National Records of Scotland

Requirement Specification

for the

Provision of Contact Centre Staff

for

Scotland's Census 2021

Ref; 17/07/05

CONTENTS

1. PURPOSE 4
2. BACKGROUND TO THE CONTRACTING AUTHORITY 4
3. BACKGROUND TO SCOTLAND'S CENSUS 5
4. DEFINITIONS 7
5. SCOPE OF REQUIREMENT 7
6. THE REQUIREMENTS 11
7. OPERATIONAL KPI REPORTING 19
8. SERVICE LEVELS AND PERFORMANCE 19
9. KEY MILESTONES 21
10. AUTHORITY'S RESPONSIBILITIES 23
11. VOLUMES AND CALL LENGTH 24
12. CONTINUOUS IMPROVEMENT 24
13. SUSTAINABILITY 24
14. EQUALITY 25
15. MODERN SLAVERY 26
16. QUALITY 26
17. PRICE 26
18. SUB-CONTRACTORS 27
19. CONTRACT IMPLEMENTATION AND MANAGEMENT 27
20. CONTRACT COMPLAINT ESCALATION PROCEDURE 28
21. AUTHORISED PERSONNEL 28
22. EMPLOYEE STATUS 29
23. CORPORATE IDENTITY 29
24. INTELLECTUAL PROPERTY RIGHTS (IPR) 29
25. PURCHASE ORDERS 30
26. INVOICING 30
27. TRAVEL & SUBSISTENCE ARRANGEMENTS 30
28. LOCATION 30
29. SCOTS LAW 31
30. CONTRACT PERIOD 31
APPENDIX ONE: PROPOSED DATA INTERFACE 32
APPENDIX TWO: PREDICTED VOLUMETRICS 34

APPENDIX THREE: CALL TYPES 39
APPENDIX FOUR: ARCHITECTURE 41
APPENDIX FIVE: DATA SECURITY REQUIREMENTS 44
APPENDIX SIX: TECHNICAL SECURITY STANDARD DECEMBER 2019 V 2.5 54
APPENDIX SEVEN: GLOSSARY OF TERMS 66
APPENDIX EIGHT: TENDER EVALUATION 72
APPENDIX NINE: PROGRAMME TEST STRATEGY 98

1. PURPOSE

National Records of Scotland (NRS) are seeking to appoint a Supplier to deliver a multi-channel Contact Centre for the 2021 Census. The Contact Centre will be a central point of contact to provide support and advice to the public to enable questionnaire completion. The Contact Centre will support and manage customer contact by an automated call management system, phone calls, email (through eForm) and webchat. It will also answer customer enquiries which are received through social media.

This Statement of Requirements (SoR) outlines the Contact Centre requirements for the design, development, testing, implementation, hosting, reporting and decommissioning as well as the data and systems of the service.

The procurement of these services will be chosen by competition from the suppliers included on the Crown Commercial Services framework RM3815 Lot 2: Contact Centre Services.

2. BACKGROUND TO THE CONTRACTING AUTHORITY

National Records of Scotland (NRS) is a non-ministerial department of the Scottish Government (SG), supporting the Registrar General for Scotland and the Keeper of the Records of Scotland. Both roles are held by our Chief Executive, Paul Lowe.

The organisation sits within the Scottish Government's Culture, Tourism and External Affairs portfolio and employs over 400 staff.

The Department's functions, stemming in the main from the Registrar General's statutory responsibilities, are as follows:

- to administer civil registration of vital events - births and deaths, plus marriages, divorces and adoptions - and the statutes relating to the formalities of marriage and the conduct of civil marriage
- to make arrangements for the taking of periodic censuses of Scotland's population, and to prepare and publish demographic and other statistics
- Working in partnership with SG and the wider public sector to deliver improved public services through the application of digital technology
- Responsibility for the national archives of Scotland, supporting family and local history research and maintaining the Scottish Register of Tartans

The fundamental aim of NRS is to contribute to the effective administration of Scotland by recording individual registration information and statistical aggregates for the population and by making them available in accordance with its statutory and other functions.

Further information about NRS is available at the following link.

In this document the term "the Authority" will be used to refer to NRS.

3. BACKGROUND TO SCOTLAND'S CENSUS

Scotland's Census is a household survey of everyone in Scotland which takes place every ten years. For over 200 years, Scotland has relied on the census to underpin national and local decision making. The last census took place in 2011 and the Scotland's Census 2011 General Report reviews the entire operation providing a wealth of background information about how it was designed and conducted.

The census provides outputs of confidentialised census estimates which offer a highly accurate picture of the number of people and their characteristics (such as age, health, where and how people live). National and local government, the education and academic communities, the third sector, commercial business and others require reliable information if they are to conduct many of their activities effectively. The census provides this information and these outputs are particularly important when there is no other reliable source or when the ability to cross-reference or compare characteristics is necessary.

While there are an enormous number of uses and related benefits of the census outputs, the most valuable can be categorised in two broad areas:

- Supporting evidence based policy making and related research
- Informing the allocation and targeting of resources

In addition the outputs improve the knowledge and understanding of the make-up and characteristics of Scotland and its people (and related trends) and serve to inform public debate.

While many aims and elements of the 2021 Census will be similar to previous censuses, there are some significant differences in the design of the 2021 programme. The largest difference relates to the intended use and impact of technology and changes in how it will be used. Around 20% of households opted to respond online during the 2011 Census and we anticipate Census responses will be received predominantly through an Online Collection Instrument (OCI) in 2021, with others participating on paper or by other means, such as Telephone Data Capture (TDC). A unique Internet Access Code (IAC) will be sent to each household encouraging the public to complete the census online.

An increase in online participation will improve both the accuracy and timeliness of the outputs. Not only will this reflect a stepped change in how the Authority

conducts a census, the Authority believes it can also help encourage increased online participation across Scotland.

Scotland's Census 2021 will be delivered via a programme of work made up of a number of distinct projects and supporting functions. These include:

- Data Collection (including public assistance)
- Data Processing
- Admin Data
- Geography
- Communications and Engagement
- Statistical Disclosure Control and Outputs
- Question and Collection Instrument
- Policy and Legislation
- Statistical Quality Assurance

In delivering the Scotland's Census 2021 Programme, the Authority will be procuring a number of products and services, of which the Contact Centre is an important element.

As background, the overall objectives of the census programme are to:

- produce high-quality census results
- generate outputs that meet the needs of users
- maximise online response
- produce timely outputs to maximise benefits
- protect, and be seen to protect, confidential information
- do so in a cost effective way
- make recommendations for the approach to future censuses in Scotland

Scotland's Census is conducted under the Census Act (1920) which makes it a function of the Registrar General for Scotland, a role undertaken by the Chief Executive of NRS and the Scottish Parliament is currently considering the subordinate legislation for Scotland's Census 2021.

Further information about NRS is available at: www.nrscotland.gov.uk and more background information about the census is available at: www.scotlandscensus.gov.uk/2021.

The involvement of the Contact Centre will be to support the public during two data collection operations of the Census:

1. The Census operation in 2021
2. The Census Coverage Survey (CCS) in 2021

The CCS is a voluntary, sample survey which will take place towards the end of the Census collect phase in 2021 to provide additional data to match with Census data.

In 2019, National Records of Scotland carried out a major public test of the systems and services that will be used in Scotland's Census 2021, including the online portal and paper response channels.

This rehearsal was conducted in three local authority areas, namely parts of Glasgow City, Dumfries and Galloway and Na h-Eilieanan Siar, reaching 72,000 households. These areas were selected to allow National Records of Scotland to test approaches in rural, urban and diverse communities.

The rehearsal took place between 7 October and 7 November 2019, using a reference day of 13 October. We are aiming to publish an evaluation report in March and use the lessons learned to improve process and systems

In the run up the census in 2021 the authority will work with suppliers to test operational solutions iteratively.

4. DEFINITIONS

Definitions used in this document are given in Appendix Seven: Glossary of Terms.

5. SCOPE OF REQUIREMENT

The Contact Centre in 2021 will be the central point from which the majority of customer contacts will be managed during the collect phase with the exception of contacts out in the field. This is the period where the Authority will make initial contact with every household and communal establishment enumeration address in Scotland, collect an appropriate response from that address, follow-up non-responding addresses and encourage increased response. It will present a professional and efficient service and image and will strive to achieve first contact resolution. It will use enabling technology to provide a high quality, joined up and consistent approach to handling customer contacts. Information gathered will be used to inform the management of field activities and general management of census operations.

The Supplier must provide a multi-channel Contact Centre which provides a central point of contact for the public to get advice and support to help them participate in Scotland's Census 2021**.**

Telephone contact will be the primary channel for customers looking to contact the Authority directly for support although webchat, social media and email through single enquiry eForms will also be available to customers.

The Authority has partial technical options for inbound webchat, social media and email. The Supplier must be able to interact with these channels. The Supplier can propose an alternative technical solution based on their own preferred approach, or use the services directly or incorporate into their own multi-channel service offering.

The Supplier must provide a Contact Centre service that will:

- Support and manage customer contact by phone and social media for the 2021 Census and the Census Coverage Survey (CCS).
- Support and manage customer contact by email (through eForm) and webchat for the 2021 Census.
    - Webchat internet access can be provided through secure login to the RocketChat service provided by the Authority.
    - Social Media access can be provided either through the Authority's aggregator or through an aggregator used by the Supplier.
    - Email. The Authority will allow the supplier to manage and control a selected email domain to be able to receive and respond to customer emails. The Supplier will ensure that Authority has access to all emails and this is maintained to ensure quality assurance and statistical analysis.
    - Access to each of these services and all corresponding data will be transferred back to the Authority at the decommissioning phase at the end of the programme. At the end of the decommissioning phase no census or CCS data will remain with the supplier.
- Deliver an automated system (eg a 3 level IVR) to allow customers to order paper questionnaires using their unique code (provided by the Authority) 24/7 without having to speak to an advisor and potentially find answers to the most common questions.
- Enable advisors to be able to access the two main census support systems, the Data Collection Operational Management System (DCOMS) and the Online Collection Instrument (OCI). Both will be accessible through web access and secure login.
- Be capable of managing high daily / weekly variation in call and contact volumes with potentially over 300,000 calls and 200,000 automated contacts during the 18 weeks of the census collect period in 2021. Daily

variation will be influenced by official communications, advertising activity, field operations, other events or even service disruptions which could affect customer contact volumes, durations and types. Predictive modelling has been carried out by the Authority which has been used to inform the estimated volumes detailed within this document in Appendix Two. Following any contract award resulting from this mini-competition it is envisaged that further analysis of the predictive modelling data will be undertaken with the Supplier and the Authority.

- Respond to general queries on the Census and CCS operations, provide advice and support to enable questionnaire completion, arrange for public fulfilment of new, replacement or additional digital and / or paper materials and verify field staff identity. An analysis of call types from the 2011 Census and 2019 rehearsal is available in Appendix Three.

- Provide consistent, accurate and timely advice, support and guidance to customers by trained, professional staff who will deliver a high quality, consistent and measurable service throughout the operation.

- Enable advisors to carry out Telephone Data Capture (TDC) requests where an advisor completes an online census questionnaire via the OCI on the telephone with a customer. For CCS, advisors will capture data on paper.

- Provide a secure, robust service that will protect and be seen to protect customers' personal information and the security of the Census and CCS Data and will comply with all NRS and Scottish Government security measures and systems found in Appendix Five: Data Security Requirements.

- Deliver a business continuity and disaster recovery strategy to avoid and mitigate risks associated with any disruption of operations. The Supplier will ensure it is able to continue to serve the public throughout the collect phase and that all ICT systems and all data and equipment related to the census is secure in the event of a catastrophic event.

- Commit to meeting the overall service levels determined to deliver an acceptable service. The Authority will determine the acceptable service levels (SLs), for example calls answered, abandonment rate, First Contact Resolution, etc. The service levels which the Suppliers performance will be measured against are detailed in Section Eight**,** with any additional Service Levels agreed between the Authority and the Supplier prior to contract commencement.

Operational reporting requirements will be determined by the Authority and will include real time reporting of operational Key Performance Indicators (KPIs),

customer contact outcomes and overall performance and productivity levels. These KPIs are detailed in Section Seven with any additional KPIs agreed between the Authority and the Supplier prior to contract commencement.

6. THE REQUIREMENTS

The full set of functional and non-functional requirements are listed below indicating the priority (Must or Should) and the acceptance criteria.

