protective marking of printed documents including Day Books, Notebooks and Case Decision Logs and Forms are suffixed "when completed";

7 HMRC ensures all CI, RIS-CIG and Detection audio tapes and photographs are protectively marked in accordance with GPMS;

8 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;

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

10 CI, RIS-CIG and Detection ensure that protectively marked waste is appropriately secured or shredded;

11 HMRC ensure operational information displayed on whiteboards is appropriately secured to reflect its GPMS status;

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 on manifold cabinets are changed in accordance with instructions;

13 HMRC make the CONFIDENTIAL infrastructure available to all staff within CI, RIS-CIG and Detection;

14 HMRC re-evaluate the protective marking and transmission of Human Contact Reports;

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

16 HMRC introduce a structured assurance regime for GPMS compliance, with corporate responsibility at a senior management level to enforce the importance of the GPMS.

Considerations:

Consideration should be given to:

1 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;

2 Locating all CI and RIS-CIG units that regularly handle CONFIDENTIAL, SECRET or TOP SECRET material in lockable offices with additional entry security systems such as privacy locks and swipe cards;

3 Equipping all CI, RIS-CIG and Detection offices with Brent telephones in an environment where conversations cannot be overheard;

4 Removing the requirement for the creation of CONFIDENTIAL, SECRET and TOP SECRET material to be authorised.

Chapter 1

Introduction

Origins of the Inspection

1.1 In November 2007, the loss by HMRC of data relating to 25 million child benefit recipients focussed media and political attention on Government procedures for protecting personal data. In response to the loss of the data, the Government commissioned Kieran Poynter, Chairman of PricewaterhouseCoopers to investigate security processes and procedures for data handling in HMRC. In addition, the Cabinet Secretary was charged with conducting a review to ensure that all Government departments and agencies checked their procedures for storage and use of data and that they undertook their own security assessments.

1.2 Whilst HMRC immediately reviewed its data security handling and transmission procedures there was an identified need to look at the compliance with the GPMS within the law enforcement entities, namely Criminal Investigation (CI), Risk & Intelligence Service - Criminal Intelligence Group (RIS-CIG) and Detection, to ensure that the required standards were being met.

Protective Security

1.3 Protective security as defined within the Cabinet Office Manual of Protective Security (MPS) encompasses information security, personnel security, IT security and communication security. The MPS is aligned to the standards relating to information security as laid down by ISO/IEC 17799:2000 (BS7799 Part 1)[2]. These standards enable the MPS to create baseline controls to achieve a minimum level of protection for assets across Government.

1.4 The GPMS, outlined in the MPS, specifies the classification and protection of assets. The Scheme is a mandatory baseline for the classification of all types of sensitive assets and has five levels of protective marking. The Scheme was devised for National Security purposes and the original four classifications of RESTRICTED, CONFIDENTIAL, SECRET and TOP SECRET[3] are still known as such, although it is widely recognised that they are now utilised in respect of assets that fall outside this narrow remit. Since 2007, a sub-national security marking called PROTECT has also been introduced to cater for official information that requires protection but does not need to meet the criteria for national security information at the RESTRICTED level.

1.5 Government departments, agencies and UK law enforcement bodies are responsible for developing their own security policies based upon the standards set by the MPS. They are expected to adapt the GPMS to meet their own business requirements without diluting the MPS minimum standards for the creation, marking, handling, receipt, transmission and storage of material.

[2] This refers to the international standard for information security developed by the International Organisation for Standardisation, which is the accepted authority for standards throughout the European Union.

[3] For the MPS's definitions of the five GPMS classifications, see Annex C.

Chapter 2

Policy and Guidance

2.1 This chapter examines and evaluates, in turn, the:

- HMRC's Departmental GPMS Guidance;
- guidance produced following the Department's data loss;
- specific guidance and training provided to meet the needs of its law enforcement staff

It further highlights the:

- interpretation by HMRC of a key aspect of GPMS as being a fundamental barrier to Departmental compliance with the intended objectives of the Scheme;
- inconsistencies between various current guidance;
- problems inherent in the specific focus of recent instructions;
- need to develop bespoke guidance for staff working across the UK law enforcement community.

HMRC's Departmental Security Standards Manual

2.2 In HMRC, Security and Business Continuity is responsible for tailoring the MPS's guidance for the needs of the Department. This is contained within the departmental security rules known as the Departmental Security Standards Manual (DSSM). This inspection raises concerns with key aspects of the GPMS guidance included in the DSSM that seriously limit CI, RIS-CIG and Detection staff's ability to comply with the principles of GPMS.

Non-marking of Protectively Marked Material

2.3 The MPS states that, where practicable, the protective marking on an asset must be conspicuous so that its sensitivity is clearly seen, however, in some instances it may not be possible or practicable to physically mark or label assets. HMRC interpret this key element of the MPS in a way that fundamentally differs from the Cabinet Office and other major government departments and law enforcement agencies. HMRC has determined that due to the large volume of taxpayer information that they hold, which merits a RESTRICTED marking, it would be impractical to physically mark every item. Furthermore, it was determined that RESTRICTED would act as a departmental baseline marking and that only material requiring a higher classification would have to be marked. Following the introduction of the new PROTECT marking, the DSSM was amended to lower the departmental baseline to PROTECT.

2.4 Whilst the issue of practicability is clearly subjective, neither the Cabinet Office, HM Treasury, nor any other government department or agency approached

during this inspection interpret the practice of physically marking sensitive documents and data as being 'impractical'. They tend to interpret 'impracticality' as being in respect to assets such as military hardware that should not be marked, as doing so might attract unwanted attention or simply be just impractical. Furthermore, all those consulted see the non-marking of protectively marked documents as going against the concept of the GPMS.

2.5 The security policies of other UK law enforcement agencies also differ from HMRC's DSSM and state that all protectively marked documents should be marked. The Explanation of the Protective Marking System for Police Documents, produced by the Association of Chief Police Officers (ACPO) for the Police Service in England and Wales, instructs staff to include a protective marking on all logs, reports or papers that are produced.

2.6 Although the DSSM stipulates that staff must handle ALL protectively marked assets as if they were marked and protect them to the required level, HMRC's policy of setting a baseline level of classification and not mandating the marking of all sensitive assets has a number of significant implications:

- Firstly, this policy limits HMRC staff's ability to tell if an unmarked document they receive is either non-sensitive or whether it has been assessed to require the baseline protective marking. The guidance contained in the latest draft version of the DSSM, due to be issued in mid 2008, makes the situation even more confusing as it states that certain categories of both RESTRICTED and PROTECT material, including customer folders used in day to day business, should **NOT** show a marking[4]. Consequently, an unmarked document could be PROTECT, RESTRICTED or Not Protectively Marked;
- Secondly, by adopting this policy, HMRC is unable to comply with the MPS's instruction that all PROTECT documents should be accompanied by a suffix, known as a descriptor, such as POLICY or STAFF, which indicates the nature of the sensitivity of the asset[5].

2.7 HMIC recognises that the marking of all protectively marked material generated by HMRC would be a large undertaking and will require modification of numerous computerised systems and databases. However, given the importance of GPMS as the cornerstone of security, HMIC recommends that guidance is produced for HMRC's law enforcement entities, that includes the mandatory marking of all protectively marked documents and data they produce.

RECOMMENDATION 1: HMIC 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.

