IPCO

Investigatory Powers Commissioner's Office

Inspection Report – MI5 (Audit of [the Technology Environment]) Version 2, issued 29 March 2019

Contents

1 Introduction 2
2 Inspection methodology 2
3 Key findings 3
4 Data flow 4
4.1 Methodology 4
4.2 [Data Type 1] 5
4.3 [Data Type 2] 5
4.4 [Data Type 3] 7
4.5 [Data Type 4] 8
4.6 [Data Type 5] 9
4.7 [Data Type 6] 9
5 LPP material 10
6 System-wide safeguards 11
7 Institutional knowledge and governance 12
8 Conclusion 15
9 Annex: list of updates 16

For a list of updates included in this version, see Annex.

1 Introduction

1.1 [*MI5 uses different technology environments. One of these technology environments will be referred to as "the Technology Environment, or TE". This TE holds operational data. MI5 judge the TE as being important to delivering mission capabilities.*]

1.2 On 27 February 2019, MI5 briefed the IPC about compliance risks which had been identified with the [*TE*]. Some initial background had been provided by MI5 in a letter of 21 February, and the briefing itself was summarised in a further letter to the IPC of 11 March 2019.

1.3 The key compliance risks highlighted in MI5's briefing were that, within [*the TE*], MI5 had less assurance than they would wish regarding [*compliance risks*]. There are two specific aspects to [*the TE*] which are relevant to these compliance risks:

- **File shares:** files within [*the TE*] can be written to file shares, either in an automated way as data flows between systems within [*the TE*], or manually by an analyst [*REDACTED*]
- **Data stores:** data stores are used to store [*REDACTED*] data required by applications in [*the TE*]. MI5's letter stated that *they "have, or will have, automatic RRD process[es] for our main Data Stores although the RRD rules vary according to the* [*nature*] *of that data or, in some cases, are system specific. Some [Data] Stores and other areas may not have an RRD process."*

1.4 In response to MI5's letter, the IPC commissioned this review of [*the TE*], focussing on the extent to which [*the TE*] complies with the relevant IPA safeguards for warranted data. He also asked inspectors to consider the extent of MI5's institutional knowledge of the issues, given the statement in MI5's letter that compliance risks in [*the TE*] had been identified as early as January 2016.

2 Inspection methodology

2.1 On 18-22 March 2019, IPCO examined the systems and processes within [*the TE*] in depth. The inspection included detailed discussions with technical experts in MI5 as well as a live demonstration of parts of the system and a review of relevant documentation. The inspection team was comprised of [*three Inspectors and a member of the Technology Advisory Panel*]

2.2 MI5 is still investigating some of the problems associated with [*the TE*], and this short notice inspection was subject to time constraints. As such, any conclusions presented in this report are provisional and may be revised as further information becomes available.

2.3 This report presents our provisional findings in the following areas:

- **Data flow:** a summary of how data obtained under various investigatory powers available to MI5 flows through [the TE], assessed against the relevant safeguards set out in the IPA and Codes of Practice.
- **LPP material:** a specific examination of the extent to which data handling within [the TE] complies with the IPA's particular safeguards for LPP material.
- **System-wide safeguards:** our provisional judgements on how and to what extent system-wide safeguards, applied over and above the protections around particular species of operational data, provide further assurance that IPA safeguards are being adhered to.
- **Institutional knowledge and governance:** a summary of MI5's evolving corporate knowledge of the compliance problems in [the TE] and how the organisation responded to these.

3 Key findings

[REDACTIONS A, B AND E BELOW INCLUDE COPYING OF DATA AND ACCESS CONTROLS, BUT NOT NECESSARILY IN THAT ORDER]

A. [REDACTED]

B. [REDACTED]

C. **Review, retention and deletion (RRD):** [REDACTED] MI5 will soon be applying an automated RRD process to operational data [within a suite of systems, which hold a [REDACTED] proportion of the TE's operational data]

D. **LPP:** MI5 has a manual process in place for deleting LPP material from its systems if required to do so. [REDACTED].

