[MI5 Letterhead]

Sir Adrian Fulford
Investigatory Powers Commissioner

11 March 2019

Dear Sir Adrian

As you requested, this letter sets out in prose the details that we gave you during the presentation on 27 February on MI5's use of data in the *[Technology Environment (TE)]*. It describes in some detail how data obtained under warrants and authorisations flows through and is stored in [*two of the technology environments*]; the critical capabilities the *[TE]* hosts; the challenges we are identifying, the mitigations already underway and our strategic programme [*REDACTED*] that will transform how we manage and exploit data compliantly, securely and effectively in the future. This account is necessarily long and detailed: it seeks to cover the questions raised at the briefing and keep sufficient background to assist understanding. As you requested at the presentation, we will be writing to you separately with proposed forms of words to insert into our warrants to reflect the challenges described.

What is the [*TE*]?

2. *[MI5 uses different technology environments. One of these technology environments will be referred to as "the Technology Environment" or TE. This TE holds data including warranted data].*

Why the *[TE]* is [*important*]

3. We presented a case study during your visit that illustrated how we use the *[TE]* for mission purposes. The key points we emphasised were that our access to data is increasingly diffused across multiple forms of access which are often transitory and fragmentary. We have to keep pace with technological developments [*REDACTED*]. To be operationally effective we need to be able to access [*REDACTED*] a [*REDACTED*] range of data, using the best tools possible, in the shortest timeframe to meet mission demands. [*REDACTED*] Should you think this necessary, we would be happy to brief the Judicial Commissioners on the [*capabilities*] provided by the [*TE*].

History and development of the [*TE*]

4. [*REDACTED*]

How is data managed in the [*TE*]?

5. There are many systems in the [*TE*] that collect and process [*warranted*] data[1] from outside MI5. [*REDACTED*]

6. Once data is inside the [*TE*], it needs to be stored in different locations within the [*TE*]. Warranted data [*is stored and*] is then interrogated by a [*REDACTED*] range of applications by the

[1] We will use the term 'warranted data' to include data obtained both under IP Act warrants and under authorisations and warrants under RIPA.

[analysts] who work in the [TE]. Analysts then produce [formal products] which [REDACTED] form our [record] in [different systems] [REDACTED]. [Some data is copied and stored in file shares or on a Desktop where it is processed further.] [REDACTED] File Stores, which are network storage areas used to store a [REDACTED] range of data and information are used for testing and training purposes. [REDACTED]

7. Some warranted data, on the other hand, may merely transit through the [TE], after limited processing, [to another TE for storage]. [REDACTED]

8. We have a range of data stores, typically focused on specific types of warranted data, rather than keeping all data in one 'big pot'. We use applications to range across different data stores and types [REDACTED]. We have, or will have, automatic RRD process for our main Data Stores although the RRD rules vary according to the intrusive and technical nature of that data or, in some cases, are system specific. Some File Stores and other areas may not have an RRD process.

The developing picture of the [TE] challenges

9. Much of MI5's work to address potential risks in the [TE] has, until relatively recently, been pursued from the quite particular perspectives of different specialists, including [REDACTED] compliance and [REDACTED]. This work was brought together in a truly holistic manner for the first time for the Executive Board (EB) in October 2018, in a series of detailed briefings. This was later than would have been ideal, as our focus through 2017/18 was on essential changes to ensure compliance with the IP Act. Since October, we have continued to invest significant effort and are constantly finding new ways of analysing and mitigating issues. Our understanding will evolve: in some areas we are confirming strong assurance while, regrettably, in other areas we are likely to discover more compliance issues. Indeed, we have learned more even since our 27 February briefing.

10. Initial investigations into [TE] issues were prompted by specific concerns. [REDACTED]. This was perceived at the time as an information management issue which did not require substantial remedial work beyond this specific issue. In January 2016, as part of a wider review of legal compliance in anticipation of new legislation, the [REDACTED] problem led the team conducting the compliance review to identify, at a high level, that data might be being held in ungoverned spaces in contravention of our policies and recommended that we should examine whether we could build a tool to delete all such material, save for material selected for preservation. This risk, together with [another risk], were subsequently identified in a report to the Management Board and reported in a dashboard from early 2018. Mitigation work had been tasked to the [legal compliance programme] but it became apparent that the task of examining the [TE] was too large [for the legal compliance programme] as it had to remain focused on the urgent changes needed to be compliant with the Investigatory Powers Act. We had also by this stage initiated the [TE improvement programme], which was set up in 2017 following a report which raised concerns about [other potential] issues (as requested, we shall share this report with you). Later in 2017 we added a compliance strand to the [TE improvement programme]'s work and, while we have made progress on [mitigating risks] [REDACTED].