Functional Requirements			
No	Requirement	Priority	Acceptance criteria
	Multi-Channel Contact Centre Service		
CC-FR-001	The Supplier must provide a multi-channel service during Census and Census Coverage Survey (CCS) collection operation that will support and manage customer contact by: - phone - email - direct messages on social media - webchat (not for CCS) The Authority has partial technical options for inbound webchat, social media and email. The Supplier must be able to interact with these channels. The Supplier can propose an alternative technical solution based on their own preferred approach, or use the services directly or incorporate into their own multi-channel service offering. The Supplier must be able to provide the mechanism to make outbound calls to UK mobile and landline numbers and send outbound emails in order to respond to individual customer enquiries and must be able to transfer live calls to the Authority or an external supplier.	M	Contact Centre that manages customer contact by phone, email, social media, webchat Outbound calls to UK mobile and landlines can be placed Live calls can be transferred to the Authority or a third party supplier
	Self Service		
CC-FR-002	The Supplier must provide an automated solution (eg IVR) that allows members of the public to do the following, without speaking to a Contact Centre Advisor: - request a paper questionnaire (through validation of a customer's unique numeric code) - get answers to the most common questions - interface with the Authority's systems to allow data transfers between systems Automated options for CCS may differ	M	Member of public can request a paper questionnaire through an automated solution Member of public can get answers to most common questions through automated solution
	Contact Centre Staffing		
CC-FR-003	The Supplier must ensure that there is appropriate staff resource available during the Census and CCS collection operation to ensure contacts are answered within service level agreements Details of the Volumetrics for Census and CCS are included in the Volumetrics Appendix	M	80% of calls answered within 45 seconds (from SLAs)
	Contact Handling		

CC-FR-004	The Supplier must provide a call management system to: - manage calls received through 4 different lines - queue calls if a Contact Centre Advisor is not available - play front end automated messages (content to be defined by the Authority) - play in queue messages and music (content to be defined by the Authority) - inform members of the public how long it will take for their call to be answered - allow pre-defined groups of callers to skip call queues (e.g. Field Workers who may have general enumeration based enquiries) The supplier must provide a mechanism to capture all contact types (e.g. reason for call and outcome/resolution code). The Supplier and the Authority will work together to define an escalation process for questions that cannot be answered by the Supplier. Details of the Volumetrics for Census and CCS are included in the Volumetrics Appendix	M	Call management system can: - manage calls received - queue calls - play appropriate messages - allow pre-defined groups of callers to skip call queues Mechanism to record contact types and outcomes
	Systems Access		
CC-FR-005	The Supplier must have the means to provide access to the Authority's web based systems for Census, including, but not limited to: - Online Collection Instrument (OCI) - Data Collection Operational Management System (DCOMS) This access will allow Contact Centre Advisors to: - search for addresses - access addresses - amend addresses - record an address from a member of the public - view notes against an existing address - record notes against an existing address - view the enumeration status of an address - following a contact with a member of the public, record an outcome - order physical products to be sent to that address - perform telephone data capture for Census by putting respondent data into OCI	M	Contact Centre Advisor can access and use OCI Contact Centre Advisor can access and use DCOMS
	3rd Party Suppliers		

CC-FR-006	The Supplier must work with the Authority's third party to provide 3 way calls for, but not limited to: - live interpretation service - text relay service - BSL interpretation service for both Census and CCS	M	3 way calls can take place
	KPIs		
CC-FR-007	The Supplier must provide the Authority with specified Key Performance Indicator reports as follows: · Number of calls presented · Number of calls resolved via the automated system (IVR) · Number of calls abandoned in the advisor queue · Number of calls answered by the advisors · Average customer wait time · Average handling time · Wrap time · Advisor talk time · Advisor busy time? · Number of Webchats · Webchat time to answer · Webchat requests answered · Webchat AHT (Average handling time) · Webchat customer satisfaction · Longest hourly queue length and average queue length · Number of repeat customer calls · Call / contact types · Automated telephone system (IVR) usage and taxonomy analysis · Number of paper questionnaires requested through the automated system (IVR) · Number of paper questionnaires requested through advisors · Number of calls escalated to HQ · Escalation reason and outcome · Number of Telephone Data Capture requests · Number of completed Telephone Data Captures · Length of Telephone Data Capture calls · Number of language translation calls using third party translation service · Handling time of language translation calls · First contact resolution numbers and percentage · Number and type of any complaints	M	Reporting is available on all KPIs

	Training		
CC-FR-008	The Supplier must work with the Authority to provide training to Contact Centre advisors, team leaders, managers and support staff. This training should promote a "right first time" approach and cover: - census specific training material, including general support for Field Workers - briefing notes - FAQs and other knowledgebase content - customer service - systems training - sensitivity training - providing support to customers with additional support needs (e.g. physical or mental impairments including sight loss, hearing loss, speech impairments) - how to address digital exclusion issues (lack of access or lack of skills, literacy issues, learning difficulties or confidence issues) - webchat and email training - security and confidentiality training The Supplier will work with the Authority to ensure that advisors will have the skills required to capture customers data over the phone as part of the telephone data capture process	M	Delivery of agreed training
	CCS Paper Questionnaires		
CC-FR-009	The Supplier must perform telephone data capture (TDC) of Census Coverage Survey (CCS) on paper questionnaires as follows: - receive and securely store blank CCS paper questionnaires - supply suitable space for Call Centre staff to complete CCS paper questionnaires (desk space) - securely store completed CCS paper questionnaires - secure transport of completed CCS paper questionnaires to Data Capture Supplier	M	The contact centre must store blank and completed CCS paper questionnaires in a secure area Suitable space to complete CCS paper questionnaires Procedure in place for secure transit to Data Capture Supplier

Non-Functional Requirements			
No	Requirement	Priority	Acceptance Criteria
Performance			
CC-NFR-001	Supplier must comply with the agreed Service Levels.	M	Targets agreed in the SoR for Performance to be adhered to
CC-NFR-002	For Telephone Data Capture: - approximately 100 man hours required for Census - approximately 625 man hours required for CCS	M	Contact Centre Advisors will assist some members of the public by completing the Census questionnaire on their behalf (Telephone data capture). Working assumption for census is 200 TDCs.

			Working assumption for CCS is 2,500 calls at 15 minutes each
CC-NFR-003	The Supplier must be capable of managing all forms of customer contact including calls, emails, plus webchats and social media in accordance with the Volumetrics Section.	M	Please see predictive modelling for call volumes during operation period.
CC-NFR-004	The Supplier must be capable of managing potentially over 300,000 live calls to advisors and 200,000 automated (IVR) contacts (paper questionnaire ordering) during the 2021 census operation and 3,500 calls for CCS.	M	Please see predictive modelling for call volumes during operation period.
CC-NFR-005	A sufficient number of staff must be trained to answer contacts from members of the public at any point of the Census and CCS collect phase.	M	80% of calls answered within 45 seconds (from SLs)
Availability			
CC-NFR-006	The Contact Centre must be available to public assistance queries during the Census and CCS collect phase between: 8am to 8pm (Monday - Friday)* and 9am to 4pm (Weekends)* * Working Assumption	M	Contact Centre is assumed to be operational for the duration of the Census collect period from 8-8 on Mondays to Fridays 9am-4pm on Saturday/Sunday in line with Field Force operational times.
CC-NFR-007	The Contact Centre must be open during Census 2021 Weekend (20 and 21 March 2021) from 8am-8pm	M	Contact Centre is required to be operational for the Census 2021 Weekend from 8am-8pm on Saturday/Sunday.
CC-NFR-008	The Contact Centre must be available from no later than 4 weeks prior to Census day until the end of the Census and CCS Collect phase, i.e. from 28th February to 30th June 2021*. * Working Assumption. End of Census Collect phase 2nd May	M	The Contact centre will provide public assistance for the duration of the census collect phase, with exact dates to be confirmed.
CC-NFR-009	Webchat, email and social media response service will be available and supported during Contact Centre opening hours	M	Webchat will be available only during Contact Centre opening hours.
CC-NFR-010	The Automated solution (IVR) should be available 24/7 for the duration of the Census Collect Phase.	M	The automated system will allow processing of calls 24/7 for the duration of operation.
CC-NFR-011	The Automated solution (IVR) should allow re-tries in the event of a respondent making errors. If the respondent makes multiple errors, they should instead be directed to Contact Centre Advisor (in hours) or a recorded message (out of hours). Automated options for CCS may differ.	S	If respondent makes 1 mistake, the system allows them to retry If respondent makes a 2nd mistake and Contact Centre is open, the respondent is directed to a Contact Centre Advisor If respondent makes a 2nd mistake and Contact Centre is closed, the respondent is played a recorded message

CC-NFR-012	The Contact Centre must work with the list of browsers supported by the Authority's web based systems, including, but not limited to: - Online Collection Instrument (OCI) - Data Collection Operational Management System (DCOMS)	M	Contact Centre must work with list of browsers supported by OCI and DCOMS. This list is drawn from Government Digital Service (GDS) and can be seen here: https://www.gov.uk/service-manual/technology/designing-for-different-browsers-and-devices.
CC-NFR-013	The Supplier must work with the Authority and the Integration Service Provider to ensure that, where needed, interfaces can be provided with other required systems.	M	Works with the Authority and Integration Service Provider to provide interfaces to other required systems
Security			
CC-NFR-014	All Contact Centre staff must be on Suppliers premises for the duration of their contracted hours	M	This requirement is specifically about not allowing Contact Centre advisors to be remote/home workers and therefore subject to all security and data protection policies in place.
CC-NFR-015	The supplier must provide a secure, robust service that will protect and be seen to protect the customers' personal information and the security of the census data and will comply with all census and Scottish Government security measures and systems. Supplier must comply with all Data Security Requirements (Appendix 2 of the SoR).	M	Targets agreed in the SoR for Security to be adhered to
CC-NFR-016	All persons either employed in processing the Census, or otherwise contracted to supply other services to the Registrar General for Scotland in connection with the 2021 Census will be subject to the strict confidentiality provisions of the Census Act.	M	All Census staff sign confidentiality undertaking
CC-NFR-018	The Supplier must ensure all Contact Centre personnel have a valid UK Government Baseline Personnel Security Standard (BPSS) before the start of the operation	M	All Census staff have BPSS certification
CC-NFR-019	Where, due to nationality or residence issues, it is not practical to obtain BPSS, vetting to BS 8758:2012 will be required.	M	Vet staff to BS 8758:2012
CC-NFR-021	All Contact Centre staff must also have a valid, Basic Disclosure Scotland certificate before the start of the operation and must ensure they each have a valid certificate throughout the operation.	M	All Contact Centre staff have Disclosure Scotland certification
CC-NFR-022	The Supplier must develop a business continuity plan and strategy to avoid and mitigate risks associated with any disruption of service that will present a significant impact on the operation. The BCDR designation is Essential for Census.	M	Business Continuity plan must exist and be reviewed and accepted by the Authority

CC-NFR-023	The Supplier must ensure the Contact Centre is able to continue to serve the public throughout the collect phase and all ICT systems and all data and equipment related to the census is backed up and secure in the event of a catastrophic event.	M	Business Continuity plan must exist and be reviewed and accepted by the Authority
CC-NFR-024	The Supplier must ensure that the Contact Centre complies with security requirements as specified in the NRS Technical Security Standard, and the security section in the SoR.	M	Contact Centre complies with Technical Security Standard
CC-NFR-025	The Supplier must supply all data to the Authority at the end of the collect phase of the Census and Census Coverage Survey and will not retain any data	M	Provider does not retain any data at end of Collect Phase Provider supplies all data to Authority at end of Collect Phase
CC-NFR-026	The personnel working on the Census 2021 and Census Coverage Survey must be segregated from other personnel such that overhearing and overlooking is not possible.	M	Provider staff working on Census 2021 cannot be overheard or overlooked by other non-Census staff
CC-NFR-027	The Contact Centre Supplier must have controls and procedures in place to ensure that unauthorised personnel cannot enter into the premises, and that visitors are appropriately controlled.	M	Provider security controls are in place
Scalability			
CC-NFR-028	The Automated solution (IVR) must be able to withstand a major upsurge in calls of a maximum of 18,000 calls daily. Volumetrics.	M	The systems should also allow for any major upsurge in demand at short notice (for reasons out with our control, for example the website not being available even for a short period of time would generate increased demand) without the need for any software refactoring
Evolution			
CC-NFR-029	The Contact Centre must be closed and decommissioned (with secure data disposal) at an agreed date.	M	The Supplier must securely decommission the Contact Centre at the end of the collect phase at a time determined by the Authority. This will include but is not limited to the handover of copies of all data collected, all written and online records, all customer and customer contact data, all training and support material and all data relating to the census
CC-NFR-030	The Supplier must confirm that no Census Data will remain in their possession at the end of the collect phase of Census 2021 and the Census Coverage Survey, at a time determined by the Authority.	M	No Census data remains at the end of Collect Phase across all Supplier environments and platforms (including backup)

Other NFRs			
CC-NFR-031	The Supplier must work with the Authority to ensure that staff training and the scripts used to collect Census Data over the telephone minimise the risk of statistical bias in the customers' answers and support the Digital First Approach.	M	Training material to be approved by the Authority Scripts to be approved by the Authority
CC-NFR-032	The Supplier will provide and manage all HR functions for Contact Centre staff, including recruitment, staff scheduling and adherence. Staff scheduling should be designed to manage service levels and also to maximise value for money.	M	Provide full HR functionality Manage full HR functionality
CC-NFR-033	The Supplier will work with the Authority to create scripts for advisors and the Authority will have final sign off and approval for all scripts and census material.	M	Scripts to be approved by the Authority
CC-NFR-041	The Supplier must ensure there are no audio recordings of any calls received or made by the Contact Centre	M	No call recordings

Priority Coding: M = Must, S = Should

7. OPERATIONAL KPI REPORTING

The following specific operational reporting and KPIs will be required daily for the duration of the 2021 Census collect period and CCS:

• Number of calls presented by 60 minute period • Number of calls resolved in the automated system (IVR) by 60 minute period • Number of calls abandoned in the automated system (IVR) • Number of calls passed to the advisors by 60 minute period • Number of calls abandoned by 60 minute period • Average customer wait time by 60 minute period • Average handling time • Wrap time • Advisor talk time • Advisor busy time • Number of Webchats • Webchat time to answer • Webchat requests answered • Webchat Average Handling Time (AHT) • Webchat customer satisfaction • Volume of social media enquiries • Social media enquiries time to answer	• Longest hourly queue length and average queue length • Resolution status by call / contact • Call / contact types • Automated system (IVR) usage and taxonomy analysis • Number of paper questionnaires requested through the automated system (IVR) • Number of paper questionnaires requested through advisors • Number of calls escalated • Escalation reason and outcome • Number of Telephone Data Capture requests • Number of completed Telephone Data Captures • Length of Telephone Data Capture calls • Number of language translation calls • Handling time of language translation calls • First contact resolution numbers and percentage • Level and type of any complaints

The Contact Centre reporting will also be required to feed into any consolidated programme management daily reporting process and format which will be agreed before the operation begins.

