SCHEDULE 2

SERVICES DESCRIPTION

Schedule 2 *(Services Description)*

1 Introduction

1.1 This Schedule contains the description of the Services to be provided by the Supplier pursuant to this Contract. This includes the scope of the Monitoring Devices and Systems Services (MDSS) to be provided by the Supplier.

1.2 For context, a separate Field and Monitoring Service (FMS) Supplier will be responsible for provision of the operational services to process Orders and to fit and maintain Monitoring Equipment to Device-Wearers. The FMS Supplier will also be responsible for Monitoring the Events and Alerts generated by Monitoring Equipment.

1.3 This introduction section has been included to provide context information on the Authority's requirements.

1.4 The general scope of service for the Supplier is:

1.4.1 to provide Monitoring Equipment and services to monitor Device-Wearers;

1.4.2 to provide Applications that will collect and interpret data generated from the Monitoring Equipment provided by the Supplier;

1.4.3 to provide Applications to configure and manage the Monitoring Equipment provided by the Supplier; and

1.4.4 to provide Application and Infrastructure support services to ensure continued availability of the Services.

1.5 Paragraph 2 of this Schedule sets out the Operational Services including the following:

1.5.1 General Supplier Capabilities;

1.5.2 Device and Network Supply Provision;

1.5.3 Application Development and Operation; and

1.5.4 Infrastructure.

1.6 Paragraph 3 of this Schedule sets out the Implementation Services including the following:

1.6.1 Implementation Methods and Approach;

1.6.2 Data Migration;

1.6.3 MDSS Implementation Constraints;

1.6.4 Interface / Integration Responsibilities; and

1.6.5 Testing.

2 Operational Services:

2.1 General Supplier Capabilities

2.1.1 Collaboration Supply Chain management and Supplier management

2.1.1.1 The Supplier shall ensure that their Sub-Contractors and their performance are managed effectively to support the seamless provision of Services to meet the Performance Indicators specified in Schedule 3 (*Performance Levels*). (EMFSREQ-583)

2.1.1.2 The Supplier shall on request by the Authority demonstrate to the Authority that its Sub-Contractors are performing efficiently and effectively this may include undertaking, or supporting the Authority's undertaking, supply chain satisfaction surveys. (EMFSREQ-1590)

2.1.1.3 The Supplier shall, no later than the date specified in the Detailed Implementation Plan, establish the Application Development and Operation Capability. (EMFSREQ-1694)

2.1.1.4 In accordance with Part A of Schedule 22 (*Change Control Procedure*), the Supplier shall increase and decrease the number of Supplier Personnel providing the Application Development and Operation Capability to process Changes as directed by the Authority. (EMFSREQ-1553)

2.1.1.5 The Supplier shall enter into the Collaboration Agreement in accordance with Clause 4 of the Contract. (EMFSREQ-1405)

2.1.1.6 The Supplier shall provide continuity of service and expertise across its workforce, ensuring there is no single point of failure (EMFSREQ-1876)

2.1.2 Knowledge Management

2.1.2.1 The Supplier shall in accordance with the timescales set out in paragraph 2.1.2.2 below provide to the Authority up to date comprehensive and detailed documentation explaining the Service, including but not limited to:

(a) High and Low Level Design;

(b) Interface Control Documents;

(c) operational processes including a definitive operational manual detailing how Services are provided;

(d) detailed technical documents;

(e) relevant business process maps;

(f) training materials;

(g) Knowledge Articles for End Users, the Authority and/or Other Suppliers;

(h) relevant Device-Wearer facing materials;

(i) security risk assessments;

(j) Test Strategy and Test Plan; and

(k) Security Management Plan in accordance with Schedule 5 (*Security Management*) (EMFSREQ-1375)

2.1.2.2 The Supplier shall provide documentation as described in paragraph 2.1.2.1:

(a) in accordance with the timescales set out in the Implementation Plan;

(b) annually as directed by the Authority; and

(c) where a Change as undertaken in accordance with Schedule 22 (*Change Control Procedure*), results in the documentation not reflecting the Services. (EMFSREQ-1376)

2.1.2.3 The Supplier shall gather, store and share Knowledge Articles about the IT services they are contracted to provide, in order to allow Stakeholders and staff who use it to carry out their jobs effectively. (EMFSREQ-373)

2.1.2.4 The Supplier shall provide all documentation, Knowledge Articles and problem workarounds relating to the Service to the Authority in a readily accessible, electronic, unprotected format via the Virtual Library. (EMFSREQ-831)

2.1.2.5 The Supplier shall update Knowledge Articles whenever a material change to the Supplier System is implemented. These updated materials shall be re-circulated by the Supplier to relevant Stakeholders and staff. (EMFSREQ-374)

2.1.2.6 The Supplier shall provide satisfactory evidence to the Authority to demonstrate that the functionality delivered by the Supplier Solution meets all relevant functional and non-functional requirements prior to any integrated testing phases. (EMFSREQ-568)

2.1.2.7 The Supplier shall include (within its designs) any external references (e.g. standards, whitepapers) with a valid URL or ISBN reference. (EMFSREQ-1093)

2.1.2.8 The Supplier shall design and provide documentation to the Authority on use of its interfaces (systems, sub systems and services) for use, re-use and reference by the Authority and the Other Suppliers. (EMFSREQ-1092)

2.1.3 **Evidence Management and Court support**

2.1.3.1 The Supplier shall ensure that Monitoring Data is received, stored in the Supplier System, and made available in a manner that meets all relevant security and evidential standards, including but not restricted to BS10008 (Evidential weight and legal admissibility of electronic information). (EMFSREQ-183)

2.1.3.2 The Supplier shall handle and store all evidence and Monitoring Data to ensure that it can be used as evidence in court, if required. All data stored shall be in accordance with Data Protection Legislation. (EMFSREQ-1392)

2.1.4 **Training**

2.1.4.1 The Supplier shall ensure that Supplier Personnel remain up to date with mandatory training expectations, including training on: Data Protection Legislation, Modern Slavery, Cyber Security, Health & Safety, and refresher training for the Service including any updates to the Service. The Authority may spot-check compliance with this requirement at any point over the course of the Contract. (EMFSREQ-803)

2.1.4.2 The Supplier shall assist the Authority in the preparation and delivery of training to CJS Stakeholders and other relevant Stakeholders, where required by the Authority in accordance with time frames detailed in paragraph 3.2 Schedule 7 (*Authority Responsibilities*). (EMFSREQ-804)

2.1.4.3 The Supplier shall support the Authority to train members of the wider Criminal Justice System and other relevant Stakeholders in any Change that is implemented to the Service through the provision of training materials and through attending and facilitating training when required by the Authority (EMFSREQ-1183)

2.1.4.4 The Supplier shall ensure that all training on the Supplier System takes place in a non-live environment and has no impact on the Live Service. If data is required, test data should be used. (EMFSREQ-570)

2.1.4.5 If Supplier input into training materials is required, following submission by the Supplier, the Authority will provide feedback on Supplier content two (2) weeks prior to the training date, and approve/not approve the amended content one (1) week prior to the training date. (EMFSREQ-1833)

2.1.5 Software

2.1.5.1 All Software used in the Service will be maintained to at least the latest version -1, and have licences and support agreements in place. (EMFSREQ-1161)

2.1.6 Risk Management

2.1.6.1 The Supplier shall identify and report on internal and external EM IT risks for the Services in accordance with Schedule 24 (*Reports and Records Provision*). (EMFSREQ-371)

2.1.6.2 The Supplier shall ensure that mitigations are planned and executed against identified IT risks. (EMFSREQ-372)

2.1.7 Quality management

2.1.7.1 The Supplier shall ensure their systems, sub systems and services synchronise their time and time zone (GMT) with the British National Physical Laboratory (NPL). (EMFSREQ-1186)

2.2 Device Supply

2.2.1 Device Provision

2.2.2 Fitted Location Monitoring Devices

2.2.2.1 The Supplier shall provide Fitted Location Monitoring Devices for Location Monitoring, where the Location Data is captured by Monitoring Equipment that is Fitted to the Device-Wearer. (EMFSREQ-1852)

2.2.2.2 The Supplier shall provide Fitted Location Monitoring Devices to monitor compliance with Location Monitoring requirements. (EMFSREQ-412)

2.2.2.3 The Supplier shall provide Fitted Location Monitoring Devices to monitor compliance with Exclusion Zone and Inclusion Zone requirements. (EMFSREQ-411)

2.2.2.4 The Supplier shall ensure that Fitted Location Monitoring Devices providing Location Monitoring shall be able to monitor compliance for a Device-Wearer with both Location Monitoring and Curfew Monitoring requirements. The Fitted Location Monitoring Device shall enable Curfew Monitoring in the same way as a Curfew Only Device. (EMFSREQ-1865)

2.2.2.5 The Supplier shall ensure that Fitted Location Monitoring Devices support Inclusion Geofences, for which the Device Monitoring Platform shall immediately record an associated Inclusion Geofence Non-Compliance Event when the Device enters and leaves an active Inclusion Geofence. (EMFSREQ-1351)

2.2.2.6 The Supplier shall ensure that Fitted Location Monitoring Devices support Exclusion Geofences, for which the Device Monitoring Platform shall immediately record an associated Exclusion Geofence Non-Compliance Event when the Device enters and leaves an active Exclusion Geofence. (EMFSREQ-1347)

2.2.2.7 Any systems or services required to support the Fitted Location Monitoring Devices in assessing Exclusion Zone Violation Events or Inclusion Zone Violation Events shall be provided by the Supplier. (EMFSREQ-1350)

2.2.2.8 The Supplier should ensure that each Exclusion Zone is capable of being configured by the FMS Supplier, with a buffer distance, in order that a Buffer Zone Violation Event is triggered before the Exclusion Zone Violation Event takes place. (EMFSREQ-1349)

2.2.2.9 The Supplier should ensure that each Inclusion Zone is capable of being configured by the FMS Supplier, with a buffer distance, in order that a Buffer Zone Violation Event is triggered before an Inclusion Zone Violation Event takes place. (EMFSREQ-1352)

2.2.3 **Non-Fitted Location Monitoring Devices**

2.2.3.1 The Supplier shall provide Location Monitoring Devices which:

(a) are suitable to monitor where a Device-Wearer is at all times;

(b) are not fitted permanently to the Device-Wearer for the duration of the Monitoring Requirements;

(c) can certify that the correct Device-Wearer is being Monitored; and

(d) do not require the Device-Wearer to have a fixed address. (EMFSREQ-823)

2.2.3.2 The Supplier shall provide Non-Fitted Devices capable of validating the identity and presence of the Device-Wearer, by biometric means, to ensure that Electronic Monitoring is being conducted on the correct Device-Wearer and within the terms of their Monitoring Requirements. (EMFSREQ-824)

2.2.3.3 The Supplier shall ensure that the Non-Fitted Device carries out biometric identification of the Device-Wearer to the ANSI/NIST-ITL 2011/AN-2013 standard (or successors thereof). (EMFSREQ-1585).

2.2.3.4 The Supplier shall ensure that the Non-Fitted Device shall reliably and easily enrol, under supervision of a Field Officer, the biometric characteristics of a Device-Wearer into the identity verification regime, such that this forms a reliable baseline against which to perform matching. (EMFSREQ-825)

2.2.3.5 The Supplier shall provide Non-Fitted Devices to which the entire user population can provide relevant biometric information. (EMFSREQ-829)

2.2.3.6 The Supplier’s Non-Fitted Device should enable biometric enrolment to occur locally without the need for Network connection at the time of enrolment. This should enable a Field Officer to complete biometric enrolment within a single Visit. (EMFSREQ-1243)

2.2.3.7 The Supplier should provide Non-Fitted Devices that provide randomised prompts to the Device-Wearer to verify their identity and enable the Device-Wearer to provide their biometric sample(s) irrespective of the quality of Network connectivity at the time of the prompt. (EMFSREQ-827)

2.2.3.8 The Supplier shall ensure that the Non-Fitted Device operates an automated and randomised regime of identity verification checks on Device-Wearers within a configurable number and time range of checks per day. (EMFSREQ-828)

2.2.3.9 The Supplier shall ensure that the Non-Fitted Device allows Field Officers to supervise testing of the Device-Wearer's ability to submit a biometric identity verification. (EMFSREQ-826)

2.2.4 Fitted Location Monitoring Devices and Non-Fitted Location Monitoring Devices (Technical specification)

2.2.4.1 The Supplier shall provide Location Monitoring Devices which are suitable for Device-Wearers both with and without a fixed address. (EMFSREQ-1369)

2.2.4.2 The Supplier shall provide Devices which determine and log the type of location signal received in real time. Receivable location signals shall include:

(a) Location Data obtained by Global Navigation Satellite System (GNSS);

(b) Location Data obtained on Global System for Mobile communication cells (GSM); and

(c) Location Data obtained from Location Based Services (LBS). (EMFSREQ-794)

2.2.4.3 The Supplier shall provide Devices with a GNSS based primary location technology. The secondary location technology shall provide Mobile Network information for the FMS Supplier to derive location fix data. (EMFSREQ-1346)

2.2.4.4 The Supplier shall ensure that the Location Monitoring technologies to be used for recording location fix data in each Message and Event are configurable, including in cases where the primary Location Monitoring technology is unable to take a fix. (EMFSREQ-1366)

2.2.4.5 The Supplier shall provide Location Monitoring Devices capable of supporting a Tertiary Location Identification Technology (e.g. LBS, Wi-Fi). (EMFSREQ-1365)

2.2.4.6 The Supplier shall ensure that, where Wi-Fi is supported, Location Messages contain the raw data from the associated Wi-Fi chip-set, irrespective of whether any transformation is applied. The following data shall be provided in each Location Message:

(a) date/time of data acquisition;

(b) Basic Service Set Identifier (BSSID) / Media Access Control (MAC) address; and

(c) received signal strength.

(EMFSREQ-1364)

2.2.4.7 The Supplier shall ensure that Location Monitoring Devices can record the real-time environment that the GNSS receiver is experiencing, using the most suitable messaging protocol including but not limited to by way of example NMEA and/or UBLOX. (EMFSREQ-1362)

2.2.4.8 The Supplier shall provide Location Monitoring Devices which record reasons for not taking a location fix in the Location Message, instead of the associated location fix data, if the Device does not take a complete location fix when scheduled to do so. Devices must record location fix data for as many location technologies as are available, rather than abandon if no location fix is available for one technology. (EMFSREQ-1361)

2.2.4.9 The Supplier shall provide Location Monitoring Devices which support multiple Exclusion Geofences and multiple Inclusion Geofences, and which are configurable remotely via the FMS Supplier's software. The Supplier shall ensure that Location Monitoring Devices support polygons with a maximum of two thousand (2000) sides or be able to support up to two thousand (2000) polygon vertex points. (EMFSREQ-1360)

2.2.4.10 The Supplier should provide Location Monitoring Devices which are capable of locally storing multiple Exclusion Geofences and multiple Inclusion Geofences. (EMFSREQ-1826)

2.2.4.11 Location Monitoring Devices provided by the Supplier must call into an always on Assisted–Global Positioning System server to download relevant ephemeris and almanac data. (EMFSREQ-1358)

2.2.4.12 The Supplier shall ensure that Location Messages contain the raw data from the associated GSM chip-set, irrespective of whether any transformation is applied. The following data shall be provided in each Location Message:

(a) date/time of data acquisition;

(b) Mobile Country Code (MCC);

(c) Mobile Network Code (MNC);

(d) Location Area Code (LAC);

(e) Base Station Identity Code (BSIC);

(f) Cell Identity (CI);

(g) received signal level;

(h) indication as to whether this cell is the attached/serving cell; and

(i) all of (f) – (h) above for each cell within range of the Location Monitoring Device for the attached Mobile Network. (EMFSREQ-1356)

2.2.4.13 The Supplier should ensure that Location Messages shall contain the raw data from the associated GNSS chip-set, irrespective of whether any transformation is applied. The following data shall be provided in each Location Message:

(a) Global Positioning System Fix Data (GGA);

(b) GNSS Dilution of Precision and Active Satellites (GSA);

(c) GNSS Satellites in View (GSV); and

(d) Recommended Minimum Specific GNSS Data (RMC). (EMFSREQ-1829)

2.2.4.14 The Supplier shall ensure that the GNSS receiver used in the Monitoring Equipment shall have sensitivity better than or equal to minus one hundred and sixty Decibel-milliwatts (-160dBm). (EMFSREQ-1354)

2.2.4.15 The Supplier shall ensure that GNSS Location Messages contain the number of the satellites used to calculate location fix, and an indication of the accuracy of the location fix, including HDoP. (EMFSREQ-1345)

2.2.4.16 The Supplier should ensure that GNSS Location Messages contain the identities of the satellites used to calculate location fix. (EMFSREQ-1832)

2.2.4.17 The Supplier shall ensure the Location Monitoring Devices have the functionality to enable them to be located, if powered on, in circumstances when they are lost or stolen. (EMFSREQ-1579)

2.2.4.18 The Supplier shall ensure that Devices can be remotely configurable by the FMS Supplier to be able to change the Monitoring behaviour upon the occurrence of specific Monitoring Events e.g. alter Sampling Rate, Recording Rate and/or Reporting Rate. (EMFSREQ-1348)

2.2.4.19 On request from the Authority and for a limited number of use cases (including, but not limited to, Special Case

Monitoring), the Supplier shall provide Location Monitoring Devices with the ability to use multiple accredited Networks which shall ensure availability of Monitoring if one Network is lost. (EMFSREQ-1396)

2.2.4.20 For Device types which require a location signal to carry out Electronic Monitoring, the Supplier shall provide Devices which have a measured CEP of three (3) metres or better. (EMFSREQ-528)

2.2.4.21 For Devices which capture Location Data, the Supplier shall provide Devices which support a range of:

(a) Sampling Rates (from sixty (60) seconds to two (2) hours, accurate to one (1) second),

(b) Recording Rates (from sixty (60) seconds to two (2) hours, accurate to one (1) second),

(c) Reporting Rates (from sixty (60) seconds to twenty-four (24) hours.

