SCHEDULE 1 Part IB – SECONDARY SERVICE PROVIDER SPECIFICATION

Section	Requirement
1	General Requirements
2	General Requirements in relation to Warrants and Orders
3	Appeals
4	Code of Conduct
5	Complaint Handling
6	Dealing with Customer Queries
7	Finance and Accounting
8	IT
9	Security and Information Assurance - General
10	Translation Service
11	Use of Forced Entry
12	Vulnerable Defendant
13	Warrant of Control
14	Welsh Language
Annex 1	Definitions
Annex 2	Table of HMCTS Regions and Areas
Annex 3	List of Warrants
Annex 4	Return Codes
Annex 5	Table of Retention Periods
Annex 6	Associated Process Map(s)
Annex 7	NOT USED
Annex 8	IT Cyber Security & Information Assurance Requirements Guidance
Annex 9	Security Aspects Letter

1.	GENERAL REQUIREMENTS
1.1	The Service Provider shall perform all requirements in accordance with all applicable Law.
1.2	The Service Provider shall obtain its own legal advice, as required, in order to ensure that it is performing the requirements in accordance with all applicable Law.
1.3	The Service Provider shall ensure that all data in respect of the Authority's work will be held in the United Kingdom.
1.4	Any collection technique or enforcement activity which is not contained in these requirements and which the Service Provider proposes to use in its performance of the Services may only be implemented with prior written approval from the Authority.
1.5	The Service Provider shall maintain an audit trail on the Service Provider IT System of all: • actions, enforcement steps and decisions taken by the Service Provider • contact with a Defendant or third party • correspondence sent and received by the Service Provider • enforcement action outcomes and Court directions notified to the Service Provider by the Authority • payments made to or made by the Service Provider • complaints received • claims against the Service Provider in the County Court in connection with these requirements.

1.6	All Staff involved in the handling of any Authority Data shall have security clearance appropriate to the security classification that has been allocated to the relevant Authority Data or activity. HM Government's security classifications (OFFICIAL, OFFICIAL SENSITIVE, SECRET and TOP SECRET) indicate the increasing sensitivity of information AND the baseline personnel, physical and information security controls necessary to defend against a broad profile of applicable threats. The Service Provider shall be expected to handle information classified as "Official" and "Official-Sensitive" only and shall ensure that all Staff have undergone an appropriate Disclosure Barring Service ("DBS") check. This shall include all temporary and relief personnel whether employed directly by or contracted to work for the Service Provider.
1.7	The Service Provider shall respond to any request for information from the Authority in respect of any Defendant within 1 (one) Working Day unless an alternative time scale for responding is specified within the Contract.
1.8	The Service Provider shall offer a variety of methods for members of the public (including any Defendant) to make an enquiry in respect of the activities performed by the Service Provider pursuant to these requirements. Such methods shall include, as a minimum, telephone, email, letter and online facilities. The Service Provider shall respond to all enquiries promptly and courteously and all responses provided shall be correct in accordance with all applicable Law. The Service Provider shall ensure that all Staff receive appropriate training to advise and deal with all enquiries received in relation to the provision of the Services.
1.9	The form of any standard templates for written communication sent from the Service Provider to any Court, Defendant, or other member of the public shall be approved by the Authority.
1.10	The Service Provider shall, prior to the Service Commencement Date, agree with the Authority a protocol for dealing with any complaints made to, or in respect of, the Service Provider in connection with its provision of the Services, the protocol shall be implemented by the Service Provider throughout the Contract Period.

1.11	All hard copy records held by the Service Provider containing Personal Data shall be stored, transported and disposed of securely. Sensitive waste paper must be collected separately from normal waste, and stored securely pending confidential destruction.
1.12	On expiry or termination of the Contract, the Service Provider shall support business continuity and migrate any required information to a Replacement Service Provider(s) or to the Authority, as detailed in Clause H9 (Retendering and Handover) to Clause H12 (Warrants and Orders on Expiry or Termination).
2. GENERAL REQUIREMENTS IN RELATION TO WARRANTS	
2.1	The Service Provider shall comply with all applicable Law when executing any Warrant.

2.2	Any written Initial Contact Notice shall, as a minimum, include the following: • The name and address (if specified) of the person whom the Warrant was issued against • the specific details of the Warrant issued, including any reasons stated on the Warrant • the name of the issuing Court and date of issue • the full contact details of the Service Provider, including details of any assistance available for contacting the Service Provider such as language preferences, hearing loop • a clear explanation of the Service Provider's responsibilities and duties in relation to that Warrant • where legislation permits, the statutory basis on which, any fees, disbursements, charges or costs are applicable to the enforcement of the Warrant • the details of any such fees, disbursements, charges or costs applicable to the enforcement of the Warrant at all stages of the process • details of the consequences of non-payment or non-compliance with the Warrant • where payment applies, details of payment methods available to the Defendant • A summary of the actions that the Defendant shall take to comply with the conditions of the Warrant If an Initial Contact Notice is issued to a Defendant who is a Youth, the Service Provider shall ensure the notice includes all of the above and the following additional information: • Name and address of Parent or Guardian (if specified) if the Warrant is issued in respect of a Youth • Shall send a copy of the Initial Contact Notice to the Parent or Guardian if specified on the Warrant

2.3	Upon notification that a Warrant has been issued, the Service Provider shall ensure the Warrant is entered onto the Service Provider IT System within 1 (one) Working Day (Close of Business) of receipt. Acknowledgement shall be provided to the Authority to confirm numbers received. The details required will include: • Warrant issued type • the name of the issuing Court and date of issue • the Authority case or account reference number • any details relating of the original offence connected to the Warrant • where applicable any details provided relating to the original financial imposition of the Court • all specific instructions or directions specified on the individual Warrant • the Defendant's name, date of birth and address • in the case of fines having been imposed on a Parent or Guardian for a conviction against a Youth, the details of the fine against the Youth • in the case of fines having been imposed on a Youth, the details of the Parent or Guardian if specified
2.4	NOT USED

2.5	The Service Provider shall ensure that all Warrants are suitably and sufficiently risk assessed, including in respect of all health and safety risks to Staff, prior to a visit taking place. The Service Provider shall ensure that a process is in place pursuant to which it continually assesses risk during the execution of any Warrant. The Service Provider will inform the Authority by the agreed method of any risk information which may indicate a health and safety risk to any Court Staff or Court Users as soon as practicable.
2.6	The Service Provider shall ensure adherence to instructions from the Authority in respect of all applicable Law. Before exercising the Forced Entry Powers as set out in Section 17 all relevant Staff must have successfully completed an appropriate search and entry course.
2.7	The Service Provider shall ensure that any Staff who are responsible and authorised for executing Warrants and/or Orders receive appropriate training in accordance with Good Industry Practice and have appropriate security clearance and operate in accordance with applicable Law. See section 1.6
2.8	The Service Provider shall ensure that all Warrant information is stored in accordance with Schedule 8 Information Assurance and Security.
2.9	All Warrants shall be managed and returned securely and removed from systems within timescales stated within this Contract or as agreed with the Authority in writing.
2.10	The Service Provider shall provide any supporting documents to the Authority in relation to executed Warrants; returned Warrants; vulnerability or any applications to the Magistrates Court by the method agreed with the Authority, as specified in Annex 4, Return Codes.
2.11	If a Defendant requests to see a relevant Warrant the Service Provider shall show the Defendant the legally required Warrant information in electronic form. The Service Provider shall not create any copies or reproductions of Warrants under any circumstances.

2.12	The Service Provider shall ensure that all records of the Defendant on the Service Provider IT System are at all times maintained and kept up to date with full details of all actions and contacts with the Defendant, the Authority and/or relevant third parties.
2.13	Information relating to a Defendant or Vehicle Registration Number ("VRN") associated with the Defendant held on the PNC may under certain circumstances be accessed by the Authority's authorised PNC users at the request of the Service Provider. This is only applicable at the Authority's discretion in line with the memorandum of understanding for the Authority's use of PNC. The Service Provider shall provide adequate evidence that the PNC enquiry is in relation to a subject to a criminal Warrant at the time of the request. Any requests for PNC Information shall be made via the Service Provider's administrative office using secure email for both the request and response from the Authority; under no circumstances will the Authority provide PNC Information in any other way. It is illegal to perform unauthorised or speculative searches on the PNC, and shall only be used for official use. Any PNC requests which are found to be either unauthorised or inappropriate will be reported to the Police and may lead to criminal proceedings being taken against the individual. Under no circumstances shall the Service Provider pass PNC Information to any individual who does not require access to such data for the purposes of enabling the Service Provider to fulfil its obligations under this Contract, or discuss the data with such people.
2.14	If the Service Provider has any uncertainty in relation to the instructions which it is required to follow in relation to the execution of any Warrant, it shall contact the Authority to seek further clarification prior to the execution of such Warrant..
2.15	If the address of the Defendant is unknown or unverified, the Service Provider shall use its best endeavours to obtain a valid current address or to validate the address information provided by the relevant Court.
2.16	The Service Provider shall ensure that any visits made to a Defendant for the purposes of enforcing a Warrant is conducted in accordance with the requirements for the relevant type of Warrant as set out in the Contract and in accordance with applicable Law.