E. [REDACTED]

F. **Institutional knowledge:** we judge that, by January 2018 if not earlier, MI5 had a clear view of some of the compliance risks around [the TE], to the extent that they should have carefully considered the legality of continuing to store and exploit operational data in [the TE]. The risks were also sufficiently clear that they should have been communicated to the IPC.

[1] [REDACTED]

4 Data flow

4.1 Methodology

4.1.1 [For some categories of data] we have assessed [the TE] against the following IPA safeguards, which are identical across the IPA for each of the powers:[2]

- [REDACTED]
- [REDACTED]
- **Retention and deletion:** Every copy of the material obtained under a warrant must be destroyed as soon as there are no longer any relevant grounds for retaining it.
- **LPP (where relevant):** If the IPC approves the retention of material subject to LPP, he may nevertheless impose such conditions as he considers necessary for the purpose of protecting the public interest in the confidentiality of items subject to legal privilege. He also has the power to direct that an item containing LPP be destroyed if he considers that the public interest test has not been met.

4.1.2 [For a category of data] the safeguards which are set out in [the Code of Practice] are broadly analogous to the above, [REDACTED]

4.1.3 For BPD, the statutory requirement is that the Secretary of State considers that "*the arrangements... for storing bulk datasets... and for protecting them from unauthorized disclosure are satisfactory*".[4] However, the Code of Practice imposes specific obligations which broadly mirror the safeguards above.[5] The LPP safeguards rarely if ever apply to MI5's BPD holdings.

4.1.4 [For a category of data], the Code of Practice imposes very similar requirements [to those listed above]

4.1.5 The safeguards that apply to [a category of data] are also very similar to the list above.[7]

4.1.6 Given the broad similarities between the safeguards which apply to all of these powers, we have provided provisional RAG ratings against the above list for each type of operational data we examined. The RAG ratings give a broad indication of the extent to which we assess [the TE] complies with the safeguards (red: serious compliance gaps; amber: some compliance gaps; green: largely compliant).

4.1.7 The data flow diagrams below are rough approximations of the way data moves through [the TE] and capture the most relevant aspects of the system only. We were

---

[2] [REDACTED]
[3] [REDACTED]
[4] [REDACTED]
[5] [REDACTED]
[6] [REDACTED]
[7] [REDACTED]

provided with much more detailed schematics in discussion with MI5 technical experts.

[REDACTED]

4.2 *[Data Type 1]*

[REDACTED]

4.2.1 [REDACTED]

[REDACTED]

[REDACTED FIGURE]

4.2.2 [REDACTED]

4.2.3 [REDACTED]

4.2.4 **Deletion:** there are no automated deletion processes in place for content stored in [*a system*] [REDACTED]. MI5 has already made us aware of an error where [*for a type of data stored in a system data older than a specified period was not deleted*]. However, MI5 is introducing a new system [REDACTED] to remedy this error. This is currently expected to be live by [REDACTED]. In the interim, MI5 is manually deleting any [*type of data*] in [*the relevant system*] which is more than [*a specified period*] old.

4.2.5 [REDACTED]

Compliance with IPA safeguards

4.2.6 Our provisional conclusions are as follows.

[THE REDACTIONS IN COLUMN 1 OF THE TABLE BELOW INCLUDE LPP, COPYING OF DATA AND ACCESS CONTROLS, BUT NOT NECESSARILY IN THAT ORDER]

IPA safeguard	RAG rating	Rationale
[REDACTED]	GREEN	[REDACTED]
[REDACTED]	AMBER	[REDACTED]
Review, retention, and deletion (RRD)	RED	[REDACTED]
[REDACTED]	AMBER	[REDACTED]
[REDACTED]	RED	[REDACTED]

4.3 *[Data Type 2]*

Context

4.3.1 [REDACTED]

4.3.2 [REDACTED]

