SCHEDULE 23

Cyber Security

1. DEFINITIONS AND INTERPRETATION

1.1 In this Schedule, in addition to the words and expressions given specific meanings in Clause 1 and Schedule 22 (Data Protection), the following words and expressions have the meanings given to them as follows:

Information Laws	means all applicable laws and regulations in each case pertaining to the security, confidentiality, integrity, availability and protection or privacy of information, as amended or re-enacted from time to time, including (to the extent applicable) Data Protection Law (as defined in Schedule 22 (Data Protection)) and the NIS Regulations;
IT Systems	means any and all Software, Source Code, hardware, network, data hosting / storage facilities (including any electronic, magnetic, optical or tangible media), databases, and information and/or communication technology systems (whether or not installed on or forming part of the Purchased Equipment) delivered or made available to the Operator or the Owner pursuant to this MSA;
Malicious Software	means any software programme or code which does, or which is intended to, destroy, interfere with, corrupt or cause undesired effects on program files, hardware, network, data hosting / storage facilities (including any electronic, magnetic, optical or tangible media), databases, information and/or communication technology systems, data or other information, executable code or application software macros or programs, whether or not its operation is immediate or delayed, and whether or not it is introduced wilfully, negligently or without knowledge of its existence, including any viruses, worms, trojan horses, adware, spyware, logic bombs or other similar things or devices;
NIS Regulations	means The Network and Information Systems Regulations 2018, as amended or re-enacted from time to time;
OT Systems	means programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment) and detect or cause a direct change through the monitoring or control of devices, processes and events (whether or not installed on or forming part of the Purchased Equipment) delivered or made available to the Operator or the Owner pursuant to this MSA;
Security Incident	means: (a) any Personal Data Loss Event; and/or (b) the occurrence of one or more events which, either individually or collectively, have an adverse effect on the confidentiality, integrity, availability or security of the railway, any data and/or the IT Systems and/or the OT Systems;
Security Policy	means the Operator's IT/Information Security Policy as may be notified to the Manufacturer from time to time; and
Security, Continuity &	has the meaning given in paragraph 3.1 and as updated from time

Recovery Plan	to time in accordance with paragraph 3.

2. CYBER SECURITY

2.1 The Manufacturer shall:

2.1.1 implement and maintain, and procure that its Sub-contractors implement and maintain, a comprehensive cyber security program with cyber security industry standard safeguards in place; and

2.1.2 regularly test and monitor the effectiveness of the Manufacturer's, and use all reasonable endeavours to regularly test and monitor the effectiveness of its Sub-contractors', security program relating to data, services, IT Systems and OT Systems.

2.2 This programme shall be supported by a comprehensive cyber security risk assessment undertaken in accordance with the requirements of a recognised cyber security by design standard for rail operating technology, such as TS50701. The risk assessment shall be maintained by the Manufacturer, in its role as Design Authority, and will be available on request to the Owner and the Operator, to the extent that they need to see it for their respective business purposes.

2.3 The Manufacturer shall, to the extent relevant to this MSA, have sole responsibility for the maintenance of the IT Systems and OT Systems, ensuring that it carries out all necessary updates, patches and upgrades in a timely manner so as to ensure the availability, integrity and continuity of service and protection of networks, communications systems and data for the Operator, and shall comply with the following in respect thereof:

2.3.1 legal and regulatory requirements;

2.3.2 best industry practice;

2.3.3 latest technological developments;

2.3.4 threat intelligence (e.g. from National Cyber Security Centre alerts);

2.3.5 sections [A35 to A40][53] of the Functional Specification (on an ongoing basis);

2.3.6 the security requirements set out in this Schedule; and

2.3.7 any reasonable security guidelines and/or instructions provided by the Operator to the Manufacturer from time to time.

2.4 The Manufacturer shall continually measure, review, provide evidence of and document its compliance with all security requirements (including details of the version of anti-virus software and cyber security measures) as set out in this Schedule, and shall report such compliance to the Operator on request. The Manufacturer shall allow the Operator and/or the Owner to carry out independent penetration testing of IT Systems and OT Systems and co-operate with the Operator and the Owner in remediating any vulnerabilities identified.