8. SERVICE LEVELS AND PERFORMANCE

The Authority proposes to measure service quality and performance daily through the following SLs:

SLs	Service Area	SLs description	Target

1	Automated call management	Automated system availability per 24 hours.	99%
2		The speed of automated telephone system response to a call both in and out of Contact Centre opening times.	90% in 10 seconds.
3		Speed of changes to options on automated system (IVR).	Within 3 hours of script/options agreement.
4	Advisor Availability / Customer Service Level	Percentage of calls answered by an advisor within a timeframe.	80% within 45 seconds.
5		The average wait time that callers are queuing for an advisor to answer divided by the number of calls handled by live advisors.	<60 seconds
6		Abandonment Rate. The percentage of calls that are abandoned in the automated system (IVR) and in the advisor queue.	<8%
7	Customer Satisfaction	Customer satisfaction level (methodology to be agreed with the Supplier).	>70%
8	Process Management Efficiency	Speed of turnaround for escalation contacts processing.	4 hours
9		Speed of turnaround for content update requests and referrals.	4 hours
10		Speed of response for customer emails.	80% within 6 hours (during opening hours)
11	Webchat	Number and percentage of webchats abandoned by the customer before response.	<5%
12		The amount of time customers have spent waiting for an advisor to answer them on webchat.	<2 minutes

13		Percentage of chats answered by an advisor within a timeframe.	80% within 45 seconds
14	Social Media	Percentage of enquiries answered by an advisor within a timeframe.	80% within 6 hours (during opening hours)

Note: In the event of increased volume of demand, the Authority will offer flexibility on the Service Levels and will work with the Supplier to prioritise channels.

9. KEY MILESTONES

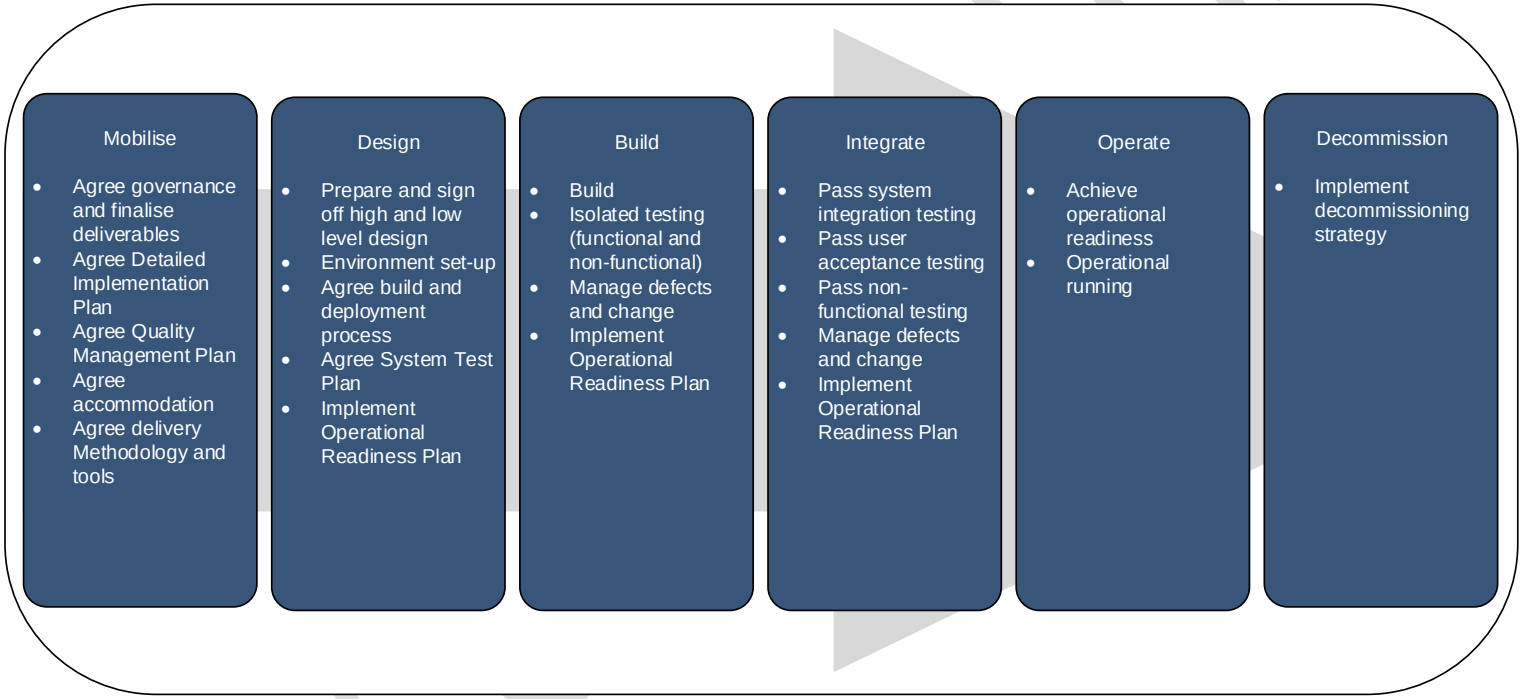
The Supplier must work with the Authority's Project and Senior Management Team to create an Implementation Plan for delivery to meet the Key Milestones and other delivery dates which will be refined during the design phase.

Key Milestones & Activities:

Milestone	Scotland's Census 2021 Activity
August – November 2020	Testing Phase
3 August 2020	Programme System Integration Testing (SIT) Testing
31 October 2020	Census Operational Readiness Review Date
1 January 2021	Start Census Operation
1 March 2021	Census Contact Centre go live
21 March 2021	Census Date
2 May 2021	Census Data Contact Centre at reduced capacity
1 June CCS	Census Coverage Survey begins for 4 weeks
1 July 2021	Complete Census Contact Centre Operation
31 July 2021	Decommissioning Complete

Proposed phases of development and operation:

The Authority has listed the following phases with an indication of the deliverables (not exhaustive) to be completed in order to achieve the Key Milestones. The Authority has resource retained in-house such as Subject Matter Experts to assure the delivery of the project.



10. AUTHORITY'S RESPONSIBILITIES

The Authority will provide sufficient access to knowledge and personnel and will provide a team to work with the Supplier to support the service including a Contract Manager, a Project Delivery Manager, a Technical Representative and Subject Matter Experts.

The Authority will nominate a Contract Manager to be the point of contact for the Supplier. The Contract Manager will liaise with the Supplier on all operational issues and contractual issues, liaising with relevant Authority personnel where required.

The following roles shall be filled by the Authority to fulfil our contractual obligations.

The Contract Manager (supported by a Senior Procurement Specialist) will:

- Chair regular supplier review meetings
- Manage the contract implementation
- Provide focus for supplier relationships
- Monitor supplier performance
- Manage commercial risk management
- Manage contract variations and commercial issues

The Project Delivery Manager will:

- Manage delivery timelines and plans

The Technical Representative will:

- Manage delivery of technical requirements (Architect, Quality, Security, Testing etc.)
- Provide focus on design and functionality delivery

Subject Matter Experts will:

- Provide business rules for operational set up and running
- Define business processes
- Support training and scripting set up and delivery
- Provide escalation path for customer enquiries

11. VOLUMES AND CALL LENGTH

Suppliers must consider two important factors. First, the call demand can fluctuate from one day to the next and unexpected challenges (eg website down time, unplanned publicity) could increase the number of customer contacts dramatically and suddenly.

Second, call length. The uptake of Telephone Data Capture (TDC) will have a dramatic impact on the average handling time of contacts. While the majority of customer census telephone queries are of a simple nature and can be resolved with an average call length of 2.5 minutes (based on recent tests), recent experience shows a TDC call will typically take 25 minutes to complete.

The volume of TDCs is something that we will have to control and therefore Potential Suppliers should price the TDC service separately in their response and allow for 200 TDC calls for Census 2021 at 25 minutes each and 2,500 for CCS at 10 minutes each.

As well as telephone call volumes, potential fluctuations in contact demand will also include fluctuations in web chats, emails and social media.

12. CONTINUOUS IMPROVEMENT

The Supplier is expected to improve the way in which the required Services are delivered continually throughout the Contract duration.

Any changes to the way in which the Contact Centre services are to be delivered must be brought to the Authority's attention and agreed prior to any changes being implemented.

13. SUSTAINABILITY

The Authority is committed to the delivery of high quality public services, and recognises that this is critically dependent on a workforce that is well-motivated, well led, has appropriate opportunities for training and skills development and is engaged in decision making. These factors are also important for workforce recruitment and retention, and thus continuity of service. Public Bodies in Scotland have adopted fair work practices, which include:

- a pay policy that includes a commitment to supporting the Living Wage
- being a Living Wage Accredited Employer
- clear managerial responsibility to nurture talent and help individuals fulfil their potential
- developing a workforce which reflects the population of Scotland in terms of age, gender, race and disability
- a strong commitment to Modern Apprenticeships

- support for learning and development
- no inappropriate use of zero hours contracts
- flexible working (including for example practices such as flexi-time and career breaks) and support for family friendly working and wider work life balance
- Trade Union recognition and representation where possible; otherwise alternative arrangements to give staff an effective voice
- gender balance and wider representative workforce
- promoting workplace innovation

In order to ensure the highest standards of service quality in this contract we expect the Supplier to take a similar positive approach to fair work practices as part of a fair and equitable employment and reward package.

The Supplier will be expected to have a comprehensive system which demonstrates an on-going and systematic approach to identifying and managing risks relating to labour standards, working conditions and use of child labour in the supply chains relevant to this requirement.

The Supplier must work with the Authority during the term of any contract resulting from this mini-competition to ensure compliance with new and emerging legislation.

The Supplier must, where practical:

- minimise the environmental impacts of products and associated packaging
- minimise the environmental impact of the delivery of products
- contribute to a more circular economy
- provide relevant opportunities for community benefits
- provide opportunities for the involvement of SMEs and/or third sector organisations in delivery of this framework
- provide assurance regarding workforce matters

Additionally, the Authority is committed to sustainable procurement and to this end the Supplier must have appropriate standards for its organisation and its supply chain regarding legal, ethical and social issues.

14. EQUALITY

The Authority requires the Supplier to meet their duties under the Equality Act 2010 and may ask for evidence that they are aware of and operate in accordance with those requirements at any point throughout any contract resulting from this mini-competition.

15. MODERN SLAVERY

The Authority adopts a zero tolerance approach to modern slavery and human trafficking. We are committed to respecting human rights, including the rights of children. We expect all those who work for and with us to adhere to our zero tolerance approach to slavery and human trafficking.

In relation to direct employees, the Supplier must undertake appropriate pre-employment checks to ensure a right to work in the UK, and further identity checks where required. Contracts of employment, and pay, are directly with the individual.

The breadth, depth and interconnectedness of our supply chain make it challenging to manage business and sustainability issues. While respecting human rights is ultimately the Supplier's responsibility, as the customer we expect those in our supply chain to respect our values and to adopt suitable anti-slavery and human trafficking policies and practices.

Any breach of the Modern Slavery Act by the Supplier, their sub-contractor(s), and/or consortia members can result in the immediate termination by the Authority of any contract resulting from this mini-competition.

16. QUALITY

The Supplier must prepare, deliver, maintain and adhere to a Quality Management Plan that identifies the procedures to be carried out to measure, collect, monitor, demonstrate, maintain and report on Service Levels and Key Performance Indicators specified by the Authority.

The content of the Quality Management Plan will be agreed with the Authority and will include as a minimum:

- Overall approach
- Roles and responsibilities
- Activities and deliverables to be measured
- Measurement standards and procedures
- Reporting arrangements
- Corrective action procedures
- Quality improvement activities

17. PRICE

Prices must only be submitted via the Pricing Schedule, which must be completed in full. You should not leave any cell blank

18. SUB-CONTRACTORS

All sub-contractors appointed by the Supplier must be approved in advance by the Authority.

Where changes are made (with the agreement of the Authority's Contract Manager, or their appointed representative / agent) during the period of any contract resulting from this mini-competition to the entities (sub-contractors and / or consortium members) that the Supplier relies on in order to meet the selection criteria set out in any contract entered into with the Authority they must provide a separate European Single Procurement Document Scotland (ESPD Scotland) for each new / replacement sub-contractor and/or consortium member to the Authority's Contract Manager, or their appointed representative/agent.

