[redacted]

[redacted] **document**

[redacted]

10 December 2018

[redacted]

[A **– Legal Issues and IPCO engagement**

Key Points

- *[A volume of data obtained from warrants and authorisations is currently being held on the TE, an environment with issues related to auditing]* ;
- The data is subject to legal requirements, in particular the Investigatory Powers Act Codes of Practice and Handling Arrangements; many of those requirements (particularly RRD) are not being followed. Significant legal and compliance issues arise from this non-compliance;
- The [redacted] *[TE]* Strategy paper discussed by EB on 30 October 2018 sets out the work which needs to be done to fully mitigate these risks under the [redacted] programme which is due to begin in FY 2019/20;
- We are required to report failures to comply with Codes of Practice requirements to IPCO (see para 16 for more detail). Our knowledge regarding compliance risks is not complete, however we know enough to be able to articulate the issues discovered. Failure to report in a timely fashion, would, if discovered by IPCO or by the Investigatory Powers Tribunal, be considered a significant breach of trust and is likely to lead to public censure, damage to reputation and calls to curb our powers. **We therefore recommend reporting to IPCO ASAP in the manner recommended in this paper.**

Background:

What is the *[TE]* **?**

1. [redacted] Whilst we know which [redacted] *[platforms]* operate within the *[TE]* , we do not have a comprehensive inventory of all the

[redacted]

data that resides within it [redacted]. Despite its range of issues, the *[TE]* is *[important to delivery MI5's mission strategy]* . [redacted]

2. A number of attempts have been made to improve the *[TE]* over recent years. *[In October 2018 EB endorsed the establishment of a programme to commence at the beginning of 2019/20 which included addressing the legal and compliance risks]*

[redacted]

5. **As you know, data obtained by a warrant/authorisation must be managed in accordance with the relevant Code of Practice and/or statutory/internal Handling Arrangements.** Insofar as any data within the *[TE]* wasn't obtained by a warrant/authorisation it is likely that it is covered by other legislative requirements such as Data Protection legislation and/or The Security Service Act Handling Arrangements.

6. The different Codes of Practice/Handling Arrangements that govern different data types set out the rules that govern how we must handle the relevant data. The requirements vary from general requirements to keep the data only for as long as is necessary and proportionate to perform our functions ("RRD"), to detailed requirements that require specific treatment for particular data types e.g. to delete/flag LPP material or requirements to audit access.

Are we Compliant with Legal Requirements?

002

[redacted]

7. [redacted] However, it is important to note that we are likely to encounter other potentially significant risks as we broaden out this work [redacted]. The following observations are based on the 'known knowns' about our data holdings:

- The main IT systems held on the *[TE]* are compliant with most of the legal requirements regarding the management of data within those systems. [redacted]

- The general risks relating to access controls [redacted] in the *[TE]* are *[legal compliance risks]* in that the Codes of Practice contain *[specific]* requirements to ensure that that data is kept safe. [redacted]

- [redacted]

- *[Certain users are able to access information in TE without having a clear n&p case for doing so]*

- [redacted]

- There is no clear policy, guidance and governance to ensure consistent compliance across the *[TE]* [redacted]

[redacted]

003

[redacted]

Is there a plan to mitigate the legal risks associated with the *[TE]* **?**

8. [redacted] LPP initiated the *[TE]* programme of tactical work in summer 2017 which sought to mitigate *[risks]* . The legal compliance risks presented by the *[TE]* were logged on the legal compliance risk register when this was created in November 2017, although it was not formally introduced and endorsed until Q1 2018/19.

9. *[The compliance strand of the TE programme tactical work only began substantially from mid-2018 when the necessary resources became available.]* . Many of the legal risks could be mitigated by deletion of data once it is no longer required for statutory purposes. [redacted] At this stage we do not know how long the work to delete the data is likely to take although it is likely to be on the scale of many months.

10. [redacted] from mid/late 2019 believe that we will have a sophisticated tool available [redacted] to search for [redacted] different types of data obtained under authorisations, [redacted] However, until we begin using such a tool we cannot be certain how effective it will be or how long it will take to work through the different areas of the *[TE]* , and it will require substantial business involvement.

