

IPCO

Investigatory Powers
Commissioner's Office

Inspection Report: Technology Environment follow up inspection, 15-16 April 2019

Contents

1	Introduction	2
2	Inspection methodology	2
3	Recommendations	3
4	MI5 mitigations	6
4.1	<u>[REDACTED] [New local processes for data]</u>	6
4.2	New file shares policy	6
4.3	<u>[REDACTED] [Consideration of mitigation steps and progress in implementation]</u> ..	7
4.4	<u>[REDACTED]</u>	7
4.5	Retention, review and deletion (RRD)	7
4.6	<u>[REDACTED]</u>	7
5	Residual compliance risks	8
5.1	Legacy data	8
5.2	Storage of data outside <u>[in other areas]</u>	8
5.3	Joiners, movers and leavers (JML) process	9
5.4	<u>[A set of material]</u>	9
5.5	LPP material	10
5.6	Error reporting	11
6	Conclusion	11

1 Introduction

- 1.1 On 18-22 March 2019, IPCO conducted a detailed audit of the [Technology Environment, or TE] at MI5 in response to briefings given to the IPC about compliance risks in the system (our report of 29 March refers).
- 1.2 Following that inspection, MI5 set out the mitigations they were putting in place to deal with those compliance risks as set out in our inspection report; these were recorded in what is now “Annex H” of the Judicial Commissioners’ MI5 Handbook.
- 1.3 In light of both of these documents, the IPC then made a determination on 5 April on the extent to which MI5 could be said to comply with the relevant IPA safeguards (para 15 of the IPC’s decision refers)
- 1.4 The IPC concluded that, subject to certain critical caveats, he was satisfied that MI5 had the capability henceforth to handle warranted data in a way which was compliant with the IPA. He emphasised that *“all the relevant activities must be susceptible to inspection and audit – in other words, MI5 and IPCO must be able to check in sufficient detail that there has been compliance with the legislation”*.
- 1.5 In coming to this decision, the IPC also noted:

“This is a serious and inherently fragile situation. The future will entirely depend on compliance by MI5 with the legislation and the adequacy of the internal and external inspection regimes. IPCO will need to be reassured on a continuing basis that new warranted material is being handled lawfully. In the absence of this reassurance, it is likely that future warrant applications for data held in [the TE] will not be approved by the Judicial Commissioners, and I will expect that the proposed mitigations are progressed at pace. The weaknesses outlined above are of sufficient magnitude to mean that the immediate mitigatory steps, which will be sufficient for the short term, cannot be expected to provide a long term solution, and the proposals made by MI5 in Part II must be implemented in their entirety in the shortest reasonable timeframe. Without seeking to be emotive, I consider that MI5’s use of warranted data in [the TE] is currently, in effect, in “special measures” and the historical lack of compliance [REDACTED] with the law is of such gravity that IPCO will need to be satisfied to a greater degree than usual that it is “fit for purpose”.”

2 Inspection methodology

- 2.1 The inspection was conducted on 15-16 April 2019. Present from IPCO: [an Inspector and a member of the Technology Advisory Panel]
- 2.2 In light of the IPC’s judgment, the inspection focused on a) MI5’s implementation of the mitigations set out in “Annex H”, to apply to new warranted data acquired by MI5 (see Section 4); and b) any residual compliance risks in the [TE] which were not caught by these mitigations (see Section 5).
- 2.3 It must be emphasised that, in the two days available on this inspection, it was not possible to explore all of the relevant issues in sufficient depth. We have therefore made a number of recommendations setting out how we intend to follow up on this inspection.

3 Recommendations

3.1.1 The key recommendations arising from the inspection are listed in Table 1 below.

Number	Section reference	Recommendation	Recommendation type
R1	5.2	[REDACTED]	Critical recommendation: affects compliance status if not addressed
R2	4.1	MI5 should urgently complete the implementation of business processes for the handling of warranted data in [the TE] and immediately inform IPCO when these processes became or will become fully operational in each relevant business	Critical recommendation: affects compliance status if not addressed
R3	4.6	[REDACTED]	Core recommendation: improvements must be made
R4	4.6	[REDACTED]	Core recommendation: improvements must be made