The ESPD(S) will be reviewed by the Authority's Contract Manager, or their appointed representative / agent, and the Authority's Procurement Services to determine the appropriateness of the new/replacement sub-contractor and / or consortium member. The Authority's decision on whether or not to allow the change / addition will be final.

The Supplier will be fully liable for the performance of all sub-contractors appointed in relation to this Contract, and any act or omission by any sub-contractor will be deemed to be an act or omission of the Supplier.

The Authority may, at any time and within reason, require any sub-contractor appointed by the Supplier in relation to any contract resulting from this mini-competition to be replaced.

19. CONTRACT IMPLEMENTATION AND MANAGEMENT

The Authority will appoint a Contract and Supplier Management Team to ensure successful delivery of the requirements.

The Contract and Supplier Management Team will comprise of representatives from the Authority who will fulfil the following roles:

- Contract Delivery Manager – responsible for day-to-day management of any contract resulting from this mini-competition
- Commercial Contract Manager – responsible for managing all commercial / contractual aspects of any contract resulting from this mini-competition
- Technical Support Manager – responsible for managing all technical aspects relating to any contract resulting from this mini-competition

- Authority Finance – responsible for managing and monitoring financial transactions with the Supplier.

The Supplier will be given full details on the names and contact details for the Authority's Contract and Supplier Management Team.

There will be regular Contract Reviews between the Supplier and the Contract and Supplier Management Team (as well as any other representatives that the Contract and Supplier Management Team deem necessary), which will cover all aspects of the contract and service provision from both parties. Frequency and location will be agreed during the design phase.

The Supplier must co-operate fully with all reasonable requests received from the Contract and Supplier Management Team.

The Supplier must appoint their own dedicated Contract Manager who will:

- Act as the main point of contact with the Authority in relation to all aspects of any contract resulting from this mini-competition
- Fully support the Authority in resolving any problems prior to formal escalation
- Attend monthly review meetings with the Authority's Contract and Supplier Management Team that will cover all aspects of any contract resulting from this mini-competition and service provision from both parties. If the need arises, further meetings may be arranged to discuss any outstanding problems or issues or to resolve any invoice issues
- Work with the Authority to identify and implement efficiencies and / or innovative solutions where opportunities arise

The Supplier must meet any milestones agreed by the Supplier and the Authority during the design phase. Failure to fulfil this part of the Supplier may result in termination of the contract.

20. CONTRACT COMPLAINT ESCALATION PROCEDURE

The Supplier must have appropriate, documented escalation procedures in place in the event that an issue relating to any contract resulting from this mini-competition is not resolved by their appointed Contract Manager to the satisfaction of the Authority.

21. AUTHORISED PERSONNEL

The Supplier must only accept purchase orders, change control notices, and instructions from the Authority's staff that are authorised to do so. A list of Authority staff authorised to undertake these duties will be issued to the

Supplier by the Authority's Contract Delivery Manager (who will also be responsible for maintaining and issuing any updated list of the Authority's Authorised Staff to the Supplier as and when required).

22. EMPLOYEE STATUS

Nothing whatsoever within this mini-competition, associated documents, or any contract resulting from this mini-competition shall result in any Supplier, their staff, sub-contractors, and/or consortia members claiming any employee status rights with the Authority.

The Supplier will at all times be responsible for ensuring that they instruct and direct their staff, sub-contractors, and/or consortia members in order to meet the requirements of the Authority in relation to any contract that may result from this mini-competition, as agreed with the Authority at any time throughout the duration of any contract resulting from this mini-competition. The Authority will not be responsible for instructing and/or directing the Supplier's operational staff, their sub-contractors, and/or their consortia members.

23. CORPORATE IDENTITY

Scotland's Census 2021 will develop unique branding and this will be shared with the Supplier once appointed. The Authority will sign off on all use of logos, branding, corporate imagery, personality, tone of voice and every facet of brand identity. All aspects of customer contact will follow the brand guidelines and corporate identity including all scripts, templates and customer contact methodology.

24. INTELLECTUAL PROPERTY RIGHTS (IPR)

It shall be a condition of any contract resulting from this mini-competition that, except to the extent that the services incorporate designs furnished by the Authority, that nothing done by the Supplier in the performance of the services shall infringe any patent, trade mark, registered design, copyright or other right in the nature of intellectual property of any third party and the Supplier shall indemnify the Authority and the Crown against all actions, claims, demands, costs and expenses which the Authority or the Crown may suffer or incur as a result of or in connection with any breach of this Condition.

All rights (including ownership and copyright) in any reports, documents, specifications, instructions, plans, drawings, patents, models or designs whether in writing or on magnetic or other media:

- furnished to or made available to the Supplier by the Authority shall remain vested in the Crown absolutely
- prepared by or for the Supplier for use, or intended use, in relation to the performance of this Contract are hereby assigned to and shall vest in the Crown absolutely
- (without prejudice to Official Secrets Acts, etc.) the Supplier shall not and shall procure that the Supplier's servants and agents shall not (except to the extent necessary for the implementation of this Contract) without the prior written consent of the Authority use or disclose any such reports, documents, specifications, instructions, plans, drawings, patents, models, designs or other material as aforesaid or any other information (whether or not relevant to this Contract) which the Supplier may obtain pursuant to or by reason of this Contract, except information which is in the public domain otherwise than by reason of a breach of this provision
- in particular (but without prejudice to the generality of the foregoing) the Supplier shall not refer to the Authority or the contract in any advertisement without the Authority's prior written consent.

The provisions of this Condition shall apply during the continuance of this Contract and after its termination howsoever arising.

25. PURCHASE ORDERS

Purchase Orders will be issued to the Supplier by post or through the Authority's finance / eProcurement system.

26. INVOICING

The Supplier will issue invoices by email to; invoices@nrscotland.gov.uk

The Supplier must ensure the repayment of any overpayments, or duplicate payments, within five working days of being notified by the Authority of the overpayment or duplicate payment.

27. TRAVEL & SUBSISTENCE ARRANGEMENTS

The Supplier will be required to attend meetings at the Authority's premises and all travel and subsistence will be at the Supplier's expense.

28. LOCATION

The location and hosting of the services will be carried out at the Supplier's premises.

29. SCOTS LAW

Regarding any call-off made under this mini-competition, please note the following in relation to Law and Jurisdiction (Clause 57) of the call-off order form and call off terms that would apply:

a. References to "England and Wales" in the original Clause 57 of the Call Off Contract (Law and Jurisdiction) shall be replaced with "Scotland".

b. Where legislation is expressly mentioned in the Call Off Contract the adoption of Clause 4.1.1 (a) shall have the effect of substituting the equivalent Scots legislation.

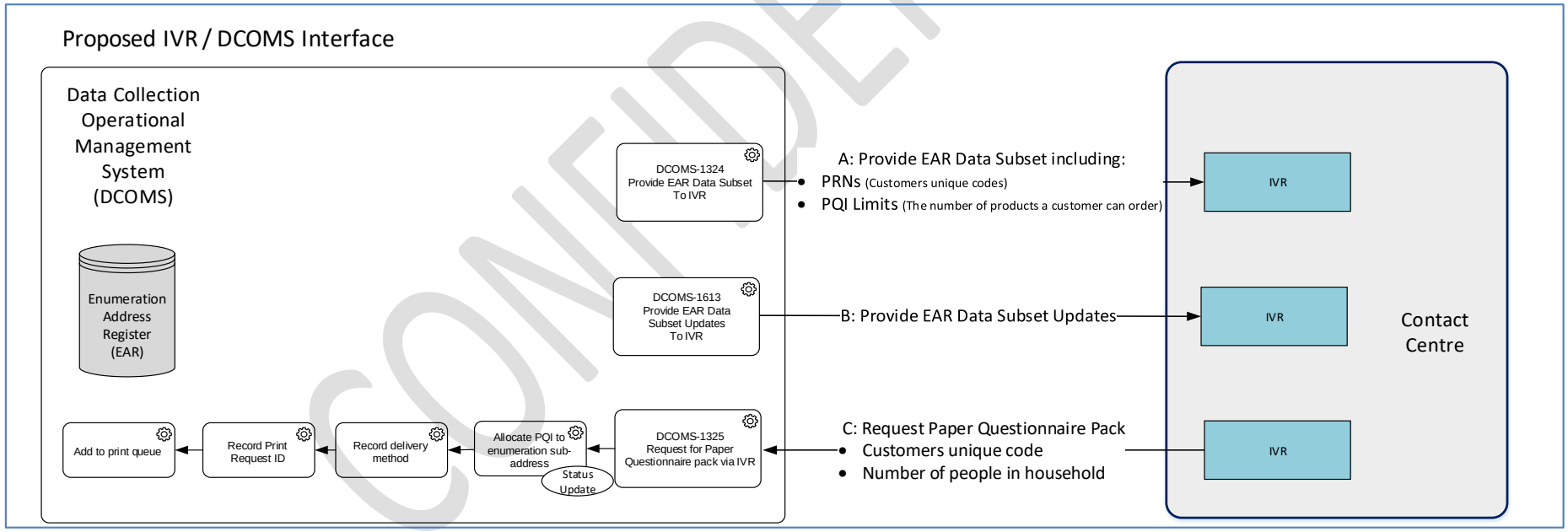
30. CONTRACT PERIOD

The Contract will be effective from 30 March 2020 to 31 July 2021. With option for a contract extension (for a maximum of 6 months from 31 July 2020) should this be deemed necessary by the Authority.

APPENDIX ONE: PROPOSED DATA INTERFACE

This section describes the data interface between the Supplier's IVR and DCOMS as defined so far during the requirements gathering phase of the programme. This may be subject to change as the Authority engages with Suppliers and data format, frequency of update and the structure of the interface are agreed.

The interface is required to allow customers to enter a unique numeric code into an IVR, answer a further question about the number of people in their household and the IVR will then have the information required to send to DCOMS so a paper questionnaire can be sent out without the customer having to speak to an advisor. Every household in Scotland will be allocated at least one unique code (2.7 million) and up to 7-10 million could be issued.



System	Purpose	DCOMS Data	Customer Process	Data Transfer from IVR
Automated Paper Questionnaire Ordering.	Customers can order a paper household questionnaire without having to speak to an advisor.	DCOMS holds or transfers data on unique numeric codes to the automated system.	1. In the IVR a customer enters their unique numeric code and the number of people in their household. 2. The IVR verifies the number keyed in by the customer as a valid number. .	1. Customer's unique numeric code. 2. Number of people in the customer's household.

APPENDIX TWO: PREDICTED VOLUMETRICS

Introduction

As Scotland's Census 2021 moves to more digital customer involvement any previous Census customer contact information is of limited value in terms of predicting and planning for the volume of contacts. However, previous data gives us a base level starting point from which to begin to develop predictive modelling to assess the level of customer contacts we can expect.

This demand forecasting has utilised data from international partners, the recent UK rehearsals and from previous censuses.

Background & Methodology

1. Each country that is moving to or has moved to an increased digital Census response has experienced a significantly increased level of calls that have left the contact centre unable to meet the call demand within planned service levels.

2. Recent tests have all shown three characteristics:

    a. Significantly higher than predicted number of customer calls
    b. Calls coming much earlier in the process than previous years
    c. Census team actions and events generate significant call levels (reminder letters, field force visits etc) compared to previous censuses

3. In Scotland there is a slightly higher digitally excluded rate than the rest of the UK so we would expect up to 20% of households will still require paper questionnaires (a total of 471,000). We anticipate the breakdown of paper requests to be as follows:

    - Order Online 123,000
    - Order by Phone (automated) 168,000
    - Order by Phone (Advisor) 145,000
    - Order through Field Force 35,000

4. 100 hours should be allocated for Telephone Data Capture (TDC) where a contact centre advisor completes a census questionnaire live on the phone with a customer.

5. 625 hours should be allocated for CCS TDC where a contact centre advisor completes a 15 minute paper based survey live on the phone with a customer.

