SCHEDULE B

ADDITIONAL SAFEGUARDS

1. The Data Importer will assess whether the laws applicable to it provide adequate protection under European Data Protection Laws. To the extent that it determines that any such laws are not in line with the requirements of the Standard Contractual Clauses and European Data Protection Laws, it undertakes to comply with the safeguards set out in this Schedule.

2. The Data Importer undertakes to adopt supplementary measures to protect the Personal Data transferred under the Standard Contractual Clauses from the Data Exporter ("SCC Personal Data") in accordance with the requirements of European Data Protection Laws, including by implementing appropriate technical and organizational safeguards, such as encryption or similar technologies, access controls or other compensating controls, to protect SCC Personal Data against any interference that goes beyond what is necessary in a democratic society to safeguard national security, defence and public security.

3. The Data Importer warrants that:

(a) it has not purposefully created any means by which a public authority can bypass the Data Importer's security mechanisms, authentication procedures and/or software to gain access to and/or use its systems and/or the SCC Personal Data, such as a back door or similar programming;

(b) it has not purposefully created or changed its business processes, security mechanisms, software and/or authentication procedures in a manner that facilitates access to its systems and/or the SCC Personal Data by public authorities; and

(c) it is not required by national law or government policy to create or maintain any means to facilitate access to its systems and/or the SCC Personal Data by public authorities, such as a back door, or for the Data Importer to be in possession or to hand over the encryption key to access such data.

4. Any audits, including requests for reports or inspections, carried out by the Data Exporter or a qualified independent assessor selected by the Data Exporter (the "Independent Assessor") of the processing activities will include, at the choice of the Data Exporter and/or Independent Assessor, verification as to whether any SCC Personal Data has been disclosed to public authorities and, if so, the conditions under which such disclosure has been made.

5. In the event that the Data Importer receives a legally binding request for access to the SCC Personal Data by a public authority, the Data Importer will:

(a) promptly notify the Data Exporter of such request to enable the Data Exporter to intervene and seek relief from such disclosure, unless the Data Importer is otherwise prohibited from providing such notice, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation. If the Data Importer is so prohibited and in the event that, despite having used its reasonable best efforts, the Data Importer is not permitted to notify the Data Exporter, it will make available on an annual basis general information on the requests it received to the Data Exporter and/or the competent Supervisory Authority of the Data Exporter;

(b) promptly inform the public authority if, in the Data Importer's opinion, such request is inconsistent and/or conflicts with its obligations pursuant to the Standard Contractual Clauses. The Data Importer will document any such communication with the public authorities relating to the inconsistency and/or conflict of such request with the Standard Contractual Clauses;

(c) not make any disclosures of the SCC Personal Data to any public authority that are determined to be massive, disproportionate and indiscriminate in a manner that it would go beyond what is necessary in a democratic society; and

(d) upon request from the Data Exporter, provide general information on the requests from public authorities it received in the preceding 12 month period relating to SCC Personal Data. Where possible, such information will include the following:

(i) an overview of laws and regulations that permit access to the SCC Personal Data in the jurisdiction to which the Data Importer is subject, to the extent the Data Importer is reasonably aware of such laws and regulations;

(ii) any measures taken to prevent access by public authorities to the SCC Personal Data;

(iii) information about the nature and number of such requests received by the Data Importer;

(iv) the type of data requested;

(v) the requesting body;

(vi) the legal basis to disclose the SCC Personal Data to the public authority; and

(vii) whether the Data Importer reasonably believes that it is legally prohibited to provide the information in subsections (i) to (vi) above and, if so, the extent to which such prohibition applies.