Annex H - Section II: further information about [*the TE*] and the mitigations being progressed, issued 1 April 2019.

1. This note sets out the mitigations in place to deal with the ~~[*risks*]~~ compliance risks within the [*TE*], as set out in the IPCO Inspection report dated 29 March (version 2). It explains how MI5 consider the requirements of ~~[*the Act*]~~ section 53 are met when those mitigations are taken into account.

2. It is worth noting at the outset that this is a live situation. This note represents the current position but we are still investigating and further mitigations and measures may be possible.

The [*TE*]

3. As set out in the letter to the Investigatory Powers Commissioner of 11 March, the opportunities and capabilities offered by the [*TE*] are [*important to MI5*]. In order to fulfil our statutory requirement to protect national security, MI5 needs to be able to access and [*REDACTED*] range of data, using the best tools possible [*REDACTED*].

4. Continued use of the [*TE*] is necessary to enable MI5 to protect national security. It is not possible simply to stop using the [*TE*] for the processing or storage of warranted data without [*impairing*] effectiveness.

5. ~~[*REDACTED*]~~ [*The TE was originally intended as a temporary place for data processing, and not as a place for data storage such as it now contains, and technical fixes are not straightforward.*]

Legal requirements

6. The Investigatory Powers Act applies consistent safeguards across all types of warrant. The Secretary of State, before issuing a warrant, must consider that satisfactory arrangements are in force in relation to the warrant, setting out safeguards for the retention and disclosure of material obtained under the warrant. The requirements of section 53 in relation to targeted intercept material are replicated across each of the warranted powers, targeted and bulk (save for bulk personal datasets under Part 7, for which there is no directly equivalent provision – the Secretary of State must consider that there are satisfactory arrangements for storing bulk personal datasets and protecting them from unauthorised disclosure but there is no further provision as to these arrangements).

7. The requirements of section 53 (and equivalent provisions in the Act) are as follows:

   - Arrangements must be in place to secure that each of the following is limited to the minimum necessary:
     a. the number of persons to whom any of the material is disclosed or otherwise made available;
     b. the extent to which any of the material is disclosed or otherwise made available
     c. the extent to which any of the material is copied
     d. the number of copies that are made.

   - The arrangements must include arrangements to secure that every copy made of the material is stored in a secure manner.

- Every copy made of any of the material must be destroyed as soon as there are no longer any relevant grounds for retaining it.

8. Specific handling safeguards apply to certain categories of material – for example material subject to legal professional privilege (section 55 and equivalent provisions).

9. In addition, the IP Act requires additional safeguards for the selection for examination of material obtained in bulk (e.g. in section 152).

    - The selection for examination must be:
        a. carried out only so far as necessary for the operational purposes specified in the warrant
        b. necessary and proportionate in all the circumstances.

~~6. The Investigatory Powers Act applies consistent safeguards across all types of warrant. The Secretary of State, before issuing a warrant, must consider that satisfactory arrangements are in force in relation to the warrant, setting out safeguards for the retention and disclosure of material obtained under the warrant. [*REDACTED*] – the Secretary of State must consider that there are satisfactory arrangements for storing [*REDACTED*] and protecting them from unauthorised disclosure but there is no further provision as to these arrangements).~~

~~7. The requirements of [*the Act*] are as follows:~~

~~• [*REDACTED*];~~

~~• [*REDACTED*];~~

~~• [*REDACTED*].~~

~~8. Specific handling safeguards apply to certain categories of material – for example material subject to legal professional privilege ([*REDACTED*] and equivalent provisions).~~

~~9. [*REDACTED*].~~

Compliance

10. MI5 has in place high level handling arrangements for each type of warranted product, supported by underlying policies and guidance. Handling Arrangements exist to reassure the Secretary of State that we have arrangements in place to govern the handling of the product of each type of authorisation. Policies articulate, at a relatively high level, how MI5 will operate within the legislation. Guidance provides advice to individuals on how to conduct individual processes in accordance with policy and may be team, role or system specific.

11. For all MI5 systems, we provide training and guidance for staff on how to comply with the handling arrangements and policies. For our core systems and main data flows, the policies and guidance are supported by technical controls that [*among other things*] ensure data is deleted when it should be. [*REDACTED*].

12. All [*TE*] users are DV cleared and are required to have completed our [*mandatory legal*] training and Data Protection Act training, alongside their job specific training and guidance.

13. This note sets out the compliance risks in relation to the Act, internal policies and guidance and identifies the measures that are being put in place ~~[REDACTED]~~ in the immediate term (*[a matter of weeks]*) to remedy those defects in relation to new warranted data being ingested into the [*TE*]. The note focusses on the measures that are being put in place for new data being obtained under warrants and does not set out in any detail the measures that are also being put in place in relation to data which has already been ingested into the [*TE*], although such measures are being deployed.

14. [*REDACTED*].

Measures being put in place

15. [*REDACTED*] Fixing the immediate [*TE*] compliance problems has been assigned the highest priority within our IT capability build teams.

16. Beyond the immediate term measures described below, we are currently exploring systematic processes and monitoring that will allow us to further mitigate compliance risks. [*REDACTED*].

17. In the longer term, a major programme has been commissioned to transform MI5's ways of working with [*sensitive*] information, particularly in the [*TE*]. The programme will be realised through working practices, data and technologies that improve mission effectiveness, mission efficiency and provide better safeguards, helping to reduce [*the*] risks.

18. The paragraphs below set out the measures that have been and will be taken in the immediate term to mitigate the compliance risks, using the structure of the IPCO Inspection Report (version 2, dated 29 March).