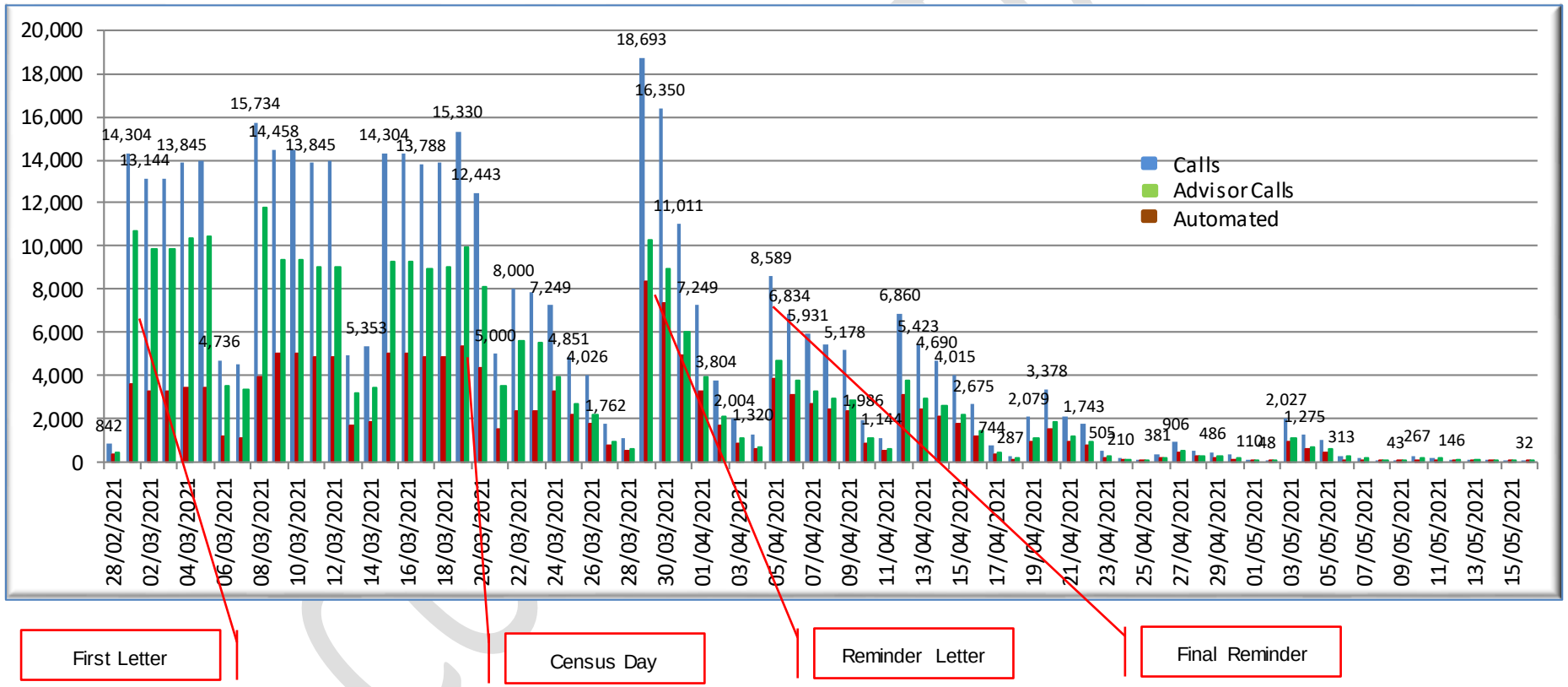
6. The experience of the rehearsal indicates social media response may be low however some social media contacts should be expected and included.

7. Research on email volumes (based on response in New Zealand census in 2018 and the NRS and ONS rehearsals in 2019) indicates at least 8,000 emails should be expected for the census in 2021.

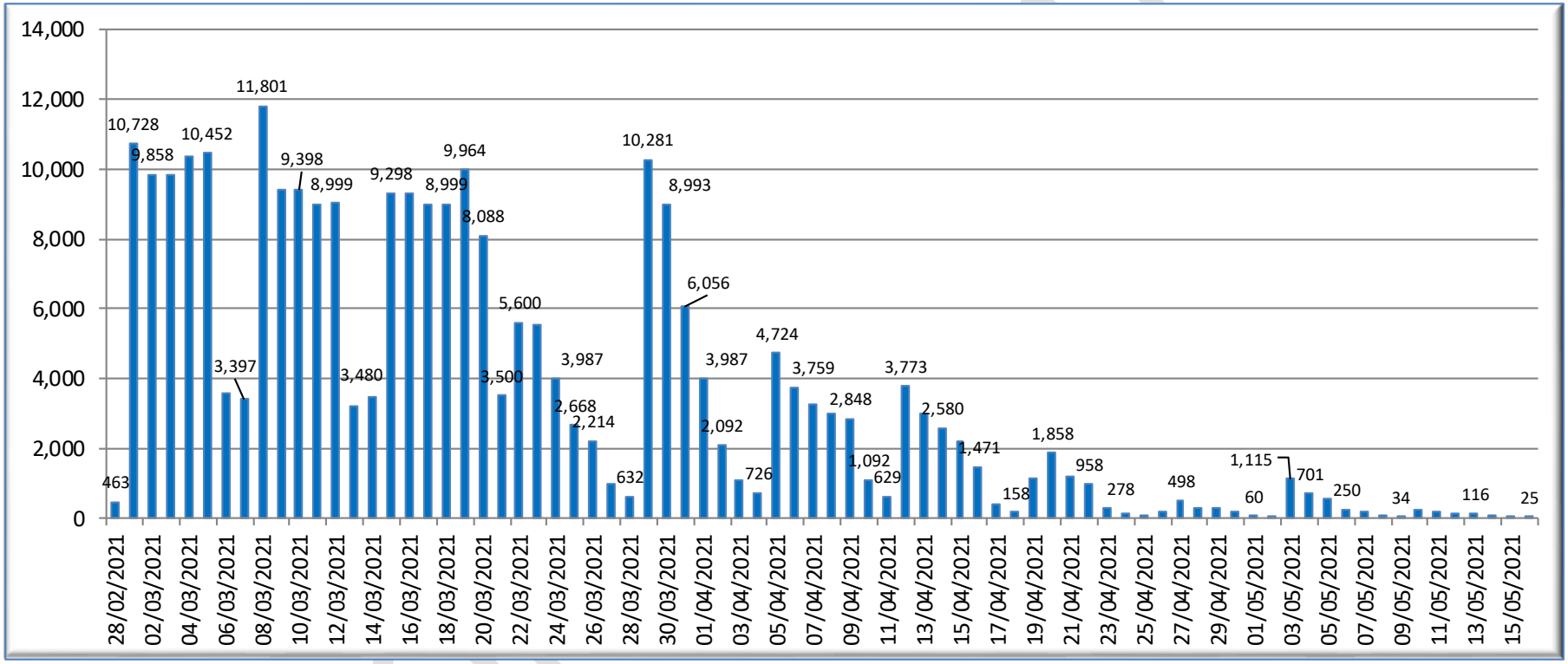
8. Call volumes and timings are heavily dependent on delivery of letters and reminders and are subject to change if the timelines change.

Census 2021 Predictive Demand

All Calls (Daily)



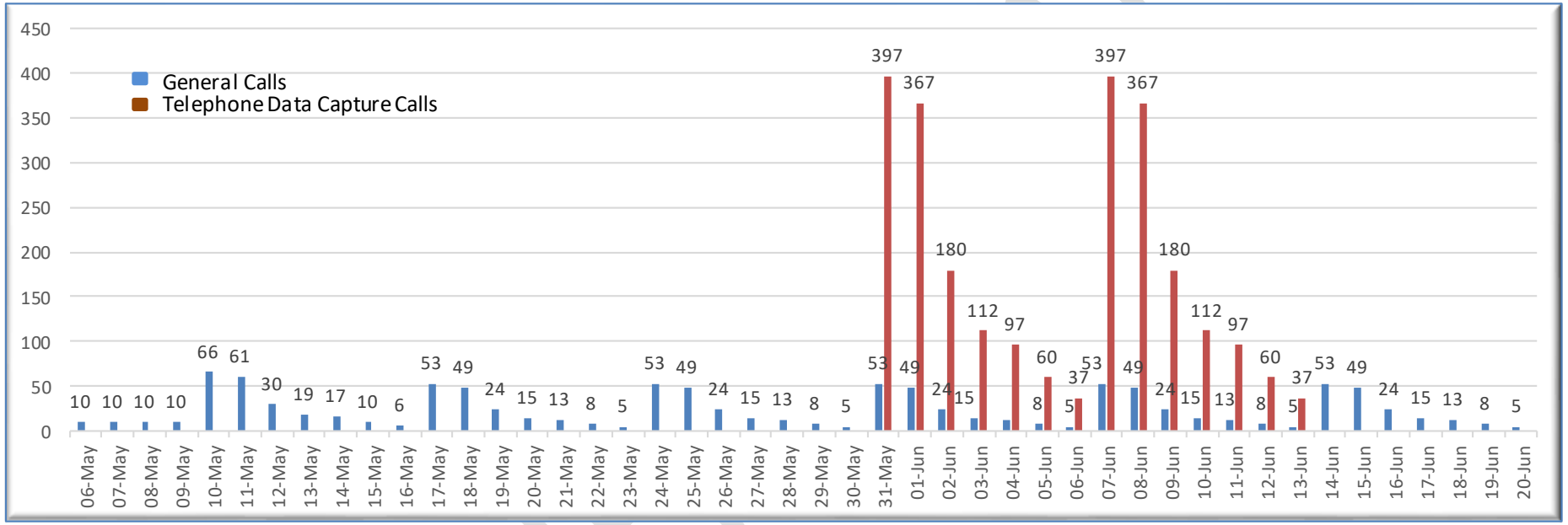
Census 2021 Advisor Calls (Daily)



Total General Information Advisor Calls (average 2.5 minutes)	262,445
Total Telephone Data Capture Calls (average 30 minutes)	200

The call spread figures will be reviewed once the enumeration strategy is finalised to reflect the exact dates when the remin der letters will be sent out.

Census Coverage Survey 2021 Advisor Calls (Daily)



Total General Information Calls (average 2.5 minutes)	1,084
Total Telephone Data Capture Calls (average 15 minutes)	2,500

APPENDIX THREE: CALL TYPES

The call types below detail analysis of the call outcomes from the 2011 census.

Call Types	Example	% of Total Calls
Property Questions	This is a business address, do I complete the form? I have two properties, which should I use? My address is incorrect, what do I do?	19.6%
Advisor Paper Questionnaire Requests		13.3%
Reminder Questions	I received a reminder but sent the questionnaire back two weeks ago, was it not received?	8.1%
Questions Clarifications	What is the Scots language? I'm here for six months, am I a permanent resident or a visitor?	7.4%
Field Force Visit	The enumerator didn't arrive yesterday, what happened?	7.1%
Customer Away / On Holiday on Census Day	I will be on holiday for two weeks, what do I do? My husband will be away for the weekend, do I include him?	6.6%
Household Questions	Should my baby be included? I have family staying that weekend, should they be included?	6.4%
Enumeration Process	Can I send it in now? Why have I not received it yet?	5.3%
Support Material Requests	Language print requests, braille questionnaire.	4.7%
Telephone Data Capture		3.4%
Language Requests	Requests to speak in another language.	2.8%
IAC Questions	My IAC and address don't match, how do I change it? My IAC doesn't work, can you fix it?	2.2%
Total		**86.9%**

Potential Escalations	
Call Subject	**Example**
Questionnaire	What is the methodology behind this question? Why is xx religion not included?
Suppliers	Can you send me a list of all your suppliers, I want to check they're all companies I approve of?
Census Management	How much does the Census cost the taxpayer? I don't see why I should complete a census, I'm writing to my MSP.

The volume of these question types is expected to be relatively small, however resolution and escalation paths will be created.

In the rehearsal in 2019, 68% of calls were customers asking for paper questionnaires as no paper questionnaires were sent out to customers in the first instance.

APPENDIX FOUR: ARCHITECTURE

1. Purpose of census architecture function

1.1 The census programme is a high profile, complex set of interdependent processes spanning multiple years and required to be delivered by many partners in time critical delivery periods throughout its lifecycle. For this reason an effective architecture function within the programme is crucial to aid successful coordination and delivery between the Authority and its delivery partners.

1.2 The programme has established an architecture function to hold the architectural vision, identify and manage the boundaries of census products and ensure the business objectives are met while maintaining a horizontal viewpoint.

1.3 Census suppliers will be expected to work closely with the architecture function and ensure that the delivery of solutions is aligned to the architectural principles and vision of the programme.

1.4 The architecture function operates on the principle of "just enough architecture" and thus aims to keep the function light and relevant to enable delivery of the programmes business objectives.

1.5 The 2021 Census programme is both a statistical exercise as well as a digital public service in Scotland. For this reason the census programme follows the Digital First Service Standard (DFSS) and the Generic Statistical Business Processing Model) (GSBPM). Other statistical architectural resources such as the Common Statistical Processing Architecture (CSPA) are also used as inputs to the 2021 Census Architecture.

1.6 Within this Appendix of the SoR further detail will be provided on:

- The architectural vision and context of the Contact Centre
- Census architectural principles, standards and reference material
- Architectural governance

2. Architectural vision and context of the Contact Centre

2.1 The architecture function has developed and will continue to develop the architectural vision for the census programme. The vision will enable all suppliers to have an understanding of how their product delivers to the census objectives and

vision as well as the interactions, interfaces and integration it requires with other census products.

3.0 Census Architectural Principles, standards and reference material

3.1 As noted in section 1.5 the census vision and architectural operating model is aligned to the DFSS and GSBPM. Additionally the programme has its own architectural principles to which we expect all census suppliers to adhere. When there is strong business justification for not following a principle, the Authority will consider this through the appropriate governance channels. It is also worth noting that principles will be regularly reviewed and updated throughout the census lifecycle, when any updates occur all suppliers will be informed.