[4] HMRC SECURITY AND BUSINESS CONTINUITY (2008) Draft version of DSSM1105 – Working with Protectively marked assets: Choosing the Correct Level of Marking. Unpublished. Formatting as appears in the DSSM.

[5] For details of descriptors see Annex C.

Policy and Guidance

Evaluation of Other Guidance Contained in the DSSM

2.8 Notwithstanding the issues highlighted above regarding the problems inherent in the DSSM's guidance on the marking of RESTRICTED and PROTECT assets, it provides detailed guidance and instruction on the handling, transmission and destruction of protectively marked material. In a number of these areas, the guidance in the DSSM is more comprehensive than that contained in the MPS. Moreover, the DSSM guidance is more prescriptive on the way that protected documents should be marked. Whilst the MPS state that markings will be more conspicuous if they are applied in a larger, bolder print than the main text, the DSSM goes further than this instructing staff:

"on paper documents, type or print the markings at the top and bottom of the page using Capital [sic] letters and bold print." [6]

Furthermore, the DSSM mandates MPS's discretionary guidance on additional procedures for the marking of SECRET and TOP SECRET material[7]. HMIC views these aspects of the DSSM's guidance as good practice, however, there are certain areas where the guidance in the DSSM lacks detail and clarity:

- Whilst the MPS states that protectively marked assets sent to overseas organisations and governments must be appropriately marked and that in such cases the protective marking must be prefixed 'UK', the DSSM does not cover this issue. It therefore, is unsurprising that there is no consistent approach by CI and RIS-CIG staff in respect of whether material destined for overseas agencies is marked;[8]
- The DSSM omits MPS's instructions on how assets received from overseas posts or agencies should be handled;
- Although the DSSM provides guidance upon how to handle, transmit and dispose of PROTECT material, it fails to define the PROTECT marking. Consequently a majority of CI, RIS-CIG and Detection officers interviewed expressed confusion as to what constituted a PROTECT document and questioned its relevance in a law enforcement context. This omission is addressed in the draft version of the revised DSSM which includes PROTECT in a table of protective marking definitions, broken down into sub-categories such as international relations and law and order.

Neither the new draft nor the current DSSM include explanatory text or examples of assets handled by the Department that would fall into each of the five protective markings.[9]

[6] HMRC SECURITY AND BUSINESS CONTINUITY (15 February 2008) *DSSM 11030: Working with Protectively Market Assets: How to Show the Protective Marking.* Unpublished.

[7] For details of these requirements, see Paragraph 3.2.

[8] See Paragraph 3.15.

[9] The lack of clarity of the definitions of the GPMS markings outlined in Paragraphs 3.19 to 3.24.

2.9 In addition to these problems, the intranet DSSM is also difficult to navigate. It lacks a clear structure thus making items difficult to find. For example, the requirement to store CONFIDENTIAL material in a combination locked security cabinet or container [10] is outlined in the section of the Manual relating to management security checks but not in the section on storage of protectively marked material. It is, therefore, not surprising that many officers within CI, RIS-CIG and Detection are unaware that CONFIDENTIAL material should be stored in a combination cabinet.[11]

2.10 HMIC understand that HMRC are looking to fundamentally redesign the DSSM to make it more intuitive and user-friendly, however, as the current DSSM is out-of-date and the draft revised version yet to be published there is a gap in up to date guidance.

The Data Security Programme

2.11 Following the loss of the data disks, a Data Security Programme was initiated within HMRC to review data security procedures. One strand of this programme was responsible for the production of a Data Security Booklet. This Booklet, issued to all HMRC staff, summarised and updated various ad hoc security guidance that was published on the HMRC's intranet in the aftermath of the data loss.

2.12 The Booklet provides detailed guidance particularly relating to the new operating standards for transferring protectively marked assets in HMRC. This is supplemented with a 'decision tree' for sending data and four specific examples that explain the procedures in a HMRC context. It also outlines practical examples of departmental material that would necessitate a PROTECT, RESTRICTED and CONFIDENTIAL marking.[12]

2.13 It is commendable that the Booklet provides a good, concise guide on these issues, that it was issued quickly and was supplemented by mandatory training. However, concerns have been raised about aspects of its content. The Booklet has primarily been introduced as a consequence of the data loss and to strengthen procedures under examination by the Poynter Review. As Poynter's focus is on HMRC's practices and procedures in the handling and transfer of confidential data on taxpayers and benefit/credit recipients[13], it is unsurprising that the booklet concentrates on the security of transmitted material. Consequently, many staff erroneously believe that only that material which is going to leave their control requires protection under GPMS. This message is reinforced by the current data security workshops that followed the issue of the Booklet, in which staff are told that only material that leaves the office requires a protective marking.

[10] HMRC SECURITY AND BUSINESS CONTINUITY (15 February 2008) *DSSM 11080: Working with Protectively Marked Assets: Checks on the Document Control System*. Unpublished.
[11] Issues relating to the storage of material are further explored in Chapter 4. See Paragraphs 4.3 to 4.7.
[12] The booklet also reiterates the departmental interpretation of GPMS that PROTECT documents do not require marking.
[13] See HM TREASURY (23 November 2007) *Terms of reference for the Poynter Review* [online] Available at **http://www.hm-treasury.gov.uk/newsroom_and_speeches/press/2007/press_133_07.cfm.**

2.14 As the Booklet's focus is on addressing the areas that fall within the Poynter Review's explicit remit, the practical examples it provides of how to transfer protectively marked documents in accordance with the new operating standards all relate to personal taxpayer or benefit recipient data. These examples primarily relate to HMRC revenue collection and payment processes. Although this is understandable, since these types of documents are typical of those handled by the large majority of departmental staff who work in processing environments, as with the DSSM, the Booklet does not cater for the specific needs of those HMRC officers working in law enforcement.

2.15 CI, RIS-CIG and Detection staff express confusion as to whether they should follow the guidance in the Booklet or the DSSM. The Booklet specifies that it supplements rather than replaces the DSSM and refers staff to the DSSM for further comprehensive instruction. However, the Booklet's guidance conflicts with the DSSM policy on the transmission of data. Furthermore, other important subjects, such as storage of material, are omitted completely from the Booklet. These factors and the emphasis upon transmission of data have resulted in a lack of clarity in respect to the wider application of the GPMS.

Training

2.16 Within HMRC's law enforcement entities, new recruits to CI undertake Foundation Training, which has replaced the Basic Investigation Course, and those to Detection undertake the National Anti-Smuggling Programme. Both of these require students to pass the mandatory[14] *Security in HMRC* e-learning unit[15]. The aim of the package is to make the student aware of security issues and measures within HMRC, how they can contribute to successful security, and covers other issues, such as building security beyond GPMS. The unit provides guidance that *"The default position is that all HMRC customer information merits at least a PROTECT marking"* and sets individual responsibility to treat information securely when storing, sending, transmitting or disposing of information, warning them that failure to comply with the procedures, rules and instructions, including the DSSM, may lead to disciplinary or even criminal proceedings. Although a law enforcement officer can apply the training to their own particular role, its general guidance is aimed at those working in the taxpayer-facing network, as is reflected in the style of the examples given and the content of the final knowledge test.