[REDACTED]

[REDACTED FIGURE]

4.3.3 [REDACTED]

4.3.4 [REDACTED]

4.3.5 [REDACTED]

4.3.6 [REDACTED]

4.3.7 [REDACTED]

4.3.8 [REDACTED]

4.3.9 [REDACTED]

[REDACTED]

4.3.10 [REDACTED]

[THE REDACTIONS IN COLUMN 1 OF THE TABLE BELOW INCLUDE LPP, COPYING OF DATA AND ACCESS CONTROLS, BUT NOT NECESSARILY IN THAT ORDER]

IPA safeguard	RAG rating	Rationale
[REDACTED]	GREEN	[REDACTED]
[REDACTED]	AMBER	[REDACTED]
Review, retention, and deletion (RRD)	RED	[REDACTED]
[REDACTED]	AMBER	[REDACTED]
[REDACTED]	RED	[REDACTED]

4.4 *[Data Type 3]*

[REDACTED]

4.4.1 [REDACTED]

4.4.2 [REDACTED]

[REDACTED]

4.4.3 [REDACTED]

4.4.4 [REDACTED]

4.4.5 [REDACTED]

4.4.6 [REDACTED]

Compliance with IPA safeguards

4.4.7 Our provisional conclusions are as follows.

[THE REDACTIONS IN COLUMN 1 OF THE TABLE BELOW INCLUDE LPP, COPYING OF DATA AND ACCESS CONTROLS, BUT NOT NECESSARILY IN THAT ORDER]

IPA safeguard	RAG rating	Rationale
[REDACTED]	GREEN	[REDACTED]
[REDACTED]	RED	[REDACTED]
Review, retention, and deletion (RRD)	AMBER	[REDACTED]
[REDACTED]	N/A	[REDACTED]
[REDACTED]	RED	[REDACTED]

4.5 *[Data Type 4]*

[REDACTED]

4.5.1 [REDACTED]

4.5.2 [REDACTED]

4.5.3 [REDACTED]

[REDACTED]

[REDACTED FIGURE]

4.5.4 [REDACTED]

4.5.5 [REDACTED]

4.5.6 [REDACTED]

4.5.7 [REDACTED]

4.5.8 [REDACTED]

4.5.9 [REDACTED]

4.5.10 [REDACTED]

Compliance with IPA safeguards

4.5.11 Our provisional conclusions are as follows.

[THE REDACTIONS IN COLUMN 1 OF THE TABLE BELOW INCLUDE LPP, COPYING OF DATA AND ACCESS CONTROLS, BUT NOT NECESSARILY IN THAT ORDER]

IPA safeguard	RAG rating	Rationale
[REDACTED]	GREEN	[REDACTED]
[REDACTED]	RED	[REDACTED]

Review, retention, and deletion (RRD)	RED	[REDACTED]
[REDACTED]	N/A	[REDACTED]
[REDACTED]	RED	[REDACTED]

4.6 *[Data Type 5]*

Context

4.6.1 [REDACTED]

4.6.2 [REDACTED]

4.6.3 [REDACTED]

4.6.4 [REDACTED]

[REDACTED]

4.6.5 [REDACTED]

4.6.6 [REDACTED]

Compliance with IPA safeguards

4.6.7 Our provisional conclusions are as follows. [REDACTED]

[THE REDACTIONS IN COLUMN 1 OF THE TABLE BELOW INCLUDE LPP, COPYING OF DATA AND ACCESS CONTROLS, BUT NOT NECESSARILY IN THAT ORDER]

IPA safeguard	RAG rating	Rationale
[REDACTED]	AMBER	[REDACTED]
[REDACTED]	RED	[REDACTED]
Review, retention, and deletion	RED	[REDACTED]
[REDACTED]	N/A	[REDACTED]
[REDACTED]	RED	[REDACTED]

4.7 *[Data Type 6]*

[REDACTED]

4.7.1 [REDACTED]