R5	5.2	<p><u>[MI5 should implement a solution as soon as reasonably practicable to ensure that warranted data is deleted as soon as there are no longer any relevant grounds for retaining it.]</u></p> <p>[REDACTED]</p>	<p>Core recommendation: improvements must be made</p>
R6	4.1	<p><u>[REDACTED]By 23 April 2019, MI5 should provide a summary of all of the local business processes which have been implemented in response to paragraph 33 of Annex H [REDACTED]. This should set out clearly how each process complies with the [REDACTED] key requirements of MI5's new policy on [REDACTED] warranted data in [the TE]</u></p>	<p>Recommendation: further information required</p>
R7	4.1	<p><u>MI5 should facilitate a detailed IPCO inspection in May to examine the extent to which relevant [teams] have implemented the new policy [REDACTED].</u></p>	<p>Recommendation: further information required</p>
R8	4.2	<p>On our next inspection, MI5 should facilitate an inspection of the file share structures in use by those [departments] which make most use of [the TE], focusing on whether their structure and contents mirrors the central records held by the relevant information [teams].</p>	<p>Recommendation: further information required</p>

R9	5.1	MI5 should provide IPCO with fortnightly updates on their project to delete legacy data from storage areas in <u>[the TE]</u> , alongside other technical remediations. MI5 should provide IPCO on their assessment of how much warranted data is likely to be held <u>[in other areas]</u> as soon as they have been able to come to a view based on their current "discovery" work.	Recommendation: further information required
R10	5.2	MI5 should update IPCO on their analysis of data within the sample of <u>[areas in the TE]</u> once this analysis is complete. If MI5 assesses that <u>[areas in the TE]</u> may hold warranted data they should set out how they plan to ensure these <u>[areas]</u> meet the IPA minimisation, destruction and LPP safeguards.	Recommendation: further information required
R11	5.4	[REDACTED]	Recommendation: observed potential for improvements
R12	5.5	MI5 should revert with advice on whether, and to what extent, LPP items within [REDACTED] warranted data held in <u>[the TE]</u> are covered by MI5's inseparable LPP policy; if not, MI5 should set out how they would delete such items if required to do so.	Recommendation: further information required
R13	5.6	[REDACTED]	Recommendation: further information required
R14	5.6	MI5 should write to IPCO to make clear that previous disclosures about <u>[the TE]</u> constitute notification of an error under IPA Section 235(6), and as such IPCO's ongoing inspections of <u>[the TE]</u> constitute an error investigation.	Recommendation: further information required

Table 1. Key recommendations resulting from inspection

4 MI5 mitigations

4.1 [REDACTED][New local processes for data]

4.1.1 [REDACTED]

4.1.2 [REDACTED]

4.1.3 [REDACTED]

4.1.4 [REDACTED]

4.1.5 [REDACTED]

4.1.6 [REDACTED]

4.1.7 [REDACTED]

4.1.8 [REDACTED]

4.1.9 [REDACTED]

4.1.10 [REDACTED]

4.1.11 [REDACTED]

4.1.12 [REDACTED]

4.1.13 [REDACTED]

4.1.14 [REDACTED]

4.1.15 [REDACTED]

4.1.16 [REDACTED]

4.1.17 [REDACTED]

4.1.18 [REDACTED]

4.1.19 [REDACTED]

4.1.20 [REDACTED]

4.1.21 [REDACTED]

4.2 New file shares policy

4.2.1 In making his determination, the IPC summarised this mitigation as follows:

"In the future, with new file-shares the name of the file that is created will follow a naming convention... whenever a new file-share is created, it must be registered in line with the processes established by the information teams, and each information team will from this point onwards hold a log of all new file-shares that will be available for inspection. [REDACTED] This will not be implemented

[REDACTED]6

immediately but instead as quickly as possible... [The naming convention would also] require users to identify in the title of the file whether [the data] includes LPP material”.

- 4.2.2 On the basis of the descriptions we were given of the local business processes which have been introduced, it was apparent that relevant [departments] in MI5 have implemented this requirement or are in the process of doing so. However, we were unable to test the extent to which this process had taken effect by examining data in file shares.

On our next inspection, MI5 should facilitate an inspection of the file share structures in use by those [departments] which make most use of [the TE], focusing on whether their structure and contents mirrors the central records held by the relevant [information teams].