2.17	The Service Provider shall, prior to the Service Commencement Date, agree with the Authority a protocol for the use of force by Staff when executing Warrants. The Service Provider shall implement and act in accordance with the agreed protocol throughout the Contract Period. To the extent that the Service Provider's proposed protocol for the use of force is not approved, the Service Provider shall not use force in relation to the execution of any Warrant without the Approval of the Authority in each case. In all cases the Service Provider shall obtain the approval of the Authority before use of Forced Entry in accordance with the Use of Forced Entry requirement in this Contract. The use of Forced Entry Powers are set out in Section 17.
2.18	The Service Provider shall ensure that any Staff who conducts a visit to a Defendant for the purposes of executing a Warrant displays a Letter of Authority to the Defendant, if requested to do so by the Defendant or a relevant third party. The Service Provider shall ensure that the Letter of Authority includes the full name of the Staff executing the Warrant and details of their Authority to execute the Warrant. The Service Provider shall ensure that the Letter of Authority complies with all applicable Law, including the Criminal Procedure Rules.
2.19	The Service Provider shall ensure that all actions it takes to execute a Warrant are recorded on the Defendant's record on the Service Provider IT System as soon as practicable and in any event within 1 (one) Working Day. The Service Provider shall ensure that such records also include any contact with the Service Provider made by the Defendant or any third party on the Defendant's behalf, or any other relevant third party.
2.20	During any execution activity, the Service Provider shall: • offer a variety of secure payment methods to Defendant and relevant third parties by which to make payments in relation to any Warrant during any execution activity, such payment methods to include, at a minimum: cash payments; credit/debit card payment, postal payments; and • ensure that either a physical or secure electronic receipt, which shall contain details as specified in Section 12 (Finance and Accounting), is issued to the Defendant upon immediate receipt of any payment taken

2.21	All unexecuted Warrants shall have enforcement activities undertaken as a minimum no less than every 60 (thirty) calendar days until it is executed, withdrawn by the Court or returned to the Authority at the end of the Retention Period. These activities will include new intelligence checks, and further contact visits at different times of the day to include early morning and evening should be made as appropriate.
2.22	All Warrants which are executed, withdrawn by the Court, or returned to the Authority at the end of the Retention Period, shall be returned with sufficient new information or confirmation that the Defendant is unable to be traced to enable the Authority to take further actions on the account.
2.23	Where any Warrant is requested back because it is permitted legally or within any of the Contract terms, the Service Provider shall not charge the Authority for request and the return of the Warrant.
2.24	The Service Provider will provide the Authority electronic data sets of current or completed Warrants by type held on the Service Provider IT System as requested to enable a reconciliation to take place against the Authority records.
2.25	If the Service Provider requires an application for a Data Disclosure Order, the request with all relevant information shall be sent to the Authority in the agreed format. The Service Provider will update the Service Provider IT System with details of the application; the outcome will be updated on the Service Provider IT System within 30 (thirty) minutes of receipt.
2.26	If the Service Provider requires any application in relation to a Warrant the request with all supporting information shall be sent to the Authority in the agreed format. The Service Provider will update the Service Provider IT System with details of the application; the outcome will be updated on the Service Provider IT System within 30 (thirty) minutes of receipt.
2.27	The Service Provider shall on request provide the Authority, its representatives and or the National Audit Office with such access to those records and data in connection with this Contract as may be required.

2.28

Successful Execution

Warrant of Control	
	• Payment in full of the outstanding balance of the Court Imposition.
Progression	
	Where any Warrant has not been successfully executed or satisfied within the Retention Period, and the Service Provider has undertaken all mandatory steps stated in the relevant requirement in order to execute or satisfy the Warrant, at the end of the relevant Retention Period all outstanding Warrants shall be returned to the Authority using the agreed Return Codes. This is to provide the Authority with details of the outcome of the execution activities and where applicable the most up to date information regarding the Defendant's whereabouts. Supporting evidence will be provided as required. Examples could include: • visit(s) which establishes the Defendant has moved away and relevant enquires and tracing have not been able to identify a new address or the Defendants whereabouts • the Defendant is deceased • the Defendant is in Prison • all visits and remote contact has been undertaken but no contact has been made with the Defendant and relevant enquires and tracing has been unable to confirm the Defendant's residency at the address or their whereabouts

3.	APPEALS ~ APPLICATIONS UNDER SECTION 142 OF THE MAGISTRATES' COURTS ACT 1980, STATUTORY DECLARATIONS AND APPEALS ETC.
3.1	When the Authority is notified by the Court that an application has been made by a Defendant for example under section 142 of the Magistrates' Courts Act 1980; Statutory Declaration; application to remit; application in respect of a penalty notice for disorder, application to review compensation, unlawful profit order, or slavery and trafficking reparation order; or an appeal, and there is a Warrant of Control outstanding the Authority will make the decision on how to proceed on a case by case basis and inform the Service Provider whether to place the Defendants account on the Service Provider IT System on hold pending further instructions or to continue with enforcement action.
3.2	• In appropriate cases the Authority shall notify the Service Provider to suspend enforcement action on the relevant Defendant's Warrant until it is notified of the outcome of the application. • The Service Provider will update the Defendant's record on the Service Provider IT System within 30 (thirty) minutes that an application has been made for 1 (one) of the above reasons
3.3	When the Authority is notified of the outcome of the application, they shall notify the Service Provider and the following action shall take place: • If the application or appeal is granted, any relevant Warrant shall be returned to the Authority by the Service Provider in batches each week with reason specified in writing. • If the application is not granted, the Service Provider will continue to enforce the Court Imposition In both cases the Service Provider must update the Defendant's record on the Service Provider IT System of the outcome of the application within 30 (thirty) minutes of receipt of the information.
3.4	Where any Warrant is requested back because it is permitted legally or within any of the Contract terms, the Service Provider shall not charge the Authority for request and the return of the Warrant or Order.

4. CODE OF CONDUCT	
Corporate Conduct	
4.1	The Service Provider acknowledges that is discharging a public service duty on behalf of the Authority. The Service Provider, the Sub-Contractors and the Staff shall at all times whilst performing the Services observe and comply with the principles of public service being: • **selflessness -** holders of public office shall act solely in terms of the public interest. They shall not do so in order to gain financial or other benefits for themselves, their family or their friends • **integrity** - holders of public office shall not place themselves under any financial or other obligation to outside individuals or organisations that might seek to influence them in the performance of their official duties • **objectivity** - in carrying out public business, including making public appointments, awarding contracts, or recommending individuals for rewards and benefits, holders of public office shall make choices on merit • **accountability** - holders of public office are accountable for their decisions and actions to the public and shall submit themselves to whatever scrutiny is appropriate to their office • **openness** - holders of public office shall be as open as possible about all the decisions and actions that they take. They must give reasons for their decisions and restrict information only when the wider public interest clearly demands • **honesty** - holders of public office have a duty to declare any private interests relating to their public duties and to take steps to resolve any conflicts arising in a way that protects the public interest • **leadership** - holders of public office shall promote and support these principles by leadership and example

4.2	The Service Provider shall at all times whilst it is performing the Services observe and comply with "The Good Governance Standard for Public Services, 2004-The Langlands Report", which identifies six core principles of good governance in the delivery of public services, being: • focusing on the organisation's purpose and on outcomes for citizens and service users • performing effectively in clearly defined functions and roles • promoting values for the whole organisation and demonstrating the values of good governance through behaviour • taking informed, transparent decisions and managing risk • developing the capacity and capability of the governing body to be effective • engaging stakeholders and making accountability real
4.3	The Service Provider shall provide the Authority with a copy of its code of conduct at the Commencement Date, upon request and following any updates being made to its code of conduct.
4.4	The Service Provider shall ensure that the Staff operate under the direction and control of the Service Provider and the Service Provider shall be responsible for their conduct and discipline at all times.

4.5	The Service Provider shall inform the Authority by a report, as specified below, and in writing within 1(one) Working Day, of any situation listed below occurring: a) where public confidence in the Service Provider is, or likely to be undermined b) becoming aware of any gross misconduct, suspected or known, involving Staff, in respect of any of the following: • any criminal offence or conviction involving dishonesty or violence • falsifying records, or knowingly aiding and abetting others to do so • misappropriation of money or property • abusive or threatening behaviour; or • assault or offence against the person c) where any investigation by the Service Provider or any other organisation (e.g. Police) in relation to any of the instances in b) above is being conducted.
4.6	The Service Provider shall ensure that all Staff receive the appropriate training to ensure that they are fully conversant with and shall follow the requirements of the Contract, the relevant Law and Good Industry Practice.
Employee Conduct	

4.7	Whilst performing the Services, the Service Provider shall comply with and ensure the Staff comply with the Service Provider's code of conduct. The Service Provider shall ensure that the Staff carry out their duties and perform the Services in accordance with the following: **Integrity** <u>Staff shall:</u> • fulfil their duties and obligations responsibly • always act in a way that is professional and that deserves and retains the confidence of all those with whom they have dealings • carry out their fiduciary obligations responsibly (that is make sure public money and other resources are used properly and efficiently) • deal with the public and their affairs fairly, efficiently, promptly, effectively and sensitively, to the best of their ability • ensure they have Ministerial Authorisation for any contact with the media • keep accurate official records and handle information as openly as possible within the legal framework • comply with the law and uphold the administration of justice <u>Staff shall not:</u> • misuse their official position, for example by using information acquired in the course of their official duties to further their private interests or those of others • accept gifts or hospitality or receive other benefits from anyone which might reasonably be seen to compromise

	their personal judgment or integrity; or • disclose official information without authority (this duty continues to apply after they leave the Service Provider's and/or the Sub-Contractors' (as relevant) employment). **Honesty** <u>Staff shall:</u> • set out the facts and relevant issues truthfully, and correct any errors as soon as possible • use resources only for the authorised public purposes for which they are provided <u>Staff shall not:</u> • deceive or knowingly mislead ministers, Parliament or others; or • be influenced by improper pressures from others or the prospect of personal gain **Objectivity** <u>Staff shall:</u> • provide information and advice, including advice to Ministers, on the basis of the evidence, and accurately present the options and facts • take decisions on the merits of the case • take due account of expert and professional advice

