[MI5 Letterhead]

[REDACTED]
[REDACTED]
IPCO

3 May 2019

Dear [REDACTED],

At the recent [Technology Environment (TE)] follow-up inspection (15-16 April), we undertook to write with a summary of all investigations into potential errors currently being progressed which bear on the [TE]. We would also like to take this opportunity to outline our proposed approach to errors we identify in the [TE] more broadly: we would be grateful for your views on this.

The [TE] as a source of errors

2. As recently discussed, we propose that [Director Policy, Compliance, Security and Information's] letter to the IPC of 11 March 2019 can be considered the formal initial notification confirming that there will be reportable errors stemming from the issues associated with the [TE], and that the subsequent IPCO inspections constitute the investigation into the detail of those errors. What follows is our proposed approach to reporting those errors. Note that we will in all circumstances bring to the IPC's attention any aspect of an error where significant prejudice or harm to an individual could be argued to have occurred (as per s231(2) of the IPA). ~~[REDACTED]~~.

Detailed Approach

3. The contexts in which potential errors within the [TE] may arise are diverse, and are summarised below. We will be happy to discuss further with IPCO how errors reported in line with the proposals below are most effectively represented for statistical purposes.

- **Retention [REDACTED] of warranted material when not necessary and proportionate:**
  - **In fileshares.** We anticipate a range of material may have been handled in error for one or more reasons as above across fileshares. **Proposed approach:** we will report each case where erroneously-handled, discrete sets of material have been identified as indications are that volumes of material falling into this category are not as high as originally considered likely.
  - **In datastores.** The number of datastores is limited and thus far we assess that any issues with the operation of safeguards are not intrinsic across datastores, but rather derive from applications and other sources of data. **Proposed approach:** to notify per datastore as necessary where an issue stems from a problem in the datastore itself, indicating type and volume of data to the degree reasonably possible.
  - **In applications.** [The number] of applications operating in the [TE] are likely to include some where material has been handled in error for one or more of the reasons above. **Proposed approach:** we will report each case individually on a per

application basis, outlining the nature and volume of data affected to the degree reasonably possible.

- *[Other areas]*. We are in the earlier stages of understanding issues associated with *[other areas]*, but we anticipate there will be cases where material has been handled in error for one or more of the reasons above. **Proposed approach:** we will notify in respect of each type of area at the point of sufficient understanding of the nature and indicative scale of any errors, with supplementary reports as appropriate.

- **Retention *[REDACTED]* of *[data]* when not necessary and proportionate.** We recognise the *[nature]* of [*this*] data and will therefore ensure that where such material is engaged by an error, we report the extent and nature of that material to the fullest extent possible. *[REDACTED]*, but we will have particular regard to the *[REDACTED]* results of selection for examination in reporting errors.

- **Failure to appropriately protect material attracting LPP.** We appreciate the importance attached to LPP material, including the specific provisions in the IPA. We will ensure that where such material is engaged by an error, we report the extent of that material to the fullest extent possible.

- **Other notable errors.** The nature of the *[TE]* is such that we may well encounter errors which do not fit neatly into the descriptions above. In these cases we will discuss with IPCO the best means of reporting.

Other errors

4. At the end of the first *[TE]* inspection (22 March) we provided a verbal indication that we were investigating potential issues related to *[two areas of another technology environment: TE2]*. These do not form part of the wider *[TE]* problem, but there are potentially some similarities in terms of the operation of minimisation safeguards. For this reason we include an update on our investigations here, and will continue to incorporate them into our prioritised *[TE]* error investigations work.

5. Many of the routine errors investigated and reported by *[the Oversight and Errors team]* relate to data held in or transiting the *[TE]*. The cause of error in the vast majority of these cases is human error or IT failure unrelated to *[TE]* compliance issues. We will of course continue to report such errors, but we do not intend to make specific reference to the *[TE]*. The exception to this is where any requirement for deletion of material is affected by the problems in the *[TE]*; this will be referenced explicitly in the error notification.

Current error investigations under the *[TE]* workstream

6. The table below highlights current potential errors under investigation, but not confirmed as an error unless indicated otherwise. The descriptions here are summaries and do not comprehensively outline mitigations. Final notifications will of course do so.

[REDACTED]	A large number of *[files]* from 2012-2013 have been found in a *[TE]* Fileshare. These appear to have been used for training purposes and were not subject to RRD processes, which were

	applied to *[data]* retained for investigative purposes. The data has been quarantined and will be deleted after *[a period of time]*
[REDACTED]	*[REDACTED]*. A mitigation plan has been proposed and is awaiting final sign off.
[REDACTED]	*[This workspace]* allows for a user to save their results *[REDACTED]*
[TE2 Area 1]	*[Area 1]* on *[TE2]* is used for storage and analysis of data, including warranted data. *[REDACTED]* Our initial scans of *[Area 1]* have been completed and we have identified files which may contain warranted material. *[It is a complex area and is challenging to investigate. We have therefore only been able to scan some of the files and are working towards scanning other files. We may also need to use dip sampling in some areas]* As previously indicated, knowledge of some compliance risk associated with *[Areas 1 and 2]* (see below) was held by MI5 in 2016; we are seeking to establish whether any error should have been reported historically.
[TE2 Area 2]	*[Area 2]* on *[TE2]* is used for storage and analysis of data, including warranted data. *[Area 2]* also hosts some applications. *[REDACTED]*. As with *[Area 1]*, we are still working to confirm the scale of the data and data types affected. Some mitigation work has taken place previously and we are seeking to understand whether this means there is no ongoing error, but equally whether there was an error which should have historically been reported.
[REDACTED]	*[An application]* within *[TE]*. *[REDACTED]* We are investigating whether we have retained data beyond our agreed RRD policies. Our current assessment is that this is not a reportable error, but we are awaiting legal confirmation.
[REDACTED]	*[A fileshare containing data was found in an area of the TE]*. All data held is within the agreed retention period and correctly authorised for retention and examination. However, aspects of handling these *[data]* may not conform with MI5's *[data]* handling arrangements. The data has now been quarantined.
[REDACTED]	*[An application which manages dataflow into a suite of tools. Data is usually retained in for a limited period of time. We have identified that some data has been retained beyond this period*

	which has meant automated RRD did not occur.]

7. If you have any questions or would like to discuss any of these cases please contact *[the Oversight and Errors team]* in the first instance.

Many thanks
[The Oversight and Errors Team], [MI5]