4.7.2 [REDACTED]

4.7.3 [REDACTED]

4.7.4 [REDACTED]

4.7.5 [REDACTED]

Compliance with IPA safeguards

4.7.6 Our provisional conclusions are as follows.

[THE REDACTIONS IN COLUMN 1 OF THE TABLE BELOW INCLUDE LPP, COPYING OF DATA AND ACCESS CONTROLS, BUT NOT NECESSARILY IN THAT ORDER]

IPA safeguard	RAG rating	Rationale
[REDACTED]	GREEN	[REDACTED]
[REDACTED]	GREEN	[REDACTED]
Review, retention, and deletion (RRD)	GREEN	[REDACTED]
[REDACTED]	N/A	[REDACTED]
[REDACTED]	GREEN	[REDACTED]

5 LPP material

5.1.1 We discussed MI5's arrangements for LPP material in relation to the [the TE]. If MI5 needs to delete an item subject to LPP – either because MI5 decides there is no necessity case for retaining it, or if directed to destroy it by a JC – there is a manual process to delete the data from the relevant data store in [the TE].

5.1.2 [REDACTED]

5.1.3 In this sense, MI5 is unable to comply fully with the IPA's safeguards around legally privileged material, as set out in the relevant Codes of Practice. The [Code of Practice] sets out the requirement as it applies to all similar types of warranted data:

"Privileged items must be securely destroyed when their retention is no longer needed for those purposes. If such content is retained, there must be adequate information management systems in place to ensure that continued, retention, for purposes other than their destruction, remains necessary and proportionate for the authorised statutory purposes."

5.1.4 In addition, *[REDACTED]*, it is unlikely MI5 could give complete assurance it had complied with any conditions imposed by a JC as to the use or retention of legally privileged items.

5.1.5 Following the inspection, MI5 also informed us of a further risk of LPP material in specialist systems. 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 raw product within [the TE] is not replicated in a copy retained in a file share. MI5 is working to establish whether this is an appreciable risk and what mitigations may be available.

6 System-wide safeguards

[REDACTED]

6.1.1 [REDACTED]

6.1.2 [REDACTED]

6.1.3 [REDACTED]

Data transfer and sharing arrangements

6.1.4 We were briefed on MI5's internal process for approving the transfer of data into or out of [the TE]. In theory, users wishing to transfer data must seek approval from the [Strategic Engagement and Change] team, who consult relevant stakeholders and ensure the appropriate safeguards and risk mitigations are in place.

6.1.5 The [Strategic Engagement and Change] team has a process by which [REDACTED] data transfers in or out of [the TE] are managed. However, in practice, it was clear that not all data transfers do go through the [Strategic Engagement and Change] team. [REDACTED]. [The biggest difficulty for those implementing this process is that various business areas have a range of local processes in place for transferring data]

[REDACTED]

6.1.6 [REDACTED]

6.1.7 [REDACTED]

6.1.8 [REDACTED]

Remediation work on file shares

6.1.9 [REDACTED]

6.1.10 MI5 also has a process in place to identify, quarantine and delete old data in file shares for which there is no longer a necessity and proportionality case for retaining it. To date, [a percentage] of file shares have been "scanned" to determine their contents. Analysis has been completed on [a percentage], and the required action (deletion or moving data) has completed for [a percentage] of file shares.

6.1.11 MI5 informed us that, on current plans, they expect to have completed the process of scanning file shares and quarantining data [in 2019]; the data will be held in quarantine [for a period of time] before being deleted. While in quarantine

these files will only be accessible to [a limited group] [REDACTED]

6.1.12 [REDACTED]

7 Institutional knowledge and governance

7.1.1 By reference to a selection of internal papers provided by MI5, we reviewed the extent of MI5's knowledge of the compliance problems within [the TE]. The summary which follows is illustrative, as we have not reviewed all of the relevant paperwork.