11. The *[TE programme]* has already delivered improvements [redacted] there remains a risk [redacted] could be viewed as a failure to comply with our legal compliance obligations.

12. [redacted].

13. [redacted] **it is likely to take many months to understand and then mitigate the most pressing legal risks.** [redacted]

004

[redacted]

[Work on the compliance strand of the TE programme tactical work will bring important mitigations in the short term and help shape and inform the transformative work that the [REDACTED] programme will deliver on guidance, governance and culture]

What is our legal obligation to report the issues identified and under whose remit do they fall?

14. [redacted] LPP It is worth noting that the data within the *[TE]* could cut across the remit of both IPCO and the Information Commissioner but we need to ascertain precisely what data is held in the *[TE]* before we can advise further.

15. We could choose not to report the compliance obligations identified, but obviously were the issues to be discovered by IPCO and/or the ICO e.g. through a whistleblower, a data loss, forced disclosure in an IPT hearing etc, the failure to report would significantly undermine the trust we have built up with IPCO and would be likely to lead to public criticism and censure. If we report voluntarily, rather than appear to have the information forced from us, IPCO may be less likely to take a hard-line response.

How might IPCO view the compliance problems if reported?

16. IPCO are likely to want to know when we first became aware of the legal compliance problems identified above and we will need to be prepared to explain this to them. It is only in recent months that the full extent of the issues have become clear and we have been able to better scope the legal compliance issues sufficiently to be able to report them.

17. Once we have brought IPCO up to a sufficient level of understanding, they are likely to regard aspects of data management within the *[TE]* as not complying with legal requirements. They are likely to be sympathetic to our problems, but they will want to be seen to be doing what is required of them as an oversight body. There are likely to be a number of consequences:

    a) [redacted] LPP

    b) IPCO may wish to write about the issue in their annual report, due in December 2019. This could have the effect of alerting privacy groups who might seek to bring a case before the IPT in order to probe the issues identified;

    c) IPCO may consider that the legal compliance issues should be taken into account by the Secretary of State and IPCO when they consider our warrants. At first blush, it is possible (though we think unlikely) that they could, as their Canadian oversight counterparts have done in similar cases, view the matters identified as so serious as

[redacted]

to opine that warrants [redacted] should not be authorised [redacted];

d) IPCO may respond by seeking greater scrutiny of IT systems and their operation through the inspection regime.

Approach to IPCO engagement

18. Sir Adrian and his Judicial Commissioners/inspectors are of course reasonably familiar with IT issues. However, they are unlikely to have come across an issue of this size and complexity and we will need to be very considered in the way the issues are explained to them. We recommend first sending a short letter outlining the issues in basic terms and inviting Sir Adrian to a presentation in which we can explain the issues in more detail. We recommend that this briefing is followed up by a more detailed letter that ensures we have an accurate record of what has been formally reported (something that IPCO can also use within their organisation to explain the issues clearly, as we have recent experience of briefings not being accurately cascaded).

19. Given IPCO's possible range of responses outlined above, we think that it would be prudent to have a course of action ready to suggest to them during/after the first briefing, to ensure that their energies are directed as constructively as possible. For example, we could suggest that Sir Adrian call upon the TAP[2] to investigate further, check what we are telling them and validate our mitigation plans. Recent experience of the TAP is that members are keen to provide assistance to work together with both IPCO and UKIC; they have been well engaged at briefings on our work and have made helpful observations on such matters as [redacted]

20. Before we brief IPCO we also recommend:

- [redacted]
- Given the likelihood that Sir Adrian will suggest the Home Secretary should be made aware of the issues, we recommend also first briefing Home Office policy and legal colleagues (who may well recommend briefing the Home Secretary to cover off his awareness of the issues from a warrant signing perspective);

Meanwhile

21. Briefing IPCO and going through the other steps outlined above may take some time to complete. Meanwhile [redacted] and [redacted] will continue to work alongside the *[TE]* programme team as it becomes established to ensure that compliance remains a core priority as part of programme outcomes and business change.

[redacted]

[2] The Technical Advisory Board has been established to provide advice to the IPC and Secretary of State on (i) the impact of changing technology on the exercise of investigatory powers and (ii) the availability and development of techniques to use such powers whilst minimising interference with privacy.

006