[NOTE: REDACTIONS ARE INDICATED AND GISTS ARE IN BOLD, DOUBLE-UNDERLINED AND ITALICS]

[Exhibit D]

Annex D – *analytical systems area* Code of Practice

Code of Practice

This code sets out the rules governing the use of ***analytical systems area***. By signing this document you consent to comply with the contents of this code. It is important that you read and ensure that you have understood your responsibilities under this code before signing it. You will be required to re-sign this Code of Practice on an annual basis. If you are unsure how this code affects you and your work, please seek definitive guidance from the ***monitoring team***. Line Managers, ***counter-signing officers***, Service Sponsors of contractors/consultants and/or ***analytical systems area*** key users may also be able to provide advice.

The provisions of this Code operate in addition to those set out in the ***relevant code of practice*** to which you consent each time you log on to ***the IT system***.

Why is this Code of Practice necessary?

The success of the Service depends on effective sharing and exploitation of information in accordance with the law. The ***analytical systems area*** programme provides an immensely powerful aid to investigation and an integrated means by which to search and exploit data. However, in addition to its considerable benefits ***analytical systems area*** brings information sharing risks for the Service. These need to be managed to ensure that the privacy of those whose data is within ***analytical systems area*** is respected and that data is only held, accessed and disclosed to the extent to which this is necessary for the purpose of our statutory functions and proportionate to those aims. ***analytical systems area*** 's effectiveness is dependent on making information available; the more we lock information down, the more connections potentially will be missed. But this powerful and sensitive capability brings responsibility and we must commit to working scrupulously within the laws that define our purpose, responsibilities and methods, our relationship with Ministers and our accountability for our work. It is extremely important that all users understand, and comply with, the legal requirements and record keeping conventions that apply to their use of ***analytical systems area***.

In order to identify leads and counter fast-moving threats we have access to data from large external databases - about individuals of interest to us - but also, inescapably, about those who are of no security interest. Use of bulk data is therefore a particularly sensitive area, requiring careful consideration and strict adherence by users to that which is necessary and proportionate for their work.

Logging and Monitoring

The **use of *analytical systems area* is monitored on a continuing basis** through a variety of means – including technically – in order to detect misuse of the system and any unusual activity that gives rise to security concerns. Users will also be subject to **random and routine spot checks** to account for their activities on ***analytical systems area*** at any time.

Breach of the Code

The Service will take disciplinary action against any detected abuse or misuse of ***analytical systems area***, or information and intelligence derived from ***analytical***

[NOTE: REDACTIONS ARE INDICATED AND GISTS ARE IN BOLD, DOUBLE-UNDERLINED AND ITALICS]

systems area. This includes, but is not restricted to, those activities expressly identified under **Conduct and Behaviour** below. For Service staff, offences will be handled in accordance with the Service's disciplinary procedures, as set out in the ***relevant part of staff terms and conditions***. Deliberate or repeated abuse of electronic facilities, including breaches of the ***analytical systems area*** Code of Practice, will be treated extremely seriously and could amount to gross misconduct resulting in dismissal; in other circumstances, users may receive an automatic Security Breach. For non-permanent Service staff members (e.g. contractors / consultants / secondees / alongsiders), such misconduct is similarly likely to result in removal from site. In all cases, fitness to hold ***developed vetting*** will also be examined. Furthermore, activity that cannot be justified by reference to our functions would be likely to be unlawful in ECHR Article 8 terms, and could in some cases even constitute a criminal offence.

Conduct and Behaviour

Individuals with access to ***analytical systems area*** must not misuse the systems or any data obtained from them. At all times you must ensure that your activity on ***analytical systems area*** systems is **necessary and proportionate** to your current work, and in the interests of national security.

Analytical systems area systems are powerful analytical tools that are extremely effective in the protection of national security – users are actively encouraged to use these systems creatively, proportionately and for legitimate business reasons, as they will help you do your job more effectively. However, users must also be aware of their
responsibilities when using these powerful tools.

You **have a responsibility to**:

□□Comply with the ***analytical systems area*** Code of Practice (including any supplementary protocols to which you may be subject), and adhere to the procedures explained during your ***analytical systems area*** training;
□□Structure and target activity on ***analytical systems area*** systems in a way that is most likely to retrieve information that is relevant to your enquiry;
□□Report any accidental transgressions to the ***monitoring team*** at the earliest opportunity;
□□Raise any concerns you may have about how others are using ***analytical systems area*** systems with the ***monitoring team*** and your Line Manager or ***counter-signing officer***.

Additionally, Line Managers of *analytical systems area* users are required to ensure their staff members have signed the Code of Practice and are aware of their responsibilities under it.

