[4.1] Telephony and IT Solution

Provide details of your Telephony systems and equipment, including indexing, storing and retrieving electronic calls; including:

- A full Telephony and IT system and equipment specification;
- How you ensure that the Telephony and IT systems and equipment you will use to deliver are secure and auditable;
- The capacity/scalability of your systems and equipment;
- How it meets the telephony standards required by the Authority, including in queue messaging requirements such as long wait times, business disruption and out of hours treatment;
- Details of your plan to accurately capture, store and transfer (via Symantec PGP encryption or similar as directed by the Authority) customer data (especially sensitive personal data records – aggregated and un-aggregated), in line with Departmental Information Systems Security Standards and Cabinet Office security standards (Security Policy Framework);
- Details of the MI production capabilities, how those MI capabilities meet the requirements in the Statement of Requirements both in real time and historically;
- Arrangements for DWP to supply and maintain audio message files to be uploaded as needed;
- Details of your process to ensure DWP information can be archived in accordance with DWP requirements;
- Support and maintenance arrangements for your telephony and IT system and equipment, and provision of back-up systems and equipment for Disaster Recovery;
- How you will operate and manage the various call recording and retention requirements to meet DWP requirements;
- The facility for three-way conference call, when accessing the Authority's translation service;
- How you will deal with service interruptions due to unavailability or slow running of DWP systems;
- DWP wishes to be assured that all data will be handled adequately and proportionately secured, in line with the relevant DWP Security Standards and Policies. Please describe as a minimum:
    - Security Incident Management & Reporting;
    - Secure destruction and sanitisation of physical media used to store DWP data e.g. paper documents, CDs, IT equipment etc.;
    - Access controls and segregation of the LAN, IT equipment and staff;
    - Storage of information including call recordings;
    - Transfer of information;
    - Describe any sub-contracting arrangements and access to call recording;

- Outline the call recording systems to be utilised;
- Include specific detail on your Disaster Recovery provisions including time to resume normal service;
- Details of your controls to ensure safe and timely destruction of DWP data when it is no longer necessary to be held.

Supplier Name	*G4S*	**Package**	*Package A*

Present your response, within these pre-set side margins, in Arial font size 12, up to 5 sides of A4.

G4S will provide a telephony and IT solution which meets the Statement of Requirement (SoR) sections 7 and 8, including indexing, storing and retrieving electronic calls. The telephony solution (including call recording and management information) will be provided by {Redacted} using their Software-as-a-Service cloud based platform, {Redacted}. This is a secure industrial strength service which G4S uses on other contact centre services. It is fully integrated to our Workforce Management solution from {Redacted}. IT equipment comprises: desktop of equipment for team leaders and management staff (to manage the service); Ethernet cabling to all desks for connection to IP telephones and DWP desktops; printers; and networking infrastructure in our contact centre. The Case Management System (CMS) will be DWP provided and connected to G4S provided cabling physically air-gapped from G4S equipment and cabling.

Full Telephony and IT Specification: Using our Wath-upon-Dearne contact centre, G4S will provide a secure comms room for our local infrastructure with controlled access, lockable equipment racks and minimum of CAT5e cabling. This infrastructure will connect to the {Redacted} platform. Local infrastructure will be provisioned with segregated cabling, ports and switching to enable Agent connectivity to the {Redacted} platform. All contact centre and telephony functions are delivered through {Redacted}, allowing G4S to use the inherent scale, flexibility and resilience of a cloud service. The {Redacted} suite of applications satisfies all contact centre Agent interfaces, supervisor interfaces, administrative applications, real-time monitoring (including engineer access), call recording and storage (up to 72 months) capabilities as required in SoR 7.3. The high level architecture is given overleaf. The {Redacted} platform is embedded into the G4S MPLS platform (certified to CAS-T appropriate for the classification of data to 'OFFICIAL') to deliver optimal service performance. Mirroring the technical makeup of the platform, the {Redacted} network is designed to ensure no single points of failure, meaning that the failure of a single node or any other network component will not cause service disruption but instead trigger automatic failover on to an alternate route. Through the Audio Conferencing Module (ACM) the {Redacted} platform provides Audio Conference Bridge, providing the facility for multi-caller conversations. Embedded within tier one carrier network infrastructure, the platform connects to the PSTN (Public Switched Telephony Network) to make/receive calls and send/receive SMS messages. TDM and VoIP calls are handled by INX (Intelligent Network Xchange) clusters comprising multiple DNX units. The platform connects to G4S's network to route SIP calls and data via an MPLS data network. Portal administration and real-time and historic reports are delivered via firewalled web servers and across the public internet to facilitate both internal G4S and Authority administrator access.