2.17 Since the data loss incident, the Department has revised its GPMS training and has introduced, in support of the Data Security Booklet, a Data Security Workshop. This additional training is mandatory for all staff and is to be completed in conjunction with an associated e-learning module. The training is centrally organised but cascaded from Central Training to each of the individual directorates' training teams who have responsibility to adapt to their business area and deliver it to their staff. The workshop is intended to assist the students

[14] The course is mandatory for new staff and highly recommended as refresher training.
[15] Prospectus number 0010931.

to play their part in protecting the Department's data and assets and includes exercises aimed at applying the correct GPMS marker to a range of scenarios. Examples deal with material up to CONFIDENTIAL, which is considered sufficient for the majority of HMRC. Whereas it reflects the earlier discussed *Security in HMRC* e-learning unit, as it instructs that the "default setting is PROTECT", it goes on to confirm that if there is no GPMS marking on a document it is to be treated as having PROTECT status. The training event that HMIC attended advised attendees that any documents that were to be circulated had to have a marker applied to them, but conversely advised that there was no requirement to mark documents that were going to "sit on your desk". Although the training referred to the Data Security Booklet throughout, no mention was made of the additional information that could be found in the DSSM.

The Requirement for Specific Law Enforcement Guidance

2.18 As mentioned above[16], HMRC's internal security guidance does not interpret the GPMS requirements of the MPS for law enforcement practitioners. Due to the size of the Department and pressure upon Security & Business Continuity's (S&BC) resources, the responsibility for bespoke GPMS guidance and policy, tailored to any specific directorate, falls to that business unit. However, at the time of writing, neither CI, RIS nor Detection have produced bespoke policies and there is a lack of understanding across these three Directorates as to their perceived role in producing this.

2.19 The lack of specific guidance for CI, RIS-CIG and Detection staff has been raised as a concern throughout the course of this inspection. This results in a general confusion amongst staff as to how they define the GPMS protective markings. Consequently, differing interpretations are being used across and within the three directorates. In particular, there is general uncertainty amongst officers as to which assets should be classified as RESTRICTED and those that are CONFIDENTIAL.

2.20 The MPS definitions relating to the protective markings specifically related to law enforcement activity, duplicated in the DSSM and other HMRC guidance, are clearly open to interpretation:

Figure 2: GPMS Definitions Specifically Relating to Law Enforcement

Marking	Impact
PROTECT	Prejudice the investigation or facilitate the commission of a crime (depending upon the severity of the circumstances)
RESTRICTED	Prejudice the investigation or facilitate the commission of a crime
CONFIDENTIAL	Impede the investigation or facilitate the commission of a serious crime

[16] See Paragraph 2.14.

For example, whilst the difference between impede and prejudice may be seen as semantic, the issue as to what is a crime or a serious crime requires clarification. Furthermore, how should an asset that is assessed as potentially impeding the investigation or facilitate the commission of a crime or alternatively prejudicing the investigation of a serious crime, be marked? Equally, what severity of circumstances require crime related assets to be marked RESTRICTED rather than PROTECT?

2.21 Officers state that, in the absence of clear guidance, they determine what should be RESTRICTED and what should be CONFIDENTIAL based upon experience or others' advice. The majority of investigation casework and intelligence development within HMRC is currently treated as RESTRICTED by default[17]. However, if one uses the definition of serious crime as being an offence specified in the Serious Crime Act 2007, which includes offences in relation to the public revenue[18] and money laundering, there is scope to infer that the majority of HMRC criminal investigation and criminal intelligence could be categorised as such and therefore cases could be classified as CONFIDENTIAL. Historically, all National Crime Squad cases have been regarded as requiring at least a CONFIDENTIAL marking as they all relate to serious crime. This enforces the need for a consistent interpretation of GPMS across law enforcement agencies.

2.22 Other UK law enforcement agencies have attempted to address the subjectivity inherent in the MPS definitions. ACPO's *Explanation of the Protective Marking System for Police Documents*, provides numerous examples of types of assets that would be appropriate for each level of protective marking. For example, ACPO guidance states that documents relating to on ongoing operations are likely to be at least CONFIDENTIAL because their compromise would impede the investigation of serious crime[19]. The ACPO *Handling Protectively Marked Material – a Guide for Police Personnel*, provides a clearer explanation of PROTECT including that it is "not to be used for operational issues"[20]. Additionally it outlines further criteria related to law enforcement activity that do not appear in MPS. For example material, where the loss could result in, "a breach of statutory restrictions on disclosure of material…"[21] is defined as RESTRICTED.

2.23 In addition to issues surrounding the GPMS definitions of specific assets, there is no clarity across law enforcement agencies relating to 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. Likewise, there is no guidance specifying how original prosecution material and uplifted evidence, which may enter the public domain during court proceedings, should be protectively marked.

[17] Exceptions to this include CHIS related material.
[18] This includes smuggling as specified in S.170 Customs & Excise Management Act 1979.
[19] ACPO (2001) *Explanation of the Protective Marking System for Police Documents*, Page 4 [online]. Available at **http://www.acpo.gov.uk/asp/policies/Data/prot_marking_scheme_report_19feb01.doc.**
[20] ACPO and ACPO's *Handling Protectively Marked Material – A Guide for Police Personnel* Page 2.
[21] ibid.

2.24 Although the GPMS guidance provided by other UK law enforcement agencies to their staff can be viewed as good practice, there are inconsistencies between them. There would, therefore, be clear inherent benefits for all of UK law enforcement if a joint approach to GPMS was adopted. This would ensure, as far as possible, that all sensitive assets are marked and handled in a consistent, GPMS compliant manner. It would be especially beneficial to those assets that are shared or passed between agencies or produced during joint agency initiatives. Any such guidance should look to resolve the definitional uncertainties around the markings and provide robust guidance, along with suitable examples, on the full range of GPMS issues, for all those operating within the UK law enforcement framework. It should also take into account the new definitions outlined in the HMG Infosec Standards.

RECOMMENDATION 2: HMIC 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.

Chapter 3

Production, Marking, Filing, Registration and Destruction of Material

The Marking of Assets

a) SECRET and TOP SECRET

3.1 Although HMRC's policy does not mandate the physical marking of PROTECT and RESTRICTED assets, it does stipulate that all CONFIDENTIAL, SECRET and TOP SECRET material is physically marked. The DSSM also includes further compulsory controls on how SECRET and TOP SECRET material is to be handled:

- Give a serial number to any documents issued in a series;
- Number each page of the document;
- Number each appendix or annex of a document in a separate series to the main text;
- Indicate on every document, its author, title, name of the originating office, reference or copy number and date of publication.[22]

3.2 Whilst TOP SECRET material is not, as a matter of course, generated by HMRC staff in CI, Detection or RIS-CIG, a limited number of SECRET documents are produced by RIS-CIG Source Management Units (SMUs) and Fiscal Crime Liaison Officers (FCLOs). HMRC is inconsistent in its application of the requirements for the SECRET documents it produces. Although the overwhelming majority of those documents viewed during the inspection complied with the first three criteria, very few contained the full details of the author, title and name of originating office.

RECOMMENDATION 3: HMIC recommends that HMRC ensure that all SECRET documents produced by CI, RIS-CIG and Detection are fully compliant with GPMS.