The Supplier shall ensure that Electronic Monitoring Equipment records and sends Location Data according to the applied configuration, which will vary depending on:

(a) Device type; and

(b) Electronic Monitoring requirement type. (EMFSREQ-744)

2.2.4.22 For Devices which capture Location Data, the Supplier should ensure that such Devices can be configured to support a higher frequency range of:

(a) Sampling Rates (below sixty (60) seconds up to three (3) seconds, accurate to one (1) second),

(b) Recording Rates (below sixty (60) seconds up to three (3) seconds, accurate to one (1) second),

(c) Reporting Rates (below sixty (60) seconds up to fifteen (15) seconds). (EMFSREQ-1827)

2.2.5 **Fitted Transdermal Alcohol Monitoring Devices**

2.2.5.1 The Supplier shall provide Fitted Devices that Monitor compliance with Alcohol Monitoring requirements or Licence Conditions through transdermal methods. (EMFSREQ-413)

2.2.5.2 The Supplier shall provide Transdermal Alcohol Monitoring Devices to measure the time and duration of the consumption of alcohol at any point during the Monitoring Requirements. (EMFSREQ-530)

2.2.5.3 The Supplier shall provide Transdermal Alcohol Monitoring Devices that can provide a reading of the amount of a Device-Wearer's alcohol intake at any point during the course of the Monitoring Requirements. (EMFSREQ-1163)

2.2.5.4 The Supplier shall provide Transdermal Alcohol Monitoring Devices that can distinguish between Ingested Alcohol and Environmental Alcohol. (EMFSREQ-516)

2.2.6 **Remote Breathalyser Alcohol Monitoring Devices**

2.2.6.1 The Supplier shall provide Devices that test Compliance with Alcohol Monitoring requirements or Licence conditions through the use of a Remote Breathalyser Device. (EMFSREQ-1401)

2.2.6.2 The Supplier shall provide Remote Breathalyser Devices that provide a reading of the amount of a Device-Wearer's alcohol intake at regular and/or random points during the course of the Monitoring Requirements. (EMFSREQ-1402)

2.2.6.3 The Supplier shall provide Remote Breathalyser Devices that can distinguish between Ingested Alcohol and Environmental Alcohol. (EMFSREQ-1404)

2.2.6.4 For Device-Wearers on Alcohol Monitoring requirements, the Supplier shall provide Remote Breathalyser Devices that can confirm, through biometric methods, the identity of the Device-Wearer providing each breath sample. (EMFSREQ-1584)

2.2.6.5 The Supplier shall provide Remote Breathalyser Devices which are portable. (EMFSREQ-1591)

2.2.6.6 The Supplier shall provide Remote Breathalyser Devices which do not require recalibration more than once a year. (EMFSREQ-1592)

2.2.6.7 The Supplier shall provide Remote Breathalyser Devices which provide feedback to the Device-Wearer as to whether the sample has been provided successfully. (EMFSREQ-1594)

2.2.6.8 The Supplier shall provide Remote Breathalyser Devices which record the date and time of each breath sample. (EMFSREQ-1595)

2.2.6.9 The Supplier shall provide Remote Breathalyser Devices which can alert the Device-Wearer to provide a remote breath sample. Remote breath samples may be requested:

(a) on a pre-arranged schedule as determined in the Monitoring Requirements;

(b) on a random schedule; and/or

(c) on a prompt from the Monitoring Centre. (EMFSREQ-1596)

2.2.6.10 The Remote Breathalyser Device shall be capable of raising a Non-Compliance Event to the Device Monitoring Platform when the Device-Wearer has not submitted a sample as detailed in paragraph 2.2.6.9. The period of time between the request and the raising of the Event, shall be configurable. (EMFSREQ-1830)

2.2.7 **Curfew Monitoring Devices**

2.2.7.1 The Supplier shall provide Devices that Monitor Device-Wearers' compliance with Curfew Monitoring requirements, including provision of Devices limited to only Curfew Monitoring. (EMFSREQ-410)

2.2.7.2 Each Curfew Absence shall immediately be recorded as an Event. (EMFSREQ-1572)

2.2.7.3 During Curfew Absence, and where Location Monitoring is also available, the Device-Wearer's location should be recorded and reported in accordance with the pre-configured recording and reporting regime for Curfew Absence. (EMFSREQ-1574)

2.2.7.4 The Supplier shall supply Devices which uniquely identify and Monitor up to fifty (50) Device-Wearers at the same Curfew Location at the same time. (EMFSREQ-542)

2.2.7.5 The Supplier shall supply Devices that Monitor Device-Wearers' compliance with Curfew Monitoring Requirements in situations where the Device is in an area of low or no signal. (EMFSREQ-543)

2.2.7.6 The Supplier shall ensure that any Electronic Monitoring Equipment used for Curfew Monitoring that is to be located in the Device-Wearer's residence shall record a Tamper

Event which alters the Device-Wearer's Curfew Boundary. (EMFSREQ-1353)

2.2.7.7 The Supplier shall ensure that any Device used for Curfew Monitoring, that is to be located in the Device-Wearer's residence, incorporates Location Monitoring capabilities, to aid confirmation that the Device is present at the Curfew Location. (EMFSREQ-1363)

2.2.7.8 The Supplier shall ensure that any Device used for Curfew Monitoring that is to be located in the Device-Wearer's residence should transmit status information regularly. Transmissions shall be at intervals remotely configurable by the FMS Supplier to between five (5) minutes and twenty-four (24) hours. (EMFSREQ-1576)

2.2.7.9 The Supplier shall ensure that any Device used for Curfew Monitoring that is to be located in the Device-Wearer’s residence connected to an external power supply shall have a battery backup capability of at least twenty-four (24) hours in event of loss of its external power supply. (EMFSREQ-1558)

2.2.7.10 The Supplier shall ensure that any Device used for Curfew Monitoring that is to be located in the Device-Wearer’s residence connected to an external power supply shall immediately record an associated Event for each loss of external power where the loss of power is for greater than one (1) second. (EMFSREQ-1559)

2.2.7.11 Any Device used for Curfew Monitoring that is to be located in the Device-Wearer’s residence should not overheat, and should continue operation, when fabrics and non-porous materials are placed on the Monitoring Equipment at an ambient temperature of twenty-one (21) degrees Celsius for a period of eight (8) hours. (EMFSREQ-1562)

2.2.7.12 Any Device used for Curfew Monitoring shall Monitor guest data when it is proximate to other sets of Electronic Monitoring Equipment. In open air environments the Device shall Monitor guest data when it is within a one hundred and fifty (150)m radius of Electronic Monitoring Equipment. (EMFSREQ-699)

2.2.8 **All Devices**

2.2.8.1 The Supplier shall supply Devices that comply with the requirements of Clause 9.7. (EMFSREQ-416)

2.2.8.2 The Supplier shall proactively Monitor Devices for Monitoring Equipment Incidents. (EMFSREQ-696)

2.2.8.3 The Supplier shall ensure that all Electronic Monitoring Equipment is composed of easily recycled and recyclable materials. (EMFSREQ-729)

2.2.8.4 The Supplier shall ensure that all Electronic Monitoring Equipment goes through a process of repair, refurbishment, re-use and recycling. Recycling must happen within the UK or in cases where the Supplier is not based in the UK, the Supplier's main operational country. Material sent to landfill shall be minimised and reported on by the Supplier to the Authority in accordance with the provisions of Schedules 4 (*Standards)* and 24 (*Reports and Records Provision*). (EMFSREQ-727)

2.2.8.5 The Supplier shall provide Devices with a minimum expected lifespan of whichever is the longer of:

(a) three (3) years;

(b) the relevant Warranty Period; and

(c) the average duration of the Monitoring Requirement type which the Device is relevant to. (EMFSREQ-748)

2.2.8.6 The Supplier shall provide guidance to the FMS Supplier to ensure that Device-Wearers with diverse physical and/or mental health conditions can be Monitored. Examples include but are not limited to:

(a) pregnancy/maternity;

(b) medical conditions e.g. prosthetic limbs; and

(c) neurodiversity. (EMFSREQ-749)

2.2.8.7 The Supplier shall provide Devices which become detached at a load, between 500N and 600N, in order to prevent injury to the Device-Wearer. Devices shall not become detached during normal day-to-day use. (EMFSREQ-702)

2.2.8.8 The Supplier shall ensure that each Device and its components are uniquely identifiable. Unique identifiers shall be recorded and updated in the Asset Register. (EMFSREQ-415)

2.2.8.9 The Supplier shall ensure that all Monitoring Equipment uses a unique internal identifier that is different to the external identifier that should be incorporated into each

Event. The association of external and internal identifiers should be provided to the FMS Supplier. (EMFSREQ-1569)

2.2.8.10 The Supplier shall provide Monitoring Equipment that carries an indelible inscription showing the Monitoring Centre telephone contact number as specified by the FMS Supplier. The telephone number on a Device should be visible to the Device-Wearer when the Device is fitted. (EMFSREQ-1566)

2.2.8.11 The Supplier shall ensure that Straps and Clips carry a unique physical identifier which is visible when in use. (EMFSREQ-1570)

2.2.8.12 The Supplier shall provide expected lifespan estimates for components within each Device type. These shall include but are not limited to the battery. This information shall be provided annually. (EMFSREQ-514)

2.2.8.13 The Supplier shall provide Devices which work continuously, so long as they have battery life. There shall be no downtime aside from when unavoidable to complete necessary software updates. (EMFSREQ-518)

2.2.8.14 The Supplier shall provide Devices that can receive and apply Supplier managed operating system and/or firmware updates and security patches remotely with minimal downtime and loss of service/data. (EMFSREQ-523)

2.2.8.15 The Supplier will ensure that all Events and audit/system logs stored within the Monitoring Equipment are time-stamped in Coordinated Universal Time (UTC). (EMFSREQ-1582)

2.2.8.16 The Supplier shall provide Devices which hold captured data during periods where the Device battery dies and when the Device is powered off and that Device enables such data to be transmitted to and be retrievable by the Monitoring Centre when the Device is subsequently powered on. (EMFSREQ-525)

2.2.8.17 The Supplier shall provide Devices which continue to collect and store data when the Device is unable to connect to the Mobile Network. Once Mobile Network connection is restored, the data shall be gathered and processed by the Supplier's Device Monitoring Platform. (EMFSREQ-1166)

2.2.8.18 The Supplier shall ensure that Events and Alerts relating to availability of Monitoring Equipment are gathered and

processed by the Supplier's Device Monitoring Platform. (EMFSREQ-1172).

2.2.8.19 The Supplier shall ensure that the Monitoring Equipment generates Events and Alerts relating to the availability and technical functioning of the Monitoring Equipment. (EMFSREQ-524)

2.2.8.20 The Supplier shall ensure that both Tethered Charging and Untethered Charging methods must be available for Fitted Devices. (EMFSREQ-520)

2.2.8.21 The Supplier shall ensure that all Monitoring Equipment and Devices meet the security requirements in accordance with Schedule 5 (*Security Management*). (EMFSREQ-558)

2.2.8.22 The Supplier shall provide to the Authority and/or FMS Supplier any and all tools required to fit and/or remove Electronic Monitoring Equipment to/from a Device-Wearer. (EMFSREQ-1411)

2.2.8.23 The Supplier shall ensure that any fitting tools provided to fit or remove Devices have a batch number and are uniquely identifiable. Unique identifiers shall be recorded and updated, as necessary in the Asset Register. (EMFSREQ-1245)

2.2.8.24 Where Devices contain batteries that must be re-charged, the Supplier shall supply Devices with batteries which last for a minimum of twenty-four (24) hours after a full charge, when used normally. Charging from empty to a full charge shall not take more than one (1) hour. (EMFSREQ-1174)

2.2.8.25 Where it is the responsibility of the Device-Wearer to charge the Device's battery, the Supplier shall provide Devices that can be configured by the FMS Supplier to provide discrete Notifications to the Device-Wearer that the Device has low battery. The trigger for this notification shall be linked to the battery percentage and shall be agreed with the Authority and FMS Supplier. (EMFSREQ-527)

2.2.8.26 Where a Device contains a battery that the Device-Wearer cannot charge, the Supplier shall ensure that the Notification threshold can be configured to enable the FMS Supplier to arrange a Device replacement Visit before the Device battery dies. (EMFSREQ-1609)

2.2.8.27 Where the Device requires charging by the Device-Wearer, it shall record the following types of Event:

(a) Start of Charging Event;

(b) End of Charging Event; and;

(c) Low Battery Event.

Each such Event shall include the battery charge level. (EMFSREQ-1563)

2.2.8.28 Where the Device does not require charging by the Device-Wearer, it shall provide the battery charge level in Events that are recorded regularly. (EMFSREQ-1565)

2.2.8.29 The Supplier shall provide a model to the Authority and FMS Supplier prior to the Technical Service Commencement (Milestone) date for assessing potential battery usage for different operating configurations. The model shall be based on scenarios provided by the Authority in accordance with paragraph 3.3 of Schedule 7 (*Authority Responsibilities*). (EMFSREQ-1359)

2.2.8.30 The Supplier shall provide Devices made from materials which are non-irritant when worn close to the skin for extended periods of time. (EMFSREQ-703)

2.2.8.31 The Supplier shall supply Devices which comply with the requirements set out in Schedule 4 (*Standards*). (EMFSREQ-417)

2.2.8.32 In the event of a Device Incident, the Supplier shall at its own cost swap a Defective Device component for a new component to prolong the lifespan of the Device as set out in paragraph Error! Reference source not found.. C omponents include, but are not limited to, batteries. (EMFSREQ-587)

2.2.8.33 Where a Device-Wearer has multiple Monitoring Requirements, the Supplier should aim to minimise the number of Devices needed to Monitor compliance with all Monitoring Requirements. (EMFSREQ-414)

2.2.8.34 Subject to the Monitoring Requirements, the Supplier should ensure that the Device does not interfere significantly with the Device-Wearer's daily life, such as their ability to sleep or work. (EMFSREQ-519)

2.2.8.35 The Supplier shall ensure that Monitoring Equipment does not have external aerials, should be discreetly styled, does not exhibit any indication of its purpose and should not carry any displays, logos, labels, markings other than

those explicitly required by the requirements set out in this Schedule. (EMFSREQ-1567)

2.2.8.36 The Supplier shall ensure that, for the duration of the relevant Monitoring Requirement, it is not possible for the Device-Wearer to remove or interfere with the functionality of a Fitted Device, without a Tamper Event being registered. Devices shall detect and immediately report a Tamper Event to the FMS Supplier where:

(a) any activity prevents the Device from normal operation;

(b) reduction or interference of signal by electromagnetic shielding, signal jamming or replay is evident;

(c) imitation or alteration of signals would otherwise falsify evidence of the presence of other Monitoring Equipment, including (but not limited to) by Spoofing; and

(d) a fault or damage that affects the Device's ability to function is detected, including for disconnection of its internal power supply.