[THE HEADINGS IN BOLD BELOW BEFORE PARAGRAPHS 19, 28 AND 54 INCLUDE COPYING OF DATA AND ACCESS CONTROLS, BUT NOT NECESSARILY IN THAT ORDER]

[*REDACTED*]

19. [*REDACTED*]

20. [*REDACTED*]

21. [*REDACTED*].

22. [*REDACTED*]

23. [*REDACTED*]

24. [*REDACTED*]

25. [*REDACTED*]

26. [*REDACTED*]

27. [*REDACTED*]

[*REDACTED*]

28. [*REDACTED*]

29. [*REDACTED*]

30. [*REDACTED*]

31. [*REDACTED*]

32. [*REDACTED*]

33. [*REDACTED*]

34. A mandatory naming convention will be introduced for new File Shares, [*REDACTED*] We will ensure that we better link local records with the [*register*] so that there is effective central oversight [*REDACTED*].

35. MI5 has embedded teams of information experts [*REDACTED*] across all business areas. To date, they have focused on [*managing records*] on corporate systems. In those areas of MI5 which use the [*TE*] we are now training them to play a direct role, [*REDACTED*].

36. [*REDACTED*]

37. [*REDACTED*] we have identified [*tools*] that may help us [*REDACTED*]. It will take time to evaluate their efficacy and integrate them into the [*TE*] environment but this offers the prospect of generating potentially valuable data for the Audit team in the future.

38. In addition to these practical measures, a new policy and supporting guidance on use of the [*TE*] is being drafted, setting out at a high level how users should manage data and information, including, but not limited to, managing warranted data. This will be issued [*soon*], as we complete our review of business processes across the [*TE*], ensuring that the policy and guidance fully encapsulates necessary and proportionate activity on the [*TE*].

Review, retention and deletion (RRD)

39. The IPCO report provisionally rates the compliance risk in relation to RRD as RED for [*some data*], and AMBER for [*some data*].

40. Again, the compliance risk is primarily that [*for some data*], no automatic RRD is applied to that data, and so [*it is difficult to assess*] whether it has been retained for longer than is necessary for the relevant statutory purpose.

41. In addition, part of the system within the [*TE*] for storing [*a type of*] material has no automatic deletion processes in place. Automated RRD will be introduced across this system [*in 2019*], and in the interim manual deletion is being carried out periodically so that data is not retained for longer than the relevant RRD policy. We are scheduled to deliver automated RRD across the wider suite of systems handling other [*other warranted data by 2019*] [further detail is set out in paragraph 4.2.4 of the IPCO report].

42. [*REDACTED*]

[*REDACTED*]

43. As set out above, the creation of new file shares is necessary for MI5 to be [*effective*]. The measures described above in relation to the creation of new file shares and introduction of new or enhanced business processes will reinforce existing RRD policies and provide greater visibility of the data [*REDACTED*] and the period for which that data should be retained, enabling monitoring of whether data has been retained for longer than necessary and providing greater assurance.

44. In particular, the high-level guidance referred to above, reinforced by the Director General communication, reminded [*TE*] users of their responsibility to delete data when there is no longer any need to retain it.

45. [*REDACTED*].

46. The involvement of [*information teams*] will provide greater assurance in this area since they will have knowledge of the business practices of the [*TE*] users in their team and will be better equipped to identify where and for how long data is retained.

47. The automated tools for data discovery which are being developed will also assist in identifying any data which has been kept for longer than necessary.

48. The [*TE*] Policy to be introduced will set out how MI5 RRD policy should be applied to warranted data stored on the [*TE*].

Legal Professional Privilege

49. The IPCO Report provisionally rates compliance with LPP safeguards as an AMBER risk in relation to [*some data*] [*REDACTED*]

50. The risk is that while there is a manual system in place for deleting LPP material if required to do so, given the compliance gaps in relation to RRD there can be very little assurance that [*REDACTED*] any conditions imposed by a Judicial Commissioner on the use or retention of such material have been complied with.

51. The measures in place to mitigate the compliance risks in relation to [*REDACTED*] RRD will also mitigate the risk in relation to LPP. [*REDACTED*]

52. There is an additional compliance risk which relates to the requirement to mark LPP material. The MI5 policy requires LPP material, once identified as such, to be flagged if it is to be retained. A small number of specialist systems within the [*TE*], used by specialist analysts, do not have the functionality to allow material to be flagged or to reflect flags applied to material in other systems. Guidance is in place which requires users to seek the deletion of any LPP material they do encounter directly in these specialist systems.

53. Additionally, there is a risk arising from the fact that flags do not automatically carry over to a file share. It is possible that copies of identified LPP material exist in file shares without the LPP flag. We are working to establish the extent of this risk and the extent to which it can be addressed through specific guidance and the new naming convention for file shares.

[*REDACTED*]

54. [*REDACTED*]

55. [*REDACTED*]

56. [*REDACTED*]

57. [*REDACTED*]

58. [*REDACTED*]

59. The information to be recorded on the [*register*] will assist the [*REDACTED*] audit teams to provide assurance [*REDACTED*]

60. [*REDACTED*]

Conclusions

61. While the measures set out above may not provide a complete answer to the compliance risks identified in relation to the [*TE*], we consider that taken together with the handling arrangements, policies and guidance already in place, and the vetting and training of users of the [*TE*], they represent a satisfactory level of protection for new warranted material being ingested into the [*TE*].

62. We consider that these additional measures will [*mitigate the compliance risks].* [*REDACTED*]

63. To the extent that there remains a compliance risk because of the [*REDACTED*] limitations of the [*TE*], we will continue to seek to identify additional measures to reduce that risk. Where our existing arrangements, policies and guidance cannot be complied with, we will amend or flag those documents to make that clear.