3.2 As a statistical organisation, the Authority aligns the census programme to the GSBPM. This is evident in the descriptors used in the architectural vision. The GSBPM describes and defines the set of business processes needed to produce official statistics. It provides a standard framework and harmonised terminology for statistical organisations. Some of the terminology may be different to industry standard terminology used so it is recommended bidders familiarise themselves with the GSBPM as we expect all census suppliers to understand and be familiar with it. The GSBPM can be found at the following hyperlink: Generic Statistical Business Processing Model V5.0

3.3 The 2021 Census will be the largest single digital public services event of its time in Scotland. As a non-ministerial department of the Scottish Government, the Authority is also a key player in delivering the Scottish Government's digital vision. The digital strategy can be accessed at the following hyperlink: Realising Scotland's Full Potential In A Digital World: A Digital Strategy For Scotland

3.4 The DFSS is also a key reference point for census bidders. The DFSS is a set of criteria that all digital services developed must meet. The three themes within the standard are:

- User needs
- Technology
- Business capability and capacity

The DFSS can be found at the following hyperlink: Digital First Service Standard

The CSPA is an international reference architecture for the statistical industry. It provides a link between the conceptual link between the GSBPM and statistical production.

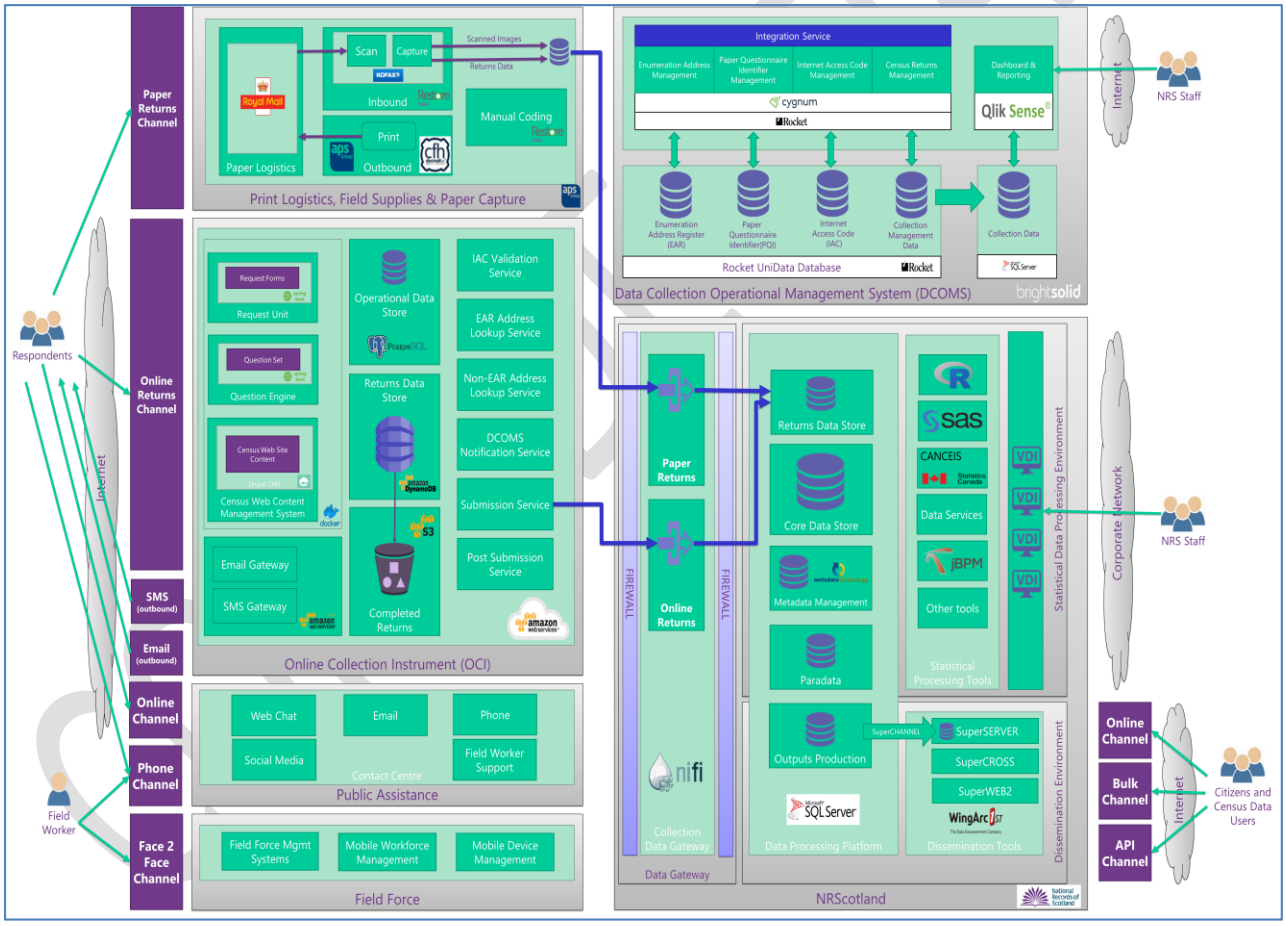
Further information on the CSPA can be found at the following hyperlink: CSPA

4.0 Architectural governance

4.1 In line with the overall programme governance, The Authority will employ architectural governance for all census suppliers. This will take shape in the form of a Technical Design Authority (TDA). Census suppliers will be expected to demonstrate to the TDA their compliance with the principles outlined and detail how the technical delivery of solutions will meet the business requirements. It is expected this will include technical detail on the tools, technology, and infrastructure including details of the technical design.

4.2 The TDA will meet as frequently as is necessary and the Authority expects to work with census suppliers to agree this as part of the delivery approach.

5.0 Architectural Overview



APPENDIX FIVE: DATA SECURITY REQUIREMENTS

1.	Data Security Requirements
Standards and Compliance	
1.1	Standards
1.1.1 Critical	The service and component services or products must be compliant with the UK Government's Minimum Cyber Security Standard (v1.0 issued June 2018). Compliance requirements with any updates or revisions will be managed through revisions of the Technical Security Standard (Appendix I).
1.1.2 Critical	Bidders are required to be compliant with the UK Government's Cyber Essentials Scheme and either be certified to the scheme (or Cyber Essentials Plus). Bidders who are not currently certified may submit their plan to be certified to the scheme with a target date.
1.2	**Cloud Security Principles**
1.2.1 Critical	Where any service is provided using public, hybrid or private cloud instances, or where cloud technologies are used to provide or support elements of the Service, the Supplier must meet the requirements detailed in the HMG Cloud Security Principles. Security reporting and alerting thresholds must be agreed with the Authority and documented. The Supplier will be required to document all Logging and Monitoring capabilities within component applications and infrastructure, even if these are not proposed to be implemented in the service delivered for the Authority. The Supplier shall demonstrate clearly, when asked, for any public, hybrid or private cloud data hosting services utilised in the provision of the Services, how solutions comply with and which of the designated levels of assurance they will provide for each of the Principles within the relevant NCSC Cloud Security Guidance referenced below: i. Cloud Standards and Definitions ii. Implementing Cloud Security Principles iii. Having confidence in cyber security.
1.2.2	The Supplier will need to describe how they shall demonstrate the solutions and services meet the applicable good practice measures outlined in the NCSC Protecting Bulk Personal Data guidance.

Data Protection	
1.3	Data Protection
1.3.1 Critical	The Supplier (including their Sub-contractors) will need to ensure that any proposed solution is both compliant with their obligations under Data Protection Act 2018 (DPA 2018) and enables Scotland's Census 2021 to comply fully with its obligations under DPA 2018. Particularly, suitable and sufficient records should be kept, and made available to the Authority on request, of design and implementation criteria, evidence and decisions for any functionality affecting personally identifiable data processing to meet both parties' obligations under Article 5 Para 2 and Article 25. The Supplier should describe their DPA 2018 compliance regime and how they intend to assure the operational use of the Service complies with their, and the Authority's, responsibilities under Articles 34(3) (Controller Responsibilities and Compliance) and Articles 57 and 103 (Data Protection by Design) in Technical Question 4 where mentioned.
1.3.2 Critical	To comply with legal obligations only certain development and operational activities will be permitted outside of the UK. Where a Supplier is proposing to host any data or provide development or operational activities concerned with their solution or service out with the United Kingdom, the Supplier should note that any such solution may require external approval by Central Government. Such approval may be out with the control of the Authority and the Supplier should be aware that approval may not be granted automatically.
1.3.3 Critical	Where a Supplier is proposing to host any data concerned with the solution or service out with the European Economic Area they should demonstrate how they intend to ensure that they comply with Sections 72 to 78 of the DPA 2018 (Transfer of Personal Data To Third Countries).

1.3.4 Critical	Census data must be stored in a manner that allows secure migration to systems or locations specified by the Authority and are securely retained until its secure deletion and/or destruction is ordered by the Authority. Any storage media which is used for non-ephemeral storage of census record data will either require transferring to Scottish Government custody when no longer required for the delivery of the service or product or be destroyed in accordance with the HMG destruction requirements in force at time of disposal. For information, current requirements can be found in the CPNI "Secure Destruction Standard."
1.3.5 Critical	The Supplier is required to protect Census data even when legislation (either from the country in which they, or their parent company, work or the jurisdiction in which they reside) exists which may compromise confidentiality by requiring them to disclose information of a confidential nature and with which they must comply. Example of such legislation would be the US CLOUD and PATRIOT Acts. The Supplier must provide a solution where: - the proposed solution avoids a conflict between non-UK legislation and the confidentiality requirements as expressed in this SOR and/or UK legislation (e.g. The Census Act as amended or the Data Protection Act 2018); - you would jointly work with the Authority to manage the public perception of the risk to data confidentiality presented by such external legislation, including example key messages. The Supplier must provide a solution whereby any Census Data able to be related to specific individuals will never be held or controlled by employees of companies who are subject to the Patriot Act, or similar legislative requirements. The Authority reserves the right to award only a contract that meets this requirement.
1.4	Data Confidentiality & Classification
1.4.1	All Census data is subject to the confidentiality and retention requirements of the Census Act 1920. Census record data and some census data will contain Sensitive Personal Data in accordance with Section 42 of the DPA 2018.

	Census record data has been classified as OFFICIAL SENSITIVE in accordance with the **HMG** Security Classification Policy. In addition, a local descriptor of CENSUS will be used to differentiate those data sets to which Section 8.2 of the Census Act 1920 applies. Other data sets or elements will be treated either as OFFICIAL SENSITIVE or OFFICIAL.
1.5	Security Governance
1.5.1 Critical	The Authority security requirements differ from and, in many cases exceed, those for other government services operating at the same classification. As such, all services and products will require the validation of security controls implementation and efficacy via the governance process before they can be used to support the Census in 2021. The Authority is establishing a rigorous Information Security Governance and management Framework programme to provide assurance of the solutions and activities undertaken to deliver the Census in 2021. Formal Accreditation of the systems, services or products supplied for the use of the Census 2021 Programme is mandatory and will be owned and facilitated by the Authority's in-house Security and Assurance Team. It will be the responsibility of the Technical Representative and/or Subject Matter Expert to manage the progress of the systems, services or products through the Formal Accreditation Process to gain accreditation. Successful completion of this process shall be one of the factors contributing to the successful delivery and completion of contractual milestones. The Formal Accreditation process will involve the signed approval from various business teams including, but not limited to, Architecture, Security, Testing and specific Subject Matter teams. This signed approval will attest to the satisfactory completion of deliverables and any associated remediation activities for the Governance arrangements under their specific remit e.g. formal acceptance of security Health Checks etc. The Supplier must comply with the policies, standards, processes and any other measures involved in the Governance Framework Programme.
1.5.2 Critical	It is the responsibility of the Supplier to ensure that they are meeting all the requirements of the Governance Framework and that they are fully engaged with the Security and Assurance team throughout their Contract duration.

1.5.3 Critical	The Supplier must ensure that any sub-contracts involving the transmission, processing or storage of data on behalf of the Authority contain appropriate clauses to cover the Census's responsibilities as detailed in this Section and the supporting Schedules.
1.6	Security Documentation
1.6.1 Critical	When asked, the Supplier must produce design and operational documentation to allow the Authority to assess the level of security designed in to and implemented within the product or service properly.
1.7	**Risk Assessment**
1.7.1 Critical	Information Risk Assessments will be conducted to the multi-stage Census 2021 "Attack Tree" Risk Assessment methodology. Support will be provided from the Authority and its independent security advisors to enable the Supplier to conduct and document the Risk Assessment for the service. The Supplier must be aware that a separate security risk assessment will be conducted, by the Authority, on the Supplier's corporate presence and capabilities. The scope of the assessment will depend on the delivery model that the Supplier is proposing and will include relevant sub-contractors.
1.8	**Accreditation**
1.8.1	A full Accreditation Documentation Set will be required for each separate system supporting the Service Provision. This will include the following items, as well as any documentation specific to the system: • System Description • Privacy Impact Assessment (completed by the Authority requiring co-operation from the Supplier and, if appropriate, their sub-contractors). PIAs will require to cover DPA 2018 Section 34(3) (Accountability and Compliance) and, DPA 2018 Sections 57 and 103 (Data Protection by Design) issues in detail. • Risk and Issues Register • Controls Statements – aligned to ISO27001:2013 • Business Continuity Plan – aligned to ISO22301:2012 • Forensics Readiness Pack – aligned to Census 2021 standards.