Tamper types which must be detected by Devices are listed in Table 1 below. (EMFSREQ-521)

Table 1: Tamper Types

Ref	Tamper Type	Trigger event	Location - Fitted	Location – Non-Fitted	Curfew	Transdermal alcohol	Remote Breathalyser alcohol
1	Strap cut	The Strap or fixings are cut open or broken in a way that the Device can be removed from the person's limb	X		X	X	
2	Case open	The HMU or Device case is open. Can also be caused by the case or HMU being damaged.	X	X	X	X	X
3	HMU moved	Motion detected - The HMU is moved beyond a configurable tolerance from where it was positioned at time of Installation.	X		X		
4	HMU mains to battery power	The HMU moves to battery power instead of mains power	X		X	X	
5	HMU phone damaged	The HMU's phone line and/or handset (as applicable) is disconnected and/or damaged.	X		X	X	

6	Signal blocked – RF	Radio jamming - The Radio Frequency (RF) antenna signal has been blocked or distorted.			X		
7	Signal blocked – GNSS	The GNSS signal is blocked or distorted.	X	X			
8	Signal blocked – 3G/4G/5G/WiFi	The Device cannot transmit information to the Monitoring Centre	X	X	X	X	X
9	Biometric spoof	The biometric functionality is blocked or distorted. Biometric liveness check. Presentation attack detection.		X			X
10	Alcohol reading blocking	Device-Wearer does something to interfere with the Device's ability to take alcohol samples.				X	X

2.2.8.37 Where it is possible for a Strap to be stretched (under force only), the Supplier should ensure Devices detect when a Device-Wearer has applied force in an attempt to interfere with the functioning of the Strap and/or Device. (EMFSREQ-1825)

2.2.8.38 The Supplier shall ensure that the sensitivity of detection mechanisms shall be configurable by the FMS Supplier such that False Tamper Events and other false Non-

Compliance Events are kept to a minimum. The sensitivity shall be agreed with the Authority and FMS Supplier and notified to the Supplier. (EMFSREQ-1560)

2.2.8.39 The Supplier shall provide Monitoring Equipment that continues normal operation after detecting a Tamper Event where such Tamper Event has not made the Monitoring Equipment unavailable. (EMFSREQ-1557)

2.2.8.40 The Supplier shall provide Monitoring Equipment which has a method of contacting the Monitoring Centre by voice communication for Device-Wearers subject to Curfew Monitoring and Fitted Location Monitoring requirements (excluding Home Office Fitted Location Monitoring) (EMFSREQ-1263)

2.2.8.41 The Supplier should provide Monitoring Equipment which has a method of contacting the Monitoring Centre by voice communication for Device-Wearers subject to any of the following Monitoring Requirements - Alcohol Monitoring, Home Office Fitted Location Monitoring and Non-Fitted Location Monitoring. (EMFSREQ-1264)

2.2.8.42 The Supplier shall ensure that Devices record Messages providing the following data in relation to each Voice communication:

(a) caller/dialled phone number;

(b) whether the call was answered / not answered;

(c) ringing duration of the phone call; and

(d) duration of the phone call (EMFSREQ-1571)

2.2.8.43 For Fitted Devices, the Supplier shall ensure that Straps used to secure the Device to the Device-Wearer shall be made of a material which shows when a Tamper has occurred or been attempted. (EMFSREQ-1397)

2.2.8.44 Where Straps are required to fit Devices, the Supplier shall provide Strap lengths which can fit both Children (over the age of twelve (12)) and Adults. If longer Straps are required, these shall be supplied by the Supplier on request with Clips fitted. Both Strap ends shall lock into different sides of the Device with no tail. (EMFSREQ-1549)

2.2.8.45 The Supplier shall ensure that Fitted Devices can be quickly removed from the Device-Wearer with non-specialist tools. (EMFSREQ-1561)

2.2.8.46 The Supplier shall ensure that Devices shall not cause irritation, injury or harm to the Device-Wearer nor damage to their place of residence, except where this is the result of deliberate, negligent actions of the Device-Wearer. (EMFSREQ-1550)

2.2.8.47 The Supplier shall provide Devices which send an Alert to the Monitoring Centre when recalibration is necessary. (EMFSREQ-1593)

2.2.8.48 For Devices utilising GSM digital Mobile Networks, the Supplier shall provide Devices which can be disabled and enabled remotely by the FMS Supplier in the event that they are lost or stolen. (EMFSREQ-1692)

2.2.9 **Monitoring Equipment Stock Management**

2.2.9.1 The Supplier shall supply the quantity of Monitoring Equipment in line with the Authority's equipment needs over the Term of the Contract based on Caseload Forecasts plus contingency requirements provided by the Authority. Caseload Forecasts will be provided by the Authority no less than twice a year. (EMFSREQ-423)

2.2.9.2 The Supplier shall work effectively with the FMS Supplier to ensure a robust supply chain is in place and there is always sufficient Monitoring Equipment to meet the needs of the EM Service. (EMFSREQ-1244)

2.2.9.3 When supplying a new batch of Monitoring Equipment to the FMS Supplier, the Supplier shall provide the FMS Supplier with the unique identifiers for each item of Monitoring Equipment provided in that batch in a format agreed by both parties. (EMFSREQ-1165)

2.2.9.4 The Supplier shall ensure that each Monitoring Equipment batch is uniquely identifiable. (EMFSREQ-697)

2.2.9.5 The Supplier shall be able, at any time, to identify and determine which Monitoring Equipment is actively undertaking monitoring of Device-Wearers. (EMFSREQ-701)

2.2.9.6 The Supplier shall monitor the performance of the Device manufacturing and delivery supply chain and resolve any identified issues. The Supplier shall report any supply chain issues, which may impact its ability to meet the Authority's demand and/or the Supplier’s obligations, to the Authority as soon as they arise. (EMFSREQ-427)

2.2.9.7 The Supplier shall ensure that Monitoring Equipment is transported, handled and cleaned in a manner which protects it from damage and shall share information on how to do this with the FMS Supplier. (EMFSREQ-549)

2.2.10 **Device configuration**

2.2.10.1 The Supplier shall provide the FMS Supplier with access to all Monitoring Equipment Management Tools (for the avoidance of doubt, this will be the provision of user interfaces for FMS Supplier's staff including EM Contact Centre, Field Officers and Monitoring Centre staff) in order that the FMS Supplier is able to configure Monitoring Equipment to undertake Electronic Monitoring. (EMFSREQ-1372)

2.2.10.2 The Supplier shall provide Monitoring Equipment that can be deployed, initialised and configured within less than fifteen (15) minutes by a trained operative of the FMS Supplier (excluding any configuration of the Curfew Range, and explanation to the Device-Wearer and Network delays). (EMFSREQ-1577)

2.2.10.3 For Device-Wearers on Curfew Monitoring Requirements, the Supplier shall ensure that the FMS Supplier or other relevant actors shall be able to configure the Device to record whenever the Device-Wearer enters or exits the Curfew Area. (EMFSREQ-540)

2.2.10.4 For Device-Wearers on Alcohol Monitoring Requirements, the Supplier shall ensure that the FMS Supplier or other relevant third parties shall be able to configure Transdermal Alcohol Monitoring Devices and Remote Breathalyser Devices to measure the units of alcohol ingested at any point during the Monitoring Requirements. (EMFSREQ-531)

2.2.10.5 For Device-Wearers on Location Monitoring requirements, the Supplier shall ensure that the FMS Supplier or other relevant third parties shall be able to configure the Device to Monitor where a Device-Wearer is located at all times during the Monitoring Requirements. (EMFSREQ-546)

2.2.10.6 The Supplier shall ensure that Devices should autonomously and dynamically manage operating profiles, such that the Device’s behaviour does not need to be directed at all times by the FMS Supplier, recording each change in state as an Event. (EMFSREQ-1568)

2.2.10.7 For Device-Wearers on Location Monitoring requirements, the Supplier shall ensure that the FMS Supplier or other

relevant third parties shall be able to configure the Device Monitoring Platform and/or Devices to Monitor whether a Device-Wearer enters and leaves an Area of Interest at any point during the Monitoring Requirements. (EMFSREQ-700)

2.2.10.8 For Device-Wearers on Location Monitoring requirements, the Supplier shall ensure that the FMS Supplier or other relevant third parties shall be able to configure the Device Monitoring Platform and/or Devices to Monitor whether a Device-Wearer enters and leaves an Exclusion Zone or leaves and re-enters an Inclusion Zone at any point during the Monitoring Requirements. (EMFSREQ-544)

2.2.10.9 The Supplier shall permit the FMS Supplier to provide the Authority and other Stakeholders access, through Location Monitoring Applications, to data which allows them to easily understand the historic and current location of the relevant Device-Wearer. (EMFSREQ-537)

2.2.10.10 The Supplier shall ensure that all Devices, at all times, support a minimum of the current version -1 of the relevant operating system, firmware and security patches installed. (EMFSREQ-419)

2.2.10.11 The Supplier shall proactively manage the security of Devices it supplies, identifying vulnerabilities that could affect the normal operation of the Device and making available to the FMS Supplier any software or hardware changes required to fix vulnerabilities. (EMFSREQ-1600)

2.2.10.12 The Supplier shall ensure that only the FMS Supplier and other relevant Authority-approved personnel, are able to activate, re-configure or deactivate Devices. (EMFSREQ-534)

2.2.10.13 Where a Device is re-configured, activated or deactivated, the Supplier shall ensure that the following information is recorded: the name of user, time of use and configuration actions taken. Each record created shall be stored by the Supplier. The Supplier shall maintain the store of records. The records in the store shall be auditable by the Authority on request. (EMFSREQ-535)

2.2.10.14 Where the Supplier provides Field Officer Equipment that is capable of re-configuring or disabling Devices, the Supplier shall ensure that the Field Officer Equipment is protected from use by unauthorised individuals. (EMFSREQ-1578)

2.2.10.15 The Supplier shall ensure that configuration of Devices can be undertaken by Field Officers using mobile devices (e.g. tablets) via a secure app or natively through a browser interface. Any browser interface must support the current version -1 or later of all commonly used browsers, including, by way of example only: Firefox, Google Chrome and Microsoft Edge. (EMFSREQ-1123)

2.2.10.16 The Supplier should provide Electronic Monitoring Equipment which is able to receive and display communications by voice or text to specific cohorts of Device-Wearer. (EMFSREQ-698)

2.2.11 **Device Training**

2.2.11.1 The Supplier shall develop and deliver training for FMS Supplier staff and other relevant personnel on how to use Monitoring Equipment to undertake Monitoring of Device-Wearers. This shall include, but not be limited to, Installation and configuration of Monitoring Equipment. This shall be updated when necessitated by a change, for instance a new type of Tamper not previously seen. (EMFSREQ-430)

2.2.11.2 The Supplier shall train all relevant personnel in all aspects of Electronic Monitoring Equipment and the Device Monitoring Platform(s) to undertake Monitoring of Device-Wearers, including following any changes to the Device Monitoring Platform. Relevant personnel include, but are not limited to, FMS Supplier staff and the staff of CJS Stakeholders. (EMFSREQ-431)

2.2.11.3 The Supplier shall produce and maintain documented guidance on the suitability of the Electronic Monitoring options to ensure the individual options are used in the correct circumstances. This documentation shall be provided to:

(a) FMS Supplier staff; and

(b) Courts. (EMFSREQ-186)

2.2.11.4 The Supplier shall provide guidance to the FMS Supplier to give to Device-Wearers at the Device-Wearer's Induction on matters regarding battery lifespan, including:

(a) expected battery lifespan from full charge; and

(b) scenarios which cause battery to run down quickly. (EMFSREQ-551)

2.2.12 **Device Failure Root Cause Identification**

2.2.12.1 On request from the Authority and/or the FMS Supplier, the Supplier shall investigate the root cause of any Incidents with Electronic Monitoring Equipment in accordance with timeframes set out in Schedule 3 (*Performance Levels*). (EMFSREQ-299)

2.2.12.2 The Supplier shall receive, store, investigate and either dispose of (in line with paragraph 2.2.8.4) or recondition and re-use (if the nature of the Device Fault allows for this) faulty Devices which are returned to them by the FMS Supplier. (EMFSREQ-1312)

2.2.12.3 The Supplier shall develop and implement fixes and/or document workarounds, for any Incidents or Device Faults identified through:

(a) Root Cause Analysis of Problems; or

(b) any other method. (EMFSREQ-422)

2.2.12.4 In the Event of an Incident – P1, the Supplier shall produce a Major Incident Report (MIR) within five (5) Working Days of the Incident being closed. (EMFSREQ-1834)

2.2.13 **Device Repair**

2.2.13.1 If a Device Fault occurs, the Supplier shall collect the relevant Device from the FMS Supplier and shall confirm to the FMS Supplier whether the Device Fault is covered by the scope of the warranty.

(a) If a Device Fault occurs which is not covered by the warranty and the relevant Device is repairable then, at the Authority’s request, the Supplier shall repair and return the Device to the FMS Supplier.

(b) If a Device Fault occurs which is not covered by the warranty and the relevant Device is not repairable then, at the Authority's request, the Supplier shall dispose of the Device in accordance with the requirements of the Contract.

(c) If a Device Fault occurs which is covered by the warranty and the relevant Device is repairable then the Supplier shall repair and return the Device to the FMS Supplier.

(d) If a Device Fault occurs which is covered by the warranty and the relevant Device is not repairable then the Supplier shall dispose of the Device in accordance with the requirements of the Contract

and provide a replacement Device to the FMS Supplier. (EMFSREQ-1890).

2.2.13.2 Where Devices are returned to the Supplier for repair under warranty, the Supplier shall acknowledge receipt of Devices via the FMS Supplier's stock management Application. (EMFSREQ-1831)

2.2.13.3 The Supplier shall co-ordinate the return of repaired / refurbished Devices to the FMS Supplier using the FMS Supplier's stock management Application. (EMFSREQ-1835)

2.2.13.4 The Supplier shall securely dispose of any faulty equipment that is not capable of being or will not be repaired, in accordance with requirements set out in paragraph 6.1 of Schedule 5 (*Security Management*). (EMFSREQ-1857)

2.2.14 **Device Development and Enhancement**

2.2.14.1 At the Effective Date and annually thereafter, the Supplier shall provide a road-map(s) providing a detailed twelve (12) month view and high level medium to long term view, covering three (3) years, outlining the Supplier's plans for release of updates to the existing Service, including products, and the introduction of new Services and products. (EMFSREQ-756)

2.2.14.2 The Supplier shall enhance the Devices and Applications it supplies to stay abreast of wider developments in technology and functionality. (EMFSREQ-1384)

2.2.14.3 The Supplier shall continue to develop new Devices in response to wider market demand. (EMFSREQ-1385)

2.2.14.4 The Supplier shall seek opportunities for Innovation in the delivery of the Service wherever possible including, without limitation, in discharging its obligations under Clause 8 (Service Improvement). (EMFSREQ-1863)

2.2.15 **Evidential Device Handling**

2.2.15.1 The Supplier shall retain Monitoring Equipment suspected of being Tampered with as evidence, and be able to provide it as evidence, if required, for court proceedings or as otherwise directed by the Authority. A continuity of evidence log shall be maintained by the Supplier. The Authority shall give the Supplier two (2) weeks' prior notice of when Supplier Personnel are required to attend court for

evidential purposes, in accordance with Schedule 7 (*Authority Responsibilities).* (EMFSREQ-272)

2.2.15.2 The Supplier shall ensure that Monitoring Equipment which shall or may be required as evidence is catalogued - including updating the Supplier's Asset Register - transported and stored in a way which preserves evidential integrity. Evidence must be held to the latest version of BS10008 or any successor thereof. (EMFSREQ-493)

2.2.15.3 The Supplier shall be able to forensically examine Devices to an evidential standard to provide evidence for prosecution. This is required for, but not exclusive to, Special Cases' Devices suspected of Tampers. (EMFSREQ-1256)

2.2.15.4 If an external forensic examination body is used, the Supplier shall securely bag any Monitoring Equipment which needs to undergo forensic analysis and make it available for collection within twenty-four (24) hours of the request being submitted. (EMFSREQ-505)

2.2.16 **Device Provision Service Management & Reporting**

2.2.16.1 The Supplier shall report on Device provision in accordance with Schedule 24 (*Reports and Records Provision*). (EMFSREQ-1690)

2.2.17 **Field Service Application Integration**

2.2.17.1 The Supplier shall ensure that Devices can be remotely configured using the FMS Supplier's end user Devices. (EMFSREQ-1382)

2.3 **Mobile Network Provision**

2.3.1 **Mobile Network Service Management & Reporting**

2.3.1.1 The Supplier shall provide the Mobile Network service to support the Performance Indicators specified in Schedule 3 (*Performance Levels*). (EMFSREQ-444)

2.3.1.2 The Supplier shall monitor the performance of the Mobile Network Service. (EMFSREQ-442)

2.3.1.3 The Supplier shall report on the performance of the Mobile Network in accordance with Schedule 24 (*Reports and Records Provision).* (EMFSREQ-443)

2.3.2 **Mobile Network Provision**

2.3.2.1 The Supplier shall provide Mobile Network services and Infrastructure to collect and backhaul data from Network components and/or SIM cards used within Monitoring Equipment. (EMFSREQ-439)

2.3.2.2 For Monitoring Equipment which uses Mobile Networks, the Supplier shall commission Monitoring Equipment, ensuring it connects to the correct Mobile Network(s). (EMFSREQ-1398)

2.3.2.3 The Supplier shall be able to identify and stop any high spending SIMs identified during service operation. (EMFSREQ-1696)

2.3.2.4 In certain cases when specified by the Authority, including Special Case Monitoring, the Supplier shall use more than one Mobile Network provider to ensure availability of Monitoring. (EMFSREQ-1597)