11. In late 2018 the EB noted the scale of the challenges involving the [TE], endorsed the creation of a transformative programme, [REDACTED], to address these risks, as well as supporting tactical mitigations already underway. The EB also formally agreed that we should brief IPCO and we extended the invite to you shortly afterwards. I apologise if you consider we should have briefed you on these matters earlier. The truth is that we did not sufficiently understand the issues ourselves until

the EB discussions in late 2018 and our understanding is still developing. However, we considered the issues were of sufficient importance to brief you at this stage.

Challenges and Mitigations

12. The challenges we face in the [*TE*] broadly relate to [*REDACTED*] compliance, [*REDACTED*]. For context, it is important to set out that as a [*secure*] environment, the *[TE]* has a range of extensive security protections in place. These include both technical security measures but also that all users are DV cleared, which provides an important mitigation to potential people-related risks. In terms of compliance, all [*TE*] users are required to have completed our *[mandatory legal]* training and Data Protection Act training, alongside their job specific training and guidance.

[Security Considerations]

13. [*REDACTED*]

i. [*REDACTED*]
ii. [*REDACTED*]
iii. [*REDACTED*]

[*REDACTED*] However, given [*issues*] it is challenging to manage [*risk*]. In response, we have both an ongoing programme to mitigate such risks on our current infrastructure, and the [*TE programme*] to provide a strategic solution.

14. [*REDACTED*]

Internal access controls

15. [*REDACTED*]

16. Many of [*TE's areas*] have [*mitigations*], though some do not. For those that do not, this means that [*users*] could theoretically [*an issue*]. [*These files may contain warranted material*]. As you would expect, we are therefore undertaking [*mitigations against this*]. This will take some time [*REDACTED*]. We are therefore working through the [*areas*] to assess [*REDACTED*]. We have developed a capability to [*enable this*]. Given the variables, completion timelines are difficult but we expect [*REDACTED*].

17. [*REDACTED*]

18. [*REDACTED*]

19. [*REDACTED*]

Understanding where and how warranted data is [*processed and managed*] through to deletion

20. Historically we focused on managing data and information in [*another technology environment*] and especially our [*record*]. We have invested significantly in this area, including [*a new document management system*] [*REDACTED*] and improvements to the [*Centrally Retrievable Record*] (recommended by the Operational Improvement Review, commissioned after the terrorist attacks of 2017). As explained above, data in the [*TE*] was previously regarded as ephemeral: it was there to be processed and turned into [*products*] that were sent to a system in *[another technology*

environment]. This starting point, coupled with the rapid growth of data, users and systems and complexity of where data is stored, has resulted in less effective management of data and information and less assurance of compliance. We now have [*a register*] in a standalone application which is improving our picture of where data is. The [*register*] began development after our initial review of information management in the [*TE*] in 2015. We are currently focusing our efforts on recording [*types of warranted*] data, [*REDACTED*].

21. Broadly speaking, the applications used by the majority of [*TE*] Users provide good assurance that warranted data is only accessible by [*users*] in accordance with our RRD[2] policy. However, we are examining whether all of our data stores give full effect to that policy. [*REDACTED*]. Unfortunately, we have recently identified a reportable error [*within one data store*]. While [*users*] cannot view [*product*] older than [*a period of time*], this material has persisted [*in the system*] since October 2016 (not 2015 as reported at the briefing) because of a failure to implement an automatic RRD/deletion process. We have written to you separately on this specific error. We are working to increase automatic RRD (as opposed to a manual review and deletion process). [*REDACTED*]

22. As we go through our systems and File Shares (see below) we have identified and are investigating further potential errors. These include warranted data persisting beyond the time when they ought to have been considered for deletion or have been deleted in accordance with our RRD policy and so risking there being no clear necessity and proportionality case to do so. We will of course alert your office to any further reportable errors as and when we confirm them.