	Staff shall not: • ignore inconvenient facts or relevant considerations when providing advice or making decisions; or • frustrate the implementation of policies once decisions are taken by declining to take, or abstaining from, action which flows from those decisions **Impartiality** Staff shall: • carry out their responsibilities in a way that is fair, just and equitable and reflects the civil service commitment to equality and diversity Staff shall not: • act in a way that unjustifiably favours or discriminates against particular individuals or interests **Political Impartiality** Staff shall: • serve the government, whatever its political persuasion, to the best of their ability in a way which maintains political impartiality and is in line with the requirements of this code, no matter what their own political beliefs are • act in a way which deserves and retains the confidence of ministers, while at the same time ensuring that they will be able to establish the same relationship with those whom they may be required to serve in some future government • comply with any restrictions that have been laid down on their political activities Staff shall not: • act in a way that is determined by party political considerations, or use official resources for party political purposes;

	or • allow their personal political views to determine any advice they give or their actions. To support the principles above, the Service Provider shall ensure that all Staff shall: • take responsibility for their actions • treat people with respect • be polite, reasonable and fair in dealings with all Defendants, third party customers and the Authority personnel; • ensure compliance with this Contract (to the extent applicable) • ensure that when accepting payments from third parties, they comply with all applicable Law and Good Industry Practice The Service Provider shall ensure that all Staff shall not: • discriminate against any person or group for any reason • harass, victimise or bully through language, actions or behaviour; or • deal with any of the Warrants or Orders under this Contract belonging to family or friends.
4.8	The Service Provider shall ensure that whilst performing the Services, the Staff shall comply with: • all applicable Law • Good Industry Practice • this Contract

5. COMPLAINT HANDLING

5.1	The Service Provider may receive complaints directly from a Defendant, or a third party or via the Authority, all complaints will be subject to the same process and level of investigation. The Service Provider shall have an effective system for recording complaints. The Service Provider shall have a clear complaints procedure that involves the Authority when necessary and it shall be advertised on all relevant paperwork and the Service Provider's website. At a minimum, the policy shall require the Service Provider: • to ensure all complaints are recorded on the Service Provider IT System for recording complaints, responded to and that the response is made within 10 (ten) Working Days • to ensure all complaints are dealt with confidentially, fairly and impartially • to ensure that any potential improvements to the Service Provider's systems, procedures and/or approach to delivery of the Services that are identified in the course of handling a complaint are incorporated where reasonably practicable • to ensure the complainant receives an explanation, an apology or redress when complaints are upheld • to ensure the complainant receives an explanation when a complaint is not upheld • to provide details of how to escalate the compliant if not satisfied with the response The complaint handling procedure shall include the following stages: • complaint received, acknowledgement sent and complaint recorded on the Service Provider IT System • the complaint manager will carry out an investigation into the complaint by gathering all relevant information, which may include statements and viewing footage from body camera • once the investigation has concluded the Service Provider shall review the complaint and identify any lessons learnt, and implement any recommendations or actions required to improve their Service

	• once the investigation has concluded a response shall be sent to the complainant and copied to the Authority, with a covering letter outlining any lessons learnt and actions taken to implement improvements to their Service • details of the outcome of the complaint to be recorded on the relevant Defendant account on the Service Provider IT System The Service Provider should respond to any complaint regarding the execution of any Warrant or Order. The following are examples of these types of complaints: • query on Fees • working on Warrants or Orders – steps taken to execute – letters sent, visits etc • actions or behaviours of Staff including call centre staff **For any serious complaints or incidents, for example:** allegation of assault; criminal damage; unlawful actions; actions of Staff resulting in the Defendant or third party needing urgent medical attention; **the Authority shall be notified immediately and no later than 1 (one) Working Day from receipt of the complaint, via the agreed method.** **Escalation** Where the complainant is not satisfied with the response the Service Provider shall have an escalation route in place so complaints can be reviewed the Service Provider. All escalated complaints shall be reviewed and considered within 10 (ten) Working Days from the escalation date.

5.2	Where a Field Operative is issued with a body camera the Service Provider shall have the capability to allow the Authority access to view the footage for a period of 35 (thirty-five) calendar days to assist with any complaints. Where it has been established that body camera footage is available and this is needed as part of an ongoing investigation the Service Provider shall ensure the footage is retained and the Authority is provided with access to view the footage. Should the Authority request the footage within 35 (thirty-five) calendar days, the Service Provider further shall retain the footage until the investigation has concluded and all avenues of appeal have been exhausted.
5.3	The Service Provider shall ensure that all actions taken and any lessons learnt from complaints to improve the Service will be recorded to enable it to be included as part of performance review meetings.
5.4	If the Service Provider receives a complaint in respect of the Authority, this shall be referred back to the Authority in the agreed format within 1 (one) Working Day of receipt of the complaint.
6. DEALING WITH CUSTOMER QUERIES	
6.1	The Service Provider shall adhere to Data Protection Laws, ISMS and all applicable Law when dealing with all customers enquiries; customers may be Defendant or any third party.
6.2	The Service Provider shall provide a facility for telephone calls to be charged at a local rate for the Defendant, which should be advertised on all correspondence.
6.3	The Service Provider shall ensure that all Staff who respond to customer enquiries receive appropriate training including regarding conflict resolution.
6.4	The Service Provider shall offer as a minimum the following methods of communication, telephone, email, letter, and online facilities for members of the public (including any Defendant) to make an enquiry in respect of the Services performed by the Service Provider.
6.5	The Service Provider shall respond to all enquiries promptly and courteously and all responses provided shall be correct unambiguous and in plain language.

6.6	The Service Provider shall respond to all written queries within 5 (five) Working Days of receiving the written query.
6.7	The Service Provider shall have the facility to receive and answer telephone queries as a minimum on the days and between the hours agreed with the Authority.
6.8	The Service Provider shall answer all incoming telephone queries relating to the Services in accordance with the Performance Measures set out in Schedule 4 (Pricing and Performance) and ensure it has the appropriate number of call handlers to do so.
6.9	The Service Provider shall ensure that the Defendant's record is updated on the Service Provider IT System on receipt of any written query from or relating to that Defendant (including queries from third parties) and record the outcome when the query has been dealt with, within 1 (one) Working Day.
6.10	The Service Provider shall ensure that the Defendant's record is updated on the Service Provider IT System immediately with details of the call and the outcome (including calls/queries from third parties).
6.11	The Service Provider shall ensure that any queries which it determines, acting reasonably, are escalated as a complaint to the Service Provider's appropriate manager and are managed in accordance with the Complaint Handling requirement contained within Section 9 of this Schedule.
6.12	The Service Provider shall on request by the Authority provide to the Authority the details of any Defendant query.
6.13	The Service Provider shall provide performance data regarding customer queries to the Authority upon request, including: • volumes of calls and correspondence by type • time frame for resolution of queries • call waiting times • numbers of missed calls

7.	FINANCE AND ACCOUNTING
Payments	
7.1	The Service Provider shall ensure that all of its payment processes align to all applicable Law, accounting standards and all Authority policies in relation to the security, handling and protection of monies and data (which form part of this Contract) including Schedule 10 (Policies and Standards).
7.2	The Service Provider shall have 1 (one) bank account exclusively for the management of payments for the Authority work. The Service Provider shall not under any circumstances use this bank account for any other clients work or for the running of the Service Provider's business operations.
7.3	The Service Provider shall have a secure method to ensure that any cash payments are deposited via a secure method promptly (and no later than 1 (one) Working Day of the payment being taken).
7.4	The Service Provider shall have in place and implement controls to manage the risk of fraud and errors on all receipts and payments processed.
7.5	The Service Provider shall report any incidents of fraud or attempted fraud to the Authority immediately (and no later than within 1 (one) Working Day upon discovery).
7.6	The Service Provider shall comply with industry standard guidance and all applicable Law in relation to money laundering notification procedures for cash payments.
7.7	The Service Provider shall ensure that all transactions are recorded against the correct accounting period.
7.8	The Service Provider shall ensure that all payments received by whatever method are brought to account completely, accurately within 1 (one) Working Day of receipt on the Defendant's record on the Service Provider IT System.

7.9	The Service Provider shall have a system to process any payments which cannot immediately be allocated to a specific Defendant account, by holding the payment in suspense until enquires can be made to ensure that the payment is allocated to the correct account; for example, when a Defendant has sent a payment with insufficient details to allocate. This process shall ensure that further enquires are undertaken and that all monies should be allocated to the account within 7 (seven) calendar days. A full audit trail shall be available to track payments through the process.
7.10	The Service Provider shall agree a process with the Authority to manage Charge Backs (rejected credit/debit card payments) and Referred to Drawer cheques. All cheque payments received from Defendant shall be retained in the Service Provider's client account for up to 5 (five) Working Days until cleared before being remitted to the Authority. This will ensure that no payment made by a Defendant to the Authority is dishonoured. The Service Provider shall ensure that the Defendant record on the Service Provider IT System is updated immediately or within 1 (one) Working Day of all steps taken in relation to rejected payments. The Service provider should then continue to enforce the Warrant.
7.11	The Service Provider shall apply all sums in accordance with the Law and pay any outstanding balance owed to the Authority. The Service Provider shall update the Defendant account on the Service Provider IT System to show that the money has been paid to the Authority. Any overpayments received must be returned to the Defendant or relevant third-party payee; the Service Provider shall update the Defendant's account on the Service Provider IT System to provide a full audit trail that the overpayment has been returned.
7.12	The Service Provider shall retain financial records for 7 (seven) years after the final payment has been attributed to a Defendant’s account in accordance with the Authority retention policy set out under Schedule 10 (Policies and Standards).

7.13	The Service Provider shall make available any audit and related action plans for financial management that include, but are not limited to, fraud and risk which is relevant to this Contract.
7.14	The Service Provider shall account for 100% of the receipts received. The Service Provider will not under any circumstances utilise the receipts received to fund any of the operational costs of running the service.
7.15	The Service Provider shall allow the Authority and National Audit Office to carry out open book accounting processes, at any time. The Authority must be able to access performance and accounting data with regards to Warrants and Orders.
7.16	The Service Provider shall be able to provide a complete list of all outstanding accounts, in the format agreed upon request or at specified points in the year.
7.17	The Service Provider shall be able to provide as required a full transactional list of the following items: • All Payments received from the defendant or third party • All Payments received by the Service Provider and transferred to Authority • Charge Backs / Referred to Drawer cheques • Suspense items • Defendant's Listings
7.18	The Service Provider shall forward to the Authority any Payments received from a Defendant or third-party payee after the relevant Warrant or Order has been return to the Authority. No monies can be retained by the Service Provider. The Service Provider shall return any fee payments to the Defendant or third-party payee; the Service Provide shall update the Defendant's account on the Service Provider IT System to provide a full audit trail that the fees have been returned.