2.3.3 **Mobile Network Request Fulfilment**

2.3.3.1 The Supplier shall connect Monitoring Equipment to the Mobile Network provided as part of its supply chain. (EMFSREQ-441)

2.3.3.2 The Supplier shall provision the relevant Mobile Network equipment, for example SIM cards, from its supply chain. (EMFSREQ-440)

2.3.4 **Mobile Network Outage Notifications**

2.3.4.1 The Supplier shall notify the Authority and the FMS Supplier of any Mobile Network outages within thirty (30) minutes of them becoming aware of it. This shall include either planned or unplanned Network outages. (EMFSREQ-437)

2.3.5 **Mobile Network Incident Resolution**

2.3.5.1 The Supplier shall manage its supply chain to resolve any Incidents relating to the Mobile Network and restore service to normal operation in accordance with the performance levels set out in Schedule 3 (*Performance Levels).* (EMFSREQ-436)

2.3.6 **Mobile Network Service Desk Provision**

2.3.6.1 The Supplier shall ensure their proposed Mobile Network provider provides the Supplier and the FMS Supplier access to a Service Desk which operates twenty-four (24)

hours per day, seven (7) days per week, three hundred and sixty-five (365) days per year (for the avoidance of doubt, three hundred and sixty-six (366) days per year in leap years) to resolve any Incidents relating to the use of Mobile Networks by Monitoring Equipment. (EMFSREQ-1377)

2.3.7 Mobile Network Capacity Management

2.3.7.1 The Supplier shall ensure that the capacity of the Mobile Network is sufficient to meet forecast demand from the Authority, in line with the Authority provided Caseload Forecast. (EMFSREQ-435)

2.3.7.2 The Supplier shall monitor the capacity of the Mobile Network to ensure availability of the Electronic Monitoring service. (EMFSREQ-434)

2.3.7.3 The Supplier shall ensure that the capacity of the Mobile Network is scalable up or down. (EMFSREQ-1552)

2.4 Application Development and Operation

2.4.1 Application Service Management and Reporting

2.4.1.1 The Supplier shall provide day to day management of Application support services. (EMFSREQ-333)

2.4.1.2 The Supplier shall report Application performance metrics in accordance with Schedule 24 (*Reports and Records Provision*). (EMFSREQ-334)

2.4.1.3 The Supplier shall provide a technical Service Desk to allow Other Suppliers and the Authority to contact the Supplier to raise and manage the progress of any technical issues relating to the Services. (EMFSREQ-1689)

2.4.1.4 In the Event of an Incident – P1, the Supplier shall produce a Major Incident Report (MIR) within five (5) Working Days of the relevant Incident being closed. (EMFSREQ-1856)

2.4.1.5 All user actions on the Applications and Infrastructure provided by the Supplier, shall be logged and retained by the Supplier to provide records of the user undertaking the activity, when they did it and if/what changes were made for audit purposes. Any logs shall be made available by the Supplier to the Authority on request and in a timely manner. The Supplier shall retain this information in

accordance with the Authority data retention policy. (EMFSREQ-1823)

2.4.2 **Application Development**

2.4.2.1 The Supplier shall ensure that the Supplier Solution utilises Commercial Off the Shelf Software (COTS) or existing products that would require limited or no additional development effort. (EMFSREQ-1878)

2.4.2.2 The Applications provided by the Supplier should be capable of meeting the Authority's requirements through configuration or existing software products alone. Any development required should be minimal, by exception only and agreed with the Authority in writing in advance. (EMFSREQ-1879)

2.4.2.3 The Supplier shall have Application development capability in place to:

(a) continually improve the Services; and

(b) address any defects in the tooling supporting the Service in accordance with Incident Recovery timeframes set out in Schedule 3 (*Performance Levels).* (EMFSREQ-1296)

2.4.2.4 All potential deployments will be presented to the Authority by the Supplier with a Release Note. Release Notes must include (as a minimum):

(a) a brief summary of the proposed release;

(b) proposed duration of the deployment;

(c) cross references to any defects fixed by the release;

(d) any updated design artefacts relating to the release

(e) any testing test artefacts relating to the release;

(f) a rollback strategy; and

(g) a communication plan to cover all scenarios e.g. successful deployment, or failed deployment and subsequent rollback (EMFSREQ-1131)

2.4.2.5 The Supplier shall maintain the configuration of all Applications used in the provision of the Services. (EMFSREQ-1181)

2.4.2.6 The Supplier shall create, maintain and manage a configuration repository for all Applications, systems and

services used in the provision of the Services. (EMFSREQ-1127)

2.4.2.7 The Supplier shall be responsible for producing detailed design documentation to describe the Services, providing this to the Authority and agreeing with the Authority. This shall include:

(a) Requirements;

(b) Scope;

(c) Overview of Service;

(d) Business Architecture;

(e) Data Architecture;

(f) Application Architecture;

(g) Technology Architecture;

(h) Security Architecture; and

(i) Service Architecture.

(EMFSREQ-711)

2.4.2.8 The Supplier shall illustrate within its design documentation:

(a) what provision has been made for error management and handling;

(b) how their design copes with errors.

(c) the expected capacity limits the design is able to support; and

(d) what provision has been made for fault tolerance and describe how their solution has been configured to manage, monitor and handle fault tolerance. (EMFSREQ-1156)

2.4.2.9 The Supplier shall ensure its development lifecycle for Applications includes rigorous testing and assurance processes agreed with the Authority using a representative test environment prior to deployment in the live environment. The number and purpose of each test environment must be agreed with the Authority. (EMFSREQ-811)

2.4.2.10 The Supplier shall detail within its design documentation the expected capacity limits the Application and technology architecture should provide. (EMFSREQ-1297)

2.4.2.11 The Supplier shall, when designing its systems and related interfaces, ensure that designs comply with the latest version of the Authority's Data Dictionary. (EMFSREQ-1679)

2.4.2.12 The Supplier shall ensure that the response time for interactions with the user interface, excluding report generation, shall not exceed one second, to maintain the ability to freely navigate the system user interface. (EMFSREQ-1114)

2.4.2.13 The Supplier shall ensure that the response time for page loading and page refreshes, excluding report generation, shall not exceed two (2) seconds. (EMFSREQ-1113)

2.4.2.14 The Supplier shall ensure that the system response time from clicking on a report to the report being displayed, shall not exceed five (5) seconds. (EMFSREQ-1112)

2.4.2.15 The Supplier shall ensure their systems, subsystems and services are designed, engineered and implemented with a capability to facilitate changes, future expansion and additional users. This shall be evidenced through the provision of integration with the other systems, namely:

(a) other Authority Systems;

(b) external systems; and

(c) new user interfaces.

The Authority will supply any required API documentation in accordance with paragraph 3.12 of Schedule 7 (*Authority Responsibilities*) (EMFSREQ-1091)

2.4.3 **Database Administration**

2.4.3.1 The Supplier shall ensure that its data retention processes align with the Authority's data retention policies (as provided to the Supplier from time to time). (EMFSREQ-1237)

2.4.3.2 The data model in the Supplier Solution will be discussed and agreed with the Authority and the FMS Supplier to reflect the Data Dictionary and any subsequent changes communicated to the Authority and the FMS Supplier in

advance. Any change to the data model that impacts the Data Dictionary data structure is subject to the Authority's and the FMS Supplier's prior written approval. (EMFSREQ-1234)

2.4.3.3 The Supplier must create and provide access to the Authority to its Applications including, data schemas, target objects and technical architecture in a process and timescale agreed with the Authority. (EMFSREQ-1224)

2.4.3.4 The Supplier shall have a Service Management System with the capability to allow for two-way data transfer to and from Authority Systems, the FMS Supplier's systems and other systems as required. (EMFSREQ-1232)

2.4.3.5 The Supplier shall host source data and provide this to the Authority and the FMS Supplier, to allow the Authority to monitor and track data ingestion rates, data ingestion errors, data files provided (by type and date) and Device Monitoring Platform availability. (EMFSREQ-1134)

2.4.3.6 The Supplier shall make all data stored in its systems available to the Authority at times to be agreed with the Authority through a mass data download. (EMFSREQ-1223)

2.4.3.7 Where requested by the Authority, the Supplier shall provide the Authority with direct, real-time access to specified live data captured by the Supplier in a format agreed by the Authority, via Authority Systems. (EMFSREQ-1221)

2.4.3.8 The Authority shall have access to live or very near real time, specified data, captured by the Supplier through an API interface of the Supplier's preferred method to avoid compromising live production performance via Authority Systems. (EMFSREQ-1828)

2.4.3.9 The Supplier shall provide direct access to Monitoring Systems to approved Authority staff (as indicated in the Individual Protocol) from the Notifying Organisation for each Special Case to enable live, direct Continuous Monitoring of Special Cases. (EMFSREQ-1684)

2.4.3.10 The Supplier shall not store any data outside the United Kingdom unless granted express written permission by the Authority. (EMFSREQ-1239)

2.4.3.11 The Supplier shall ensure the Supplier Systems enable the Supplier to meet the availability Performance Indicators

set out in Schedule 3 (*Performance Levels*) (EMFSREQ-342)

2.4.4 **Application Event Monitoring and Management**

2.4.4.1 The Supplier shall provide Application monitoring tools. (EMFSREQ-328)

2.4.4.2 The Supplier shall provide Application performance monitoring tools to monitor the availability and performance of all Applications provided as part of the Service. (EMFSREQ-1465)

2.4.4.3 The Supplier shall deploy Application Event Monitoring and Management tools to monitor Applications to ensure their availability and performance. Functionality provided by these tools shall include, at minimum:

(a) gathering of Application events; and

(b) filtering and correlating Application events. (EMFSREQ-1466)

2.4.4.4 The Supplier shall deploy Application Event Monitoring and Management tools to monitor Applications from an actor and/or user perspective, including where the actor may be another Application which interacts with the Services, to ensure the Applications provided by the Supplier remain available and performant from that actor/user perspective. (EMFSREQ-1467)

2.4.4.5 The Supplier shall configure Application monitoring tools in such a way that their output can assist with triaging and resolving Incidents. (EMFSREQ-331)

2.4.4.6 The Supplier shall monitor Applications for activity which may lead to an Incident. (EMFSREQ-329)

2.4.4.7 The Supplier shall take proactive action to ensure Service availability if Application monitoring suggests that an Incident may be impending. (EMFSREQ-330)

2.4.4.8 In the event the Supplier detects an Incident relating to the Applications provided as part of the Services, the Supplier shall raise the Incident to the Authority's Service Desk. This shall include Incidents detected with:

(a) the Device Monitoring Platform; and

(b) Monitoring Equipment Management Tools (EMFSREQ-1688)

2.4.5 **Event Monitoring Toolset Provision**

2.4.5.1 The Supplier shall provide Infrastructure, Application and Network monitoring tools. (EMFSREQ-349)

2.4.5.2 The Supplier shall provide Application monitoring tools, which shall include Application performance monitoring and/or user journey monitoring. (EMFSREQ-350)

2.4.5.3 The Supplier shall monitor their Technical Services, including, but not limited to:

(a) Applications;

(b) servers and the hosting environment; and

(c) Networks, including the monitoring of Network traffic (EMFSREQ-348)

2.4.6 **2nd Line Incident Resolution**

2.4.6.1 The Supplier shall restore Service operation in the event of an Application Incident in accordance with Incident recovery timeframes set out in Schedule 3 (*Performance Levels*). (EMFSREQ-320)

2.4.6.2 The Supplier shall ensure the Applications they provide meet the availability targets in accordance with Schedule 3 (*Performance Levels*). For the avoidance of doubt, availability targets must be met inclusive of any routine Application maintenance activity which needs to be undertaken. (EMFSREQ-1298)

2.4.6.3 All Suppliers shall use an ITSM toolset to log the progress of Incidents. The ITSM toolset will either be:

(a) the Authority's ITSM tool; or

(b) the Suppliers ITSM tool integrated to the Authority's ITSM tool. (EMFSREQ-322)

2.4.7 **3rd Line Application Support**

2.4.7.1 The Supplier shall generate fixes to Problems. (EMFSREQ-325)

2.4.7.2 The Supplier shall produce Root Cause Analysis reports in accordance with Schedule 24 (*Reports and Records Provision*) (EMFSREQ-326)

2.4.7.3 The Supplier shall produce workaround and Known Issue documentation for Problems. (EMFSREQ-324)

2.4.8 **Application Request Fulfilment**

2.4.8.1 The Supplier shall be able to fulfil Application Service Requests, for example the addition or removal of an Application access from a published, central service catalogue. (EMFSREQ-332)

2.4.8.2 The Supplier shall maintain a list of Application Service Requests in a service catalogue. (EMFSREQ-367)

2.4.9 **Availability Management**

2.4.9.1 The Supplier shall monitor availability of Application Services and Technical Services (EMFSREQ-338)

2.4.9.2 The Supplier shall ensure that its system, subsystems and services are capable of scaling to meet future demand, without re-designing the Supplier Solution. (EMFSREQ-1124)

2.4.9.3 The Supplier shall produce an Availability Plan which documents how its systems will achieve desired availability targets. (EMFSREQ-1587)

2.4.10 **Capacity Management**

2.4.10.1 On at least an annual basis, the Supplier shall size Technical Services to meet expected demand. Future expected demand will be defined by the Authority no less than annually. (EMFSREQ-339)

2.4.10.2 The Supplier shall monitor future demand projections and proactively ensure Technical Services will be scalable (both up and down). (EMFSREQ-341)

2.4.10.3 All Applications provided by Supplier must be able to scale up or down automatically based on real time demand for the Service. (EMFSREQ-1182)

2.4.10.4 The Supplier shall provide capacity metrics to the Authority on a monthly basis in accordance with Schedule 24 (*Reports and Records Provision*). (EMFSREQ-340)

2.4.11 **Release Management**

2.4.11.1 The Supplier shall package and prepare releases. (EMFSREQ-1300)

2.4.11.2 All proposed releases must be agreed with the Authority and treated as a Change. (EMFSREQ-1301)

2.4.11.3 For each release, the Supplier shall produce Test Plans and Test Scripts. Where possible the Supplier shall incorporate automated testing into the Continuous Improvement/Continuous Deployment pipeline. (EMFSREQ-812)

2.4.11.4 For each release, all Test Plans produced by the Supplier shall be reviewed and approved by the Authority prior to the release. (EMFSREQ-1187)

2.4.11.5 The Supplier shall carry out regression testing and test the preparation, configuration, distribution, download and installation of software to ensure that deployment is only carried out if it has been proven to meet Test Success Criteria agreed with the Authority. (EMFSREQ-809)

2.4.11.6 The Supplier shall provide the Authority with evidence to demonstrate that sufficient testing has been carried out prior to making any change to Applications. (EMFSREQ-813)

2.4.11.7 The Supplier shall prepare and share release guidelines to all relevant stakeholders when changes are deployed to Applications and/or IT systems. (EMFSREQ-347)

2.4.11.8 The Supplier shall prepare and share release guidelines in a timely manner to all relevant stakeholders when changes are deployed to Applications and/or IT systems. (EMFSREQ-815)

2.4.12 **Deployment Management**

2.4.12.1 The Supplier shall undertake deployment of new and/or changed services to live environments when required by the needs of the Service. (EMFSREQ-345).

