[Redact]

IPCO

Investigatory Powers Commissioner's Office

PO BOX 29105,
London,
SW1V 1ZU

Gists are shown in italics and are double-underlined

Additional disclosure 18.10.17 is highlighted

15 September 2017

Dear [REDACTED]

This draft report summarises the findings of the 2017 BPD audit.

Purpose

1. In August and September 2017 IPCO conducted an audit of BPD holdings by the Intelligence Agencies. The audit constituted the first phase of a BPD review, which was ordered by the Investigatory Powers Commissioner in response to matters raised within the Investigatory Powers Tribunal. The following areas were considered:

    - *Precisely what may have been shared and for what purpose;*
    - *Whether any sharing was a one-off or continuous process;*
    - *To the extent that any sharing may have taken place, that the minimum necessary data has been shared and that data has been selected to result in the minimum intrusion into privacy;*
    - *Any transfers of BPD have been logged;*
    - Handling instructions are in place with any recipient of BPDs;
    - *To the extent that any sharing may have taken place, compliance with the handling instructions are adequately overseen by the agency;*
    - *All systems (including systems of any non UKIC sharing partners) holding BPD are secure and access is controlled.*
    - *Any retention of data by non-UKIC entities is reviewed and recorded.*
    - *Adequate protective monitoring arrangements are in place (including at any non-UKIC sharing partners);*
    - *Any BPD/BCD shared with non UKIC partners is deleted once no longer necessary.*

2. The second phase of this review will review the use of contractors, secondees and integrees by the agencies. In the main, these accesses have not been factored into this review by UKIC.

[Redact]

Overview of findings

3. *MI5 confirmed the position in relation to any sharing that might take place. No concerns were noted.*

4. *GCHQ demonstrated that they had considered the necessity and proportionality of any sharing that might take place and that it would be in accordance with the requirements of the legislation and their handling arrangements (post 2015). However, it was felt that GCHQ fell short of providing IPCO complete assurance of their compliance in some areas. Those included:*

    - *That when questioned staff were not considering steps to minimise the level of intrusion from any sharing (Handling arrangements 6.3).*
    - *Identifying and classifying BPDs appeared to cause some difficulty because of the complexity of GCHQ's acquisition methods. There is some question of whether all BPDs held by GCHQ have been adequately identified, while some datasets identified as BPD were not.*
    - *GCHQ have not provided clear and specific briefings to the Foreign Secretary, other than via the Choice Letter. There is some question of whether the Foreign Secretary has provided ministerial oversight in this area.*

5. GCHQ briefed on the process of testing that had been completed by technical experts to confirm that individuals working on integree profiles were not able to access datasets on partially-restricted systems. This practice should be considered more widely and should be adopted by the other agencies.

6. *SIS demonstrated a thorough and thoughtful process for any sharing of BPD and gave a high level of confidence to IPCO that the requirements of the legislation and handling instructions would be met. SIS's compliance process demonstrated clear steps were in place to monitor the continued necessity and proportionality of any sharing, as well as adherence to the handling instruction and any MOU.*

Detail

BPD definition

7. The agencies are all working to the same definition of BPD as agreed with the Commissioner. GCHQ briefed that they have taken a cautious approach to identifying BPDs, which has meant that some of the BPDs listed are not BPDs. SIS echoed this comment, stating that in difficult cases legal advisors advise on whether a set of data, or sets of data in combination, constitute a BPD.

8. Uncertainty with the list provided to IPCO by GCHQ led to some concern that GCHQ may not be adequately identifying BPDs. GCHQ were open to working with IPCO to ensure that all

data is accurately identified, which will improve the level of confidence that IPCO inspectors have in this area.

Nature of the database

9. The handling arrangements require internal authorisations for acquisition to detail a description of the requested dataset, including details of any personal and sensitive data (4.7). Each agency has adopted a different internal form to record this information.

10. *In June 2017, the Intelligence Services Commissioner noted to MI5 that their existing acquisition forms met current requirements* [REDACTED].

11. GCHQ stated that the size and scale of a database can be difficult to set out in a way that makes it straightforward to understand during independent, non-technical, oversight. IPCO suggested that details like database size were valuable but that lines of content would be easier to understand. GCHQ raised concerns that unstructured databases are complicated to quantify in this way.

12. Typically, the agencies tick boxes to denote certain types of data, such as sensitive medical data or financial details. In such cases we are advised that it is expected that the authorisation itself will also include further details regarding the sensitive nature of material within the dataset. It can be the case with less structured databases, such as social media data, that it is possible to obtain any type of data, which renders the details a gauge of likelihood rather than a description of the data.

The Secretary of State

13. The Secretary of State has two functions set out in the handling arrangements; Ministerial Oversight (9.1) and consideration of difficult cases for disclosure (6.7).

14. GCHQ send a copy of the Choice Letter detailing all current BPD holdings to the Foreign Office, but have otherwise not provided details of BPD holdings for Ministerial oversight. SIS provide six-monthly submissions to the Foreign Secretary on BPD holdings but receive no response. SIS also share notes from the Data Retention Review board with the Foreign Office. This document sets out the case for retention for each BPD.

15. GCHQ have not referred any cases of difficult disclosure to the Foreign Secretary.

[REDACTED]

Necessity

[REDACTED]

16. *There are no concerns about the necessity for any sharing that may take place.*

Proportionality and minimal intrusion

17. *When questioned, staff at one agency were not able to demonstrate any work to ensure that only as much of the information as is necessary is disclosed were any sharing to take place (6.1). That agency explained that due to the complexities of some unstructured datasets this might not be possible.* [REDACTION]. *Following these conversations, there are no concerns about the proportionality of sharing as considered by one agency.*

[REDACTION]

Action On request log

18. *IPCO questioned whether an action on log, specific to BPDs, would be kept by an agency were any sharing to take place.* [REDACTION] *During the second phase of this audit, IPCO will discuss this matter further with the agencies. (6.6)*

Contractors, Industry and Academics

19. This audit identified a concern in relation to non-UKIC staff. This includes contractors, industry partners and academics and, to an extent, [REDACTION]. This issue will be probed during the second phase of this review.

20. GCHQ stated that they do not give BPD in full or in part to contractors or academics for the purposes of running queries and that they would not have access to the search interface. This would not preclude a contractor with system access rights going into the system, extracting data and then covering their tracks.

21. Contractors may be involved in the design and build of systems that will hold BPD. As far as possible, dummy data is used for the purposes of testing. For some systems contractors may have administrator rights. An additional screening level is required for anyone with privileged access rights including contractors.

22. The inspectors asked if any GCHQ data was held by industry off-site. [REDACTION] would need to make enquires to determine whether this was the case. GCHQ thought that if any data was held off site it might be on a small scale for desk top development.

[REDACTION]