Payments received from the Defendant during doorstep activities	
7.19	The Service Provider shall ensure that all of its payment and receipting processes align to all applicable Law, accounting standards and any policies of the Authority in relation to the security, handling and protection of monies and data which form part of this Contract.

7.20	The Service Provider shall ensure that receipts are issued for all Payments accepted during doorstep activities with the receipt including: • name of Defendant • date of receipt • receipt number • fine account reference number – Authority account number and Service Provider's unique reference number • amount received • a break down to show the Fees and Charges payable to the Service Provider and the amount to be paid to Authority • Field Operative identity • signature of Field Operative • for any credit/debit card payments, the payment acceptance reference number (if provided) The Service Provider shall ensure that the receipt is given to the person making the payment at that time and a copy retained for the Service Provider's accounting records. The Service Provider shall add a note of the payment taken to the Defendant's record on the Service Provider IT System along with the receipt number issued, and the details of the Field Operative taking the payment, within 1 (one) Working Day of the payment being taken.

7.21	The Service Provider shall ensure that where the Field Operative accepts a payment by credit or debit card during doorstep activities, the payment acceptance reference number from the payment line is provided to the person who had made the payment and the details retained by the Service Provider for its accounting records. The Service Provider shall add a note of the payment taken to the Defendant's record on the Service Provider IT System along with the payment acceptance reference number and the details of the Field Operative taking the payment within 1 (one) Working Day of the Payment being taken.
7.22	The Service Provider shall ensure its Field Operative complies with industry standard guidance PCI Data Standards and Authority policy in relation to money laundering notification procedures for cash payments set out under Schedule 10 (Policies and Standards).
7.23	The Service Provider shall ensure that financial transactions made are brought to account completely, accurately and promptly within 1 (one) Working Day of receipt against the Defendant's record on the Service Provider IT System.
Remittances to the Authority	
7.24	The Service Provider shall produce and issue to the Authority Remittances on a weekly basis in the format agreed, this should be sent to the Authority electronically. All monies transferred to the Authority shall quote the Defendant's account reference number, to ensure it is allocated to the correct account reference number. The Service Provider IT System shall show on the Defendant's record that the money in respect of the Warrant or Order has been transferred to Authority. The Service Provider shall work in partnership with the Authority to agree the changes to the format of the Remittance at no cost to the Authority.
7.25	The Service Provider shall make all payments to the Authority by BACS weekly in line with the corresponding Remittance.
7.26	The Authority will fully reconcile all Remittances back to the Service Provider IT System and this will be evidenced by a reconciliation report.

Daily Bank Reconciliations	
7.27	The Service Provider shall undertake and complete Daily Bank Reconciliation on the dedicated account, all unidentified or unreconciled items should be cleared within 5 (five) Working Days.
7.28	The Service Provider shall send the Authority copies of the Daily Bank Reconciliation reports each month. The reports shall include details of any unidentified or unreconciled items.
Payment received direct by the Authority after a Warrant of Control has been issued	
7.29	The Authority shall forward any payments it receives following the issue of a Warrant of Control to the Service Provider on a daily basis by BACS and with supporting Remittance in the agreed format and method. The Authority shall write to the Defendant to inform them that the payment has been sent to the Service Provider and they must contact the Service Provider to conclude the matter. These payments shall be allocated to the Defendant's account on the Service Provider IT System within 1 (one) Working Day of receipt of the Authority transfer.
7.30	The Service Provider shall ensure that all documents including business cards that are sent to the Defendant within Wales should be bilingual. Any Defendant that wishes to correspond with the Service Provider, either face to face, digitally or by telephone should be able to do so in their preferred language.
Fees	
7.31	No fees or charges will be paid to the Service Provider by the Authority during the implementation period between the Commencement Date and Service Commencement Date.
8. **IT**	

General Requirements	
8.1	The Service Provider IT System, management system, and supporting technology (“the System”) employed by the Service Provider shall: • have cyber essential certification ISO27001 and comply with all other relevant standards in line with IT Cyber Security & Information Assurance Requirements Guidance (Annex 8) and the Security Aspects Letter (Annex 9) • be a resilient service particularly during Normal Working Hours • be resilient with no single point of failure • be flexible and extendible to cope with varying demand and the addition of new users, services and applications. Without prejudice to Annex 8 the System shall ensure that its System it uses are secure and prevent intrusion and data loss and shall include provision for logging and auditing usage and access.
8.2	The System shall be assured for handling HMG information in line with HMG Security Guidelines as detailed in IT Cyber Security & Information Assurance Requirements Guidance (Annex 8) which include the establishment and implementation of personnel, application, technical and physical security controls. The Authority may conduct an IT health check (being a CHECK team implemented vulnerability scan and penetration test) as part of the assurance process.
8.3	The IT elements of the System shall be fully supported by the Service Provider for the Contract Period, such support to include monitoring, reporting, updates and patching, technical support and training, reporting and resolution of problems and incidents, and Change Management.
8.4	The Service Provider's instance shall be used exclusively for managing the Authority work. Under no circumstances should any other Service Provider’s work be included on the Service Provider's instance.

8.5	The Service Provider shall ensure that the location; and any IT device with access to the Service Provider IT System are capable of preventing unauthorised access to the location and the Service Provider IT System
8.6	The Service Provider shall ensure all removable device ports are disabled from the Service Provider IT Systems including any mobile devices handling the Authority Data.
8.7`	Anyone accessing the Service Provider IT System via remote access must (i) access from an authorised and supported end point device which provides encrypted connectivity, is secure and does not introduce risk to the HMCTS service; and (ii) be authorised via multi factor authentication.
8.8	On expiry or termination of the Contract, the Service Provider shall support Business Continuity in accordance with Clause H9 (Retendering and Handover) to Clause H12 (Warrants and Orders on Expiry or Termination) and Schedule 15 and migrate all required information in a readable manner to a replacement Service Provider(s) or to the Authority within the timeline dictated by the Authority free of charge.
8.9	To comply with Section 14.4, the System shall be based as far as feasible on Open Source and Open Data standards.
8.10	The Authority may introduce a new method of delivering data to the Service Provider at any time during the Contract, and the Service Provider shall ensure that their systems are adaptable.
8.11	The Service Provider IT System and associated services shall be maintained and updated in real time.
8.12	The Authority shall have separate secure access to the Service Provider's IT System with a write facility and a real-time view of all of the Authority's Accounts and the facility to enter notes and make requests on the Service Provider's IT System. The Authority shall also be able to download Management Information data and reports from the System.

Access Requirements	
8.13	The Service Provider shall ensure that the System: • provides a robust role based access at all levels from infrastructure and administration through to end user • is able to limit users to a single log in at any one time and any exceptions to this must be clearly identified • has the facility to authenticate Users. All such authentication mechanisms, including passwords, must comply with HMG Security Guidelines, see Cyber Security & Information Assurance Requirements Guidance (Annex 8) and Security Aspects Letter(Annex 9) • https://www.ncsc.gov.uk/collection/passwords?curPage=/collection/passwords/updating-your-approach
8.14	Administrators shall have the ability to reset a User's password and users shall have the ability to change their own password.
8.15	Provides for password reminders in accordance with HMG Security Guidelines.
Archive	
8.16	The System shall be able to access archived data within 24 hours of a legitimate request being made by the Authority.
8.17	It must be possible to identify and securely destroy data that is older than the Retention Period notified to the Service Provider by the Authority.
Audit, Logging and Monitoring	
8.18	The Service Provider shall put in place appropriate monitoring tools and processes to support and maintain the Key Performance Indicators and to provide Management Information in accordance with Schedule 19 (Management Information and Reporting).

8.19	The System shall maintain logs and records for audit purposes. Audit logs and records shall be maintained in a way that facilitates finding or identifying specific items within the log, and which supports a policy of forensic readiness capable of supporting the investigation and response to security breaches.
8.20	The System shall log or record all operations and changes made to data and information. As a minimum, the System should be able to identify Users, the time of System was accessed, the changes and uploads made by the Users
8.21	Audit and monitoring logs and records shall be available to designated “Authorised Users” and the Authority if so requested.
8.22	It shall not be possible to amend or delete any audit trail without a separate audit event capturing these changes.
8.23	Audit and log data shall be held for the same amount of time as the source data it pertains to (i.e. for the same data Retention Period).
8.24	When data or information is changed, a record of the original data must be maintained.
8.25	The System shall not delete from audit and monitoring logs any Authority Data relating to Users.
8.26	The creation and storage of audit logs shall not impact on the performance of the transcription service.
8.27	In the event of error or component failure, the relevant log files must provide enough information to support investigation and isolation of the point and possible cause of failure.
Availability and Resilience	
8.28	The System shall be sufficiently robust and resilient to meet the required hours of operation, with no single points of failure and designed to minimise data loss.
8.29	It must be possible to restore the System to a known point (for example in the event of a failure or for other business reason). In support of this the Service Provider shall provide a backup and storage approach that will ensure that data loss is minimised and that data can be restored within a reasonable period, to be approved by the Authority. See also Schedule 15 Business Continuity and Disaster Recovery Plan.