Ensuring the Telephony and IT Systems and Equipment are Secure and Auditable: The {Redacted} platform holds all relevant accreditations including ISO/IEC27001 information security management system, ISO9001, ISO14001, and Cyber Essentials Scheme (CES) certification. The {Redacted} platform is subject to external annual surveillance audit for each of the ISO standards and annually for CES.

The IT systems will be configured in accordance with the Security Plan. Physical access control will be in place for equipment. Role based access control will be used for authentication and authorisation for access to services based on the role, and Telephony service the Agent has been granted access to. All authentication events are audited. The equipment will be subject to IT Healthchecks. Our business operations in the Contact Centre will be certified to ISO27001.

We will conduct regular internal audits to check that our controls are adequate and effective to ensure operation in line with the recognised national and international security standards. Telephony and IT systems will be available for audit by the Authority at agreed frequencies.

Capacity/Scalability of the Systems and Equipment: The {Redacted} platform is one of

Europe's largest call centre platforms, with sufficient capacity to accommodate tens of thousands of simultaneous calls providing scalability to meet DWP's needs. Call recording uses virtualised secure equipment which can be scaled as needed. The {Redacted} platform be scaled (either through additional boards or additional servers) as the data volumes require. {redacted}

Telephony Standards required by the Authority: The {Redacted} contact centre service supports advanced queue rules, dynamically managing queues, business disruption and out of hours. {Redacted} service administrators have the capacity to make configuration changes and implement new routing as required. {Redacted} queues support dynamic queue messaging, including estimated wait time and position in queue. {Redacted} queues include 'Call-Back' options, allowing the caller to leave the queue and receive a call back from an Agent at a later time. For {Redacted} services, G.711 Pulse Code Modulation (PCM) is the preferred codec for voice traffic ensuring optimal quality of service (QoS).

Capturing, Storing and Securely Transferring Data with DWP: G4S currently captures, stores and transfers data using Symantec PGP encryption on our {redacted} contract for DWP. We will consult with DWP at contract award to develop and agree the aggregated and unaggregated data transfer plan to meet the DWP's requirements.

The {redacted} platform is located in a highly secure physical environment, with the latest version of Symantec Endpoint Protection anti-virus and drive encryption software used across the {Redacted} platform. Stored data is protected from loss using RAID technology, active/active storage servers, high-speed replications of data between sites and regularly scheduled backups. Data-in-transit protection is sent over HTTPS allowing authentication between client and server and uses Transport Layer Security (TLS 1.2) and IPsec data protection within the network to encrypt the data. This ensures compliance with ISO27001 and Cabinet Office Security Standards.

MI production capabilities, real time and historic: The {redacted} platform includes powerful statistical reporting and data analysis package (called {redacted}) that is used to present management information – both real-time and historic - and to monitor system performance and activity at a glance. It comprises two parts: 1) {Redacted}, which enables set up or reporting screens showing real-time statistics; 2) {Redacted}, which enables instant access to historic data (report layouts are created using {Redacted}).

{Redacted} enables customisable, real-time and historic feedback to monitor service performance, such as current service levels, Average Handle Time and priority callers, which is all filterable by daily, weekly and monthly statistics and consolidated per call line and/or Agent as required. Via the graphical interface dashboard, authorised users can change the scope of the reports and frequency as required. This provides the information required in section 12 of the Statement of Requirement. Data extracts can be downloaded in several formats (such as CSV, XLS and PDF). We will provide relevant MI to the Authority as detailed in 8.2d and Appendix 3 of the SoR document. We will also set up selected DWP management with on-going access to view live and historical data via a secure digital portal.

Arrangements for DWP to supply and maintain audio message files: The {Redacted} platform will support DWP in supplying and maintaining message files. {Redacted} has a rules based approach to determine which when message files are used. E.g. File xyz.WAV to be used during operational hours. This allows different IVR files to be used at different times, including special occasion IVR messages – e.g. Remembrance Day. We will provide an e-mail address to which message files (in WAV format) can be sent, and agree with DWP the appropriate encryption on the files. We recommend that PGP encryption is used. Alternatively, files can be sent by courier on secure flash drives/CDs etc. G4S will load the WAV files onto the {Redacted} platform and programme with DWP's rules. If required, G4S can record the IVR messages, using a trained voice-over artist.