2.5 The Manufacturer shall:

2.5.1 provide the capability to monitor network activity on supplied IT Systems and OT Systems;

2.5.2 use its best endeavours to ensure that all IT Systems and OT Systems are free from all Malicious Software; and

[53] ***Drafting Note***: *Functional Specification cross-reference to be confirmed prior to MSA signing.*

2.5.3 use the latest versions of anti-virus definitions, measures, tools and software available in accordance with best industry practice to prevent, check for, contain the spread of and minimise the impact of any Malicious Software.

2.6 Notwithstanding paragraphs 2.4 and 2.5, if Malicious Software is found on any of the IT Systems and/or OT Systems at any time, the Manufacturer shall (at its own cost) promptly and without undue delay:

2.6.1 notify the Operator in writing (in any event within forty eight (48) hours of becoming aware of such Malicious Software);

2.6.2 co-operate with the Operator to reduce the effect of the Malicious Software;

2.6.3 take all steps at its own cost to remove the Malicious Software; and

2.6.4 in the event that such Malicious Software causes loss of operational efficiency of any IT Systems and/or OT Systems or loss or corruption of any of the Operator's data, restore the Operator's data and the impacted IT Systems and/or OT Systems to the required operating efficiency.

2.7 The Manufacturer shall:

2.7.1 implement and maintain appropriate security, technical and organisational measures to manage the risks posed to the security of network and information systems, data and the IT Systems and OT Systems. Such measures shall meet all Applicable Laws (including Information Laws), legal standards (including any encryption requirements imposed by law) and shall meet or exceed all accepted security standards in the industry (including ISO 27001/27002 in respect of IT Systems, and TS50701, IEC63452 and IEC62443 in respect of OT Systems);

2.7.2 implement measures to ensure the security of its corporate information technology and systems, including any wayside software systems related to the operation, maintenance and engineering change of the Fleet, meets all Applicable Laws (including Information Laws), legal standards (including any encryption requirements imposed by law) and meets or exceeds all accepted security standards in the industry (including ISO 27001/27002);

2.7.3 ensure that the on-board and operating technology software, networks and systems of the Fleet are designed, built and maintained to meet all Applicable Laws (including Information Laws) and legal standards (including any encryption requirements imposed by law);

2.7.4 ensure that the on-board and operating technology software, networks and systems of the Fleet are delivered in accordance with the requirements of TS50701 (or its successor standards), compliance with the requirements of the standard shall be independently established by an expert party, prior to Acceptance of the First Unit. The expert party shall be commissioned by the Manufacturer, and selected by agreement of all Parties;

2.7.5 within six (6) months of the Contract Date, provide an initial version of the plan for how the requirements of paragraphs 2.7.3 and 2.7.4 will be met (produced in accordance with the planning requirements detailed in the standard itself); this will clarify in particular how the Manufacturer has established that the train platform and its network architecture are secure by design, and how evidence of compliance with the requirements set out in paragraphs 2.7.3 and 2.7.4 will need be sourced from the Manufacturer’s sub-system suppliers;

2.7.6 commission a white box penetration test (that assumes explicit and substantial knowledge of the internal structure and implementation detail of the assessment object) of the train fleet in advance of approval for placing in service, using a CREST

approved penetration tester; the specification for this test will be agreed between all Parties prior to it being undertaken. The Unit tested will be in a configuration state deemed to be appropriately representative of the Unit to be approved for passenger service;

2.7.7 utilise tools to maintain robust cyber security defences and detect any Malicious Software or Security Incidents that might impact the IT Systems or OT Systems or associated data;

2.7.8 ensure that it is, and remains until the expiry of the Design Life of the Last Unit, compliant with all accepted security standards in the industry (including ISO 27001/27002 in respect of IT Systems, and TS50701, IEC63452 and IEC62443 in respect of OT Systems) and conducts its activities in compliance with the principles of applicable international standards and the requirements of all Applicable Laws (including Information Laws);

2.7.9 comply with the Security Policy and ensure that all IT Systems and OT Systems and all connecting or associated systems, hardware and firmware adhere to the requirements of the Security Policy;

2.7.10 limit access to network and information systems to such of its authorised personnel that require access to such systems solely for the purpose of performing its obligations pursuant to this MSA (with access rights being reviewed on a regular basis) and that have been appropriately screened in accordance with best industry practice (provided always that such action would not put the Manufacturer in breach of Applicable Laws), the Security Policy and any other Operator standards (as notified to the Manufacturer from time to time);

2.7.11 ensure that all personnel with access to the data, network, information systems, IT Systems and OT Systems are subject to a contractual duty of confidence and are aware of, understand and comply with the Manufacturer's obligations pursuant to this Schedule;

2.7.12 comply with the Rail Cyber Security Guidance to Industry (as issued by the Department for Transport in February 2016, as may be updated or replaced from time to time) to ensure network segmentation between safety integrity levels (SILs) as set out in TS 50701 and IEC63452; and

2.7.13 comply at all times with the Security, Continuity & Recovery Plan.