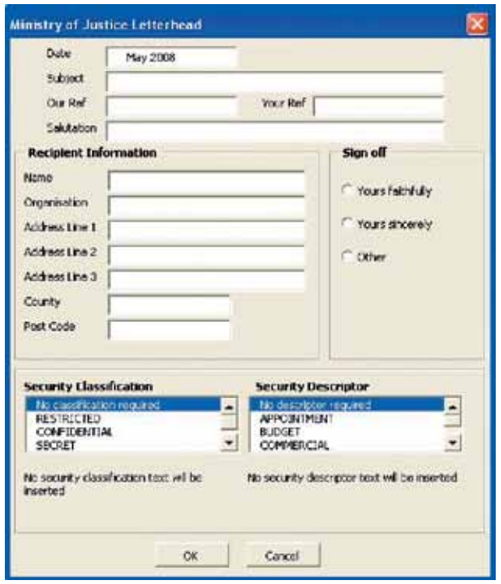
b) Other Protectively Marked Documents

3.3 The DSSM states that the protective marking and descriptor, where appropriate, must be conspicuous, so that the value of the document is shown to those who need to know it. On paper documents, the marking should be typed or printed at the top and bottom of each page using capital letters and bold print.

[22] HMRC SECURITY AND BUSINESS CONTINUITY (15 February 2008). Unpublished.

3.4 HMRC's current departmental stationery accessible from the departmental intranet are locked to prevent the user from editing the document header and footer. This effectively also prevents staff from electronically entering a protective marking on such documents, in line with the requirements outlined above[23]. Although a GPMS marking could be stamped on printed documents, the audit showed no examples of this practice being undertaken. Some other government departments' and agencies' electronic corporate stationery permit staff to edit their headers and footers; however this can lead to inconsistencies of presentation as other aspects of the header's content are also changeable. A more advantageous solution, utilised by the Ministry of Justice amongst others, is to include a GPMS marking as a requisite option when creating a new document from the corporate template. An example of this is shown at figure 3.

Figure 3: Ministry of Justice's Letterhead form



3.5 Although corporate stationery is only occasionally used, email is a key method of communication across CI, RIS-CIG and Detection staff. However, the email software available on the RESTRICTED IT system, used by the majority of staff in these units, does not contain a function to apply a GPMS classification to the electronic message. This is also the case with the CONFIDENTIAL infrastructure used by the Fiscal Crime Liaison Officer (FCLO) Network (METRO).

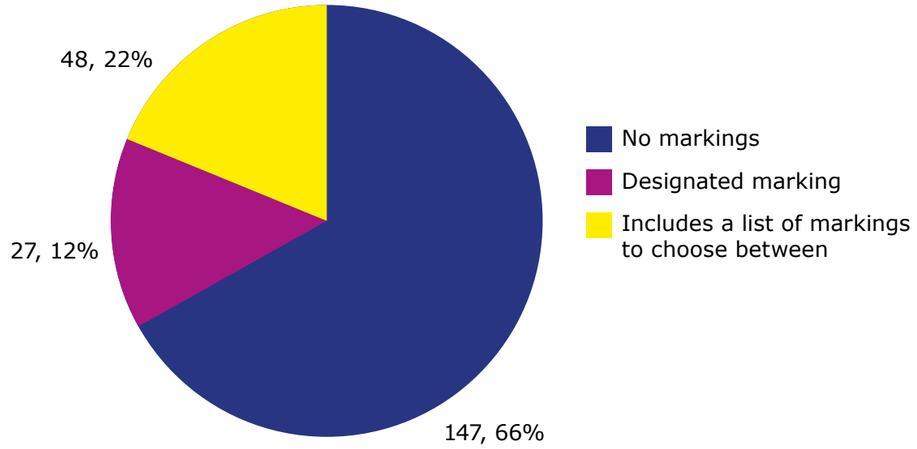
3.6 Conversely, some other government departments, have IT systems that require all email traffic to be marked even if the marking is 'Not Protectively Marked' or 'Unclassified' and this can be viewed as good practice.

[23] See Paragraph 3.2.

RECOMMENDATION 4: HMIC recommends that HMRC introduce mandatory requirement for all CI, RIS-CIG and Detection IT traffic to be GPMS marked before transmission.

3.7 Template forms are used throughout the Department. An examination of 222 different form templates used across HMRC's law enforcement business streams revealed that almost two-thirds (including witness statements and records of interviews) do not contain any GPMS marking, 12% have a designated marking and 22% provide a choice of marking, either by drop down menu or striking out/ deleting the inappropriate choices:

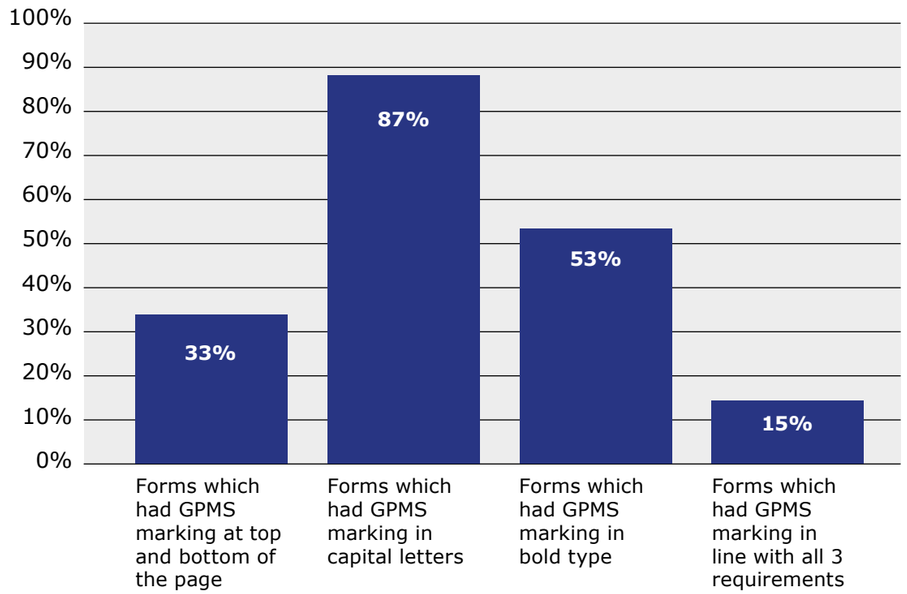
Figure 4: Pie chart showing the proportion of HMRC law enforcement related template forms that carry a GPMS marking



3.8 The review also established that even where template forms carry either designated markings, or provide a choice of protective markings, the markings are not necessarily in the prescribed format:

- 25 of the templates (33%) which are marked do not have the marking at both the top and bottom of the form;
- The marking is in capitals on 65 templates (87%);
- The marking is in bold type on 40 templates (53%);
- Only 11 meet all three requirements (15%).

Figure 5: Percentage of HMRC template forms which are protectively marked, which meet the specific requirements



3.9 26% of completed template forms examined that provided a choice of marking did not have a choice of marking selected[24].

RECOMMENDATION 5: HMIC recommends that HMRC ensure that all HMRC law enforcement template stationery and forms are marked in compliance with the regulations outlined in the DSSM.

3.10 Pre-printed documents, such as officers' Notebooks and Day Books are not currently GPMS compliant. Notebooks do not carry a protective marking and although Day Books are pre-marked RESTRICTED, they only meet the criteria for this marking once an officer has written in them. In these cases, as with the majority of template forms, under the GPMS regulations, the correct procedure is for such forms to be marked with the protective marking and then the "when complete" suffix, such as "CONFIDENTIAL – When Completed". Marking documents with such a suffix also has the additional benefit of not requiring such documents to be stored securely until they are completed.