Ensuring DWP Information can be Archived in Accordance with DWP Requirements: Call recordings will be stored on the {Redacted} shared storage environment. This recording capacity provides an unlimited storage resource. The retention period for a particular recording may be set as a service-wide parameter (i.e. six year retention by default) or be determined by the queue which handled the call. Once a recording has reached its storage lifetime it is automatically purged from the recording infrastructure. Throughout the storage period all archived call recordings will remain accessible to ensure that any required by authorised DWP representative can be retrieved within two working days.

Support and maintenance arrangements for the telephony and IT system:
First line support of the IT infrastructure (including DWP's CMS) will be delivered by G4S's IT Support Services organisation, which provide ITIL support processes, including planned preventative maintenance. Field engineers will be based at Wath-upon-Dearne. Second line maintenance will be provided by specialist maintainers and Original Equipment Manufacturers (OEMs) as needed.
The {Redacted} service will be managed and maintained by our telephony partner {Redacted} and their IT technology partner {Redacted}. An ITIL support process is in place which will be accessed by G4S's IT Support Services.

Operating and managing the various call recording and retention requirements to meet DWP requirements: The {Redacted} platform provides, via {Redacted}, a flexible, cloud-based voice recording package delivering always-on or on-demand call recording with integrated call archiving and assessment capabilities. Recordings are stored on resilient, parallel servers in multiple, physically separate and secure locations and can be archived for as long as required. Administrator access to call recordings is secured via two-factor authentication. As detailed previously recordings will be retained for agreed periods and remain accessible so as to ensure that any required by authorised DWP representative can be retrieved within two working days.

Three-way conference call: The {Redacted}acts as an Audio Conference Bridge, providing the facility for simultaneous multi-caller conversations and multiple conferences and conferees. In line with SoR 7.3k, all {redacted} call centre Agents and supervisors have the facility (service features and rights) to conference a third party in to a call. This may be set up via a 'warm' conference with an initial call between the Agent and third party (e.g. DWP's translation service), prior to connection of all three calls.

Dealing with service interruptions due to unavailability or slow running of DWP systems: We will: 1) Report any fault to the G4S IT Support Services desk who will undertake first line support. They will escalate to DWP's IT Helpdesk if needed; 2) If systems are slow but available, we will continue to deliver the service as best we can; 3) If systems are unavailable, we will revert to a paper based system and offer a limited service – this will include answering customer's queries where possible. We will update the DWP systems when they become available; 4) We will offer a call back service, capturing call back details on paper; 5) For sustained outage we will update the IVR to indicate to customers there is an issue and inviting them to call back later or to leave a message to request a call back. All paper used during the outage will be destroyed in accordance with CESG's IS5 (see later) when the data has been transferred to DWP systems on their return.

Handling Data Adequately and Securely:
1) Security Incident Management and Reporting: G4S operates a Security Incident Management Process which is used to manage any security incidents. In the event of an incident the following process is followed: ■ An initial assessment of the incident undertaken. Emergency action taken if there is an immediate risk of security compromise – e.g. open access to office, risk of data leakage. We will also determine the escalation level needed; ■ Assess the impact of the incident; ■ Take remedial action – this may include making good

physical damage or putting in place additional training; ■ If needed, discipline any staff members who breached security; ■ Debrief and identify any lessons to be learned, as part of continuous improvement programme. Incidents will be escalated to G4S and DWP management – the escalation level will depend on the severity of the incident. G4S will report all security incidents to DWP as part of the weekly reporting cycle. Severe incidents will be reported to DWP within one hour of the incident being detected.

2) Secure destruction and sanitisation of physical media used to store DWP data e.g. paper documents, CDs, IT equipment etc.; All protectively marked assets will be destroyed in accordance with the Security Plan. All paper documents and CDs (if any) will be placed in bins for secure destruction by our subcontractor Shred-it. Electronic data will be destroyed in accordance with CESG's InfoSec Standard 5 (IS5). Any electronic assets that need to be destroyed will be sent by secure courier to our {Redacted}, where they will be destroyed in accordance with IS5. Any disks that fail in the operational infrastructure will be erased/destroyed as above prior to any return to the manufacturer. Assets will either be recycled as spares or disposed of in an environmentally sound manner. At contract end, all data will be returned to DWP and any residual disk space made available will be overwritten multiple times to ensure appropriate data sanitisation.