Security Management	
1.9	Information Security Management System
1.9.1 Critical	The Supplier must develop and maintain an Information Security Management System (ISMS) and ensure alignment of their technical controls with both the Cyber Essentials scheme and the specific Census technical security controls.
1.10	Security Working Group
1.10.1 Critical	The Supplier will be required to participate in the monthly Security Working Group. This group will focus on a common understanding and implementation of "good commercial security practice"[1] throughout the Census supporting infrastructure and will lead on the Technical Security Standard reviews. It may be practical for some attendees to join by remote means rather than physical attendance at the Authority's premises or another Edinburgh location.
Security Operations	
1.11	Overview
1.11.1	The Authority requires a consistent and effective view of security status and exposure across the range of systems and services that will support Census Operations. The Supplier and, where appropriate, their sub-contractors, must provide the Authority with comprehensive data on a range of security relevant statuses. Full details are provided in the "Technical Security Controls" section below and in the Technical Security Standard.
1.11.2 Critical	The Supplier (including their Sub-contractors) must ensure that all supporting infrastructure and applications are subject to a formal change and patch management process. This is to include standard and emergency change procedures, regression testing and compliance reporting as outlined in Technical Question 4.
1.11.3 Critical	Census requires a comprehensive and effective view of security relevant events in order to detect and respond appropriately to security events and issues. Full details are provided in the Technical Security Standard (Appendix Six).
1.11.4 Critical	Whenever the Authority supporting infrastructure is exposed to the internet or to other uncontrolled or untrusted networks, full network and security event data must be provided to the Security Operations Centre (SOC). The Supplier should be aware that it is

[1] As stated in the Cabinet Office "Managing Information Riskat OFFICIAL".

	currently intended to use the Scottish Government SOC, which uses a LogRythm-based environment.
1.12	Security Incident Management
1.12.1 Critical	Suppliers must co-operate, and ensure that their subcontractors are required to, and do, co-operate throughout the duration of the service provision, with the Authority and Scottish Government Security Incident Management frameworks and processes. This may include, but is not limited to: • Attendance at incident management meetings, including outside normal working hours. • Provision of, or co-operation in the delivery of, ad-hoc vulnerability assessments of exposed or potentially exposed services. • Ensuring that supplier contacts are available to conduct investigation and / or mitigation actions upstream of the Census contracted Service. • Shutting down or restricting access to affected or potentially affected systems. • Making available suspected compromised systems for digital forensic analysis. The Supplier will be expected to take part in Incident Management exercises.
Technical Security Controls	
1.13	Security Working Group
1.13.1	The appropriate level of technical security controls will be set and managed by an Authority-led Security Working Group, with planned meetings monthly and, if necessary, on an ad-hoc basis.
1.14	End-User-Guidance
1.14.1	The Supplier must comply with the National Cyber Security Centre (NCSC) guidance for securing End-User Devices. This is available from the Guidance section of the NCSC website.
1.15	Technical Security Standard
1.15.1	The Authority is aware that security standards will continue to evolve during the life-time of this procurement and where it expects standards or industry practice to change; detailed requirements will be published in the "Technical Security Standard". As the service or solution will need to be live at various periods throughout the Census lifecycle and maintain security, the published specifications for core security controls and techniques

	will be reviewed by the Authority at various points throughout the lifecycle. Interim reviews may be necessary in response to significant threat or security environment changes. Reviews of the Standard will be managed by the Security Working Group. The current version of the Technical Security Standard is published as an appendix to this document. The Supplier (including their Sub-contractors) must comply with all relevant aspects of this and future Technical Security Standards at the "minimum" and should comply at the "desirable" level. Where it is impractical for a supplier to comply at the "desirable" level, the non-compliance must be managed through the Census Risk Management Process.
1.16	Personnel Security
1.16.1 Critical	The UK Government Baseline Personnel Security Standard will be considered the minimum necessary for any supplier staff that will have access to Census data. The Supplier must ensure that the nominated personnel have undertaken the UK Government pre-employment process known as the Baseline Personnel Security Standard (Baseline Standard) and that this is currently valid. Where, due to nationality or residence issues, it is not practical to obtain BPSS, vetting to BS 8758:2012 will be required. The Supplier (and their Sub-Contractors) should be aware that some roles, particularly where bulk access to Census data is required or involving Security Operations or investigations functions, may be required to undergo UK Security Vetting. The Authority will facilitate the sponsorship of security vetting clearances where these are not already held at cost to the Supplier. The Supplier (and their Sub-Contractors) should be aware that any role which may require the employee to be in contact with potentially vulnerable individuals will require vetting under the Disclosure Scotland "Protecting Vulnerable Groups" scheme.
1.17	Physical Security
1.17.1	**Standards and Specifications** Good commercial security practice is considered appropriate for working at OFFICIAL SENSITIVE; therefore there are no specific

	HMG or Authority requirements for physical security measures in administration and operational areas. Where, in the answers to any of the questions in the Technical Questions section any security measures are installed and maintained in compliance with British, European or International standards, the standards and the level of compliance and / or certification should be provided in the appropriate answer section.
1.17.2 Critical	Data Centres are to comply with TIA-942 at the Rating 3 or Rating 4 levels and compliance with EN-50600-2-5 is recommended. Other hosting environments will require to be secured to an appropriate level, dependant on the nature of the data being processed or stored.
1.18	Business Continuity and Disaster Recovery
1.18.1 Critical	The Contact Centre, and its supporting services, is designated as "Essential to Census Operations", in accordance with the Census 2021 Business Continuity (BC) and Disaster Recovery (DR) Strategy. Recovery Time Maximum is 4 Hours (during live operations) The Recovery Point Objective is 4 Hours. Special BC/DR Requirements: None
1.18.2 Critical	The Authority will manage business continuity plans across the census operation and feeding into this will be both fully resourced and tested disaster recovery and service continuity plans and capabilities provided as part of the solutions developed by the Supplier. The Supplier shall have in place detailed disaster recovery and business continuity plans and procedures in respect of any applicable services provided under this contract. These plans and procedures must be made available to the Authority for agreement following the award of the contract. It is then up to the Supplier to maintain appropriate technology, processes, procedures, security and testing to ensure that the Return to Operation (RTO) and Recovery Point Objective (RPO) expectations are achievable in the event of foreseeable events.

1.18.3 Critical	As a minimum the Supplier (including their Sub-contractors) must adopt to an auditable approach to ISO 22301:2012 (Business Continuity Management) to their entire dealings with the Census programme and will work with the Authority to understand any trade-offs to that standard for instance between the standard and security implications or cost. ISO 27031:2011 (Guidelines for information and communication technology readiness for business continuity) should be used for further guidance. A full disaster recovery test will be required as part of the Security Governance validation process. The Supplier should note that malicious (or suspected malicious) events will be handled within the Information Security Incident Management framework and should not be incorporated in the answer to this section.
1.18.4 Critical	The Supplier (including their Sub-contractors) must implement a backup/recovery and restore strategy that, as well as meeting the business continuity requirements, is resilient to equipment failure, and to loss or denial of access to any relevant location. The Supplier must provide the right and any assistance required by the Authority to question, test and assure the quality of any proposed and implemented solutions and shall be responsible for rectification on demand in the run up to the Census 2021.

APPENDIX SIX: TECHNICAL SECURITY STANDARD DECEMBER 2019 V 2.5

1. Introduction

1.1 Mandatory Standards

National Records of Scotland is mandated to abide by, and will ensure that all systems and services are compliant with the following standards:

- The HMG Security Policy Framework including:
  - The Minimum Cyber Security Standard
  - Personnel vetting policies.
- Cyber Essentials

It is noted that the Scottish Government has directed that organisations will achieve "Cyber Essential Plus."

1.2 Review

Minimum: This standard must be reviewed on at least an annual basis.

1.3 Changes in the landscape

Numerous updates to UK and international data security standards are expected in the period between January 2020 and the next review of this standard.

- The HMG "Government Functional Standard for Security" is being published by individual elements. The "Minimum Cyber Security Standard" was the first release but the timescale and order of future releases release is unknown. Updates to these may cause changes to this TSS.
- TLS 1.3 has been finalised and approved by IETF and is beginning to be implemented.
- Reports of supply chain attacks are beginning to proliferate but substantiated attacks, except against software releases, remain rare. All Census service providers should be aware of issues regarding supply chain security (ISO27001 A.14 & A.15).
- The increasing threat from the release of professionally engineered exploit code, particularly Day 0 threats, imposes a requirement for tight patch application cycles and comprehensive patch management. Issues affecting embedded systems are particularly concerning and all areas supporting Census will need to be fully aware of any dependence or other use of devices with embedded general-purpose computing operating systems.
- There will be an increased focus in firmware patching due to new speculative execution based attacks, like SPECTRE.
- Browser restrictions on non-CTS certificates and weak algorithms are beginning to cause end-user issues, particularly with HTTPS services provided from firmware.

1.4 Definitions.

- **Desirable**: this is a standard that should be implemented, but is not currently required. It may become the required standard in due course.
- **Minimum**: this is a configuration standard that is required.
- **Deprecated**: must not be used; this is usually an old standard that is no longer secure.

1.5 Scope

This document only applies to NRS owned or operated systems or facilities that are brought into production after 1 Jan 2019 and to all Census 2021 supporting systems regardless of initial date of introduction.

Sections B & D of this document applies to all NRS internal systems and also to all suppliers that manage or supply NRS systems.

Section C is mandatory for all NRS internal systems and to all suppliers that supply non-Census 2021 systems. Census 2021 suppliers should consider this section as the NRS Security interpretation of the equivalent Census contractual security requirements.

Section E is mandatory for Census 2021 suppliers and should be considered "good practice guidance" for other NRS suppliers.

1.6 Waivers and Dispensations.

Where a project is unable to comply with the requirements of this document, the project must apply to the NRS Architecture Review Board for a dispensation or waiver.

Where a project decides to meet the minimum requirements but not the desirable standard, this should be risk managed at the project level.

2. Mandatory for all NRS internal systems and all suppliers.

2.1 System Hardening

Minimum: All servers are to be hardened before the devices are brought into service.

2.1.1 Standards

Minimum: Machines are to be hardened to, or local standards based on, one of the following standards:

- Microsoft Security Baseline standards for Windows machines.
- Center for Internet Security hardening guides.
- Scottish Government Server Hardening Guides
- National Cyber Security Centre Guidance

Where no standards are available from the above organisations or where the available standards are inappropriate for a specific application, vendor standards should be used.

Hardening standards must be reviewed annually or following a significant and relevant vulnerability announcement. Additional ad-hoc reviews may be required as part of post-Incident activities.

2.1.2 Specific Implementation requirements

Minimum:

- Hardening the network against credential theft and lateral movement. The objective is to mitigate against lateral movement and Active Directory user/admin privilege escalation during an attack.

- The network must be segregated so that only required connections are allowed between different security domains and machines.

- Segregation of Admin groups.
  - Separate admins for separate types of machines and/or networks.
  - Domain administrator accounts and other privileged accounts must not authenticate to lower trust servers and workstations

- Hardening of all machines to make it more difficult for attackers to get passwords or hashes from machines.

2.1.3 Windows PowerShell.

Desirable : Constrained language mode – this can interfere with legitimate operational use, so testing is required before implementation;
Deprecated: PowerShell V.2 must be removed.

2.1.4 End User Devices.

- **Desirable:** Cabinet Office guidance defines standards for mobile laptops with a "thick" operating system installed, such as Linux, Windows or MacOS X. The standard and guidance can be found within the NCSC End User Device Security Collection guidance pages.

2.2 Operating System and Application Patch Status

System administrators must be able to react quickly to vendor security patches.

2.2.1 Update Frequency

Desirable: Emergency update available within 4 hours (in response to incident.) Planned updates within 1 week (this time period must include all regression testing.)

Minimum: (Internet Connected environment): Update within 1 week.

Minimum: (Isolated environment): Update on a monthly basis.

2.2.2 Reporting

Minimum: Daily reporting (suppliers should ensure that they have access to real-time or ad-hoc reporting for incident response purposes).

The implementation of patches without a security component or impact should be run within the existing Change Management process.
Service Providers should note that, contrary to the above requirements for security patches, in periods leading up to or of Census Operations the business preference is likely to be for code and component stability (i.e. a weak "code freeze"), rather than speedy update.

2.3 Anti-Malware

2.3.1 Toolsets

All systems must control unapproved code:

- **Desirable**: Application white-listing security software on the device
- **Minimum**: operating system level anti-virus/anti-malware installed
- Where appropriate, specialist application (eg database) anti-virus is to be used.

Anti-malware Updates.

- **Desirable**: Auto-update on push from the vendor or polling on an hourly basis (as applicable to the solution selected.)
- **Minimum** (Internet Connected environment): Auto-update polling on a daily basis (as applicable to the solution selected.)
- **Minimum** (Isolated environment): Update on a weekly basis.

Minimum : All software and files downloaded from the Internet must be screened and verified by anti-malware solution

2.3.2 Reporting.

- **Desirable**: Online and automated real-time dashboard (or feed to the NRS reporting toolset) showing compliance status of all relevant devices.
- **Minimum**: Daily reporting.

2.4 User Access Management & Authentication

2.4.1 Account Rules

Minimum : The use of special privilege accounts must be restricted and controlled.

Minimum: User privileges and data access rights must be clearly defined and reviewed periodically. Records for access rights approval and review shall be maintained.

Minimum: All user privileges and data access rights must be revoked after a pre-defined period of inactivity or when no longer required (NRS 3 and 6 month rule).

Minimum: Each user identity (user-ID) shall uniquely identify only one user. Shared or group user-IDs shall not be permitted unless explicitly approved by the NRS Head of Information Security.