RECOMMENDATION 6: HMIC recommends that HMRC ensure that the protective marking of printed documents including Day Books, Notebooks and Case Decision Logs and forms are suffixed "when completed".

[24] However, due to HMRC's policy of not mandating the marking of PROTECT and RESTRICTED assets, this may account for a proportion of the unmarked forms.

3.11 The compliance of non-template documents produced by HMRC's law enforcement entities with GPMS is inconsistent. Across CI, very little CI generated case material is marked, apart from that produced by Specialist Teams and that assessed to warrant a CONFIDENTIAL marking[25]. This is due, in part, to a wide understanding amongst operational CI officers of HMRC's policy that the Department operates at a baseline level of RESTRICTED and only material assessed as exceeding this baseline requires physical marking. This is compounded by a general confusion as to whether those documents they generate which subsequently enter the public domain, through the criminal justice system, are exempt from GPMS classification. Furthermore, whilst the databases used by the wider department to hold taxpayers' Self Assessment Returns, Pay As You Earn details or company's Corporation Tax information are restricted, they are not marked. Therefore, none of the screen prints, which can feature heavily in the casework relating to direct tax investigations, are protectively marked. Similarly, files containing bundles of such printouts are likewise unmarked.

3.12 The marking of Detection generated documents is also inconsistent. This is especially evident in relation to Target and Selection (T&S) staff who produce documents identifying potential high-risk passengers and consignments entering the UK. Currently, there is no nationwide corporate form used for this process and bespoke versions have been generated locally at the various T&S sites. Some of these carry a GPMS marking, whereas others do not. The same is true of deployment rosters for Detection staff, which contain detailed information of Detection presence at certain locations and for particular flights. This information clearly could be of use to smugglers and a wider criminal fraternity and should be marked, probably warranting a CONFIDENTIAL marking. In some locations, these documents are so marked[26], whereas other examples are marked PROTECT (without the requisite descriptor) and some are unmarked. The reasons generally given by staff for the non-marking of such documents included the departmental baseline and a widespread erroneous belief in Detection, and echoed in parts of RIS-CIG and, to a lesser extent in CI, that only documents that were to be transferred outside their unit require marking[27].

3.13 The situation in RIS-CIG is broadly similar to CI and Detection, in that GPMS compliance was inconsistent. However, one business unit where GPMS compliance was found to be of a high standard was Intelligence Analysis. All the Intelligence Analysis assessment reports viewed were marked to the requisite standards, with the marking conspicuously displayed on the front cover and every subsequent page.

3.14 As mentioned in Chapter 2, there is currently no departmental guidance on how to mark sensitive documents that are to be shared with overseas agencies[28]. It

[25] It is not possible to determine what proportion of those assets that the originator assessed to be CONFIDENTIAL are actually marked. Given HMRC's baseline policy, an unmarked document could be unclassified, PROTECT, RESTRICTED or be assessed as CONFIDENTIAL, but erroneously not marked.

[26] Although this creates a problem, as they do not have access to the CONFIDENTIAL IT infrastructure , see Paragraph 5.7.

[27] See Paragraph 2.13.

[28] See Paragraph 2.8.

is, therefore, unsurprising that there are inconsistencies amongst the marking of such material by FCLOs and other RIS-CIG staff that have responsibility for liaising with organisations in other jurisdictions. The inspection revealed evidence of the protective marking being removed from some protectively marked material before it is shared with host agencies.

3.15 GPMS does not only apply to printed documents, but also applies to a wide range of other documentary material, including audio tapes of interviews, surveillance and scenes of crime photographs and videos. Currently, HMRC generated photographs are not GPMS marked, apart from those related to specific covert operations, which could identify CI officers. Although the Photographic Unit would be unable to determine the appropriate GPMS classification themselves, as they are not party to the context of the images they handle, the form used to request their services could be modified to ensure that the requesting officer indicates what classification is to be used. Furthermore, audio tapes of interviews are not marked on either the tape or container.

RECOMMENDATION 7: HMIC recommends that HMRC ensures that all CI, RIS-CIG and Detection audio tapes and photographs are protectively marked in accordance with GPMS.

Registering and Filing Protectively Marked Documents

3.16 In addition to regulations concerning the marking of protectively marked assets, GPMS also includes mandatory instruction concerning the filing and registration of SECRET and TOP SECRET material, namely:

- The maintenance of a Register for Protectively Marked Documents SECRET and TOP SECRET containing details of all such material produced, transmitted, copied and destroyed;
- The marking of the file or folder containing the assets with the same marking as the highest level of the documents it holds[29].

3.17 Registers are maintained for SECRET and TOP SECRET material held by most of the units dealing with this level of material (including the FCLO Network and CI Specialist Teams); however, the lack of such registers in HMRC's Source Management Units is a matter of concern. Moreover, throughout the inspection there was no evidence of folders containing SECRET and TOP SECRET material being routinely marked.

RECOMMENDATION 8: HMIC 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.

[29] HMRC SECURITY AND BUSINESS CONTINUITY (15 February 2008) *DSSM 11055: Working with Protectively Market Assets: Registering and Filing Documents.* Unpublished.

3.18 Although GPMS does not require folders containing PROTECT, RESTRICTED or CONFIDENTIAL material to be marked, this occurs in a few units, including the National Source Unit (NSU) and Transport National Intelligence Unit: Containers. This can be viewed as good practice and provides another level of protection to documents, especially those that are currently not individually marked.

Consideration 1: Consideration should be given to mandating the marking of all to 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.

Review, Disposal and Destruction

3.19 CI, RIS-CIG and Detection's compliance with the requirements to review protectively marked material is low. The DSSM instructs the originator of protectively marked material to review the protectively marked information they hold to check if the marking is still appropriate, with the aim to downgrade or destroy the documents preventing costly and unnecessary security measures. Good examples were seen in CI Specialist Teams, but this inspection failed to uncover any examples of this practice occurring in other units.

RECOMMENDATION 9: HMIC 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.

3.20 There is also a lack of consistency in how protectively marked material is disposed of. In many offices, GPMS marked waste is disposed of in recycle bins or RESTRICTED/CONFIDENTIAL waste sacks. The inspection highlighted instances when such waste had been left intact and unsecured in such receptacles after office hours. This placed an over reliance on building security to maintain the integrity of the assets and is in breach of the principles of GPMS. Some other offices have developed local policies of shredding all protectively marked documents. The fact that not all the shredders used by HMRC law enforcement officers meet the requirements set out in the MPS is a matter of concern.

RECOMMENDATION 10: HMIC recommends that CI, RIS-CIG and Detection ensure that protectively marked waste is appropriately secured or shredded.

The Protection of other Non-Documentary Sensitive Assets

3.21 Most CI operational teams maintain a whiteboard with details of their vehicle fleet, including unmarked covert cars. Although the precise details included on these boards vary from team to team, they commonly include registration number and type of vehicle. This information is clearly sensitive. Another UK agency's guidance classifies any information that could be used to identify their undercover vehicle as CONFIDENTIAL. The level of physical security

varies across the CI estate; however all boards are visible to visiting personnel, including contractors. It would be very easy, in many locations, for a visitor to photograph the boards unseen with a camera in a mobile phone.