3) Access controls and segregation of the LAN, IT equipment and staff: The DWP Case Management System (CMS) and G4S's telephony system will have no physical connection, ensuring complete segregation of all data (voice and meta-data). The Call Recording System, within the telephony system, will only be accessible to authorised users of the G4S Management Team, and the DWP. There will be logical separation of each line's call recordings. This data will be physically separate from all other G4S systems.

4) Storage of information including call recordings; The majority of DWP information will be held on the DWP CMS system for which DWP will be responsible for managing. G4S's IT systems will only hold MI data. This will be accessed via IT servers / PCs which are held in our secure premises, with the data in our secure data centres. The use of portable media is prohibited. Call recordings will be stored on the {Redacted} platform as described above with restricted access to call recordings. The {Redacted} platform information and physical security is maintained in accordance with ISO/IEC 27001 information security management systems and the Government-backed, industry-supported Cyber Essentials Scheme (CES) certification.

5) Transfer of information; All information and data will be secured in transit. The {Redacted} platform supports Transport Layer Security (TLS) protocols to ensure encryption of administrative data, applications and call recordings between the platform and the authenticated Agent, supervisor or other systems users. As at our {Redacted} contract, G4S has experience in developing information transfer processes and will develop a comprehensive set of service specific processes and policies for the call centre services we provide.

6) Describe any sub-contracting arrangements and access to call recording: We will have second and third level maintenance contracts for the support of the IT equipment. We will have a sub contract with {Redacted} and {Redacted} for the supply of telephony services. All engineers with access to the platform and DWP recordings will be UK-based. System administrator access is via secure protocols only (SSH, HTTPS), and only from defined networks. {Redacted} engineer access to the {Redacted} platform and customer services and data is authenticated via RSA SecurID two factor authentication and audit-logged. We will have a subcontract with {Redacted}who will have no access to DWP data or call recording

7) Outline the call recording systems to be utilised: {Redacted} is a flexible, cloud-based voice recording package delivering always-on or on-demand call recording with integrated call archiving and assessment capabilities. Recordings are stored on resilient, parallel servers in

multiple, physically separate and secure locations and can be archived for as long as required and in line with relevant information retention legislation. Administrator access to call recordings is secured via two-factor authentication.

8) Include specific detail on your Disaster Recovery provisions including time to resume normal service; The {Redacted} platform has 99.999% availability, which meets DWP's requirements (SoR 7.3l – 99.96% target). The {Redacted} and {Redacted} Engineering teams are able to remotely enact disaster recovery plans and procedures, routing traffic to an alternative destinations, e.g. other agreed DWP authorised offices at either the network or platform level.

The {Redacted} platform is embedded into the G4S MPLS network to deliver optimal service performance. Mirroring the technical makeup of the platform, the {Redacted} network is designed to ensure no single points of failure, meaning that the failure of a single node or any other network component will not cause service disruption but instead trigger automatic failover on to an alternate route. As such, the time to resume normal service is not applicable.

G4S's IT ({Redacted}and management staff PCs) is connected via G4S resilient WAN (MPLS) providing access to G4S datacentres responsible for hosting back-office services including HR, Payroll and Finance systems. Our datacentres are designed in an n+1 configuration including fail-over of all servers, storage and associated networking including dynamic routing to enable connectivity through BGP. Spare equipment (telephones, G4S PCs) is held at Wath-upon-Dearne to hot-swap faulty units. The comms equipment comprises resilient switching, redundant power-supplies, fans and cabling - complemented by a four hour fix time support agreement with our external Provider (Telefonica).

9) Details of your controls to ensure safe and timely destruction of DWP data when it is no longer necessary to be held: We will protect the confidentiality of DWP information when it is no longer necessary or appropriate for it to be held on our infrastructure as follows: 1) In the event of hard disk failure, data will either be deleted or the disk destroyed and disposed of (both in accordance with CESG IS5); 2) At end of the contract all call recordings that are not passed their automatic deletion date will be identified and securely passed to the Authority; 3) We will encrypt any data to be returned to DWP and transfer using a secure courier; 4) We will agree with DWP any additional control measures for the bulk transfer of data where aggregation may increase the security risk; 5) Any paper assets will be destroyed in accordance with CESG IS5.