2.4.12.2 The Supplier shall undertake deployment in a controlled manner, releasing updated software to non-production environments prior to release to the live environment. (EMFSREQ-1302)

2.4.12.3 The Supplier shall provide, securely distribute and install updated software including operating systems, Applications, firmware, all other software on Field Officer Devices, Monitoring Centre hardware and servers used to provide the Services. (EMFSREQ-807)

2.4.12.4 The Supplier shall ensure the deployment management procedure includes contingency measures for deployments that are deemed unsuccessful. (EMFSREQ-810)

2.4.12.5 The Supplier shall provide information to the Authority regarding the installation / deployment of software in accordance with Schedule 24 (*Reports and Records Provision*) (EMFSREQ-808)

2.4.12.6 The Supplier shall prepare, package, configure and distribute software to the designated software deployment location (e.g. virtual server or end user device). (EMFSREQ-805)

2.4.12.7 The Supplier shall define and follow a well-documented process that has been agreed with the Authority in writing during Implementation for the purpose of authorising / deploying / configuring software components. (EMFSREQ-806)

2.4.12.8 The Supplier shall update code within source code repositories whenever a release takes place. (EMFSREQ-814)

2.4.12.9 Where the Supplier updates Applications, it will provide updates on the Service configuration to the Authority, allowing the Authority to update its configuration information. (EMFSREQ-1188)

2.4.13 **Provide Application Training**

2.4.13.1 The Supplier shall develop electronically accessible training materials for all Application users and shall provide it to Application users. (EMFSREQ-356)

2.4.13.2 The Supplier shall work with the Other Suppliers and the Authority to train Application users to carry out their role. (EMFSREQ-357)

2.4.13.3 The Supplier shall ensure that training materials always reflect the live service and IT systems within it. If a material change is deployed, the Supplier shall update materials and provide training for all affected Application users before releasing the change into operational service. (EMFSREQ-358)

2.4.14 **Information Security Management**

2.4.14.1 The Supplier shall maintain the information security environment across the Services they provide to ensure the integrity and security of information assets. (EMFSREQ-369)

2.4.14.2 All Application development shall be undertaken in accordance with the Information Security Management

System requirements set out in Schedule 5 (*Security Management*). (EMFSREQ-370)

2.4.14.3 The Supplier shall provide Infrastructure, Application and Networking security monitoring integration with Authority's protective security monitoring supplier, such integration must include but is not limited to;
(a) API;
(b) log shipping; and
(c) Authority protective monitoring supplier supplied monitoring agents. (EMFSREQ-1698)

2.5 Application Requirements

2.5.1 Device Monitoring Platform

2.5.1.1 The Supplier shall provide a Device Monitoring Platform which meets the requirements of this paragraph 2.5.1. (EMFSREQ-1542)

2.5.1.2 The Device Monitoring Platform shall have 99.95% availability. (EMSREQ-1120)

2.5.1.3 The Device Monitoring Platform shall have a user interface to allow users to access any and all data held within the Device Monitoring Platform. The set of users who require access to the user interface includes but is not limited to:

(a) FMS Supplier staff;

(b) the Authority's Electronic Monitoring staff, including the Contract Management Team;

(c) Probation Officers; and

(d) Police Officers. (EMFSREQ-1505)

2.5.1.4 The Device Monitoring Platform shall provide functionality to allow configuration of the rules necessary to filter and correlate Events to generate Alerts. (EMFSREQ-1528)

2.5.1.5 The Device Monitoring Platform shall provide Event correlation and filtering functionality to automatically remove Monitoring Equipment Events that have no compliance and/or technical importance. What constitutes "technical importance" shall be defined by the Supplier and agreed with the FMS Supplier provided that the Authority reserves the right to set technical importance. (EMFSREQ-1462)

2.5.1.6 The Device Monitoring Platform shall have an interface to the Acquisitive Crime Application, in accordance with

Table 3 of this Schedule, which shall adhere to the defined interface specification for the Acquisitive Crime Application. (EMFSREQ-1511)

2.5.1.7 The Device Monitoring Platform shall have functionality to allow Authority-approved users to self-serve reports. The set of reports the platform will support shall include but not be limited to:

(a) the set of Events and Alerts relating to an individual Device-Wearer on all types of Order;

(b) the set of Events and Alerts relating to an individual Device-Wearer who has potentially breached their Order; and

(c) a summary, by Order type, of the status of a range of Device-Wearers on that Order type. (EMFSREQ-1510)

2.5.1.8 The Device Monitoring Platform shall provide functionality so that users are able to view interactions with Inclusion Zones and/or Exclusion Zones, and movements for Fitted and Non-Fitted Location Monitoring Devices on a map (Trail Monitoring). (EMFSREQ-1508)

2.5.1.9 The Device Monitoring Platform shall provide role-based access controls to limit users or a group of users access to only the information held in the system which they require to undertake their roles. (EMFSREQ-1506)

2.5.1.10 The Device Monitoring Platform shall have defined interfaces to allow the Authority to extract any and all data from the Device Monitoring Platform. The set of data the Authority will extract includes all Event data (e.g. Location Monitoring Events) generated by Monitoring Equipment. (EMFSREQ-1504)

2.5.1.11 The Device Monitoring Platform shall collect and manage all data sent from Monitoring Equipment. Data collected and managed shall include but not be limited to:

(a) collect data from all Monitoring Equipment;

(b) correlate and filter Events generated from Electronic Monitoring Equipment; and

(c) business rules to identify potential compliance Alerts. (EMFSREQ-1503)

2.5.1.12 The Device Monitoring Platform shall have a defined, documented interface, in accordance with Table 3 of this Schedule, to allow new and/or emerging types of

Monitoring Equipment to transfer Event data into the Device Monitoring Platform. (EMFSREQ-1529)

2.5.1.13 The Device Monitoring Platform shall provide a Device Alert Interface in accordance with Table 3, of this Schedule. (EMFSREQ-1459)

2.5.1.14 The Supplier shall ensure that the Device Alert Interface shall transfer Event and Alert data, in accordance with Table 3 of this Schedule, from the Device Monitoring Platform to the FMS Supplier's Service Management System. (EMFSREQ-1460)

2.5.1.15 The Supplier shall ensure that the Device Alert Interface generates a set of Alerts in accordance with Table 2 of this Schedule. (EMFSREQ-1464)

Table 2 - Device Alerts Summary

Ref	Alert	Description
	Tampers	
AL02	Tamper of worn device	Interference of normal operation of the Device
AL04	Removal (Tamper) of worn device	Removal of a Fitted Device from the Device-Wearer
AL05	Power off of Curfew equipment at home	Loss of power to an HMU
AL06	Movement of Curfew equipment at home (monitor move)	Any movement to an HMU
	Location Monitoring	
AL07	Exclusion Zone Violation	See 'Exclusion Zone Violation Event' definition
AL08	Inclusion Zone Violation	See 'Inclusion Zone Violation Event' definition
	Curfew violations	
AL09	Out Past Curfew Commencement	Device-Wearer is not within Curfew Boundary at the time of Curfew commencement
AL010	Return home late	Device-Wearer enters the Curfew Boundary after the Curfew commencement
AL11	Left home during Curfew	Device-Wearer leaves the Curfew Boundary during a Curfew period

AL12	Out at end of Curfew	The Device-Wearer is not within the Curfew Boundary at the end of the Curfew period
Alcohol		
AL15	Alcohol Non-compliance	Device-Wearer becomes non-compliant with their Alcohol Monitoring conditions
	Biometrics	
AL16	Failed to verify Biometric test	A biometric sample successfully submitted by a Device-Wearer cannot be verified
	General	
AL17	Missing Status Check (e.g battery dead)	Loss of communication to the Device
AL21	Fault with Device (non-tamper)	Device registers a fault not caused by a Tamper
AL18	No movement of Device-Wearer (Curfew no movement for 3 days, Location Monitoring no movement over a twenty-four (24) hour period)	Device has not registered movement of the Device-Wearer (within confidence levels)
	Battery Alerts	
AL19	Non-charged Device low battery. Battery running low	See EMFSREQ-1609
AL20	Charged Device battery running low	See EMFSREQ-527

2.5.2 Monitoring Equipment Management Tools

2.5.2.1 The Supplier shall provide Monitoring Equipment Management Tools which meet the requirements of this paragraph 2.5.2. (EMFSREQ-1541)

2.5.2.2 The Monitoring Equipment Management Tools shall provide functionality to allow configuration and management of any tools required to undertake fitting and configuration of Monitoring Equipment. (EMFSREQ-1539)

2.5.2.3 The Monitoring Equipment Management Tools shall provide functionality to allow the FMS Supplier to configure, manage and modify all Devices to meet Monitoring Requirements. (EMFSREQ-1538)

2.5.2.4 The Supplier’s toolset shall allow the FMS Supplier to send ad-hoc breath sample checks to wearers of Remote Breathalyser Alcohol Monitoring Devices. (EMFSREQ-1589)

2.5.2.5 The Monitoring Equipment Management Tools shall provide functionality to update the firmware, operating systems and any local software of all Monitoring Equipment. This functionality shall include but not be limited to:

(a) patching of any identified vulnerabilities with the Monitoring Equipment; and/or

(b) updating Monitoring Equipment with firmware, operating systems or local Application version upgrades. (EMFSREQ-1532)

2.5.2.6 The Monitoring Equipment Management Tools should provide remote Incident diagnosis and resolution functionality to allow the Monitoring Centre provided by the FMS Supplier to remotely resolve Monitoring Equipment Incidents without the need for a site visit by a Field Officer to resolve the Incident. (EMFSREQ-1531)

2.5.2.7 The Supplier shall provide Monitoring Equipment Management Tools that have a user Interface(s) which will allow the FMS Supplier to understand, set up and amend the configuration and status of Monitoring Equipment. (EMFSREQ-1530)

2.5.2.8 The Supplier shall provide Monitoring Equipment Management Tools with functionality to configure, manage and modify Inclusion Zones and Exclusion Zones for Location Monitoring Devices. (EMFSREQ-1507)

2.5.2.9 The Supplier's Monitoring Equipment Management Tools should allow the FMS Supplier to send ad-hoc biometric verification checks to wearers of Non-Fitted Location Monitoring Devices. (EMFSREQ-1583)

2.5.2.10 The Monitoring Equipment Management Tools shall provide functionality to allow configuration and management of any tools required to undertake fitting, configuration and de-Installation of Monitoring Equipment. (EMFSREQ-1540)

2.5.3 **Infrastructure Monitoring and Management Tools**

2.5.3.1 The Supplier shall ensure appropriate Infrastructure Monitoring tools are in place to monitor the availability and performance of all Infrastructure required to deliver the Service in accordance with Schedule 3 (*Performance Levels*). (EMFSREQ-1527)

2.5.3.2 The Supplier shall deploy Infrastructure management tools to continually manage and update the Infrastructure used

by the Service. This shall include provision of management tools to determine the configuration of Infrastructure and to update the Infrastructure, including patching. (EMFSREQ-1447)

2.5.3.3 Without prejudice to the Supplier's obligations under Schedule 26 (*Service Continuity Plan and Corporate Resolution Planning*), the Supplier shall have appropriate tooling in place in order to maintain the Services in the event of a Disaster. This shall include but not be limited to backup and restore tools, to make immutable backups of systems and data. (EMFSREQ-1448)

2.5.3.4 The Supplier shall ensure that all Supplier Systems and data backups are immutable. (EMFSREQ-1545)

2.6 Server and Network Supply and Support

2.6.1 Cloud service use

2.6.1.1 Where the Supplier provides a pure SaaS solution, the Supplier shall provide to the Authority accounts on, and use of, a pre-existing system on the public internet.

Where the Supplier does not provide a pure SaaS solution, the Supplier shall host the relevant Software in the Authority's designated cloud hosting environment, in accordance with the Authority's Technical Guidance paper, "How to Host Services" provided to the Supplier, and follow any other standards and requirements applicable to the use of the relevant environments. (EMFSREQ-1854)

2.6.1.2 In the event the Supplier is providing a pure SaaS solution, the Supplier shall be responsible for the provision of appropriate Infrastructure to enable it to meet with the Performance Indicators in Schedule 3 (*Performance Levels*). (EMFSREQ-393) Where the Supplier is providing Authority dedicated Applications, the Supplier shall use public cloud services provided and/or approved by the Authority. (EMFSREQ-394)

2.6.1.3 In the event the Supplier uses the Authority's cloud platform for hosting, the Supplier shall ensure Authority-approved users have read-only access to Application and Infrastructure Monitoring tools for all services hosted on the Authority's cloud platform. (EMFSREQ-1386)

2.6.2 **Environment management**

2.6.2.1 The Supplier shall support and manage all environments required to provide the Service. This should include:

(a) Development;

(b) Test;

(c) Pre-Production; and

(d) Production. (EMFSREQ-399)

2.6.2.2 The Supplier shall ensure consistent configuration of all environments required to provide the Service, including the configuration, licensing and patching of any Infrastructure software. (EMFSREQ-400)

2.6.3 **Infrastructure capacity management**

2.6.3.1 The Supplier shall ensure that Infrastructure is appropriately sized. (EMFSREQ-378)

2.6.3.2 The Supplier shall analyse the existing caseload capacity, usage and forecasted growth (as provided by the Authority) and ensure the underlying Infrastructure systems and services can meet these demands. (EMFSREQ-1155)

2.6.3.3 The Supplier shall run non-production environments at a minimum capacity when not in use to provide better value for money. For the avoidance of doubt, the Authority requires that the Supplier to shut down any cloud environments which are not actively in use. (EMFSREQ-379)

2.6.3.4 The Supplier shall report on capacity in accordance with Schedule 24 (*Reports and Records Provision*). (EMFSREQ-1691)

2.6.4 **Infrastructure configuration management**

2.6.4.1 The Supplier shall manage the configuration of all Infrastructure and Networks they are required to provide under the Contract. (EMFSREQ-402)

2.6.4.2 The Supplier shall provide up to date, comprehensive and detailed documentation outlining the Infrastructure used in provision of the Service on at least an annual basis. (EMFSREQ-403)

2.6.4.3 On a monthly basis, the Supplier shall provide configuration information to the Authority so there is a single source of information for the configuration of all Technical Services. (EMFSREQ-404)

2.6.4.4 The Supplier shall record, control and manage the supply of Service Assets and Configuration Items in the EM IT Infrastructure they provide. (EMFSREQ-362)

2.6.4.5 The Supplier shall provide Asset and Configuration data to the Authority and/or the FMS Supplier to allow update of any central CMBDs which exist for the EM Service. (EMFSREQ-1588)

2.6.4.6 The Supplier shall audit and resolve issues within the IT environment regularly to identify any inconsistencies with the CMDB. (EMFSREQ-363)

2.6.5 Infrastructure deployment

2.6.5.1 The Supplier shall deploy new or changed Infrastructure, Network components, Infrastructure software, documentation, processes or any other components to environments as required to maintain operation of the Service. (EMFSREQ-396)

2.6.5.2 The Supplier shall deploy new or changed Infrastructure, Network components, Infrastructure software, documentation, processes or any other components to live environments, following deployment processes agreed with the Authority. (EMFSREQ-395)

2.6.6 Infrastructure event monitoring and management

2.6.6.1 The Supplier shall provide and/or ensure there are Infrastructure and Event Monitoring tools in place. (EMFSREQ-1408)

2.6.6.2 The Supplier shall set and review monthly Event monitoring thresholds for Infrastructure to detect Events and potential Incidents within the EM Infrastructure and environments they are contracted to provide. (EMFSREQ-1543)

2.6.6.3 In the event the Supplier detects an Incident relating to the Infrastructure relating to the Applications provided as part of the Services, the Supplier shall raise the Incident to the Authority’s Service Desk. This shall include Infrastructure Incidents related to:

(a) the Device Monitoring Platform;

(b) Monitoring Equipment Management Tools; and

(c) Notification tools. (EMFSREQ-1687)

2.6.6.4 The Supplier shall set and regularly review event monitoring thresholds for Infrastructure to detect events and potential Problems within the EM Infrastructure and environments. (EMFSREQ-380)

2.6.7 **Infrastructure Incident resolution**

2.6.7.1 The Supplier shall restore Service operation, in accordance with timeframes set out in Schedule 3 (*Performance Levels*), in the event of an Infrastructure Incident. (EMFSREQ-381)

2.6.7.2 The Supplier shall resolve Infrastructure Incidents in accordance with Incident recovery timeframes set out in Schedule 3 (*Performance Levels*). (EMFSREQ-382)

2.6.7.3 The Supplier shall forward information related to Infrastructure Incidents to the Authority, who will be responsible for communicating to relevant Stakeholders. (EMFSREQ-383)

2.6.7.4 Incident resolution shall be achieved when the affected component(s) returns to normal operation (either due to a functionally and operationally acceptable workaround measure being put in place or because a permanent fix is provided). (EMFSREQ-384)

2.6.8 **Infrastructure root cause analysis**

2.6.8.1 The Supplier shall investigate and remediate the root cause of Incidents. (EMFSREQ-387)

2.6.8.2 The Supplier shall develop fixes for any identified defects. (EMFSREQ-389)

2.6.8.3 The Supplier shall document Known Issues and Workarounds. This information shall be provided to the Authority. (EMFSREQ-388)

2.6.9 **Infrastructure service management and reporting**

2.6.9.1 The Supplier shall provide day to day management of Infrastructure services. (EMFSREQ-376)

2.6.9.2 The Supplier shall report on Infrastructure metrics in accordance with Schedule 24 (*Reports and Records Provision*). (EMFSREQ-377)

2.6.10 **Physical data centre provision**

2.6.10.1 By exception and subject to approval by the Authority, if the Supplier needs to provide physical data centres to fulfil its obligations under this Contract, the Supplier shall provide appropriate physical data centre environments, servers and Network components. (EMFSREQ-397)

2.6.11 **Preventative maintenance**

2.6.11.1 The Supplier shall undertake monthly preventative maintenance on all Infrastructure and Networks, including, but not limited to:

(a) updating and Patching of all operating systems;

(b) updating and Patching any Network Firmware; and

(c) managing the renewal of any digital certificates. (EMFSREQ-386)

2.6.12 **Reactive Maintenance**

2.6.12.1 The Supplier shall apply critical security patches or upgrades on all Infrastructure and Networks. These shall include:

(a) updating and Patching of all operating systems; and

(b) updating and Patching any Network Firmware,

within seventy-two (72) hours of vendor publication. (EMFSREQ-1295)

2.6.13 **Raise Infrastructure change**

2.6.13.1 The Supplier shall progress any Changes to the operational environments in accordance with the Schedule 22 (*Change Control Procedure*). (EMFSREQ-391)