8.30	Backups shall be verified to ensure that they are capable of being restored and the restore procedures shall be successfully tested on a regular basis - at least annually.
Capacity	
8.31	The System shall be capable of managing and storing the volume of data and information produced by the Service, plus all monitoring, audit and other logs.
8.32	The System shall be able to support the anticipated required number of users as during Normal Working Hours.
8.33	The System shall support changes in capacity and demand as required.
8.34	The System shall support the bulk upload of a variety of file types as required by the Service Provider's operations.
8.35	The System shall have the capability to run management reports as required by the Authority under the terms of this Contract.
Compliance and Policy	
8.36	All Staff working on the System with access to Defendants Data and User Data shall be security cleared to a minimum of baseline standard BPSS.
8.37	The System shall facilitate the Authority's compliance with all applicable Law, including but not limited to provisions for controlling access to Data and monitoring changes.
8.38	The Service Provider shall ensure that the System follows current industry and government best practices for accessibility and shall work with commonly available assistive technologies. The cross government minimum accessibility standard is https://www.w3.org/WAI/WCAG21/Understanding/
8.39	The System shall facilitate compliance with Laws relating to the use of the Welsh language including the Welsh Language Measure 2011.

8.40	The Service Provider shall maintain good practices in respect of coding, development, document management and record keeping which the Authority may access and audit on request.
8.41	The System will meet Cabinet Office digital standards, including prioritising the use of Open Source, Open Standards, Open Data standards and use of common components and services.
Data Integrity	
8.42	The System shall maintain the integrity of information that is processed. It shall ensure that changes are completed and confirmed by the user, and are auditable (and cannot be repudiated).
8.43	Ensures no more than one person can update a record at the same time to minimise the opportunity for errors.
8.44	The System shall validate Data at the point of entry. Data validation will include enforcement of any appropriate and agreed Data standards or formats.
8.45	The System shall provide the means to restore the business Data to a known, consistent state following the discovery of any fault in the application software.
8.46	Data no longer required (subject to retention rules or authorised requests from the Authority) shall be securely removed / deleted in accordance with Cyber Security & Information Assurance Requirements Guidance (Annex 8).
8.47	The Service Provider must ensure the disposal of any electronic storage media used for the Authority Data shall be securely erased and destroyed in accordance with the CPNI Standard for Secure Destruction of Sensitive Items (or an equivalent standard). Please see Schedule 10 Policies and Standards. A certificate of destruction shall be requested by the Service Provider from the company undertaking the destruction and it must be retained upon completion, and a copy provided to the Authority.
Documentation	

8.48	The Service Provider will provide sufficient training and guidance documentation to support independent technical and security assessment of the status of the System as set out in Cyber Security & Information Assurance Requirements Guidance (Annex 8).
8.49	The Service Provider shall keep all documentation up to date to reflect the current state of any technology and procedures associated with the System at all times.
Support, Maintenance, Testing and Service Provision	
8.50	The Service Provider shall support and maintain the System for the Contract Period and shall have a documented service management approach which includes but not limited to incident, problem, change and service level management disciplines.
8.51	The Service Provider shall provide a documented incident management process which should include contact points and escalation process and integrates with HMCTS incident management requirements.
8.52	NOT USED
Interoperability	
8.53	Should the Service Provider's proposal require an interface with other systems as well as with the Authority's own systems. The System shall be capable of importing or exporting data and interfacing with other services using recognised formats or protocols (e.g. XML, SOAP, CSV).
8.54	The Service Provider shall comply with the Authority's terms and conditions relating to access to its systems and in particular to changes that will be required to support HMCTS need.
8.55	It shall be possible to export all data held in the System in a recognised open format such as XML or CSV.
9 SECURITY AND INFORMATION ASSURANCE	
9.1	The System shall be protected by appropriate people, process, technology and physical security controls as part of a 'defence-in-depth' approach. See Security Aspects letter. (Annex 9)

9.2	The Service Provider shall comply with Cyber Security & Information Assurance Requirements Guidance (Annex 8).

9.3	The Service Provider shall have: • a procedure for identifying, evaluating and reporting security incidents which potentially or actually present a risk to the confidentiality, integrity or availability of Authority (including customer) data and the procedure for escalating security incidents to the Authorities Operational Security team as required and in the timescales required by the Authority (Section 14.51) • a robust methodology for ensuring information security assurance and controls are in place to ensure the confidentiality, integrity and availability of Government Security Classified (GSC) Data under its control • a list of dependencies which clearly identify the roles and responsibilities of its Staff • processes and procedures to show how the Service Provider will maintain compliance with vetting requirements for all its staff. • a framework for managing Information Assurance throughout the Contract Period • a process for keeping staff trained and fully aware on information security matters • an approach for risk assessing the Service Provider IT Systems used in providing the Services • an approach to ensuring that Information Assurance is embedded into its ICT change management and project management processes • an approach for undertaking security risk assessments of information in accordance with the requirements of the HMG Security Policy Framework ("SPF"). Please refer to Schedule 10 (Policies and Standards). • an Approach to handling Government Security Classified Data when considering data classification, data in both physical and electronic format, privacy-related legislation, policies, processes and procedures • an approach on how information security requirements will be met if any part of its service includes any element of off-shoring

10. TRANSLATION SERVICE REQUIREMENT	
10.1	The Service Provider shall adhere to all applicable Law in regards to language translation requirements in the conduct of public business and the administration of justice.

10.2	The Service Provider shall ensure that it has a facility to offer translation services for any Defendant where their first language is not English or Welsh to ensure that any customer that wishes to correspond with the Service Provider, either face to face, digitally or by telephone shall be able to do so in their preferred language.
11. USE OF FORCED ENTRY	
11.1	This procedure covers any instances where the Service Provider considers it necessary to use reasonable force to gain entry to a property in order to execute a Warrant of Control. The Service Provider shall adhere to all applicable Law and Good Industry Practice.

11.2	The Service Provider shall maintain an electronic database on the Service Provider IT System of all Forced Entry requests and their outcomes and be available to be provided to the Authority on request. The record shall include: • date and time the Authority Nominated Officer approval was requested • date and time of when the Service Provider receives the decision of the Authority Nominated Officer • Warrant Type (Warrant of Control) • name of Defendant • issuing Court and Warrant number • name and number of Service Provider's Field Operative and other staff in attendance • address where the Forced Entry was gained/attempted • details of others in attendance i.e. Police officer including name and number, locksmith including the company name, Court officials and others • a concise narrative of the event as it unfolded, including if Forced Entry proved necessary and if any force was necessarily used to restrain the Defendant. There must also be a record made of any damage to the Defendant or third party property. Where no damage has arisen then a nil return shall be recorded • the outcome including if taking control of goods was successfully executed • details of action taken to secure the property • what, if any, further action has been agreed with the Authority Nominated Officer or the Defendant Following the use of any Forced Entry the outcome shall be fully updated on the Service Provider's Forced Entry database within 1 (one) Working Day.

Entry to take control of goods (Warrant of Control)	
11.3	Prior to using Forced Entry the Service Provider shall ensure that the authority to use Forced Entry is applicable to the individual circumstances at the time.
11.4	No Forced Entry to take control of goods against a Defendant shall be attempted without securing approval of the Authority. Where applicable an application to the Court shall be made by the Service Provider using the agreed method and complying with all applicable Law. Responsibility for the actual Forced Entry will remain with the Service Provider.
11.5	Before approval can be given the Service Provider shall contact the Authority Nominated Officer via the agreed method to explain the circumstances and reasons for requesting approval to use Forced Entry and the method which is to be used i.e. use of a locksmith. This shall be short and to the point and in accordance with a format agreed with Authority. All requests for approval to use Forced Entry shall be recorded on the Defendant's record on the Service Provider IT System, together with the Authority decision. This update shall include times and dates and be recorded within 30 (thirty) minutes of receiving the decision from the Authority.
11.6	Where approval is refused further dialogue shall be undertaken between the Service Provider and the Authority within 1 (one) Working Day to agree a suitable way forward.
11.7	Following a Forced Entry, it is the Service Provider's responsibility to ensure that the premises have been secured.
11.8	The Defendant's record on the Service Provider IT System shall be updated with details of the actions and outcome of any approved Forced Entry request within 1 (one) Working Day of the conclusion of the visit.
11.9	The Defendant's record on the Service Provider IT System shall be updated with details of any refused Forced Entry request within 1 (one) Working Day of the refusal.

12.	VULNERABLE DEFENDANT AND OTHER CIRCUMSTANCES WHEN NOT TO PROCEED WITH ENFORCEMENT ACTIVITY UNTIL FURTHER ENQUIRES HAVE BEEN MADE
12.1	Claims of vulnerability shall be taken seriously by both the Authority and the Service Provider. These claims may be received via the Authority or to the Service Provider directly, by the Defendant or via appointed third party (e.g. family, friend, medical practitioner or organisations such as Citizens Advice Bureau (CAB). Legislation governing enforcement action does not define vulnerability. It requires, instead, a Field Operative to assess each case on its own merits rather than rely on a definition that does not cover every eventuality. Vulnerability is a potentially fluid state, so that some people might be constantly vulnerable (for example due to a permanent lack of mental capacity) but others temporarily (for example, suffering mental illness for a short period of time). The Service Provider shall ensure they have in place a procedure to manage all claims of vulnerability, and that these are handled in an appropriate and timely manner. All details relating to the vulnerability claim shall be treated as sensitive and the data protected accordingly. The Service Provider shall ensure compliance of this procedure. The Service Provider shall ensure that all Staff receive mandatory training which includes specific approved training on identifying and dealing appropriately with vulnerable persons. The Service Provider shall inform the Authority on the day that claims of vulnerability are received. The Service Provider shall have named Nominated Officer responsible for assessing and managing all claims of vulnerability. The Authority reserves the right to withdraw enforcement action where there is evidence that the Defendant is vulnerable and enforcement would not be in the interests of justice or may bring the Service Provider or department into disrepute. Where any Warrant or Order is requested back for this reason, the Service Provider shall not charge the Authority for request and the return of the Warrant or Order. Vulnerability is not always claimed in advance and the Service Provider may only become aware a Defendant may fall within the vulnerability procedure during attendance at the Defendant's property.