3.22 The use of whiteboards to list vehicles, equipment, personnel and telephone numbers can be a useful visual aid; however, cognisance has to be taken of the security implications. Although there is no need for them to be withdrawn, their use needs to be managed.

RECOMMENDATION 11: HMIC recommends that HMRC ensure operational information displayed on white- boards is appropriately secured to reflect its GPMS status.

Chapter 4

Physical Security

4.1 This chapter reviews the environments in which protectively marked material is produced, handled and stored by HMRC law enforcement entities. It highlights serious concerns around the availability of appropriate storage facilities and weaknesses in accommodation.

Overview

4.2 The physical marking of GPMS assets is just the first layer of a security regime required by the Scheme, which stipulates specific standards for the physical security of such material. Utilising this layered approach, the level of protection provided will be commensurate to the value of the material, with the most sensitive material being secured by the greatest number of layers. The principle of a layered approach is accepted by HMRC, its implementation across the law enforcement estate is inconsistent.

Storage

4.3 There is generally a good understanding amongst HMRC's law enforcement staff of the need to abide by clear desk policies and to use suitable cabinets to store protectively marked material. This is the case even in units with infrequent access to CONFIDENTIAL or SECRET documents. However, the ability of staff to secure material appropriately is undermined in a number of offices by the lack of suitable storage.

4.4 Across the CI estate, there is a lack of sufficient lockable cabinets, of the standard required by the DSSM. Although CONFIDENTIAL documents should be secured in manifold cabinets or containers[30] to MCL Grade III standard, in many locations such assets are stored in inappropriate cabinets, which do not have requisite combination locks. Furthermore, in certain offices, CONFIDENTIAL case material is stored in damaged units that could not be locked.

4.5 These problems are most acute in CI operational teams, which handle large volumes of evidential material relating to serious crimes. In some CI offices, the lack of storage has resulted in staff placing case material in unsealed cardboard boxes in corridors and unlocked office accommodation. Although the majority of such material relates to old cases, a number of documents physically marked RESTRICTED[31] and in one instance, CONFIDENTIAL Covert Human Intelligence Source (CHIS) related material was found to be stored in this way. Of the sites visited, the Internal Governance Unit at Slough is the only operational investigation office with adequate storage at this level.

[30] HMRC SECURITY & BUSINESS CONTINUITY (15 February 2008) *DSSM 11080*. Unpublished.

[31] This, therefore, is in breach of the GPMS requirement to secure RESTRICTED material in either locked cabinets, containers or rooms – see HMRC SECURITY AND BUSINESS CONTINUITY (15 February 2008) *DSSM 11080: Working with Protectively Market Assets: Keeping Protectively Marked Documents in the Office*. Unpublished.

4.6 During out of hours inspection, it was noted that in those RIS-CIG, CI and Detection offices that had sufficient lockable cabinets, these were generally locked and clear desk policies were adhered to. However, one senior law enforcement manager had left their manifold cabinet unlocked containing CONFIDENTIAL material, in an unlocked office. Although this is mitigated by the overall security of the building, it is in breach of GPMS regulations. Furthermore, in most locations, the combination locks on manifold cabinets are not regularly changed, as required by the GPMS.

RECOMMENDATION 12: HMIC 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 on manifold cabinets are regularly changed.

Accommodation

4.7 The security of office accommodation used by CI Specialist Teams can be viewed as good practice. They are located on the top floor of the building they occupy and entry to the floor is restricted by a keypad lock and beyond this, there are further keypad locks to individual offices. Likewise, units handling compartmentalised handling regime material are similarly located on upper floors with swipe card access for staff and visitors being signed in and out. Although the accommodation is open plan, the area is divided up with each section being responsible for its area security. The last individual that leaves each area has to sign off that all cabinets are secure and no GPMS material is left on desks. This method of operation instils a disciplined approach to security.

4.8 Conversely, there are large numbers of offices where security is not of the adequate standard. There are many examples of CI, RIS-CIG and Detection offices, which contain GPMS marked material that are not locked when unoccupied. Also, some CI operational offices handling CONFIDENTIAL material are frequently accessed by visitors and staff from other HMRC teams. In such locations, it is paramount that appropriate security requirements are maintained.

4.9 The location of several sensitive units – including an SMU - on the ground floors of buildings to which the public have exterior access is of particular concern. Another office, housing the computer servers holding all historic CHIS material, is located on the ground floor of an unsecured building, which backs on to an open car park. Although there are alarms on the windows, keypad access and deadlocks on the door, the windows are not barred or reinforced, and the door has a glass panel. Furthermore, there is no out of hours security and no perimeter security other than CCTV. The request to move to more secure accommodation has not been actioned. Considering that the concentration of highly sensitive information in the building could potentially place the level of protection at SECRET, the security afforded is inadequate. Both the material and personnel are therefore at an unacceptably high level of risk.

4.10 In conclusion, outside of the CI Specialist Teams, the physical security requirements for CI and RIS-CIG staff to provide the appropriate level of protection to the material they handle is, in general, not being met. This is, in part, because the specific needs of CI and RIS-CIG are not appreciated within the wider department and are therefore treated in line with the estate needs of other directorates. With both criminal justice and departmental integrity issues at stake CI and RIS-CIG requirements should be seen as a high priority.

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

Court Security

4.11 Given that the loss of any case material could have adverse consequences for the reputation of the Department and could undermine a prosecution, all material should be handled in accordance with GPMS procedures throughout any court hearing. Although many courts provide a Revenue & Customs Prosecution Office (RCPO), and thereby HMRC case teams, with lockable offices, very few provide appropriate cabinets for the storage of CONFIDENTIAL material. If such storage is not provided, officers should not leave CONFIDENTIAL material at court.

Chapter 5

IT Network Security and Transmission of GPMS Material

Overview

5.1 This chapter examines HMRC's law enforcement entities' compliance with the GPMS instruction for the transmission of protectively marked material and the electronic generation of such material. It raises concerns around the lack of availability of accredited IT infrastructure and encrypted voice communications.

Hard copy

5.2 The primary focus of HMRC's data security effort since the loss of the data disks has been on the transmission of material. Updated guidance on this issue has been provided to all staff and related training is being delivered across the Department. Consequently, throughout CI, RIS-CIG and Detection, officers demonstrate a sound understanding of the GPMS requirements for the routine movement of protected material. During the inspection, there was no evidence of staff transmitting hardcopy protectively marked documents incorrectly, with the requirements for posting, couriering and hand delivering such material strictly adhered to.

5.3 Directorate Data Guardians, appointed following the data loss incident, have been given a key role in granting approval for any data transfers and for providing advice to staff on procedures for non-standard data movements.

IT Transmission and Network Security

Use of RESTRICTED system for CONFIDENTIAL material

5.4 Historically, HMRC have followed a policy of permitting staff to occasionally create and email CONFIDENTIAL documents on the RESTRICTED network. This has recently been changed and now the use of the network for CONFIDENTIAL material is considered by Security & Business Continuity as constituting a security breach. Although staff in some business units which regularly handle CONFIDENTIAL material have access to dedicated CONFIDENTIAL infrastructures, the limited availability of these platforms results in many officers without such access creating, receiving or sending CONFIDENTIAL material on the RESTRICTED network. This was evidenced in a number of key business areas:

- The CONFIDENTIAL infrastructure has not been rolled-out across the Detection estate. Although the Directorate does not currently produce large quantities of CONFIDENTIAL marked material, the inspection revealed examples of:
  - CONFIDENTIAL staff rosters and CONFIDENTIAL Target and Selection profiles being produced and disseminated on the RESTRICTED network;
  - CONFIDENTIAL Intelligence logs being received from the National Co-ordination Unit (NCU) on the RESTRICTED network.
- Although Internal Governance officers do not have access to the CI CONFIDENTIAL network, they often receive CONFIDENTIAL material via email from CI, RIS-CIG and other units;
- A number of CI direct tax investigation teams only currently have the RESTRICTED network and are therefore having to occasionally complete CONFIDENTIAL template forms on this.

