Date/ Location: 21-May-2019 [redacted]

Attendees: [Information Security Compliance and Strategic Policy Director] from MI5 [redacted], Sir Martin Donnelly (SMD) and [redacted]

[redacted]

[Information, Security, Compliance and Strategic Policy Director] advised that *[the department]* was formed in [redacted] and has since evolved. [Information Security Compliance and Strategic Policy Director] has responsibility for policy (across Whitehall), [redacted] and information management, Information Security [redacted] and compliance. [redacted] *[The department]* also has the warrantry team and oversight team and compliance function [redacted] Since *[2018]* there has been more focus and understanding of the *[TE]* issue as a result.

[Redacted on relevance grounds] [redacted] * [Information, Security, Compliance and Strategic Policy Director] mentioned that the compliance team would investigate potential legal errors. Within each of the *[departments]* there are compliance and information management *[teams]* which liaise with the central compliance team. The central compliance team would liaise with the lawyers as needed and report any errors within the 10 working days as set out in the Codes of Practice to IPCO. The errors would need to be confirmed/ cleared by the lawyers. However, there are other routes which could be taken for any compliance issues to be raised internally such as through the ethics team.

[A team] undertake traditional compliance. They would engage with strategic programmes to ensure that compliance is built into it. This might be technical and business change and building moves for examples. This might also include compliance with Health and Safety and Data Protection Acts. Much broader than just IPA. This team surfaced the *[TE]* issue. There is no formal lawyer in this team and would commission advice. *[A few people have legal training]*

* [Information, Security, Compliance and Strategic Policy Director] SMD asked * to reflect on whether the commissioning of lawyers was the right model or whether more lawyers should be embedded in the teams? * personal view was that the Head of Compliance should be either legally trained or a compliance professional. *[A team]* are [redacted] people strong with the oversight team (leading on the IPCO inspections etc.) being [redacted] people. This may need to be bolstered. The ways of working to draw on legal advice might need to be strengthened or a clearer route developed.

[Information, Security, Compliance and Strategic Policy Director] SMD asked * who * thought owned the legal parameters? * asked whether he meant who owned the legal risk? * view is that the lawyers are there to "advise" and not own the risk. SMD reflected that it might appear that MI5 lawyers are more "client focussed" rather than consultative with the other lawyers such as the Home Office. The policy colleagues appear to show much closer working. * mentioned that there is a National Security network with the NSC legal bringing this together. [redacted] there were lots of informal routes into the Home Office. During the IP Act implementation, *[there was a]* very close working with UKIC- this has perhaps slipped back a bit with the reduction in the "burning Legislation Bridge". There does need to be similar links into the Cabinet

* [Information, Security, Compliance and Strategic Policy Director] Office, FCO etc. * felt that there were daily conversations and didn't feel MI5 were operating in a bubble.

SMD asked * to describe the culture of MI5. * thought it was a positive blogging culture which is much focussed on the mission and keeping the country safe. Staff are hugely motivated. The challenge can be that the mission is prioritised over everything else. Compliance can often be in conflict at times. The organisation is more used to considering security issues and this trumping the mission. Compliance is not yet seen in the same way in the organisation. * mentioned that *[a team]* raised the compliance issue and the top of the office were clear it needed fixing immediately. Perhaps the priority was not understood at the lower levels where the mission is seen as the top priority. *[A programme]* was named specifically with a mind to reinforce the need for compliance/ being core to the business.

* [Information, Security, Compliance and Strategic Policy Director] SMD asked * if * thought MI5 staff viewed compliance as a Home Office/ Ministerial/ Government responsibility or just an internal MI5 issue? * thought internally the IPA had been understood, the role of IPCO was understood. However, the broader accountability was not something that struck * as being understood within MI5. The focus was largely on reporting to IPCO on the compliance *[TE]* issue. * noted there was a conscious action to brief HO first to allow them to brief IPCO, but the internal focus was largely about briefing IPCO.

* [Information, Security, Compliance and Strategic Policy Director] SMD asked * what led to the change in tone in the MI5 correspondence with IPCO. * reflected this was largely as a result of IPCOs reaction. At the February briefing, it was felt that this had gone well and that Sir Adrian had reacted in a pragmatic and calm way. During the inspection, the inspectors and Sir John Goldring provided feedback that this was a very serious issue. [redacted] *[Redacted on LPP grounds]* [redacted] There was surprise, [redacted] at the IPCO response.

* reflected, as a very personal view, that the perceived delay in reporting the issue by MI5 had coloured the IPCO response. *[Redacted on relevance grounds]* [redacted] MI5 went to IPCO with the problem and some idea of mitigation. [redacted]

[Information, Security, Compliance and Strategic Policy Director] SMD asked why there was little consideration of how the Minister would view the red risk and the compliance issues. * stated during Jan 2018-October 2018, MI5 was thinking in a traditional sense. This was a data being in the system too long problem and that this would be criticised only by IPCO. There wasn't a joining up of the dots... compliance....therefore a warrantry problem. MI5 could have twigged earlier that the warrantry would be affected- this was very late in the day. The IPA did not change the Home Secretary responsibilities nor did [redacted] change with regard to RRD. Unfortunately it was assumed it was "always like this" and so overlooked.

* mentioned that the handling arrangements were very broad and largely aligned to the legislation. Not specific. SMD suggested that IPCO is seen as the "gold standard" of legal compliance, but this

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

doesn't take away from the Home Secretary responsibility and HO Lawyers. HO legal advice is key in supporting the Home Secretary.

* reflected that IPCO concern grew as more detail was asked for and provided. The question was more specific- how do you assure [redacted] as opposed to how do you do assurance? * wondered if Sir John is a "Black letter lawyer" as opposed to Sir Adrian who is much more pragmatic. Is this part of the reason?

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

In October 2018, the EB/MB was given an informal briefing/ taught about the [TE] for 2.5 hours. They were walked through the key risks in relation to information assurance and compliance re RRD. The second session was on the future investment focus [redacted] * remembers the Board asking for IPCO to be briefed despite it not being recorded as an action accurately. [A team] began digging into [an area of the TE] and getting more concerned. [The] note dated 10th December stated the need to brief IPCO, and there was a clear intention to do so. This was briefed into Private Office in MI5 on 21/12. The 3 DGs agreed on 25/01 to brief IPCO following the Christmas break. The script was developed and around 28th January 2019 the internal conversation regarding the linking of the compliance issue with warrant approvals took place. The period between the end of Jan- Feb 27th was likely due to IPCO availability for briefing. * stated there was a clear timeline of events developed by the team which would be shared.

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

SMD asked * how big the compliance team needs to be to affect a culture of compliance? * noted the need for the compliance to sit in one command headed up by lawyer/ compliance professional. There also needs to be a proactive compliance function to investigate suspicions. * wasn't sure on size and would be interested in other organisational models. * also mentioned governance needed to be focussed on compliance not being optional and to rebalance the priority calls for compliance over mission critical calls. * wonders if there is learning from industry and banks for compliance. Training needs to be driven by [a department] as it started to do with the [mandatory legalities training] , Data Protection Act and with a compliance function to own and drive this in a sustainable way. This needs a strong central compliance branch, stronger compliance [teams] in the [departments]/ business. These staff need to be more technically literate and maybe even more senior.

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

SMD asked * for a view on the need for a lawyer on the Management Board. * view is that if the Head of Compliance is a lawyer/ compliance professional and under * , there are the links to policy. Equally this could be under the [legal department]. The more important place is at the Executive Board where more crunchy decisions are made. Both boards are chaired by AP.

004