3. SECURITY, CONTINUITY & RECOVERY PLAN

3.1 The Manufacturer shall be responsible for developing and maintaining a detailed cyber security, business continuity and disaster recovery plan in respect of cyber security (the **Security, Continuity & Recovery Plan**), which:

3.1.1 includes appropriate processes to ensure the protection of and the response management and independent penetration testing of the IT Systems and OT Systems; and

3.1.2 sets out method(s) of recovering or updating data collected (or which ought to have been collected) during a ‘major incident’ or ‘cyber event’,

to ensure that there is no more than the accepted amount of data loss as agreed between the Parties, and to preserve data integrity and minimise the impact of any Security Incidents with a view to ensuring the availability, integrity and continuity of service and the protection of networks, communications systems and data.

3.2 The Manufacturer shall deliver to the Operator, within three (3) months of the Contract Date, a draft outline Security, Continuity & Recovery Plan which complies with the requirements of this Schedule.

3.3 The Operator shall review the draft Security, Continuity & Recovery Plan and provide any comments to the Manufacturer within eight (8) weeks of receipt of such draft.

3.4 The Manufacturer shall revise the draft Security, Continuity & Recovery Plan to incorporate the amendments reasonably required by the Operator and shall provide the Operator with an updated final version of the Security, Continuity & Recovery Plan within eight (8) weeks of receipt of the Operator's comments.

3.5 If a 'major incident' or 'cyber event' impacts the IT Systems and/or OT Systems during the period in which the Security, Continuity & Recovery Plan is being developed and finalised, the Manufacturer will provide business continuity services in respect of cyber security to the Operator in accordance with:

3.5.1 ISO22301 and ISO22313; and

3.5.2 any other applicable cyber security and business continuity and disaster recovery processes/plans of the Operator (as notified to the Manufacturer from time to time).

3.6 The Manufacturer shall keep the Security, Continuity & Recovery Plan up-to-date and shall provide any proposed updated versions of the plan to the Operator from time to time. The Operator shall review and comment on the proposed updated Security, Continuity & Recovery Plan within eight (8) weeks of receipt. The Manufacturer shall then revise the updated version of the Security, Continuity & Recovery Plan to incorporate the amendments reasonably required by the Operator within eight (8) weeks of receipt of the Operator's comments. The Security, Continuity & Recovery Plan shall continue in place without the proposed updates until such time as the updated version of it has been agreed by the Parties.

3.7 The Security, Continuity & Recovery Plan shall:

3.7.1 set out how its constituent elements related to security, business continuity and disaster recovery link to and interrelate with each other;

3.7.2 detail how the invocation of any of its elements may affect any of the Manufacturer's obligations under this MSA;

3.7.3 contain an obligation on the Manufacturer to liaise with the Operator and (at the Operator's request) any related third party with respect to issues concerning business continuity and disaster recovery, where applicable;

3.7.4 detail how it links to and interrelates with any other disaster recovery or business continuity plans of the Operator (as notified by the Operator to the Manufacturer);

3.7.5 set out the process for monitoring the supply chain and confirming that it is robust;

3.7.6 contain a communication strategy for reporting details of an incident, including key contact details (including roles and responsibilities) for the Manufacturer (and any subcontractors) and for the Operator;

3.7.7 provide references to the documentation of relevant processes and procedures;

3.7.8 identify the procedures for reverting to ‘normal service’;

3.7.9 detail the Manufacturer’s back-up methodology and approach to data back-up and data verification, including method(s) of recovering or updating data collected (or that ought to have been collected) during a failure or disruption to ensure that there is no more

than the accepted (as agreed between the Parties) amount of data loss and to preserve data integrity;

3.7.10 set out the steps to be taken by the Manufacturer upon resumption of the services in order to address any prevailing effect of the failure or disruption, including a root cause analysis of the failure or disruption and further testing and management arrangements; and

3.7.11 be upgradeable and sufficiently flexible to support any changes to the business processes facilitated by the Manufacturer and the business operations supported by the Manufacturer.