5.5 In addition to such security breaches, the limited availability of the CONFIDENTIAL infrastructure has led to many officers without access citing this as a key factor in their assessment of the required protective marking for their documents. In many instances, these officers are knowingly under-marking material in order for it to be transmitted.

5.6 Even in those units that have access to both the CONFIDENTIAL and RESTRICTED networks, there was evidence of CONFIDENTIAL emails being sent and received on the RESTRICTED system.

5.7 Access to the CONFIDENTIAL infrastructure is currently insufficient. Any re-interpretation of the protective marking definitions to be used in an HMRC law enforcement context will exacerbate this situation[32]. One example of this is in relation to the HumInt system. When a member of the public passes information to HMRC, details of the caller are passed, on a Human Contact Report (HCR) form, to the National HumInt Centre (NHC). The HCRs are currently classified as RESTRICTED and are, therefore, transmitted on the standard network, however, as some of these may be later authorised as a CHIS, they will constitute true identities of potential CHIS. As CHIS true identity information is classified as SECRET, there is an argument that HCRs should be classified at least at CONFIDENTIAL level.

RECOMMENDATION 13: HMIC recommends that HMRC make the CONFIDENTIAL infrastructure available to all staff within CI, RIS-CIG and Detection.

RECOMMENDATION 14: HMIC recommends that HMRC re-evaluate the protective marking and transmission of Human Contact Reports.

[32] The requirement for HMRC law enforcement entities to refine the GPMS definitions they use is outlined at paragraph 2.7.

IT Network Security and Transmission of GPMS Material

System Accreditation

5.8 The CONFIDENTIAL infrastructure was inspected by S&BC in 2006 who were unable to give full accreditation[33] to the system, due to shortcomings in respect of ownership, management and assurance. S&BC provided a provisional accreditation for a further six months, on the basis that their action plan was implemented to address the issues. However, this did not occur and accreditation has lapsed. This undermines the credibility of criminal justice activity and raises concerns about its ability to assure the integrity of CONFIDENTIAL material.

RECOMMENDATION 15: HMIC recommends that HMRC, as a matter of urgency, undertake any work required to ensure that the CONFIDENTIAL infrastructure gains accreditation.

Voice Transmissions

5.9 HMRC's standard telephony system is only suitable for conversations classified below CONFIDENTIAL. Encrypted 'Brent' telephones are located in many CI and RIS-CIG offices and parts of the Detection estate, but their use is inconsistent. They are widely used for conversations between CI operational teams and CI Specialist Teams, with external agencies such as Government Communications Headquarters (GCHQ) and are a standard method of voice communication for the FCLO Network. However, other teams including some SMUs that regularly handle CONFIDENTIAL material lack direct access to Brent telephones. Other units, such as the NCU, have requested additional Brent telephones, but there have been difficulties in obtaining such equipment.

5.10 Often the siting of the Brent telephone prevents it being utilised to its full potential. In some offices, it is located in a locked room, or conference room and therefore is not readily accessible by the staff that require it. In other locations, the Brent is placed in an open plan office, which can make it difficult to have sensitive conversations.

5.11 In those locations that do not have Brent, or where the siting of the equipment prevents officers from gaining immediate access to it, they adopt a guarded manner if discussing CONFIDENTIAL matters over an open line. Whilst this is not ideal, it is expedient, given the limited availability of encrypted telephony across HMRC's law enforcement entities.

5.12 Concerns were raised throughout the inspection regarding the reliability and level of technical support available for Brent. Some telephones have remained unserviceable for extended periods and many officers described instances where communication has cut out, causing them to have to redial.

[33] In accordance with Departmental and HMG standards.

IT Network Security and Transmission of GPMS Material

5.13 The use of Brent, despite the system limitations, is good practice and the wider use of such telephones is to be encouraged particularly amongst operational CI teams. If it was more widely available across CI, RIS-CIG and Detection, then it is anticipated, that its use would increase significantly.

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.

Chapter 6

Compliance and Management Assurance

6.1 Within HMRC, the responsibility for monitoring adherence with GPMS is delegated from S&BC to individual business units. However, since the data loss, S&BC and Internal Audit have initiated an audit review of HMRC offices and directorates' data security compliance, which identified shortcomings in data security and with the marking of assets.

6.2 There is no top down structured management assurance regime for GPMS across the Department. It is essential that this is introduced and is driven forward by senior management in the Department. Although individuals have been appointed to a variety of security assurance posts in CI, RIS-CIG and Detection, neither the Directorate Data Guardians, CI's Regional Operational Security Officers, nor Branch Assurance Managers have clear responsibility for routinely auditing and assuring staff compliance across the whole range of GPMS requirements. Within those areas of CI, RIS-CIG and Detection that handle material subject to the compartmentalised handling regime, an assurance programme is undertaken, ensuring compliance with the compartmentalised handling regime regulations.

Line Managers' Role

6.3 Line managers in CI, Detection and RIS-CIG are generally unaware of the responsibility DSSM lays to them, or to a designated security manager, to undertake twice yearly checks to ensure that:

- all staff who may handle protectively marked documents have seen the DSSM;
- if possible, all protectively marked documents are placed in files;
- CONFIDENTIAL and above documents are kept in approved combination locked security cabinets or containers;
- any of the standing authorities to take documents home need to be renewed;
- documents have been reviewed for downgrading or destruction.

Consequently, compliance with these requirements is generally poor. Furthermore, there is a lack of awareness amongst most managers of the departmental requirement for the creation of all material classified higher than RESTRICTED to be authorised by a Higher Officer or Senior Officer[34].

[34] The production of CONFIDENTIAL material has to be authorised by a Higher Officer or above, whereas SECRET and TOP SECRET material requires at least Senior Officer authorisation. See HMRC SECURITY & BUSINESS CONTINUITY (11 December 2006) *DSSM 11015: Working with Protectively Marked Assets: Choosing the Correct Level of Marking*. Unpublished.

The requirement for such an authorisation is unclear, as officers handling CONFIDENTIAL, SECRET and TOP SECRET material are vetted to do so.

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

6.4 CI and RIS-CIG's Enforcement Management Assurance Framework (EMAF) places further requirements on Senior Officers to ensure the correct use of the GPMS and handling requirements amongst their staff. However, given the volume of management assurances mandated by EMAF – which mandates checks in 38 distinct subject areas - and the pressures on managers' time, these checks are rarely undertaken.

RECOMMENDATION 16: HMIC 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.