4.3 **[REDACTED][Consideration of mitigation steps and progress in implementation]**

4.3.1 **[REDACTED]Consideration of mitigation steps and progress in implementation]**

4.3.2 [REDACTED]

4.3.3 [REDACTED]

4.4 **[REDACTED]**

4.4.1 [REDACTED]

4.4.2 [REDACTED]

4.4.3 [REDACTED]

4.4.4 [REDACTED]

4.4.5 [REDACTED]

4.4.6 [REDACTED]

4.5 Retention, review and deletion (RRD)

4.5.1 In making his determination, the IPC summarised this mitigation as follows:

“By the end of April 2019, automated RRD will be in place across the system to delete, when appropriate, all [of a certain category of] material, and until the end of this month this will be done manually to ensure that none is held for longer than the relevant RRD policy. For [all other areas] automated RRD will be delivered [in] 2019. Such material is currently within its agreed retention period.”

4.5.2 MI5 confirmed that, for [a certain category of] data, a new automated RRD function will be activated in [a test mode] [REDACTED] [from April 2019]. Once these test results are validated, the system will be deployed fully.

4.5.3 For all other types of warranted data [in a suite of systems], MI5 informed us that they are on track to deliver automated RRD [this year].

4.6 [REDACTED]

4.6.1 [REDACTED]

4.6.2 [REDACTED]

4.6.3 [REDACTED]

4.6.4 [REDACTED]

5 Residual compliance risks**5.1 Legacy data**

5.1.1 On our last inspection, we were briefed on the process by which MI5 was scanning the contents of file shares [in an environment] of [the TE] and deleting content for which there were no longer any relevant grounds for retaining it (including a need to retain for legal proceedings).

5.1.2 As of our last inspection, action had been completed for [a percentage] of folders. This figure has now risen to [a percentage]. In addition, MI5 has begun scanning file shares within [an environment]. [A percentage] of the files in this environment have been scanned; [REDACTED].

5.1.3 Overall, MI5 is on track to complete the quarantine and deletion of legacy data in file shares [later in 2019].

5.1.4 However, warranted data is also present in other types of storage within [the TE], including [REDACTED]. MI5 is in what they describe as the “discovery phase” for these storage areas: that is, they are seeking to quantify the scale of the problem before taking action. Given the use of [REDACTED] which may contain copies of warranted data, as well as a [range] of technologies and systems in use across [the TE], deleting legacy data [in some areas] will be [complex].

MI5 should provide IPCO with fortnightly updates on their project to delete legacy data from storage areas in [the TE], [REDACTED]. MI5 should provide IPCO on their assessment of how much warranted data is likely to be held outside of file shares, e.g. [REDACTED] as soon as they have been able to come to a view based on their current “discovery” work.

5.2 Storage of data [in other areas]

5.2.1 We reviewed MI5’s current understanding of how warranted data might be stored [in other areas].

Data stored in [REDACTED]

5.2.2 [REDACTED]

5.2.3 We were briefed on the various types of user profile [REDACTED]. These can be summarised as follows: [REDACTED]

5.2.4 [The use of some areas is being recorded as part of MI5’s new local business processes. As such, MI5 will have a record of the fact warranted data will exist

[REDACTED]8

within some areas, which will be subject to local RRD policies.]

5.2.5 [REDACTED]

5.2.6 [REDACTED]

As a matter of urgency, MI5 should implement a process to address the potential existence [REDACTED] of warranted data stored in areas. [REDACTED]

MI5 should implement a technical solution as soon as reasonably practicable to ensure that warranted data is deleted [REDACTED] as soon as there are no longer any relevant grounds for retaining it. [REDACTED].

[Data storage]

5.2.7 MI5 is also investigating storage of data [in other areas]. Where file shares exist [in other areas], these are typically used for [REDACTED] and are unlikely to contain warranted data. [REDACTED].

5.2.8 MI5 has taken a sample of data from [a number of areas] across [the TE] and are analysing the contents. [REDACTED].

MI5 should update IPCO on their analysis of data within the sample of areas in [the TE] once this analysis is complete. If MI5 assesses that [some areas] in [the TE] may hold warranted data they should set out how they plan to ensure these areas meet the IPA minimisation, destruction and LPP safeguards.