We have also put in place a process to prioritise review of File Shares (described above) to make decisions to retain or delete as necessary. As explained previously, it is necessary to [*store and process some warranted data in File Shares*], for a range of reasons as enabled by the IP Act. However, while we are broadly confident that where this is occurring, it is necessary, there is a risk that some File Shares contain warranted data that may be being retained for longer than is necessary and proportionate because there has not been a sufficiently robust process in place to review it and implement a decision to retain or delete.

23. We are prioritising our review of those File Shares(i) where data has not been accessed for [*a period of time*], and is therefore more at risk of being held outside RRD policy, (ii) where the name and other attributes of a file share indicate it is more likely than not to contain warranted data and (iii) where the document types indicate such data [*REDACTED*]. There are [*number*] high level File Shares in the Production Environment of the [*TE*] and thus far we have scanned *over half of them* of them. [*REDACTED*] For example, we have identified that part of one file share contains [*data*] obtained under authorisation or warrant and previously used for training purposes. We now have no need to retain them and have made the decision to delete them. We will however place this data in quarantine to ensure it does not break any automated processes and in the meantime we will confirm whether this might constitute a reportable error.

24. We will introduce as quickly as possible new processes, training and guidance on the use of File Shares to encourage better practice and give us better assurance of compliance.

Our Longer-Term Strategy - *[the strategic programme]*

---

[2] RRD is short for 'review, retain and delete' and is used to mean a process designed to ensure data is only kept for the minimum time necessary. This may be achieved by prescribing a set period for review and a decision to retain or delete or it may be achieved by automatic deletion, e.g. after a period of time or other conditions are met.

25. [*REDACTED*]

26. At the end of 2018 MI5's EB therefore agreed to embark on [*a programme]* to transform how and where we operate in the future. *[This will require a transformation in how we manage data].* Most importantly, we will change our operating model, setting the right conditions to work effectively, compliantly and at pace in any environment we are required to do so. This will mean more robust working practices, policies and control mechanisms to ensure we are operating at the highest assurance levels. We shall keep you informed of progress.

Reflecting [*TE*] Compliance Risks in our Warrant Applications

27. As you know, before a Secretary of State can approve an MI5 warrant (and, by extension, a Judicial Commissioner can approve the Secretary of State's decision) the Secretary of State must consider that MI5 has satisfactory arrangements in place to ensure the requirements of the Investigatory Powers Act (i.e. sections 53 and 54 and their equivalents) are being met (minimum necessary access, disclosure, copying and retention of warranted data).

28. We have briefed the Home Office in the same terms as we have briefed you and they are currently examining the issues closely and are preparing a further submission to the Home Secretary. Our view is that there are a number of key factors to examine when considering whether our current arrangements are satisfactory:

a) as we have explained above, there are risks that some warranted data contained within the [*TE*] could be [*REDACTED*]. However, we believe we are doing all that is reasonably possible to mitigate those risks [*REDACTED*];
b) there is evidence that suggests that it is likely that data has been retained beyond the point that it is necessary and proportionate (e.g. from our initial work to examine the File Shares described above). Whilst we recognise that this situation cannot be allowed to persist, we are working hard to review this data and delete it as soon as is reasonably practicable. As per a) above, there is no evidence to suggest that data being held beyond the point that it should have been deleted is being accessed inappropriately [*REDACTED*];
c) as we perform the work to mitigate a) and b) above and are able to establish specific non-compliance that amounts to an error [*REDACTED*] we are reporting it to you and the Home Office;
d) we are making significant investments through [*the strategic programme*] to approve our assurance of compliance in the long term.

We will write to the Home Office shortly proposing a suggested form of words for inclusion in our warrants (and also accompanying detail to be contained within the Warrantry Handbook).

Yours sincerely,

[Director]
Policy, Compliance, Security and Information, [*MI5*]

[*REDACTED*]

900

Annex A

[*This Annex contains a diagrammatic representation of the TE and TE2 Area 2*]

900

[*REDACTED*]