4. SECURITY INCIDENTS

4.1 If the Manufacturer becomes aware of any actual, suspected or reasonably anticipated Security Incident, including following any cyber-threat intelligence information being published by the National Cyber Security Centre or on the common vulnerabilities and exposures list available at https://cve.mitre.org/ (to the extent a vulnerability or exposure relates to the IT Systems and/or OT Systems) or equivalent, or becomes aware of any actual, suspected or reasonably anticipated unauthorised access of use by a third party or misuse, damage or destruction by any person, the Manufacturer shall:

4.1.1 notify the Operator in writing promptly and without undue delay (and in any event within forty eight (48) hours of becoming aware of or reasonably suspecting such Security Incident), such notification to include:

(a) a description of the nature of the Security Incident, including:

(i) where such Security Incident relates to Personal Data, the categories and approximate number of data subjects and Personal Data records affected or concerned; and/or

(ii) where such Security Incident relates to critical infrastructure and requires reporting under the NIS Regulations, the types of digital services provided, the approximate time and duration of the Security Incident, the nature of the incident and any cross-border impact;

(b) a description of the likely consequences of the Security Incident;

(c) a description of the measures taken or proposed to be taken by the Manufacturer to address the Security Incident, including measures to mitigate its possible adverse effects; and

(d) any other information the Operator reasonably requests;

4.1.2 immediately take all reasonable steps necessary to minimise the extent of actual or potential harm caused by any Security Incident and, in doing so, comply with any instructions issued by the Operator (acting reasonably);

4.1.3 implement the Security, Continuity & Recovery Plan and continue, in so far as is possible, to provide the affected IT Systems and/or OT Systems to the Operator and take all action necessary to restore the affected IT Systems and/or OT Systems to normal as soon as possible and in accordance with the Security, Continuity & Recovery Plan;

4.1.4 comply with any of the Operator's cyber security policies and procedures (as notified to the Manufacturer from time to time);

4.1.5 as soon as reasonably practicable, and in any event within five (5) Working Days of a Security Incident being resolved, provide the Operator with full details of the Security Incident including an initial root cause analysis; and

4.1.6 to the extent permitted by Applicable Law, assist the Operator with the provision of information in connection with any incident notification to any Government Authority, the Information Commissioner or any other competent authority, including under the Information Laws and, if deemed necessary by any such authority, assist and contribute to any investigations or inspections conducted following such notification.

5. OTHER

5.1 The Manufacturer shall certify on an annual basis that it has complied with the requirements of this Schedule. Without prejudice to any other right of audit or access granted to the Operator pursuant to this MSA, the Operator and its duly authorised representative(s) shall be entitled (on reasonable notice) (at least once per year as a minimum unless otherwise agreed, or at an additional frequency where required by a regulator, or where the Operator reasonably suspects that the Manufacturer has failed to comply with the requirements of this Schedule, or that a Security Incident has or is reasonably likely to occur) to carry out such audits and inspections as the Operator may reasonably deem necessary in order to verify the Manufacturer's compliance with the requirements of this Schedule and the Manufacturer shall provide full access and co-operation to the Operator and its duly authorised representative(s) in conducting such audit or inspection.

5.2 The Manufacturer shall use all reasonable endeavours to ensure that any Sub-contractors which are in any way engaged in relation to the matters described in this Schedule are subject to cyber security obligations that provide no less protection for the Operator, the data and the IT Systems and OT Systems than those set out in this Schedule.

5.3 The Manufacturer shall fully indemnify, keep indemnified and hold harmless the Operator on demand from and against any and all costs, liabilities and losses arising out of or in connection with any breach of the provisions of this Schedule or arising as a result of or in connection with a Security Incident or any Malicious Software to the extent caused by or contributed to by the acts or omissions of the Manufacturer (or its Sub-contractors).

6. CHARGES

In consideration for the Manufacturer performing its obligations under (i) this Schedule and (ii) Clause 45.6 (Software Updates), the Owner shall pay to the Manufacturer an annual fee of fifty thousand pounds Sterling (£50,000) (subject to Indexation) on the date falling thirty (30) months after Acceptance of the Last Unit and on each anniversary of such date therefrom until the earlier of (i) the expiry of the Design Life of the Last Unit and (ii) such date (not being earlier than the date falling ten (10) years after Acceptance of the Last Unit) on which the Owner instructs the Manufacturer to cease performing its obligations under this Schedule.