[Legal] paper on compliance risk, January 2016

7.1.2 In January 2016, a senior MI5 lawyer produced a paper on compliance risk which touched on [the TE]. The paper emphasised that:

> *"Allowing uncharted material to remain [in [the TE]] presents considerable legal risk... We may fall foul of our duty under the SSA to only hold material for as long as is necessary for our statutory functions – but auditing [the TE] manually has proven extremely resource intensive, and the work is not complete."*

7.1.3 In mitigation, the paper recommended that MI5 should:

> *"ask staff to claim that material they require for current use and then delete everything else without resorting to further audit."*

7.1.4 In the event, given the complex way in which data was in use within [the TE], this recommendation was not capable of being implemented.

[The TE] review – October 2016

7.1.5 In October 2016, a review was conducted of the [the TE]. Whilst this was focused on security risks in the system, it also considered legal risks and concluded that there was:

> *"a high likelihood of relevant material not being discovered, or being discovered when it should have been deleted, in a disclosure exercise leading to substantial legal or oversight failure."*

7.1.6 This issue had first *[been identified as being relevant to disclosure exercises in 2014]*. The author expressed concern that insufficient progress had been made in reducing this risk:

> *"I do not believe that enough has been done to ensure that this legacy risk doesn't increase and resolution of identified issues feels as though it is stalled".*

7.1.7 Whilst at this early stage MI5's concern was focused on potential disclosure risks, the paper also clearly highlighted a compliance risk around review, retention and deletion of material:

> *"in the context of information management our limited understanding of what is on the system means that we are unable to apply effective review, deletion and discovery techniques.* [REDACTED]."

Paper on [the TE] risks, March 2017

7.1.8 [The Information Central team] produced the above paper for [the Director of Strategy], four Directors and others in March 2017. It included a clear assessment of the compliance risks posed by [the TE]:

> *"There is significant risk around the absence of compliance with relevant legislation, Codes of Practice and Handling Arrangements. This includes categories of data for which there are [particular rules].*

7.1.9 The paper highlighted the deletion risk above, but also concluded:

> *"There is also a compliance risk in that MI5 would currently be unable to give sufficient assurance [around compliance with] with current legislation."*

Paper on compliance in the [the TE], October 2017

7.1.10 A year after the first [the TE] review, the author provided a further update to four MI5 Directors and others on the progress that had been made under the [the TE Improvement programme].

7.1.11 The paper remained focused on disclosure risks, concluding that:

> *"The main legal risk here remains one of disclosure in that we may not find relevant material which is held [REDACTED] on [the TE]."*

7.1.12 However, the RRD compliance risk was also clearly spelled out:

> *"many systems can't delete, [REDACTED], and we continue to build some without it."*

7.1.13 The paper also highlighted [concerns with] access controls [REDACTED]:

> *"[REDACTED]"*

7.1.14 In conclusion, the paper made a clear recommendation:

> *"we need a new plan that prioritises hard on the top compliance risks and sets out a realistic target state. This plan needs to focus in on the management and use of warranted data (or [some] forms of it if this is still too big a problem) as its first step."*

Management Board paper on compliance risk, January 2018

7.1.15 In January 2018, [the Director of Policy and Information] produced a paper for the Management Board (MB) on compliance risk. The dashboard attached to this paper included four risks specifically about [the TE]:

- *"We do not have a comprehensive, effective and implemented RRD [in one of the systems]"*
- *"Effective RRD has not been implemented across all data stores in [the TE], potentially including warranted material, and therefore there is a risk that elements of it are non-compliant."*
- *[REDACTED]*
- *"There is a risk that we are unable to guarantee that we can identify and destroy LPP and [other] material consistently across all systems where it may be present."*

7.1.16 At this point, we judge that MI5 had a clear view of some of the compliance risks around [the TE], to the extent that they should have carefully considered the legality of continuing to store and exploit operational data in [the TE]. The risks were also sufficiently clear that they could have been communicated to the IPC. There is no indication that this was contemplated by the MB, though there was a recommendation in the paper to *"update Whitehall stakeholders (particularly Home Office), through the QR process."*

7.1.17 In addition, the lack of a consistently-implemented and robust RRD process [in one of the systems] which was flagged to the MB probably constituted a relevant error: without such a policy, material was highly likely to be held [in one of the systems] which was beyond its approved retention period, as has turned out to be the case in [a data store] error reported to IPCO by MI5 on 4 March 2019 (see above).