12.2	Whilst the list below is not prescriptive or exhaustive, these are examples of vulnerability: • is in hospital or nursing home • appears to suffer from severe physical or any mental disability • is an elderly person who has difficulty dealing with his/her affairs • is suffering long term sickness, serious or acute illness or frailty, which has resulted in a recent period of hospitalisation or Defendant being housebound and can provide evidence of sickness for the period in default • has suffered a recent bereavement of close/immediate family member • is heavily pregnant • has a genuine communication problem
12.3	Below are examples of when not to proceed with enforcement activity until further enquires have been made whether or not the Defendant is making any claim in respect of vulnerability: • Defendant produces evidence to show that account has been paid • Defendant claims to have made a Statutory Declaration, or other application has been made to the Court or the Authority, for example an appeal; and any conviction or sentence or Warrant or Order has been set aside or withdrawn by the Court or the Authority; in accordance with the appeals requirement • in circumstances where the Service Provider has doubts as to the identity of the Defendant or considers that to proceed with enforcement may prejudice the reputation or credibility of either party to this Contract • any other circumstance in which the authorised employee would consider it prudent to contact the relevant Court enforcement office

12.4	**Managing the claim** The Service Provider shall consider all claims of vulnerability however received e.g. via the Authority or the Defendant or appointed third party, the Field Operative during a visit, the claim can be made via a telephone call, text message, e-mail; written or in person to the Service Provider. All claims of vulnerability shall be recorded on the Defendant's record on the Service Provider IT System within 1 (one) Working Day of receipt. The Service Provider will place the Warrant or Order on hold until vulnerability has been assessed and a decision made on how to proceed. If during door step enforcement activity, the Field Operative suspects that vulnerability, they shall immediately cease any action and explain to the Defendant or appointed third party of what will happen next. They shall then contact the Service Provider's named Nominated Officer and ensure that all details are recorded on the Defendant's account on the Service Provider's IT System. In all cases the Nominated Officer shall: • communicate with the Defendant to confirm that the claim is being treated under the vulnerability procedure and send them a copy of the procedure and inform the Court's Nominated Officer via e-mail (including timescales) • given the nature of this procedure, common sense should be used, particularly where documentary evidence is not easily to hand in support of a claim • identify which reason the claim is being considered under • if evidence has not been provided, consider requesting for further evidence shall be sent to the correspondent and / or the Defendant, as appropriate • if the vulnerability is suspected by a Field Operative during the visit the officer shall provide a full report including all relevant details to the Service Provider's named Nominated Officer for consideration

	Once the Nominated Officer has made their initial assessment they shall liaise with the Authority to agree the outcome and where appropriate agree any control measures that can be utilised in order to enable enforcement action to continue. Once the initial assessment has been completed and agreed with the Authority Nominated Officer, the Service Provider's named Nominated Officer will communicate the outcome to the Defendant or their appointed third party. This may be that: • vulnerability is agreed, and the case is being returned to the Authority • vulnerability is agreed however options for control measures have been agreed to enable the case to be enforced • vulnerability is not agreed and enforcement action is to continue as ordered by the Court In all cases the Service Provider will update the Defendant's record on the Service Provider IT System within 1 (one) Working Day. In all cases all actions, communications and decisions shall be recorded on the Defendant's record on the Service Provider IT System. Where following agreement with the Authority that no further enforcement action shall be taken, the Warrant or Order is to be completed on the Service Provider IT System and returned to the Authority using the agreed Return Codes. In these circumstances the Service Provider shall not charge the Authority for request and the return of any Warrant or Order.
12.5	Vulnerability cases will be reported as part of the agreed reporting, as outlined in Schedule 19 (Management Information and Reporting).
12.6	A copy of the Service Provider's vulnerability procedure, which shall include the name and contact details for the named Nominated Officer and their deputies, shall be provided to the Authority.
13. WARRANT OF CONTROL – ISSUED FOR FINE IMPOSITIONS	
General Requirements	

13.1	The Service Provider shall adhere to all applicable Law and Good Industry Practice when executing Warrants of Control, including in relation to the recovery of all Fees.
13.2	If the Service Provider is notified that a Magistrates' Court has issued a Warrant of Control in respect of a sum which is enforced or enforceable; or recoverable as a civil debt, the Service Provider shall execute that Warrant of Control in accordance with all applicable Law including the Magistrates' Courts Rules 1981.
13.3	Fees may be returned to the Defendant following an Appeal in accordance with Section 3 (Appeals) of this Schedule being made after the Defendant has paid the fees to the Service Provider. The Authority may at its discretion negotiate with the Service Provider a return of these costs to the Defendant.
13.4	Where the Authority requests the return of a Warrant because it was issued in error, the Service Provider will refund any relevant monies including fees received from the Defendant or a third-party payee.
13.5	If the Service Provider requires any application in relation to a Warrant of Control, the request with all supporting information shall be sent to the Authority in the agreed format. The Service Provider will update the Service Provider IT System with details of the application; the outcome will be updated on the Service Provider IT System within 30 (thirty) minutes of receipt.
Enforcement Activity	
13.6	The Service Provider will issue an Initial Contact Notice to the relevant Defendant within 10 (10) Working Days of the Warrant being entered onto the Service Provider IT System in order to encourage the Defendant to make contact with the Service Provider and make full payment of the amount owing.
13.7	Where applicable, following the issue of an Initial Contact Notice and up to the enforcement stage of the Warrant of Control, the Service Provider shall make additional attempts to contact the Defendant (including by text, telephone or email) in order to obtain full payment of the amount owing.

13.8	The Service Provider and the Defendant shall arrange for the amount owing to be paid by instalments which will satisfy the Warrant in full within a maximum of 365 calendar days from issue. If instalment Payments are agreed with the Defendant, the Service Provider shall ensure the details are updated on the Defendant's record on the Service Provider IT System.
13.9	Where the Service Provider has been unable to either obtain full Payment of the outstanding amount or made any agreement to pay the Service Provider shall attempt to execute the Warrant by conducting an initial personal visit to the Defendant, this first visit shall be carried out no later than 60 (thirty) days from date issued on the Service Providers IT System.
13.10	If no contact is made the Service Provider shall carry out further visits – a minimum of 3 (three) visits on different days and at different times of the day to include early morning and evening shall be undertaken within the initial Retention Period.
13.11	Upon receipt of a payment taken when conducting a visit, the details shall be updated on the Defendant's record of the Service Provider IT System as soon as practicable to record both the details and value of any Payment taken and include the method of payment within 1 (one) Working Day.
Taking control and sale of Goods	
13.12	The Service Provider shall use all reasonable endeavours to obtain the best value for all goods sold, and consider reserves on high value goods.
13.13	Where the sale of the goods is not sufficient to make full payment of the amount owed by the Defendant, the Service Provider shall apply the sums in accordance with the legislation and pay the balance outstanding to the Authority. In these cases the Service Provider shall contact the Authority to discuss whether the Warrant of Control shall be returned to the Authority or further enforcement action can be taken by the Service Provider.
13.14	Where the sale of the goods taken control of realises a sum greater than the amount owed by the Defendant, the Service Provider shall apply the sums in accordance with the legislation and pay any outstanding balance owed to the Authority. The Service Provider shall update the Defendant's account on the Service Provider IT System to provide a full audit trail that money in excess of that which was owed has been returned.

Managing unexecuted and cancelled Warrants of Control	
13.15	Any requests by the Service Provider to extend the Retention Period of a Warrant of Control shall be in accordance with the agreed process and timeframes as set out within the Retention Period schedule. All applications for an extension period and the Authority's decision on the application shall be updated on the Defendants record on the Service Provider IT System within 1 (one) Working Day.
13.16	At the end of the Retention Period the Service Provider will complete the relevant Warrants of Control on their system and confirm return to the Authority, this confirmation will contain details of all Warrants an outline of all efforts made to execute the Warrant including the number, dates and times of visits, and any intelligence tracing undertaken, details of any contact made by the Defendant or third parties, any payments arrangements made and payments taken. All Warrants will be returned using the agreed Return Codes.
13.17	The Authority may withdraw or recall any Warrant of Control if the financial penalty to which it has been issued against becomes subject to an Appeal, S142 application, Statutory Declaration or other legal instrument; or it has been withdrawn by the Court or the Fines Officer to allow consolidation of accounts or because it has been issued as a result of a mistake. In such cases the Authority will inform the Service Provider, who will update the Service Provider IT Systems according to the instructions of the Court within 30 (thirty) minutes. Where any Warrant of Control is requested back because it is permitted legally or within any of the Contract terms, the Service Provider shall not charge the Authority for request and the return of the Warrant of Control.
13.18	Service providers are only entitled to retain assets for the purposes of sale for the duration the warrant is active, including any extensions granted by the Authority.
14. WELSH LANGUAGE	
14.1	The Service Provider shall adhere to all applicable Law and the Authority Welsh language Scheme that states that in the conduct of public business and the administration of justice in Wales it will treat the Welsh and English languages on a basis of equality.

14.2	For services being delivered in Wales, the Service Provider shall ensure that the number of Welsh speaking employees reflects the language profile of Wales, if it is less, the company shall provide intense Welsh language lessons in order to ensure that they meet the demand within four years.
14.3	The Service Provider shall ensure that all documents including business cards that are sent to the Defendant within Wales shall be bilingual. Any Defendant that wishes to correspond with the Service Provider, either face to face, digitally or by telephone shall be able to do so in their preferred language.

Annex 1: Definitions

TERM	MEANING
Appeal	means any proceedings taken in accordance with Section 3 (Appeals) of this Schedule 1.
Applicant	means the Defendant or a third party making an application on the Defendant's behalf.
Authority Accounts	means any accounting board or authority (whether or not part of a government) which is responsible for the establishment or interpretation of national or international accounting principles, in each case whether foreign or domestic.
Authority Nominated Officer	means the individual delegated by the Authority to undertake a specific task in accordance with this Contract.
Authority's Protocol	means agreement between the Service Provider, PECS and the Authority set out under Schedule 10 (Policies and Standards).
BACS	means Bankers' Automated Clearing Services.
Business System Owner (BSO)	means an individual responsible for the overall procurement, development, integration, modification, operation, maintenance, and retirement of an information system.
Change Management	means the processes by which the actions required to make change happen, either within an organisation or to that organisation's external stakeholders or the environment in which they operate, can be managed.
Charge Backs	means rejected credit and debit card payments.
Charges	has the same meaning as Fees.
Costs	has the same meaning as Fees.