2.6.13.2 The Supplier shall ensure that any Infrastructure changes do not impact the expected operation of the Infrastructure or other related services. (EMFSREQ-392)

2.6.14 **Server software support**

2.6.14.1 The Supplier shall provide support or procure the provision of support for all Software set out in Schedule 12

(*Software*) and in design documentation), including, but not limited to, operating systems and databases. (EMFSREQ-390)

2.6.15 **Network Provision**

2.6.15.1 The Supplier shall provide any Network components within the Infrastructure environments they are providing to ensure secure access to the Services. (EMFSREQ-1246)

3 Implementation Services

3.1 Implementation Methods and Approach

3.1.1 Without prejudice to any other obligations of the Supplier (including those set out in Schedules 13 (*Implementation Plan*) and 14 (*Test Procedures*), during the Implementation Period, the Supplier shall perform the activities set out in this paragraph 3. (EMFSREQ-1882)

3.1.2 The Supplier shall follow an industry standard, robust and fully documented methodology to configure and maintain the Supplier Solution. (EMFSREQ-1645)

3.1.3 The Supplier shall provide, during the Implementation Period and by the dates set out in the Implementation Plan, Detailed Design Document(s) which shall demonstrate how the Supplier Solution will deliver the Operational Services including the non-functional requirements as detailed in this Schedule and Schedule 3 (*Performance Levels*) including how the Supplier will integrate with Event and/or Alert data generated by the Monitoring undertaken by the FMS Supplier. (EMFSREQ-1646)

3.1.4 The Supplier shall follow a recognised, robust and fully documented development and maintenance methodology to design and create the Detailed Design Document(s). (EMFSREQ-1647)

3.1.5 The Supplier shall, without prejudice to the obligations in Schedule 24 (*Reports and Records Provision*), ensure that the most current versions of the Implementation Plans, project documentation and the Detailed Design Document(s) shall be accessible to the Authority on a day to day basis (for example through a dedicated Teams channel) without the need for any specialist software to which the Authority does not already have access. (EMFSREQ-1648)

3.1.6 The Supplier shall provide an implementation close-down report, including lessons learned, when the delivery of the Implementation Services has been completed. (EMFSREQ-1649)

3.1.7 The Supplier shall provide a project management office to support the management of the Implementation Services. (EMFSREQ-1650)

3.1.8 The Supplier shall meet with FMS Supplier in accordance with paragraph 7 of Schedule 13 (*Implementation Plan*) and shall keep

Implementation Plans updated in accordance with paragraph 6 of Schedule 13 (*Implementation Plan*) (EMFSREQ-1651)

3.1.9 The Supplier shall attend implementation meetings with the FMS Supplier that ensures progress of the Deliverables against the Overarching Project Implementation Plan. (EMFSREQ-1652)

3.1.10 The Supplier shall ensure that it provides all Implementation Services according to the Standards and requirements in Schedule 4 (*Standards*). (EMFSREQ-1655)

3.1.11 The Supplier shall comply with its obligations under Schedule 28 (*Staff Transfer*). Where there is to be a Relevant Transfer, the Supplier will develop a staff transfer plan that will be included its Implementation Plan that will set out the steps to be taken in connection with any staff subject to such Relevant Transfer. (EMFSREQ-1656)

3.1.12 The Supplier shall provide as part of the Implementation Plan a detailed resourcing and staffing capacity plan for Supplier staff responsible for delivering the Services. The plan should detail those staff roles of the staff within the Relevant Transfer and shall specifically include details of those staff identified in Key Personnel and dates of when they will be onboarded. (EMFSREQ-1657)

3.1.13 The Supplier shall provide information to support business communication and engagement activity performed by the Authority as reasonably required by the Authority. (EMFSREQ-1658)

3.1.14 Transformation activity beyond the delivery of the Implementation Services will be undertaken by the Supplier as discrete projects. These will be subject to the Change Control Procedure. The Authority may require additional Implementation Plans and Test artefacts for each discrete project in accordance with Schedule 13 (*Implementation Plan*) and Schedule 14 (*Testing Procedures*) respectively. (EMFSREQ-1664).

3.1.15 The Supplier shall maintain a record of actions and critical decisions arising from the Implementation Review meetings detailed in Schedule 13 (*Implementation Plan*) within two (2) Working Days of each meeting taking place. (EMFSREQ-1653)

3.1.16 The Supplier shall provide project information to the FMS Supplier as requested by the FMS Supplier to enable the FMS Supplier to provide an end-to-end view of the Implementation Services including:

(a) Risk Register;

(b) Implementation Plan;

(c) Test Strategy;

(d) Test Design and Plan;

(e) Security Plan,

together with updated versions of the information (EMFSREQ-1659)

3.1.17 The Supplier shall provide training materials and training to support the activities performed by the Authority staff, including scripts, detailed training plan and training success criteria. (EMFSREQ-1680)

3.2 Data Migration

3.2.1 The Supplier shall produce a Detailed Design Document which details the activities to be undertaken to migrate data to enable delivery of the Supplier Solution. Such activities shall be included with a plan within the Implementation Plan, which must align with the Overarching Project Implementation Plan. (EMFSREQ-1660)

3.2.2 The Supplier shall migrate any data held in the Outgoing Service Provider's systems which may be necessary to enable the Supplier to provide the Services. (EMFSREQ-1818)

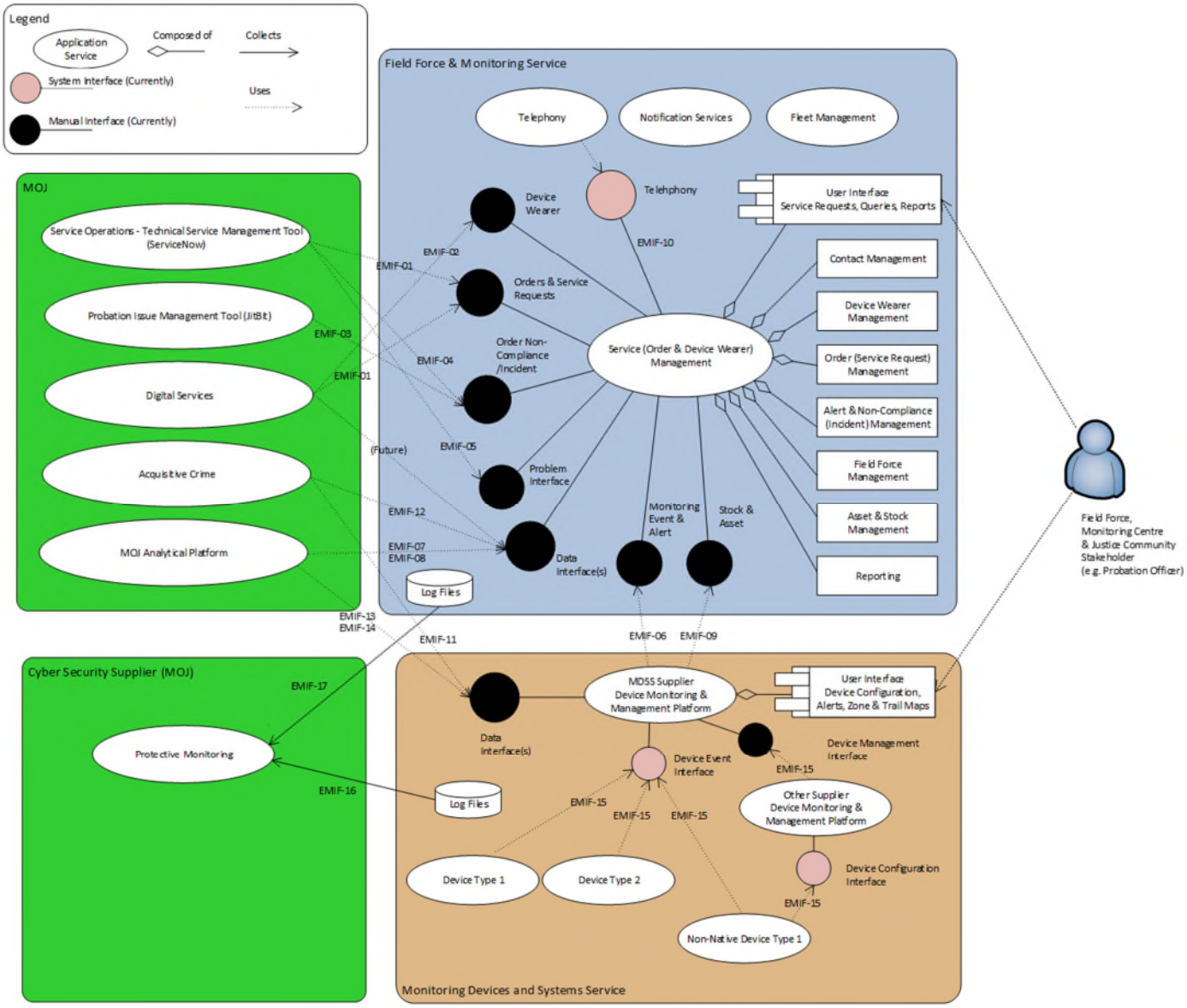
3.2.3 The Supplier shall undertake the data migration activities during the Implementation Period and in accordance with the timescales set out in the Implementation Plan. (EMFSREQ-1661)

3.3 MDSS Implementation Responsibilities

3.3.1 The Supplier shall ensure that they are able to deliver the Operational Services by no later than Milestone 3 in accordance with Schedule 13 (*Implementation Plan*). (EMFSREQ-1665)

3.3.2 For illustrative purposes, a system context diagram is shown below in Figure 1: system context diagram.

Figure 1: System context diagram



3.3.3 The Supplier shall provide or integrate with the relevant interfaces in acceptance with Table 3 below. (EMFSREQ-1860)

3.3.4 **Table 3: EM system interfaces**

Service relationships									
The need			**Reference**	**Service responsibilities**				**Proposed mechanisms**	**Implementation**
Theme	**User need**	**Why**	**EMIF ID**	**Who will present the data**	**Who will consume it**	**How frequently will it need to be accessed**	**What type of information would be included**	**End state expectation**	**Full Automation of this process no later than**
Subject monitoring	The FMS Supplier needs to know about Events and Alerts generated from Devices to do with Monitored individuals	So that they can manage the Device-Wearer (e.g. take enforcement action)	**EMIF-06**	MDSS Supplier	FMS Supplier	On demand	Device telemetry	API	MDSS Service in place - Milestone 3
Subject monitoring	All Device types need to operate through one centralised platform	To reduce complexity when working with multiple Device types including 3rd party devices	**EMIF-15**	3rd party Devices	MDSS Supplier	On demand	Device telemetry	API	MDSS Service in place - Milestone 3

Service relationships									
The need			**Reference**	**Service responsibilities**				**Proposed mechanisms**	**Implementation**
Theme	**User need**	**Why**	**EMIF ID**	**Who will present the data**	**Who will consume it**	**How frequently will it need to be accessed**	**What type of information would be included**	**End state expectation**	**Full Automation of this process no later than**
Service monitoring	MDSS Supplier need to confirm availability of Devices and that they are checking in	So that FMS have a view of the live status of Devices	**EMIF-09**	MDSS Supplier	FMS Supplier	On demand	Keep alive flag / probe	API	New Service Fully Operational - Milestone 5
Service monitoring	MOJ needs to be confident that supplier systems are secure and well managed	So that the MoJ is assured that the threat of a cyber security incident is low and that should an incident occur, the MoJ are informed through their SOC service	**EMIF-16**	MDSS Supplier	Authority Security Operations	On demand	Operational event logs	API	MDSS Service in place - Milestone 3

Service relationships									
The need			**Reference**	**Service responsibilities**				**Proposed mechanisms**	**Implementation**
Theme	**User need**	**Why**	**EMIF ID**	**Who will present the data**	**Who will consume it**	**How frequently will it need to be accessed**	**What type of information would be included**	**End state expectation**	**Full Automation of this process no later than**
Data and analytics	The Authority needs access to all Device telemetry data for analytical purposes	So that they can use this data to build insight into the detail of the service and how those who are monitored, behave, to allow the Authority to supervise effectively and improve the service	**EMIF-13**	MDSS Supplier	Authority Analytics	Weekly	Raw telemetry data from monitoring devices	API	New Service Fully Operational - Milestone 5

Service relationships									
The need			**Reference**	**Service responsibilities**				**Proposed mechanisms**	**Implementation**
Theme	**User need**	**Why**	**EMIF ID**	**Who will present the data**	**Who will consume it**	**How frequently will it need to be accessed**	**What type of information would be included**	**End state expectation**	**Full Automation of this process no later than**
Data and analytics	The Authority needs access to all Device telemetry data for analytical purposes	So that they can use this data to build insight into the detail of the service and how those who are monitored, behave, to allow the Authority to supervise effectively and improve the service	**EMIF-14**	MDSS Supplier	Authority Analytics	Weekly	Raw telemetry data from monitoring devices	API	New Service Fully Operational - Milestone 5

Service relationships									
The need			**Reference**	**Service responsibilities**				**Proposed mechanisms**	**Implementation**
Theme	**User need**	**Why**	**EMIF ID**	**Who will present the data**	**Who will consume it**	**How frequently will it need to be accessed**	**What type of information would be included**	**End state expectation**	**Full Automation of this process no later than**
Data and analytics	MOJ needs up to date GPS data on the Acquisitive Crime cohort	So that they can use this data to match against police data of reported AC crimes	**EMIF-11**	MDSS	MoJ AC Tool provider	At least every 3 mins for location data, nightly for all other data	Raw telemetry data from GPS monitoring devices for AC cohort; relevant AC cohort Device-Wearer details	Scheduled JSON file transfer	MDSS Service in place - Milestone 3

3.3.5 The Supplier shall implement and fully automate the interfaces they are responsible for, no later than the relevant Milestones shown in Table 3, in this Schedule. (EMFSREQ-1877)

3.3.6 The implementation dates for the interfaces set out in Table 3, of this Schedule, that are required by Milestone 5, shall be determined by the FMS Supplier. The Supplier shall liaise with the FMS Supplier to agree the relevant dates (such dates to be included in the Overarching Project Implementation Plan). (EMFSREQ-1862)

3.3.7 The Supplier shall ensure the integration with the Authority's Acquisitive Crime Application as detailed in the interface schema and the integration responsibilities in Table 3 of this Schedule (GPS to Acquisitive Crime) is in place and has been tested by Milestone 3. (EMFSREQ-1666)

3.3.8 Remote Breath Alcohol Monitoring and related requirements as outlined in paragraph 2.2.6 and User Access (see paragraph 2.5.1.3) for:

a) Probation Officers;

b) Other (non-Counter Terrorism) Police Officers; and

c) Notifying Organisations;

shall be provided on a date, post Milestone 5, to be agreed by the Parties in accordance with the Change Control Procedure. (EMFSREQ-1859)

3.3.9 The Supplier shall ensure its Monitoring Equipment supply plans, aligns with the requirements detailed in paragraph 2.2.9.1 and aligns to the FMS Supplier's Implementation Plan. (EMFSREQ-1667)

3.4 Integration Responsibilities

3.4.1 The Supplier shall fulfil its integration responsibilities in accordance with the Interface schema and integration responsibilities in Table 3 of this Schedule. For the avoidance of doubt, in Table 3, the column titled:

(a) "Who will present the data" lists the party responsible for providing data to an Interface

(b) “Who will consume it” lists the party responsible for providing Interfaces;

(c) “How frequently will it need to be accessed” outlines how often such input/output is expected;

(d) “What type of information would be included” outlines the expected information to be provided as an input or output; and

(e) “End state expectation” outlines the method in which the Interface is to be fulfilled. (EMFSREQ-1668)

3.4.2 Where the Supplier is responsible for integrating with third party or Authority Systems as outlined in the ‘Who will present the data’ column of Table 3 of this Schedule, the Supplier shall undertake the following integration activities:

(a) The Supplier shall obtain access to the latest version of the Interface Documentation and any associated user documentation from the relevant Interface Provider (as set out in the ‘Who will consume the data’ column of Table 3 of this Schedule).

(b) The Supplier shall put in place any Infrastructure to connect its environment with the Interface Provider’s system(s).

(c) In accordance with the Implementation Plan, the Supplier shall implement the required integration.

(d) In accordance with Schedule 14 (*Testing Procedures*), the Supplier shall test the integration. This shall include testing against the Interface Provider’s test environments and undertaking any performance testing against the Interface Provider’s pre-production, or equivalent, environment.

(e) The Supplier shall undertake release of the integration into Service operation. (EMFSREQ-1669)

3.4.3 Where the Supplier is responsible for providing an Interface as set out in the ‘Who will consume it’ column of Table 3 of this Schedule, the Supplier shall support third parties in integrating with that Interface. Support to third parties shall include but not be limited to:

(a) Provision of access to the latest Interface and provision of latest Interface documentation to the integrating party.

(b) Supply and provision of test Interfaces in any test and sub-live environments.