7.1.18 More broadly, the risks as set out clearly in [the Director of Policy and Information's] paper call into question the validity of MI5's summary of its own handling arrangements [for categories of warranted material], which were made available to JCs via the MI5 Handbook in May 2018. These stated that, amongst the arrangements *"implemented by MI5 to satisfy the requirements of sections 53, 54, 129, 130, 150, 151, 191 and 192 of the Investigatory Powers Act 2016":*

> *"Members of MI5 should access [warranted] material only where and to the extent necessary in the proper pursuit of MI5's statutory functions. [...]*
> *[Warranted] material must be destroyed as soon as there are no longer any grounds for retaining it as necessary, or likely to become necessary, for any of the [authorised] purposes*
> *[...]*
> *[Warranted] material which is not linked to a paper or electronic file [which includes [REDACTED] in [the TE]] will be destroyed as soon as there are no longer any grounds for retaining it for any of the [authorised] purposes... All such material will be destroyed as soon as reasonably practicable."*

7.1.19 In response to the paper, the MB elevated the associated risk on the [corporate register] to RED and *"noted that the Audit Risk and Assurance Committee planned to carry out a deep dive review of compliance risk in June 2018."* We have not yet seen the results of this review.

Executive Board paper on [the TE] compliance risks, October 2018

7.1.20 This paper for the Executive Board (EB) set out many of the risks above in further detail. It included a yet starker assessment of the compliance risks involved:

> "MI5 is unable to provide robust assurances to its oversight bodies that data held in the [TE] cannot be accessed unlawfully. *The risk is that the IPC may be unwilling to authorise further warrants until this is rectified, especially for [a category of data].*
>
> [...]
>
> *"Effective RRD has not been implemented across all data stores in [the TE], potentially including warranted material...[this could] lead to successful IPT challenges, loss of confidence of ministers/JCs and consequently restrictions in warrants or reputational damage."*

7.1.21 The paper hinted at communicating these risks to the IPC:

"we anticipate that MI5 will want to pre-emptively brief oversight bodies on these challenges and our plans to address them".

7.1.22 However, communication with the IPC did not appear in the paper's list of actions, and in the event the IPC was not briefed on [*the TE*] compliance risks until February 2019. The other *"oversight bodies"*, namely the ISC and IPT, have not been made aware.

8 Conclusion

8.1 On 22 March, the IPC and Deputy IPC discussed the findings of this report with members of the MI5 Management Board and other relevant staff. MI5 acknowledged the seriousness of the compliance risks within [*the TE*], and expressed regret that they had not made IPCO aware of them sooner.

8.2 Following the meeting, MI5 shared a summary of its planned mitigations for the compliance risks within [*the TE*], which will inform a Home Office submission to the Secretary of State. Following that submission, MI5 will be producing forms of words to summarise the compliance risks of [*the TE*] and proposed mitigations, which will inform decisions as to whether to approve these warrants.

9 Annex: list of updates

Updates included 29 March 2019:

- Section 4.1 updated to make clearer the statutory basis for the safeguards which apply to each category of operational data.
- References to [*the new system*] updated to correct data by which this system is expected to be live [*in 2019, but later than originally reported*]
- [*One*] section updated to clarify that *[REDACTED]*. [*applies to an application*]
- Additional risk identified for LPP material (see 5.1.5).
- Description of *[REDACTED]* throughout amended to make clear it is not an IPA safeguard in its own right, but a means to assure compliance with IPA safeguards.