5.3 Joiners, movers and leavers (JML) process

5.3.1 Since our last inspection, MI5 has implemented a JML process for [the TE]. [REDACTED]

5.3.2 [REDACTED]

5.3.3 [REDACTED]

5.3.4 [REDACTED]

5.4 [A set of material]

5.4.1 On our previous inspection, we were briefed on the extent to which MI5 was able to protect [a set of material] within [the TE] relating to [a business area]. We asked for an update on this inspection covering the other [similar business areas].

5.4.2 [In comparison, the similar business areas] have [REDACTED] warranted data in [REDACTED]9

[the TE]. [REDACTED] MI5 recognise that there is an ongoing risk in this area.

- 5.4.3 We were briefed, in outline, on the way [the departments] use file shares in [the TE]. Broadly this appeared compliant with the new policies MI5 has in place, but we will require the full details requested above to come to a definitive view.
- 5.4.4 Regarding legacy data, we were informed that [an amount of data] found in [the TE] file shares is currently being reviewed for deletion. It is highly likely that this includes [product relating to this set of material].

MI5 should seek to quantify the extent to which [this] material [in this system] is exposed to users of that suite of applications, including [a particular group of] users, and set out any further mitigations they will take to ensure [data] are properly protected.

5.5 LPP material

- 5.5.1 Following our previous inspection, MI5 informed us of an additional risk relating to the identification of suspected or actual LPP material in [the TE]. This was included the second, updated version of our inspection report, published 29 March:

“The policy in place in relation to LPP material requires that material be flagged if it is to be retained (after reporting to IPCO) or held only for the purpose of destruction. A small number of specialist systems within [the TE], used by specialist analysts, do not have the functionality to allow material to be flagged, and are not able to reflect flags applied to material in other systems. [REDACTED] Guidance is in place which requires users to seek the deletion of any LPP material they encounter in these systems and there are reminders in the systems themselves. There is also a risk that in some cases an LPP flag applied to [REDACTED] product within [the TE] is not [REDACTED]. MI5 is working to establish whether this is an appreciable risk and what mitigations may be available.”

- 5.5.2 We asked for an update. MI5 explained that, in most cases, analysts view warranted content [in particular applications]: these have a functioning capability to “flag” LPP material, at which point it is obscured from view. However, it is also possible for analysts to examine the same content in [other applications] which do not implement LPP flags applied elsewhere. There is therefore a risk that content flagged as LPP may still be visible in these applications. In mitigation, MI5 has introduced clear guidance that users [of those applications] must delete any LPP content they identify through their use of the applications. Deletion [from those applications] would render the item invisible to users of the app in future, but would not affect its visibility in [other apps]. We were satisfied with this arrangement.
- 5.5.3 Separately, we asked about LPP material which may be included in [other] warranted data [REDACTED]. If LPP items derived from that [REDACTED] product ([REDACTED]) were identified [in the system], could the relevant content in the [REDACTED] product be deleted if necessary?

MI5 should revert with advice on whether, and to what extent, LPP items within [REDACTED] warranted data held in [the TE] is covered by MI5’s inseparable LPP policy; if not, MI5 should set out how they would delete such items if required to do so.

5.6 Error reporting

- 5.6.1 We discussed MI5's obligations to report [the TE] compliance issues formally to IPCO as an error under Section 231 of the IPA and made two recommendations.

Should MI5 identify that, as a result of compliance problems in [the TE], serious prejudice or harm has been caused to an individual or individuals, they should report this to IPCO for consideration as a potential serious error under IPA Section 231(2).

MI5 should write to IPCO to make clear that previous disclosures about [the TE] constitute notification of an error under IPA Section 235(6), and as such IPCO's ongoing inspections of [the TE] constitute an error investigation.

6 Conclusion

- 6.1 Overall, MI5 has made rapid progress in implementing the mitigations set out in "Annex H" which underpinned the IPC's decision of 5 April. However, gaps remain and these must be addressed as a matter of urgency. It was not possible on this inspection to test in detail how far individual [departments] within MI5 are now complying with the new policies and procedures put in place for the handling of warranted data.
- 6.2 In response, we intend to conduct a further, detailed inspection of how individual [departments] are now handling warranted data in line with MI5's new policies. We have also made a critical recommendation to address the potential proliferation of warranted data [REDACTED], which should be addressed urgently by MI5 [pending a longer term solution].