(c) Guidance and technical support to the integrating party as they connect to the Supplier's Interface. This shall include provision of a defined mechanism to contact the Supplier’s technical staff to

address and resolve queries from the party undertaking the integration.

(d) Guidance and technical support to the integrating party as they transition integration into Service operation. This shall include support of any testing against pre-production environments before release into Service Operation (EMFSREQ-1670)

3.5 Test Environment

3.5.1 The Supplier shall create and maintain the environments required to support the Implementation Plan. These shall include the set of environments outlined in paragraph 2.6.2. (EMFSREQ-1671)

3.5.2 The Supplier shall ensure that the Test Environment is updated to represent the relevant elements of the Live Environment and shall include any test harnesses, simulators and hardware/or software updates required. (EMFSREQ-1672)

3.5.3 The Test Environment shall be available for Testing on and ongoing from the date of the first Test set out in the Test Strategy or Test Plans and thereafter as required. (EMFSREQ-1673)

3.5.4 The Test Environment shall be maintained to generate consistent results from Testing that will allow new outputs to be comparable to baseline results. (EMFSREQ-1674)

3.5.5 The Test Environment shall use Good Industry Practice test automation tools to reduce the cost of Testing and particularly the costs of repeat Testing. (EMFSREQ-1675)

3.5.6 The Supplier shall ensure it performs testing of new Releases using the Test Environment and presents test results for the Authority to review, in accordance with Release Management and Testing Procedures. (EMFSREQ-1676)

3.5.7 As part of the Implementation Services, the Supplier shall as a minimum undertake, or provide proof for assurance, the following types of testing:

(a) Unit, component, sprint, or system testing as appropriate;

(b) Third Party Interface Testing;

(c) Supplier Operational Acceptance Testing including Performance Testing, including testing of the Application Services under expected load and with expected operational data volumes; and

d) Factory Acceptance Testing (EMFSREQ-1881)

3.5.8 As part of its Implementation Plan the Supplier shall, as a minimum, support and participate in the FMS Supplier or Authority led phases of the following testing:

(a) System Integration Testing;

(b) User Acceptance Testing; and

(c) Operational Acceptance Testing including End to End Performance Testing and testing of the Application Services under expected load and with expected operational data volumes. (EMFSREQ-1677)

3.5.9 The Supplier shall include functional and non-functional tests as appropriate against the following but not limited to, components as detailed in this Schedule 2:

(a) Fitted Location Monitoring Devices;

(b) Non-Fitted Devices;

(c) Transdermal Alcohol Monitoring Devices;

(d) Remote Breathalyser Alcohol Monitoring Devices;

(e) Curfew Monitoring Devices;

(f) security logs for protective monitoring;

(g) Field Officer Equipment;

(h) Mobile Network Service;

(i) Infrastructure for the Service;

(j) Physical Infrastructure;

(k) Device Monitoring Platform;

(l) Monitoring Equipment Management Tools;

(m) Device Monitoring Platform - Data Interface JSON file;

(n) Device Monitoring Platform - Data Interface Direct Access;

(o) Device Monitoring Platform - Device Event Interface;

(p) Service Management System integration; and

(q) GPS to Acquisitive Crime Integration. (EMFSREQ-1678)

4 GLOSSARY

In this Schedule, the following definitions shall apply:

Term	Definition
Acquisitive Crime	A monitoring condition for people released from prison convicted of Acquisitive Crime (e.g. burglary). They are subject to Trail Monitoring so Stakeholders can determine their whereabouts to Acquisitive Crimes.
Acquisitive Crime Portal	An authority owned system which captures the location of people on an Acquisitive Crime Electronic Monitoring Order and matches these to the locations of overnight acquisitive crimes that have occurred.
Adult	A Device-Wearer over the age of eighteen (18).
Alcohol Monitoring	Electronic Monitoring of a Device-Wearer to ensure compliance with an alcohol requirement of an Order or Licence.
Alcohol Monitoring Device	A Device which is able to Monitor the Device-Wearer's alcohol intake, either through the means of a breathalyser or through transdermal means.
Alert	A warning that a threshold has been reached, something has changed, or a failure has occurred. Alerts are often created and managed by the Device monitoring tools and/or system management.
APIs	The Application programming interfaces used in connection with the provision of the Services.
Application(s)	A computer program designed to carry out a specific task other than one relating to the operation of the computer itself, typically to be used by end-users.
Application Service	Software and/or a set of interconnected Applications and hosts which are configured by the Supplier to offer a service to the Authority.
Area of Interest	An area which a Responsible Officer should be able to proactively monitor if a Device-Wearer enters or exits but which is not an Inclusion Zone or Exclusion Zone.
Asset Register	A database or list of assets, capturing key attributes such as ownership and financial value.
Authorised Absence	An absence requested or taken by a Device-Wearer that has been authorised by the Responsible Officer or EM Contact Centre and/or the Monitoring Centre, including but not limited to absences relating to: - Job interviews. - Attendance at Court as a witness. - Attendance at weddings or funerals of family members. - Attendance at abstinence meetings.

Term	Definition
Availability Management	The processes of ensuring that Application Services and IT services deliver agreed levels of availability to meet the needs of customers and users.
Availability Plan	A plan to ensure that all existing and future Availability requirements for Applications and IT services can be provided cost effectively.
Availability	For the purposes of this Schedule 2 only, the ability of an Application Service, IT service or other configuration item to perform its agreed function when required.
Buffer Zone Violation Event	A Monitoring Event recorded at the point the Device-Wearer is close to entering an active Exclusion Zone, or leaving an active Inclusion Zone, as defined on the Location Device.
Capacity Management	The practice of ensuring that services achieve agreed and expected performance levels, satisfying current and future demand in a cost-effective way.
Caseload	The number of Device-Wearers being Monitored at any one specific time by the Supplier.
Caseload Forecast	The forecast produced by the Authority which shows how the Authority believes Caseload will grow in the future.
CEP	Circular Area Probable is the radius of a circle centred on the true value that contains fifty (50)% of the actual Global Navigation Satellite System measurements. A receiver with one (1) metre CEP accuracy will be within one (1) metre of the true measurement fifty (50)% of the time.
Charging Event	An Event registered when a Monitoring Device is charging.
Children	Device-Wearers under eighteen (18) years of age.
CJS	See Criminal Justice System.
CJS Stakeholders	(a) Probation (including the National Security Division (NDS)). (b) HMCTS, the Judiciary, the Magistracy Crown Prosecution Service (CPS), and Defence solicitors. (c) Youth Justice Board (YJB), incorporating Youth Offending Teams (YOTs). (d) Police. (e) Prisons (public and private) and Youth Custody Service (YCS). (f) Parole Board. (g) Public Protection Casework Section (PPCS). (h) Community Accommodation Service (Tiers 1, 2 and 3) (i) Home Office (Immigration Enforcement). (j) Home Office and CTUs (TPIMs).
Clips	A mechanism which securely attaches the Strap to the Device, or which protects the point of attachment between the Strap and the Device.

Term	Definition
Community Order	Has the meaning given to it in section 177 of the Criminal Justice Act 2003.
Component Testing	Means the testing of individual software components in isolation, using stubs and drivers.
Confidentiality	The concept that information is not made available or disclosed to unauthorised individuals, entities or processes.
Configuration	An arrangement of Configuration Items (CIs) or other resources that work together to deliver a product or service. Can also be used to describe the parameter settings for one or more CIs.
Configuration Item (CI)	Any component that needs to be managed in order to deliver an IT service.
Configuration Management Database (CMDB)	A database used to store Configuration Records throughout their lifecycle. The CMDB also maintains the relationships between Configuration Records.
Configuration Record	A record containing the details of a Configuration Item (CI). Each Configuration Record documents the lifecycle of a single CI. Configuration Records are stored in the CMDB.
Contact Centre	see EM Contact Centre
Continuous Improvement	The practice of aligning an organisation's practices and services with changing business needs through the ongoing identification and improvement of all elements involved in the effective management of products and services.
Control Message	A message instructing the system or Device to perform the designated function or to switch operating state.
Court Bail Orders	The grant of bail to a Device-Wearer in criminal proceedings pursuant to section 3 of the Bail Act 1976.
Criminal Justice System	The system of law enforcement directly involved in apprehending, prosecuting, defending, sentencing, and punishing those who are suspected or convicted of criminal offences.
Curfew Absence	The state where a Device has determined that the Device-Wearer is not within an associated active Curfew Area (i.e. during the specified hours), taking account of any Authorised Absences.
Curfew Area	The area within which the Device-Wearer must remain during an active curfew (the area remains the same even when a curfew is inactive).
Curfew Boundary	The perimeter of the Curfew Area.
Curfew Location	The postal address to which Curfew Monitoring applies for the associated Device-Wearer in accordance with their Licence or Order. Will also be referred to as residence, particularly where determined by the court.

Term	Definition
Curfew Monitoring	Electronic Monitoring of a Device-Wearer to ensure compliance with a curfew requirement (or an ”overnight residence period” for TPIM Notices) in an Order or Licence.
Curfew Only Device	Fitted Monitoring Device that is configured to only carry out Curfew Monitoring
Curfew Range	The distance from the HMU to the relevant Curfew Boundary.
Data Dictionary	Centralised repository of the data fields, its contextual description and associated technical information required to provide the Services.
Defective Device	A Device which is not functioning as required to carry out the type of Electronic Monitoring it has been deployed for.
Detention and Training Order	An Order that subjects the Device-Wearer subject to the Order, for the term specified in the Order, to a period of detention and training followed by a period of supervision. Only applicable for Children.
Device Alert Interface	An interface which will receive Event and Alert data generated by the Monitoring Equipment.
Device Development and Enhancement	Research and Development undertaken by the Supplier to improve the quality or efficiency of its Devices.
Device Fault	The specific issue which is preventing a Device from Monitoring as required to carry out the type of Electronic Monitoring it has been deployed for, including but not limited to failed parts and flat batteries.
Device ID	The identifier for a Device, either internal or external, marked on the face of the Device.
Device Incident	An issue with one or more Devices which prevent a Device from carrying out the type of Electronic Monitoring it has been deployed for.
Device Monitoring Platform	The system which monitors Monitoring Events arising from Devices and follows business rules to identify which Monitoring Events need to be passed to the FMS Supplier as Alerts, both for Non-Compliance and for technical Device Alerts.
Device-Wearer	Any person who is subject to an Order, Licence or Court Bail Condition and who must wear a Device as a result of that Order, Licence or Court Bail Condition.
Electronic Monitoring	The services provided under the EM Services Contracts which relate to the interactions between the EM Contractor(s), Device-Wearers, Service Recipients, CJS Stakeholders and the Authority, which includes Monitoring.
Electronic Monitoring Equipment	Any hardware deployed to Monitor Device-Wearers in line with their Monitoring Requirements.
EM	Means Electronic Monitoring

Term	Definition
EM Contact Centre	The single point of contact between the Supplier and the Users. The Contact Centre shall manage Incidents and Service Requests, and also handle communication with the Users.
EM Services	Each and any of the services provided to the Authority by any and all of the EM Suppliers.
Environmental Alcohol	Alcohol present in a proximate location to the Device-Wearer, but which the Device-Wearer has not ingested. E.g. Alcohol-based hand sanitiser.
Event	Any change of state that has significance for the management of a service or other configuration item.
Event Monitoring	The process of inspecting Events, manually or electronically, to understand the underlying cause.
Exclusion Geofence	A virtual geographic boundary, defined by Location Monitoring or RFID technology, that enables software to trigger a response when a Device enters a particular area as defined in the Device-Wearer's Monitoring Requirements.
Exclusion Monitoring	The EM of a Device-Wearer pursuant to an Order or Licence requiring the Device-Wearer to remain outside an Exclusion Zone.
Exclusion Zone	An area outside of which the Device-Wearer must remain for the duration of the Zone's active period.
Exclusion Zone Violation Event	A Monitoring Event recorded at the point the Device-Wearer is deemed to have entered an active Exclusion Zone, as defined on the Location Device.
Factory Acceptance Testing or "FAT"	Means the testing of the Supplier's integrated system covering functional, security and non-functional testing to confirm completeness of delivery against the relevant requirements of the Contract.
False Tamper Events	Monitoring Events raised indicating that a Device has been interfered with, but which cannot be substantiated by physical evidence.
Field and Monitoring Service	Means the services provided by the FMS Supplier, namely the provision of a Field Service and the provision of a staffed Monitoring Centre and EM Contact Centre.
Field Officer	A member of the FMS Supplier’s personnel providing field support for Electronic Monitoring.
Field Officer Equipment	Communication, measurement, Installation or De-Installation devices used by a Field Officer, including any devices used in authentication and authorisation of the Field Officer.
Field Service	Means the service provided by the Field Officers.
Fitted Device	A Device which is designed to be worn by the Device-Wearer for the duration of the relevant Monitoring Requirements without being removed.

Term	Definition
Fitted Location Monitoring Device	A Fitted Device used for Location Monitoring.
Firmware	Software which is programmed onto a hardware Device.
FMS	Has the same meaning as Field Monitoring Service
FMS Supplier	Means the supplier providing the FMS elements of the EM Service.
Galileo	The global navigation satellite system created by the European Union through the European GNSS Agency.
Geofence	A defined virtual perimeter for a real-world geographic area.
Global Navigation Satellite System	A satellite navigation system, with global coverage, currently these are GPS, GLONASS, China's BeiDou Navigation Satellite System, BDS and Galileo.
GLONASS	Russian Global Satellite Navigation Satellite System
GNSS	Has the same meaning as Global Navigation Satellite System
GPS	Global Positioning System, being a specific implementation of the US GNSS service.
GSM LBS	Location Based Services associated with data received via the mobile communications network.
GSM	Global System for Mobile communication
HDoP	Horizontal Dilution of Precision (Global Positioning System)
Her Majesty's Prisons and Probation Service or HMPPS	HM Prisons and Probation Service, an executive agency of the Ministry of Justice.
HMPPS	His Majesty's Prisons and Probation Service
HMU	Home Monitoring Unit
Home Detention Curfew	An early release from custody under sections 246, 255B(7) (a) or 255C(7) (a) of the Criminal Justice Act 2003, where the offender is subject to a curfew requirement which is electronically monitored.
Home Monitoring Unit(s)	A communications device installed at a residence that is identified for a particular Device-Wearer in the relevant Notification (including any relevant variation to the Notification) and which is used with a Device as part of the Electronic Monitoring of a Device-Wearer.
Home Office Fitted Location Monitoring	Location Monitoring which is provided on behalf of the Home Office.
Immigration Court Bail	An Order for EM on a Device-Wearer under Section 36 of the Asylum and Immigration (Treatment of Claimants etc.) Act 2004.
Incident	An interruption to the expected operation of the monitoring of a Device-Wearer. This may include either non-compliance with Monitoring

Term	Definition
(also Monitoring Equipment Incident)	Requirements (a Non-Compliance Incident) or a technical interruption to the service (a Technical Incident). A Technical Incident is also an unplanned interruption to an IT Service or a reduction in the quality of an IT Service and failure of a Configuration Item that has not yet impacted Service for example, failure of one disk from a mirror set.
Incident - P1	A Technical Incident: (a) that results in a complete or substantial loss of the Service. This will include the Device-Wearer Management functions, Order Management functions, Association of Device IDs with a Device-Wearer and Field Office Scheduling Functions; or (b) that results in an essential part of the Service being unusable for all End Users; or (c) that results in all end users being unable to access the Service; or A Non-Compliance Incident, specifically an interruption in monitoring for Specials. Note this includes loss of any access or performance in the toolset used for Specials Monitoring.
Incident - P2	A Technical Incident: (a) where the Service is materially adversely affected, but can be circumvented; This includes reduced speed of access to Device-Wearer history data; or (b) where the Service remains operable, but certain material aspects of the Service are disabled; or (c) where a large group of end users is unable to access the Service; or certain material aspects of the Service. This includes access to fitting and Monitoring Equipment configuration tools for an individual FMO; or A Non-Compliance Incident: (a) that is an interruption in compliance monitoring due to a Device Tamper; or (b) that is an interruption in compliance monitoring due to a Curfew Violation or; (c) that is an interruption in compliance monitoring due to a failure to verify biometric tests; or (d) that is an interruption in compliance monitoring where the Alert type is a Missing Status Check; or (e) where compliance monitoring identifies no movement of a Device-Wearer; or (f) where Battery Level is at a level which is insufficient to enable generation of an Event (for example <20% remaining); or

Term	Definition
	(g) where the Monitoring Centre is notified by a device it is currently unable to undertake Monitoring.
Incident - P3	A Technical Incident: (a) that results in a minimal business impact for the Service where non-critical functions or procedures are down, unusable, or difficult to use; or (b) affecting a single or small group of end users; or A Non-Compliance Incident where a Non-chargeable Device battery level is low (that is, the battery in the device requires replacement).
Incident - P4	An Incident: (a) that results in little or no material impact on the Service or the Users; (b) where the Service is determined to be functioning as designed but the Incident may result in a Change Request to modify or enhance the Service; or (c) raised in response to questions, compliments, complaints, escalations or queries from Users.
Inclusion Geofence	A virtual geographic boundary, defined by Location Monitoring or RFID technology, that enables software to trigger a response when a Device leaves a particular area as defined in the Device-Wearer's Monitoring Requirements.
Inclusion Monitoring	EM of a Device-Wearer pursuant to an Order or Licence requiring the Device-Wearer to remain inside an Inclusion Zone.
Inclusion Zone	An area within which the Device-Wearer must remain for the duration of the Inclusion Zone’s associated active period.
Inclusion Zone Violation Event	A Monitoring Event recorded at the point the Device-Wearer is deemed to have departed from an active Inclusion Zone, as defined on the Location Device.
Individual Protocol	A protocol issued by a Notifying Organisation in respect of an individual Device-Wearer that sets out the requirements of said Device-Wearer's Order. For example, Special Cases will always be excluded from ports and airports.
Induction	The activity of the Field Officer explaining to a Device-Wearer the terms of that Device-Wearer’s Order or Licence and how the Device-Wearer’s Devices work.
Information Security Management System	The set of interrelated or interacting elements of an organisation to establish policies and objectives, and processes to achieve those objectives ('management system') for the preservation of Confidentiality, Integrity and Availability of information ('information security'), as defined by ISO/IEC 27000.