Appendix A

List of Recommendations and Considerations

Recommendations:

HMIC recommends that:

1 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;

2 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;

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

4 HMRC introduce mandatory requirement for all CI, RIS-CIG and Detection IT traffic to be GPMS marked before transmission;

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

6 HMRC ensures the protective marking of printed documents including Day Books, Notebooks and Case Decision Logs and Forms are suffixed "when completed";

7 HMRC ensures all CI , RIS-CIG and Detection audio tapes and photographs are protectively marked in accordance with GPMS;

8 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;

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

10 CI, RIS-CIG and Detection ensure that protectively marked waste is appropriately secured or shredded;

11 HMRC ensure operational information displayed on whiteboards is appropriately secured to reflect its GPMS status;

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 on manifold cabinets are regularly changed in accordance with instructions;

13 HMRC make the CONFIDENTIAL infrastructure available to all staff within CI, RIS-CIG and Detection;

14 HMRC consider re-evaluating the protective marking and transmission of Human Contact Reports;

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

16 HMRC introduce a structured assurance regime for GPMS compliance, with corporate responsibility at a senior management level to enforce the importance of the GPMS.

Considerations:

Consideration should be given to:

1 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;

2 Locating all CI and RIS-CIG units that regularly handle CONFIDENTIAL, SECRET or TOP SECRET material in lockable offices with additional entry security systems such as privacy locks and swipe cards;

3 Equipping all CI, RIS-CIG and Detection offices with Brent telephones in an environment where conversations cannot be overheard;

4 Removing the requirement for the creation of CONFIDENTIAL, SECRET and TOP SECRET material to be authorised.

Appendix B

Acronyms and Abbreviations

ACPO	Association of Chief Police Officers
BS	British Standard
CCTV	Closed Circuit Television
CHIS	Covert Human Intelligence Sources
CI	Criminal Investigation
CPIA	Criminal Procedure and Investigations Act 1996
DSSM	Departmental Security Standards Manual
EMAF	Enforcement Management Assurance Framework
FCLO	Fiscal Crime Liaison Officer
GPMS	Government Protective Marking Scheme
MCL	Manifold Combination Lock
MPS	Manual of Protective Security
RIS-CIG	Risk & Intelligence Service - Criminal Intelligence Group
GCHQ	Government Communications Headquarters
HCR	Human Contact Report
HMIC	HM Inspectorate of Constabulary
HMRC	HM Revenue & Customs
IT	Information Technology
NCU	National Co-ordination Unit
NHC	National HumInt Centre
RCPO	Revenue & Customs Prosecution Office
S&BC	HMRC Security & Business Continuity
SMU	Source Management Unit
SOCA	Serious Organised Crime Agency
T&S	Target and Selection

Appendix C

The MPS Definitions of Protective Markings

PROTECT	
Asset Value – Consequence of Compromise	**The compromise of assets marked PROTECT would be likely to:** Cause substantial distress to individuals Breach proper undertakings to maintain confidence of information provided by third parties Breach statutory restrictions on the disclosure of information (except the Data Protection Act – which can be addressed by other impact statements and/or the e-government Security Framework) **And, depending on the severity of the circumstances:** Cause financial loss or loss of earning potential to, or facilitate improper gain or advantage for, individuals or companies Prejudice the investigation or facilitate the commission of a crime Disadvantage government in commercial or policy negotiations with others
Descriptor	A descriptor should be used with the marking PROTECT. These might include: APPOINTMENTS COMMERCIAL CONTRACTS HONOURS INVESTIGATION MANAGEMENT MEDICAL PERSONAL PRIVATE REGULATORY STAFF DEPARTMENTAL Descriptors

RESTRICTED	
Asset Value – Consequence of Compromise	**The compromise of assets marked RESTRICTED would be likely to:** Adversely affect diplomatic relations Cause substantial distress to individuals Make it more difficult to maintain the operational effectiveness or security of UK or allied forces Cause financial loss or loss of earnings potential to, or facilitate improper gain or advantage for, individuals or companies Prejudice the investigation or facilitate the commission of crime Breach proper undertakings to maintain confidence of information provided by third parties Impede the effective development or operation of government policies Breach statutory restrictions on the disclosure of information (except the Data Protection Act – which can be addressed by other impact statements and/or the e-government Security Framework) Disadvantage government in commercial or policy negotiations with others Undermine the proper management of the public sector and its operation

CONFIDENTIAL	
Asset Value – Consequence of Compromise	**The compromise of assets marked CONFIDENTIAL would be likely to:** Materially damage diplomatic relations, that is, cause formal protest or other sanctions Prejudice individual security or liberty Cause serious damage to the operational effectiveness or security of UK or allied forces Cause serious damage to the effectiveness of valuable security or intelligence operations Work substantially against national finances or economic and commercial interests Substantially undermine the financial viability of major organisations Impede the investigation or facilitate the commission of serious crime Seriously impede the development or operation of major government policies Shut down or otherwise substantially disrupt significant national operations

SECRET	
Asset Value – Consequence of Compromise	**The compromise of assets marked SECRET would be likely to:** Raise international tension Seriously damage relations with friendly governments Threaten life directly or seriously prejudice public order or individual security or liberty Cause serious damage to the operational effectiveness or security of UK or allied forces Cause serious damage to the continuing effectiveness of highly valuable security or intelligence operations Cause substantial material damage to national finances or economic and commercial interests

TOP SECRET	
Asset Value – Consequence of Compromise	**The compromise of assets marked TOP SECRET would be likely to:** Threaten directly the internal stability of the UK or friendly countries Lead directly to widespread loss of life Cause exceptionally grave damage to the effectiveness or security of UK or allied forces Cause exceptionally grave damage to the continuing effectiveness of extremely valuable security or intelligence operations Cause exceptionally grave damage to relations with friendly governments Cause severe long term damage to the UK economy

Appendix D

Methodology

An Inspection into the Compliance of HM Revenue & Customs' Law Enforcement Entities With the Government Protective Marking Scheme.

The inspection focussed on the quality of policy and guidance available to HMRC staff working in law enforcement roles on the Government Protective Marking Scheme (GPMS) and their compliance with the requirements of the Scheme.

The first phase of the inspection involved the analysis of Government, Departmental and Directorate instructions on GPMS and related issues and was used to identify key areas that would be subject to inspection.

There followed a structured series of field visits across the CI, RIS-CIG and Detection estates between March and April 2008. Documents, physical security, systems and procedures were examined in order to assess their compliance with GPMS regulations. Interviews were conducted with senior managers with direct responsibility for security policy, management in HMRC law enforcement and with selected operational managers and staff from a cross-section of offices that regularly produce, handle or receive classified assets.

The inspection team also conducted a benchmarking exercise, which included visits to other government departments and law enforcement agencies. HM Inspector would like to extend his sincere thanks to the Cabinet Office, the Ministry of Defence, SOCA, the Metropolitan Police and West Midlands Police and security experts in other government departments. Overall, in excess of 90 interviews were conducted within HMRC and with external organisations.

HM Inspector extends sincere thanks to the Board, Directors and all HMRC staff who took part in the inspection. As was the case with our previous inspections, the inspection team were warmly welcomed at every venue. He also extends thanks to Criminal Justice & Enforcement Standards for their assistance in arranging the extensive programme of inspection visits across the Department and enabling field visits and interviews with key personnel.

HM Inspector was supported by an inspection team comprising Specialist Staff Officers with a wide breadth of experience of conducting and managing criminal investigations.

Notes:

Notes:

Issued by
HM Revenue & Customs
June 2009