It is not possible to provide an exhaustive list of prohibited ***analytical systems area*** activity. However, the following activities in particular are expressly prohibited – engaging in such activities could be unlawful and even amount to a criminal offence. The ***monitoring team intranet*** site provides further explanation regarding these prohibited activities, the reasons why they are prohibited, and the likely consequences.

You **must not**:
□□Access or attempt to access ***analytical systems area*** by any means other than your allocated username and password;

[NOTE: REDACTIONS ARE INDICATED AND GISTS ARE IN BOLD, DOUBLE-UNDERLINED AND ITALICS]

□□Share your username and password with another individual;
□□Leave your terminal unlocked and unattended;
□□Attempt to circumvent or defeat security measures;
□□Conduct searches on or attempt to use ***analytical systems area*** to access information relating to yourself, other
members of staff, neighbours, friends, acquaintances, family members or public figures;
□□Use ***analytical systems area*** to conduct searches on or attempt to access information which could reveal CHIS identities without explicit authorisation from the ***relevant team***. For example, you must not carry out unfocussed searching on a CHIS symbol or nickname, or carry out any other action which will return the entire body of reporting from a single CHIS;
□□Conduct searches on or attempt to access information beyond your current area of responsibility unless you have a legitimate business need to do so. For example, you must not access the 'Intelligence for Duty Officer Only' option on ***the IT system*** unless you are on a ***on duty officer*** shift at the time;
□□Share raw data obtained from ***analytical systems area*** with individuals who may not be not authorised to access it themselves, for example external partners (including those who may be co-located with the user for periods of time) or other Service colleagues from different sections / business areas.
Some users will on occasion have legitimate business requirements as part of their specific roles to carry out activity on ***analytical systems area*** systems which is listed as prohibited. This may include (but is not limited to) sections which: perform legitimate ***analytical systems area*** testing functions; [REDACTION]; or certain members of the ***relevant team***. This activity is authorised only when directly related to the work that these sections carry out, and in accordance with established (not ad hoc) local procedures. Failure to adhere to these established local procedures will result in disciplinary action.

Legal Context

Use of ***analytical systems area*** is only permitted where access is authorised for a legitimate purpose related to the functions of your job and where you are satisfied that use of ***analytical systems area***'s facilities for this purpose is necessary and proportionate.
DG has a legal duty to ensure that there are arrangements in place to prevent the Service from disclosing material it obtains "except so far as necessary for the proper discharge of its functions" (section 2(2)(a) Security Service Act 1989). The natural meaning of "disclosure" in this context is disclosure by the Service to another organisation or individual. The accessing of information by members of the Service, or the sharing of it between them, is not therefore a disclosure within the meaning of this provision.
However, members of the Service when considering whether to access and subsequently share information should ensure that this is only done where to do so is necessary and proportionate in accordance with the Service's functions. This is because accessing and sharing information where this is not necessary and proportionate may amount to an unlawful interference with the subject's right of privacy as guaranteed by Article 8 of the European Convention on Human Rights and/or a breach of the Data Protection Act 1998. Such a breach could form the basis of a complaint to the Investigatory Powers Tribunal and/or some other form of legal claim against the Service.
There are internal rules about the sharing or accessing of information by members of the Service, these include; this Code of Practice, the Information Handling Model and arrangements agreed by the DG under section 2(2)(a). The current arrangements, which are on the ***warrantry team*** website , refer to

[NOTE: REDACTIONS ARE INDICATED AND GISTS ARE IN BOLD, DOUBLE-UNDERLINED AND ITALICS]

vetting clearance, indoctrination and application of the "need to know" principle i.e. material must not be disclosed to any person unless their duties are such that they need to know about the material to carry out those duties. *analytical systems area* affords you the potential to view information and/or data that you do not have a need to know, it is your duty and responsibility to avoid doing so.

Data held in ***analytical systems area*** is lawfully obtained, including in accordance with section 2(2)(a) of the Security Service Act, which allows us to obtain data if it is necessary for the proper discharge of our functions. Our obligations to deal with that data lawfully do not end at the point at which we receive it. We must of course ensure that we handle the data within ***analytical systems area*** in accordance with the law. Different types of data and information held within ***analytical systems area*** are subject to slightly different legal constraints regarding how it should be held, accessed and disclosed. **The most important point to remember is that *analytical systems area* must not be a 'free for all'**. Depending on their roles users will have *potential* access to a vast amount of sensitive material. The Service's information policy is designed to be compliant with the law, which dictates that users' *actual* access to information is limited to that which is necessary and proportionate for their work. Misuse of information, including unjustified and/or inappropriate access, would be unlawful and could in some circumstances constitute a criminal offence.