Term	Definition
Infrastructure	Comprises all hardware, network devices, firmware, operating systems, middleware and database software used in the provision of the Services. It also includes all servers and network devices provided as part of a public or private cloud environment.
Infrastructure Incident	An unplanned interruption or reduction in quality to the EM Service Infrastructure.
Infrastructure Monitoring	Proactive monitoring of Infrastructure to look for signs of an impending Incident.
Ingested Alcohol	Alcohol present within a Device-Wearer's body.
Innovation	Changes to data, technology, research and practice that: 1. Sustain a product or service through significant improvements to benefits and may require business change e.g. new ways to use radio frequency data to assist police in the efficient apprehension of monitored persons; 2. Are disruptive, in that they bring about a significant change in how objectives are achieved e.g. Non-Fitted devices; and/or 3. Are radical e.g. by creating a new use or market and might require a significant change to policy and/or practice.
Installation	The act of Installing Devices on Device-Wearers and/or siting HMUs in residences (as applicable) and “Install” shall be construed accordingly.
Interface	A shared boundary across which two (2) or more separate components of a computer system exchange information.
Interface Documentation	Documents that describes how an interface works and how it should be implemented
Integrity	The property of safeguarding the accuracy and completeness of information – this may include the ability to prove an action or Monitoring Event has taken place, such that it cannot be repudiated later.
Knowledge Article	A piece of documentation that answers frequently asked questions relating to EM and/or provides instructions on common issues that occur in use of the service.
Known Issue	An Issue with an Application which is known to the Supplier, and for which a workaround is feasible.
Licence	A period during which a Device-Wearer is released from custody to serve the remainder of their sentence in the community subject to certain conditions, pursuant to section 250 of the Criminal Justice Act 2003 (including Home Detention Curfew and post release licences).
Location Based Service (LBS)	A service which translates GSM single cell tower information or a Google service which triangulates information from a number of connected cell towers into geolocation co-ordinates, typically used as a second or third source of location verification to a GNSS based source.
Location Data	Point data that is spatially referenced using latitude and longitude coordinate values. The latitude and longitude values can be

Term	Definition
	supplemented by additional detail and this varies depending on the source of the data. Typical sources include GNSS, LBS and GSM LBS.
Location Device	A Device worn by a Device-Wearer for the purposes of Location Monitoring and/or Curfew Monitoring. A Location Device may also provide the ability to perform Curfew Monitoring using RF rather than Location Data. A Location Device may also include a separate 'hand-held' or 'pocket' device paired with the body worn device which provides the Location Data.
Location Message	A message recorded in accordance with the configured Location Monitoring conditions.
Location Monitoring	EM of a Device-Wearer pursuant to an Order or Licence which requires the tracking of the Device-Wearer's location.
Low Battery	The state when the battery charge level in the Device-Wearer's Device falls below a predetermined level but where the Device-Wearer's Device continues to function.
Low Battery Event	A Monitoring Event generated when the Device-Wearer's Device enters a Low Battery state.
MAPPA	A Multi-Agency Public Protection Arrangement under the Criminal Justice Act 2003.
MDSS	Means Monitoring Devices and Systems Service
Message	A message which is logged to provide evidence of an Event.
Mobile Network	The national cellular network provided by the Supplier used for the communication of voice and data.
Monitor	See Electronic Monitoring
Monitoring	Means Electronic Monitoring
Monitoring Centre	The premises provided by the FMS Supplier from which the FMS Supplier performs the Monitoring.
Monitoring Data	All Monitoring Events and Alerts associated with Monitoring.
Monitoring Equipment	The Device-Wearer's Devices including any tags, Non-Fitted Device(s) and/or Home Monitoring Unit required to monitor compliance with the Device-Wearer's Monitoring Requirements.
Monitoring Equipment Management Tools	The Application(s) used to manage the configuration of Electronic Monitoring equipment.
Monitoring Event(s)	Any change of state registered by a Device that has significance for the management of a Device-Wearer.

Term	Definition
Monitoring Requirements	The specific type of Electronic Monitoring which an Order, Licence or Court Bail Condition requires in respect of a Device-Wearer. Monitoring Requirements will, include but not be limited to: (a) Curfew Monitoring; (b) Exclusion Monitoring; (c) Inclusion Monitoring; (d) Alcohol Monitoring; and (e) Location Monitoring
Network(s)	The set of technologies and related Infrastructure used by the Supplier to connect all nodes, for example servers, which are required to provide the Services.
Multiple Requirement Order	A Community Order, Suspended Sentence Order or Youth Rehabilitation Order in each case which is not a Single Requirement Order.
NMEA	National Marine Electronics Association
Non-Compliance	A Device-Wearer's violation of their Monitoring Requirements. “Non-Compliant” shall be construed accordingly.
Non-Compliance Event	Any instance of non-compliance by a Device-Wearer with their Monitoring Requirements pursuant to the terms of their Order or Licence. This shall also include any and all Non-Compliance Incidents
Non-Compliance Incident	Has the meaning given to it in the definition of Incident.
Non-Fitted Device	A Device which is not fitted to the Device-Wearer, but which must be in their possession at all times throughout the duration of the relevant Monitoring Requirements.
Notification	A notice provided to the Supplier by a Notifying Organisation that contains the Monitoring Requirements as set out in a particular Order or Licence including but not limited to whether: (a) the Order or Licence requires Curfew Monitoring, or Location Monitoring. (b) the Order is a Single Requirement Order or Multiple Requirement Order. (c) the Order or Licence relates to an adult or Child. (d) the terms of any variation to Monitoring Requirements under a particular Order or Licence; and/or (e) the Termination of any Monitoring Requirements under any particular Order or Licence or the Termination of such Order or Licence;
Notifying Organisation	An organisation (including a related organisation) that provides a Notification to the Supplier which shall comprise: (a) a Court.

Term	Definition
	(b) UK Visas and Immigration and Immigration Enforcement. (c) Home Office; or (d) HM Prison and Probation Service.
Operational Acceptance Testing or "OAT"	Means the testing by the FMS Supplier to validate operational readiness on the end-to-end EMFS solution by undertaking the following test activities; resilience (stability testing, backup & restore, recoverability, disaster recovery, business continuity), configuration management, service management (monitoring & alerting, logging & auditing, system start-up/shutdown), deployment & rollback/reversion, performance (responsiveness testing, load testing, volume testing, endurance testing/soak testing, stress testing), security (IT Health Check/penetration testing), service readiness, change & release management, backup & restore, monitoring & alerting, incident management, logging & auditing.
Order	An Order or other authorisation for EM on a Device-Wearer, including but not limited to: (a) Community Orders. (b) Suspended Sentence Orders. (c) Court Bail Orders. (d) a Youth Rehabilitation Order. (e) Detention and Training Order. (f) Subject to Parliamentary approval, Supervision Default Orders under the Offender Rehabilitation Act 2014. (g) Section 256B Supervision. (h) TPIMS Notices. (i) SIAC Bail Orders. (j) Immigration Court Bail (k) Domestic Abuse Protection Order / Domestic Abuse Protection Notice.
Patching	A set of changes to a computer program or its supporting data designed to update, fix, or improve it.
Pre-production	The environment used for Testing during the Mobilisation Phase and, from the Services Commencement Date, for supporting resolution of Incidents in Production as well as for the final phases of Testing of new Releases.
Problem	A cause, or potential cause, of one or more Incidents.
Production	An environment where the latest versions of software, products, or updates are pushed live to the intended users.
Recording Rate	The frequency at which a Location Monitoring Device records data from its Location Monitoring technologies and associated Status Information into its local memory.

Term	Definition
Release Note	The documentation relating to any change to the Applications and Infrastructure underpinning service operations.
Remote Breathalyser Device	A Device which allows a Device-Wearer to log their alcohol intake by measuring the alcohol present in a sample of breath.
Report/Reporting	A written account on EM data received by the relevant stakeholder(s).
Reporting Rate	The frequency at which a Device sends recorded data from its local memory to the FMS Supplier, via the MDSS Network.
Responsible Officer	Means the person who is responsible for discharging the functions conferred by this Contract in accordance with arrangements made by the Secretary of State. The Responsible Officer must be: (a) an officer of a provider of probation services, or (b) a person responsible for monitoring the offender in accordance with the Monitoring Requirements imposed by the relevant Order or Licence.
Root Cause Analysis	The process of discovering the root causes of Problems or Incidents in order to identify appropriate solutions.
Sampling Rates	The frequencies at which Location Devices sample their Location Monitoring technologies.
Section 256B Supervision	An Order under section 256B of the Criminal Justice Act 2003.
Service Asset	Resources and capabilities which make up the Service.
Service Management System	The system, provided by the FMS Supplier, containing Device-Wearer Data used to provide the Services.
Service Desk	The Service Desk provides the point of communication between Electronic Monitoring and all Stakeholders interacting with the Service. Stakeholders include all Device-Wearers, probation staff, police staff and all EM teams.
Service User	An individual who will have interaction with the EM Contact Centre, including but not limited to - Monitoring Centre staff, any EM Contractor member of staff performing a service management or service support role, Super Users and members of staff who form part of the EM Business Management team and Device-Wearers.
Service Request	A request from a Service User or a Service User's authorized representative that initiates a service action which has been agreed as a normal part of Service delivery.
SIAC	Means Special Immigration Appeals Commission
SIAC Bail Order	An Order imposing Monitoring Requirements made by SIAC.
Single Requirement Order	A Community Order, Suspended Sentence Order or Youth Rehabilitation Order that imposes one or more of the following but no other requirement:

Term	Definition
	(a) a Curfew Monitoring requirement; (b) an Exclusion Monitoring requirement; or (c) a Location Monitoring requirement.
Software as a Service or SaaS	A method of software delivery and licensing in which software is accessed online via a subscription, rather than bought and installed on individual computers.
Special Case	A small number of cases where the Device-Wearer is subject to an electronic Monitoring Requirement and an associated Individual Protocol that directs the Supplier to take specific action by way of alerting stakeholders and communicating with the individual on receipt of system notifications and Alerts or as otherwise directed by the protocol. Those subject to individual protocols are National Security, Critical Public Protection and other selected high-risk cases. The Departments managing such cases can be the Authority (Probation Service) or the Home Office. In many instances it will be necessary to liaise with the police and probation service to arrange Installation, equipment check and decommissioning visits to the individual's address. Including but not limited to any Device-Wearer with: (a) a TPIM Notice managed by the TPIMS section within the Home Office; (b) a SIAC Bail Order managed by the SIAC section within the Home Office; (c) Immigration Bail managed by the Home Office; or (d) a MAPPA.
Spoofing	The process by which a Device-Wearer causes their Device to send incorrect signals through blocking or tricking the Device, for example through use of foil to block signals, electronic jamming or signal repetition.
Sprint Testing	Means the testing of all developments contain within a development sprint, using stubs, drivers and/or test automation.
Stakeholder	A person or organisation that has an interest or involvement in the EM organisation, products, services, practices, or other aspects of the EM Service. These can include but are not limited to: i. Probation (including the NSD National Security Division). ii. HMCTS, the Judiciary, Crown Prosecution Service (CPS), and Defence solicitors. iii. Youth Justice Board (YJB), incorporating Youth Offending Teams (YOTs). iv. Police. v. Prisons and Youth Custody Service (YCS). vi. Parole Board. vii. Public Protection Casework Section (PPCS). viii. Court Bail Accommodation and Support Services (BASS). ix. Home Office (Immigration Enforcement).

Term	Definition
	x. Home Office and CTUs (TPIMs). xi. Device-Wearers
Status Information	Information about the status of a Device, including an indication of detected faults and Tampers.
Strap	The band which passes around the Device-Wearer's limb to secure the Device to the Device-Wearer for the purposes of Monitoring, using the associated Clips (the Clips may form an integral part of the Strap or be separate components).
Supervision Default Order	An unpaid work requirement or curfew requirement.
Supplier Operational Acceptance Testing or "SOAT"	Means the testing to validate operational readiness of the service components within the Supplier System by undertaking the following test activities; resilience (stability testing, backup & restore, recoverability, disaster recovery, business continuity), configuration management, service management (monitoring & alerting, logging & auditing, system start-up/shutdown), deployment & rollback/reversion, performance (responsiveness testing, load testing, volume testing, endurance testing/soak testing, stress testing), security (IT Health Check/penetration testing), service readiness, change & release management, backup & restore, monitoring & alerting, incident management, logging & auditing.
Suspended Sentence Order	An Order under section 189 of the Criminal Justice Act 2003 that contains a supervision period, as defined in that section.
System Integration Testing or "SIT"	Means the testing by the FMS Supplier of each of the Interfaces, between the MDSS, FMS and Authority Application services, including those set out in Schedule 2 - Figure 1: System Context Diagram and Table 3: MDSS Interfaces.
System Testing	Means the testing of the Supplier System against the High/Low Level Design, utilising simulators, harness and/or stubs to emulate all external Supplier, Third Party or Authority interfaces, input and output, as required.
Tampers	Any attempt by a Device-Wearer or third party to interfere with or remove a Device.
Tamper Alert	A notification to the Supplier that a Device has been interfered with.
Tamper Event	A Monitoring Event which can be used to confirm that a Device-Wearer or a third party has interfered with a Device, as notified by the Device which, along with physical evidence, is sufficient to prosecute a breach of an Order or Licence.
Technical Services	IT services that are not directly used by the Authority, but are required by the Supplier, so that it can provide the EM Services. For example, directory services, naming services or communication services.
Tethered Charging	A charger which has a charging cable permanently attached to it.

Term	Definition
Termination	Means the ceasing of an Order or Licence, by way of a Notification issued by a Notifying Organisation and “Terminate” shall be construed accordingly.
Tertiary Location Identification Technology	Location technology which is not GNSS e.g. LBS or WiFi.
Test Scripts	Test scripts describe all steps and actions to ensure a requirement, or set of requirements, have been delivered.
Third Party Interface Testing	Means the testing of all interfaces related to external third party components and Applications within the Supplier System.
TPIM	Terrorism Prevention and Investigation Measures.
TPIM Notice	An Order for EM on a Device-Wearer made pursuant to the Terrorism Prevention and Investigation Measures Act 2011.
Trail Monitoring	(also known as Whereabouts Monitoring) The location of the Device-Wearer at any point in time during their Monitoring Requirements shall be easily viewable by FMS staff and the Responsible Officer on a map. Can also be used to describe Exclusion / Inclusion Monitoring (see Exclusion Monitoring and Inclusion Monitoring)
Transdermal Alcohol Monitoring	A Device which measures A Device-Wearer's alcohol intake by measuring the alcohol content of their sweat.
Coordinated Universal Time	The standard time common to every place in the world.
Untethered Charging	A charger which has a cable which is not permanently attached to the plug.
Unit Testing	Means the testing of individual modules or configuration in isolation, using stubs and drivers.
User Acceptance Testing or "UAT"	Means the testing of the solution to validate that it supports the business processes, including time dependencies, evidential integrity (EI) requirements, operating procedures and training material.
Users	Anyone who is entitled to use the Service provided, including but not limited to Device-Wearers, the Authority, Service Recipients and CJS Stakeholders.
Wi-Fi	Local area wireless technology that allows an electronic device to exchange data over or connect to the internet.
Workarounds	A documented method which can be used to circumnavigate a Known Issue.
YOT	Means Youth Offending Teams.
Youth Rehabilitation Order	An Order pursuant to sections 1-8 and Schedule 1 of the Criminal Justice and Immigration Act 2008.
Zone	An Inclusion Zone or an Exclusion Zone.