County Court	means a Court dealing with civil matters which can hear family or business cases.
Court Imposition	means any Court order or financial imposition treated as a sum adjudged to be paid by the conviction or order of a Magistrates' Court.
Court Staff	means personnel who performs various administrative and court duties.
Court User	means people across the country who benefit from the services provided by Her Majesty Courts & Tribunals Service.
CPNI Standard for Secure Destruction of Sensitive Items	means the standard operated by the Centre for the Protection of the National Infrastructure.
Daily Bank Reconciliation	means the process of matching the balances in an entity's accounting records for a cash account to the corresponding information on a bank statement.
Data Disclosure Order	means an order which can be applied for to the Court requiring a specified person or company to provide data in relation to the person named on the Order.
Defendants Data	means the information kept by the Authority for an individual in relation to a court order.
Execution Activities	means activities undertaken by the Service Provider to execute or progress warrants, this can include tracing and doer step activities
Fees	means any and all statutory fees which the Service Provider is entitled to recover in connection with the execution of Warrants of Control in accordance with the rates and terms set out in the Warrant of Control Legislation.
Forced Entry	means to enter a person's property by force and against the occupants wishes.
Guardian	means person responsible for a Youth.

Her Majesty's Government (HMG)	means a formal term referring to the UK government.
Her Majesty's Courts and Tribunals Service (HMCTS)	means combined Her Majesty's Courts Service and the Tribunals Service into one integrated agency providing support for the administration of justice in courts and tribunals in England and Wales. HMCTS is an agency of the Ministry of Justice (MoJ).
HMG Security Policy Framework ("SPF")	means the security policy framework included under Schedule 10 (Policies and Standards).
IAO	means Information Asset Owner
ICT	means Information and Communication Technology
Information Assurance (IA)	means the practice of protecting against and managing risk related to the use, storage and transmission of data and information systems.
Initial Contact Notice	means a written notice sent to the Defendant following the Service Provider's receipt of the Warrant or Order, to inform the Defendant of the Warrant or Order and provide the following information: (i) full details of the Warrant or Order, (ii) the actions that the Defendant should take, (iii) the consequences of failing to take those actions and (iv) the contact details of the Service Provider.
Intelligence Tracing Tools	means systems available to Service Provider to assist in locating the whereabouts of a Defendant.
International Organization for Standardization (ISO)	Means an international standard-setting body composed of representatives from various national standards organizations.
Internet Protocol (IP)	means the method or protocol by which data is sent from one computer to another on the internet.
Letter of Authority	means a document that gives another person, known as an "agent", the authority to act on behalf, of the Authority.

Memorandum of Understanding	means the formal agreement between HMCTS and the Police on the use of the Police National Computer.
Minister	means a person in charge of a government department.
National Audit Office (NAO)	means an independent Parliamentary body in the United Kingdom, which is responsible for auditing central government departments, government agencies and non-departmental public bodies.
National Compliance and Enforcement Service (NCES)	means HMCTS Teams who are responsible for the collection and enforcement of fine impositions
National Cyber Security Centre (NCSC)	means an organisation of the United Kingdom Government that provides advice and support for the public and private sector in how to avoid computer security threats.
National Probation Service (NPS)	means a statutory criminal justice service within the Authority that supervises offenders in the community.
Nominated Officer	means the person responsible for the area of work
Normal Working Hours	9am to 5pm
Offender Additional Information Sheet (OAIS)	means an information sheet provided by the National Probation Service or the Youth Offenders Service giving additional personal information in respect of those Defendants who are subject to Breach Warrants.
Open Data	means data that anyone can access, use and share.
Open Source	means a program whose source code is made available for use or modification as users or other developers see fit. Open source software is usually developed as a public collaboration and made freely available.
Open Standards	means standards that are made available to the general public and are developed (or approved) and maintained via a collaborative and consensus driven process.

Order for Sale	means an Order of the Court for the sale of a vehicle clamped in accordance with courts Act 2003 and the Fines Collection Regulations 2006.
Parent	means person responsible for a Youth.
Payment	means an amount of money from a Defendant or third party towards the outstanding Court Imposition due on the Warrant or Order that is paid to someone, or the act of paying this money.
PCI Data Standards	means Payment Card Industry Data Standards that help to protect the safety of data. A set of security standards designed to ensure that all organisations that accept, process, store or transmit credit card information maintain a secure environment and set standards for the operational and technical requirements organisations have to adhere to.
Personal Contact Visits	means an attendance by a Field Operative of the Service Provider at an address with a view to executing the Warrant or Order of the Court.
PNC	means the Police National Computer.
PNC Information	means information obtained from PNC – vehicle registration information.
Public Service Network (PSN)	means the government's high-performance network, which helps public sector organisations work together, reduce duplication and share resources.
Refer to Drawer Cheques	means dishonoured cheques.
Remittance	means a letter or other communication sent by the Service Provider to confirm payment of an amount.
Security Aspects Letter (SAL)	means a set of special contractual conditions, issued by the Authority in the form set out under Annex 9.

Senior Information Risk Officer (SIRO)	means a member of the senior management board of an organisation with overall responsibility for an organisation's information risk policy. The SIRO is accountable and responsible for information risk across the organisation.
Statutory Declaration	means a formal written statement of facts declared to be true and signed by the declarant before any solicitor, justice of the peace, notary public, or other person authorised to administer an oath.
Suspense Item	means a transaction in an account in the general ledger (also called “Suspense Account”) for which there is uncertainty about that transaction.
System	has the meaning given in Section 14.1 (IT).
Tracing Activity	means the act of tracing a person using tracing systems available.
User Data	means data created by a User.
Users	means a person who uses the System.
Working Hours	means hours worked by Authority staff which is 8-5pm Monday to Friday
Youth	means a young offender aged 10 (ten) to 17(seventeen).

Annex 2: Regions and Areas

The Table below shows the HMCTS Regions and the Areas that fall within each Region:

London- Lot 1	South East - Lot 2	Midlands - Lot 3	North East - Lot 4	North West- Lot 5	South West - Lot 6	Wales - Lot 7
Greater London	Bedfordshire & Hertfordshire	Derbyshire	Cleveland	Cheshire	Avon & Somerset	Dyfed Powys
	Cambridgeshire	Leicestershire	Durham	Cumbria	Devon & Cornwall	Gwent
	Essex	Lincolnshire	Humberside	Greater Manchester	Dorset	North Wales
	Kent	Northamptonshire	Northumbria	Lancashire	Gloucestershire	South Wales
	Norfolk	Nottinghamshire	North Yorkshire	Merseyside	Hampshire & Isle of Wight	
	Suffolk	Staffordshire	South Yorkshire		Wiltshire	
	Surrey	Warwickshire	West Yorkshire			
	Sussex	West Mercia				
	Thames Valley	West Midlands				

Annex 3: List of Warrants

The table below contains a list of the Warrants that the Service Provider may execute on behalf of the Authority, and may be updated from time to time in accordance with applicable Law.

Type of Warrant	**Description**	**Allocating body**
Section 76 (1) of the Magistrates' Court Act 1980	Warrants of control (previously distress Warrants) and Warrants of commitment for default in paying a sum adjudged to be paid by a conviction or order of a Magistrates' Court	NCES

Annex 4: Standard Warrant and Order Return Codes and description

Abbreviation used in table below	Warrant or Order
WOC	Warrant of Control

Returned Code	SECONDARY PROVIDER - Description of Return Code	Warrant / order type code can be used for
Payment in Full (Successful)	The Warrant or Order is satisfied by payment in full (cleared funds).	WOC
Returned - Abroad (Progressed)	The Service Provider submits evidence that Defendant has moved aboard.	WOC
Returned – Bankrupt (Progressed)	The Service Provider submits evidence that Defendant has been declared bankrupt.	WOC
Returned – Company in Liquidation/dissolved (Progressed)	The Service Provider submits evidence that the company is in Liquidation or has been dissolved.	WOC
Returned – Debtor Deceased (Progressed)	The Service Provider submits evidence that defendant is deceased.	WOC
Returned – Debtor Serving Sentence (Progressed)	The Service Provider submits evidence that the Defendant is serving a custodial sentence.	WOC
Returned – Field Operative Threatened (Progressed)	The Service Provider submits evidence that the Warrant or Order is deemed unsafe for the Field Operative to execute and Police assistance cannot be obtained.	WOC
Returned – Gone Away No Trace (Progressed)	The Service Provider submits evidence that the Defendant as moved away and no new information regards the Defendants address or whereabouts can be established following intelligence checks undertaken within the Retention Period.	WOC

Returned Code	SECONDARY PROVIDER - Description of Return Code	Warrant / order type code can be used for
Returned - insufficient data to enforce (Progressed)	The details of the Defendant are incomplete on the Warrant or Order for example: the name only states Mr Smith; no date of birth; No Fixed Abode address; and all efforts to identify and or trace the Defendant have failed.	WOC
Returned – insufficient goods (Progressed)	The Service Provider submits evidence to support that Defendant does not have sufficient goods and payment terms have not been agreed with the Defendant.	WOC
Returned - Issued in Error (Progressed)	Use only for specific requests from issuing Court	WOC
Returned - No Contact (Progressed)	The Service Provider submits evidence that following a minimum of 3 visits to the last known address no contact has been made with the Defendant and intelligence checks are unable to verify the Defendants residency at that address or their whereabouts.	WOC
Returned – No monies received as result of vehicle/goods sale at auction (Progressed)	The Service Provider must submit full details	WOC
Returned – Time Expired (Progressed)	This is only to be used where part payments have been received on a Warrant and the Authority has refused to extend the Retention Period.	WOC

Returned Code	SECONDARY PROVIDER - Description of Return Code	Warrant / order type code can be used for
Returned - Unable to access (Progressed)	The Service Provider submits evidence that the Field Operative was unable to gain access to the address/ building despite a minimum of 3 visits and all options to gain entry have been tried. This includes travellers/hostel site where Field Operatives are unable to access site and there is no liaison officer to assist and no Police assistance can be obtained.	WOC
Returned - Unable to locate (Progressed)	The Service Provider submits evidence that the address cannot be located or does not exist and intelligence checks are unable to verify the Defendants new address or whereabouts.	WOC
Returned - Vulnerable (Progressed)	The Service Provider submits evidence that the Defendant is vulnerable and the Warrant or Order cannot be executed.	WOC
Withdrawn by the Court (Deduct from issued figure)	Where any Warrant or Order is requested back by the Authority because it is permitted legally or within any of the Contract terms.	WOC
Withdrawn by the Court – for consolidation (Deduct from issued figure)	Where any Warrant or Order is requested back by the Authority because it is permitted legally to enable consolidation of accounts.	WOC
Withdrawn by Court Stat Dec/ Sec 142/Appeal (Deduct from issued figure)	Where any Warrant or Order is requested back by the Authority because it is permitted legally or within any of the Contract terms.	WOC

Returned Code	SECONDARY PROVIDER - Description of Return Code	Warrant / order type code can be used for
Low propensity to pay (Progressed)	Where the Defendant is assessed as unlikely to have the means to pay, and would be costly to enforce the Warrant - to have a low propensity to pay.	WOC
Assessed as High Risk (Progressed)	Where the Service Provider has assessed the Defendant or location of the address as high risk area. Service Provider to provide reason for their decision.	WOC

Annex 5: Table of Retention Periods

Warrant of Control
180 (one hundred and eighty) calendar days from date of issue; extending to 365 (three hundred and sixty-five) calendar days if a payment agreement is in place when the extension request is made. All extensions are by agreement with Authority and will be 30 (thirty) calendar day extension periods, to a maximum of 365 (three hundred and sixty-five) calendar days from date of issue.

Annex 6: Associated Process Maps

Process maps related to the procedures set out in this Schedule may be provided by the Authority to the Service Provider from time to time.

Process maps relating to Warrants of Control are as provided in Schedule 1A.

ANNEX 7 – NOT USED

Annex 8: IT Cyber Security & Information Assurance Requirements Guidance

https://www.gov.uk/government/publications/cyber-essentials-scheme-overview

Annex 9: Security Aspects Letter

HM Courts & Tribunals Service

Information Assurance
102 Petty France (5.31)
London,
SW1H 9AJ
T 020 3334 3555
ICT.IA&S@justice.gsi.gov.uk
www.justice.gov.uk

Dear Service Provider
Subject: Security Aspects Letter – HMCTS

This Security Aspects Letter, hereafter known as SAL, establishes the security provisions with which the Supplier shall comply in producing, handling or storing OFFICIAL material pertaining to Her Majesty's Courts and Tribunal Services (HMCTS), hereafter referred to as "The Authority".

This letter applies to the Supplier and any subcontractor within the Supplier supply chain as required. The Supplier's contractors are under the same obligations as the Supplier.

The Authority reserves the right to conduct a design review on the architecture of the service procured at any time, and one may be required prior to signing the contract. The design review may be carried out by The Authority or a nominated third party.

All services provided by the Supplier and their subcontractors are to be Cyber Essential or Cyber Essential plus and ISO 27001 certified.

This letter formally advises the classification to apply to the various security aspects of HMCTS.

This SAL has been developed under the premise that all Information Assets pertaining to The Authority will be classified OFFICIAL and that some may carry the OFFICIAL – SENSITIVE marking. All information must be considered OFFICIAL whether it bears a marking or not. Material that is to be considered OFFICIAL – SENSITIVE must be marked as such. The SENSITIVE marking caveat requires access to the information to be on a need to know unless otherwise stated within the documentation. Items considered as OFFICIAL-SENSITIVE include but are not limited to;

- IP addresses,
- Security Vulnerabilities,
- known risks to the data, applications and infrastructure,
- detailed designs of points ingress and egress into the infrastructure,
- management accounts and authentication credentials.

Where Open Source code is used the marking will remain OFFICIAL. Where source code is of a sensitive nature the source code shall carry the existing marking i.e. OFFICIAL- SENSITIVE will remain OFFICIAL-SENSITIVE and will be handled in accordance with the additional handling requirements for the SENSITIVE marking.

The source code is considered to be marked at OFFICIAL. This applies to Production, Development and Test environment. Assurance is required for Production. Development and Test environments do not require formal assurance. The source code, infrastructure documentation and configurations for development and test are to be OFFICIAL and handled and stored accordingly. Information Assurance is required for any systems handling production data. Development and Test systems must follow the same access and security controls as Production but due to the nature of the systems, they do not require formal HMCTS Information Assurance, however the documentation must be protectively marked accordingly.

Production data cannot be used in Development or Test systems without the express written consent of The Authority's Information Asset Owner (IAO), Business System Owner (BSO) and Senior Information Risk Officer (SIRO). Where production data is required in Development and or Test, the data will be anonymised by the Supplier removing all personal identifiable data before being imported into development or test environments.

It should be noted that assigning an appropriate classification to information remains the responsibility of the creator or owner of the asset. The Authority may also provide handling instructions which the Supplier should comply with. If no handling instructions are provided by The Authority, the Supplier must assume the data to be at OFFICIAL and system, infrastructure and source code to be OFFICIAL – SENSITIVE with access to the OFFICIAL – SENSITIVE information on a need to know basis only.

Due to the role the Supplier is performing on behalf of The Authority, all documents handled will be classified OFFICIAL and in exceptional circumstances you may be handling OFFICIAL documents with more constrained distribution which are OFFICIAL documents with a SENSITIVE caveat applied and therefore labelled 'OFFICIAL-SENSITIVE' where the originator will state additional handling requirements. These will be items such as network diagrams, security incident reports etc. As such all documents that require additional controls must only be stored on approved and agreed networks or within the Public Service Network (PSN). Documents Protectively Marked under the previous classification of RESTRICTED will be handled at OFFICIAL unless otherwise stated.

In order to assist in interpreting the requirements that need to be met to handle information of the types indicated above, the Supplier shall comply with HMG security policy, including the Security Policy Framework; ISO27001:2013 and ISO27002:2013.

The majority of the IT security requirements for handling OFFICIAL data will be satisfied by the National Cyber Security Centre (formally CESG) guidance however, it is noted that, based on the risk assessment of the system or service, additional controls may be required to provide the required level of assurance, these additional controls will be documented by The Authority upon request.

Sites where The Authority's live data is processed must have physical security characteristics appropriate to the handling of OFFICIAL information. These must be in

line with The Authority's policy on physical security baseline controls and based in the United Kingdom. The sites authorised to hold and handle OFFICIAL assets are:

- Supplier sites
- All Authority Sites

All personnel assigned to HMCTS must achieve security clearance to at least BPSS. Personnel who have access to HMCTS operational data must achieve Enhanced Check BPSS. Personnel who have access to certain sites indicated by The Authority must have Vetting and Barring checks (formerly CRB). Personnel who have uncontrolled access to, or administration privileges to ICT systems containing The Authority's information assets must achieve security clearance to HMG Security Check (SC). This includes all support and development staff with administrative privileges. Personnel who develop code on the Development and Test systems must achieve security clearance to at least BPSS before being assigned access to the code or systems and must, within a period of six months of their start date, achieve HMG Security Check (SC). Any Security Check (SC) applications that extend the six-month period shall be risk managed by the Supplier and HMCTS informed of any developments. Any developer who is not able to achieve HMG Security Check will have their access to the systems and data revoked.

All required security clearances must be achieved, and The Authority informed, prior to commencement of work on HMCTS systems by the individual unless otherwise agreed. Full details of security clearance requirements are available with the Authority vetting policy.

ICT systems used to produce, process or store any of the security aspects identified above must be subject to formal security accreditation by The Authority and must achieve formal Authority assurance prior to any OFFICIAL data being processed there. Where the Supplier require formal Assurance, a request must be made to The Authority to sponsor the assurance process and the Supplier provide the appropriate resource. Where cloud services are used, The Authority will assess the cloud service provider and any additional security controls provided with the solution development as part of the solution assurance process.

The Supplier shall agree a method for the secure exchange of information assets with The Authority via electronic means. This means all Authority or Authority related data that require privacy must stay within the approved systems. This will require data in transit encryption and data at rest encryption for all of the Authorities related data.

The Supplier shall utilise their NCSC (formally CESG) Certified Professional (CCP). Security resource in understanding HMG IA requirements, and where necessary should seek guidance from The Authority including the HMCTS SIRO and IAO.

The Authority reserves the right to issue a revised SAL should The Authority amend its business impact assessment, the protective marking of the data and system or the level of protection required,

The Authority consider HMCTS.NET, justice.gov.uk and CJSM email addresses to provide adequate security to receive data marked at OFFICIAL including documents marked as OFFICIAL – SENSITIVE. Should the Supplier wish, they may encrypt attached documents and provide the Authority with the ability to decrypt the attachments.

You are requested to acknowledge receipt of this letter and your acceptance of its terms as incorporated into your contract and binding. You are also requested to confirm that the level of classification associated with the various aspects listed above have been brought to the attention of the personnel directly responsible for the security of the services provided to or in support of The Authority, that they are fully understood, and that the security and information assurance requirements set out in the contract schedules can and will be taken to safeguard the material concerned. You agree to provide a SAL in similar form to all subcontractors, obtain their acknowledgement and provide a copy to The Authority

Yours sincerely,

Balaji Anbil

Head of Digital Architecture and Cyber Security

Michael Hanley

Head of Information Assurance & Security/Deputy SIRO