2.4.2 Authentication & Passwords

All users are reminded of the change in GCHQ password advice available from NCSC.

Minimum: All vendor-supplied default passwords must be changed before any information system is brought into service

Desirable: Privileged users should start to use multi-factor authentication. MFA should be incorporated in all development or infrastructure plans.

Minimum: Consecutive unsuccessful log-in attempts shall be controlled.
Minimum: When stored, passwords must be salted[2] and hashed.
Minimum: Inactivity timeouts on management interfaces will be set to no more than 10 minutes.

2.5 Encryption

2.5.1 Key management.

- **Minimum**: Service Providers will be required to have a fully operational and auditable key management process, including disaster recovery capabilities.

[2] Salt length must be at least equal to the hash length and salts generated through a robust PRNG.

2.5.2 Encryption in Transit.

- **Minimum:** All HTTP interfaces are to be served as encrypted (TLS / HTTPS) by default.
- **Minimum**: all remote administrative access must use encrypted protocols.
- **Deprecated**: Telnet
- **Desirable:** Encryption in transit should be implemented for all data flows. Data may be transferred in clear where the data flow is entirely within a single trusted network segment.

Examples of unencrypted and encrypted protocols for guidance.

Unsecured (un-encrypted) Protocol	Secured (encrypted) Protocol
Telnet	SSH
HTTP	HTTPS
FTP	SFTP
SNMP v1, v2	SNMP v3

2.5.3 Encryption at Rest.

- **Minimum**: Where a device that forms part of any solution or product is not permanently held within a physically secure boundary, it must have storage device level encryption applied.
  - For Windows devices the default method should be Bitlocker.
- Where any element of backup provision uses tape storage, consult with NRS or Census Security, as appropriate, to determine appropriate security measures which may include tape encryption.

2.5.4 Encryption Algorithms

Notes:

1. Use of quantum cryptography resistant ciphers is not currently required, but is under regular review.
2. There is no anticipated requirement for the use of GCHQ cipher suites or KeyMat.

Requirements:

- SSL / TLS, OpenSSL
  a. **Minimum:** systems using TLS/SSL must be able to support TLS1.2;
  b. **Desirable:** TLS1.3; support for TLS1.3 must be incorporated in all development or infrastructure plans.
  c. **Deprecated:** Support for SSL and earlier variants of TLS (i.e. TLS1.0 or TLS1.1) must be disabled.

- SSH
  a. **Minimum:** SSH Protocol Version 2

b. **Deprecated:** SSH Protocol Version 1 - this must be disabled.
d. **Desirable:** Public Key or GSSAPI authentication may be required for connection to high impact services.

- Cipher Suites.
  a. **Desirable:** AES256 / SHA-256
  b. **Minimum:** AES-128 / SHA-256;
  c. **Deprecated:** RC4 (arcfour), DES, 3DES - these must be disabled;
  d. Use of Elliptic Curve ciphers is permitted;
  e. Key length and other protocol parameters for specific proposed use cases will be available from the Security team on request.

- Key Exchange
  a. **Minimum:** 2048-bit or stronger Diffie-Hellman groups, Elliptic Curve Diffie-Hellman (ECDH);
  b. **Deprecated:**
     - weaker than 2048-bit DH Groups.
     - Key exchange suites not offering Perfect Forward Secrecy, eg use of RSA for encryption and authentication such as TLS_RSA_WITH_AES. A full list of deprecated suites otherwise permitted in TLS 1.2 can be found at Appendix A of RFC 7540.

  Note that this does not imply that RSA is not permitted in encryption usages where Perfect Forward Secrecy is not required.

- Hash Algorithms.
  a. **Minimum:** SHA2 family;
  b. **Deprecated:** MD5 and SHA1 must be disabled.
  c. Hash algorithms specifically designed for password applications are permitted in context. Advice on specific algorithms and key lengths should be sought from NRS or Census security.

2.6 Forensic Readiness

Desirable: A "Forensic Readiness Pack" should be available for all systems. The purpose of this pack is to enable incident responders to quickly identify what, primarily operational, data is available from a system and how to access it.

For each data type processed by the system, the Pack should include:

- What data elements are retained.
- How long data elements are retained, in live and in archive.
- The location of data storage, in live and in archive.
- How to access the data (including 24x7 contact details for relevant shift supervisor etc.)

2.7 Web Interfaces

All interfaces using HTTP and browser technology should be able to:

- **Desirable:** Log the browser user-agent string, the security negotiation protocol and the cipher suite negotiated.
- **Desirable:** Where public access is provided to the interface, reject connections that do not manage to achieve a specified (but configurable) level of security.

Where a connection is rejected, there must be a facility to configure, depending on the level of security achieved:

- **Minimum:** Display an appropriate, NRS branded and configurable, warning page and close the connection.
- **Desirable:** Display an appropriate, NRS branded and configurable, warning page and give the user the option to proceed.
- **Desirable:** Display an appropriate, NRS branded and configurable, warning page and refresh to the main site after a short period.

Where an application is available to the internet or another large untrusted or low trust community:

- **Desirable:** A web application firewall or similar boundary protection should be in place.

2.8 Security Operations

2.8.1 Event logging and reporting.

Minimum:

- Security Devices. All security enforcing devices (including but not limited to firewalls, routers employing ACLs, IDS & IPS, I&AM and Privilege Management services) must record all relevant events and be capable of streaming them to the NRS logging and alerting toolset.
- Other Devices. All managed infrastructure devices, operating systems and applications must be capable of recording defined Security Events; be capable of and, during periods of high risk or test phases, stream them to the NRS logging and alerting toolset.

Minimum: Operations must provide regular and be able to provide ad-hoc vulnerability scan reports for all of their infrastructure in production.

Minimum: Logs shall be secured such that they cannot be modified, and can only be read by authorised persons.

Minimum: The clocks of information systems shall be synchronised to a trusted time source to ensure synchronisation of logs captured.

3. Mandatory for all NRS internal systems & non-census suppliers.

3.1 DNS

Desirable: it is recommended that the UK public sector DNS be used.

3.2 Email

Government email must be secured in line with the Government email security standards.

These include :

- **Minimum:** Using Transport Layer Security (TLS) 1.2 or later when sending or receiving email.
- **Minimum:** Using Domain-based Message Authentication, Reporting and Conformance (DMARC), Sender Policy Framework(SPF) and Domain-Keys Identified Mail(DKIM) to help protect your domain from spoofing.

3.3 VPNs

Minimum: Ensure IPSec or TLS VPN. VPN server must be maintained and patched.
Deprecated: Aggressive mode IKE, DES encryption, MD5 and SHA-1 integrity checking
Minimum: Enforce both AH and ESP features (providing authentication and confidentiality)

Desirable: Client-side certificates are recommended for machine authentication when using a VPN. Certificates have several advantages over Pre-Shared Keys (PSKs), including the ability to revoke just one certificate on your network and to store private keys securely (e.g. in a TPM or TEE).

For recommended encryption and hashing algorithms in IPsec configuration, additional information is available here.

Desirable: Regularly audit VPN users to identify rogue accounts. Attackers can persist in large environments by adding new accounts having compromised Active Directory, or other authentication vectors.

3.4 Backups

Back up media containing NRS business mission critical information shall be sited at a safe distance from the main site in order to avoid damage arising from a disaster at the main site.
Minimum: Backup media should also be protected against unauthorised access, misuse or corruption.

Minimum: Backup restoration tests must be conducted at least annually.

3.5 Security Testing

Professional independent penetration testers should be used to test whether a system/service is secure. When it comes to digital services there are two types of penetration testing that may need to be completed:

- Web app penetration testing which is concerned with the security of the applications built or deployed
- Infrastructure penetration testing which is concerned with the underlying infrastructure, networks, operating systems and platforms.

There are various different schemes which provide penetration testing services such as Tiger, CREST and CHECK. The decision regarding the security testing requirements should be cognisant with the sensitivity of the data and any security connectivity or accreditation requirements. The scope and levels of testing required should be agreed with the NRS security team.

Minimum: All externally available services must be signed up for NCSC public sector monitoring services, including Webcheck, CNR.

Minimum: For PSN connectivity an annual CHECK penetration test must be completed.

Minimum: For NRS public facing websites which hold OFFICIAL- SENSITIVE personal information an annual CHECK penetration test must be completed.

4. Personnel Security

Note: This element of the standard will be transferred to other NRS Policy documents in due course.

4.1 Vetting

Minor amendments to the UK Security Vetting, BPSS and disclosure regimes are expected to continue. Material changes are not forecast.

Details of the regimes are available in the relevant publications:

- UKSV
- BPSS
- Disclosure Scotland

4.2 Training

Service Providers are required to have induction and continuing and update security awareness training implemented for all staff, including Data Protection. Staff involved on the Census programme will be required to have specific induction and update training provided on the HMG Security Classification Scheme and the Service Provider's roles and responsibilities framework for handling Census data.

4.3 Minimum

- The minimum standard for NRS staff (including temporary staff) and supplier staff involved in Census projects is BPSS and completion of a Census Confidentiality Undertaking.
- For staff involved in non-Census projects who will not be expected to require regular and unsupervised access to NRS premises, a CCU is not required.
- Where, for reasons of nationality or residence, BPSS is not practical, vetting to BS7858 (currently 2012 issue) is acceptable.

4.4 Security and Privileged Roles

- **Minimum**. Specified security roles may require UKSV to SC level.

Suppliers should note that extending the requirement for SC to certain privileged access roles is being considered.

5. Physical Security

5.1 Data Centres

Minimum: Data Centres are to comply with TIA-942 at the Rating 3.
Desirable: It is recommended that Data Centres comply with TIA-942 at Rating 4 levels and also with EN-50600-2-5.

Note that Uptime Institute assessments at Tier 3 or Tier 4 are acceptable in place of TIA-942 Ratings.

5.2 Other Premises

Detailed guidance on the following areas of physical security is expected to be published as part of the 2019 update of this standard:

- Perimeter Security
- Security Guarding
- Access Control
- Visitor Management
- Intrusion Detection
- Limited Access Areas
- Security Containers

APPENDIX SEVEN: GLOSSARY OF TERMS

Key Word	Definition
Abandonment Rate	The percentage of inbound phone calls made to a call centre or service desk that are abandoned by the customer while waiting on hold before speaking to an advisor.
Address	A place where a residence or organization is located.
Contact Centre Advisor	Contact Centre advisors are the first point of contact for customers, dealing effectively with requests and queries. Advisors often deal with customers via telephone, e-mail, web chat and social media.
Architecture	Discrete and focused business operation or activity to support the census operation, assisting in the translation of requirements into a solution vision, high-level business and/or IT system specifications, and a portfolio of implementation tasks.
Automatic Call Distribution (ACD)	An automatic call distribution system (ACD) is a telephony device that answers and distributes incoming calls to a specific group of terminals or agents within an organization.
Average Handling Time (AHT)	Average Handling Time refers to the calculation of the average time spent on customer contact. The actual amount of time an advisor spends on all aspects of customer contacts, including any additional time spent after the direct contact, for example updating a system or contact related paperwork is divided by the number of customer contacts.
Average Talk Time (ATT)	Average Talk Time refers to the actual amount of time an advisor spends on a customer call and does not include any additional wrap time or post call paperwork.
British Sign Language (BSL)	The sign language of some deaf people in the UK.
Backup / Recovery	Process of backing up data in case of a loss and setting up systems that allow that data recovery due to data loss. Backing up data requires copying and archiving computer data, so that it is accessible in case of data deletion or corruption.
Business Continuity and Disaster Recovery (BCDR)	Business continuity and disaster recovery (BCDR) are closely related practices that support an organization's ability to remain operational after an adverse event. The goal of BCDR is to limit risk and get an organization running as close to normal as possible after an unexpected interruption.
Customer / Contracting Authority	referred to in Call Off Terms and Conditions - means "Authority" throughout this SOR
Capture	Capture is the process by which a return is converted into a suitable electronic format (in the case of paper returns) and is matched to an electronic template ready for coding.

Census Address	Any address that is used in the Scotland Census programme 2021.
Census Address Register (CAR)	The Census Address Register is dataset containing a list of all Census Addresses and their sub-addresses.
Census Coverage Survey (CCS)	The Census Coverage Survey is a voluntary, independent, post-enumeration, representative, sample survey used during coverage adjustment to produce population estimates.
Census Data	All data collected or created for the purposes of running the Census Operation and in the generation of Census Outputs.
Census Date	The day to which the census returns should relate.
Census Record Data	Individual, household or communal establishment data required for the generation of Census Outputs.
Census Rehearsal	A test of the census processing systems and operational processes using a reduced level of online census questionnaires data capture.
Coding	Coding is the process by which the value of a variable is assigned a code from the responses given by an individual or household. There are three types of coding: • Point of Contact • Traditional • Derivation Coding can occur in two ways: • Automatic • Manual
Collect Phase	This period of the census covers the capabilities and processes required to collect respondent data via online and paper channels and to load that into appropriate processing environment. The focus of this phase is on the enumeration process to make initial contact with an address, to collect an appropriate response from that address, to follow-up non-responding addresses and to encourage increased response across Scotland.
Communal Establishment	A communal establishment is typically managed residential accommodation where there is full-time or part-time supervision of the accommodation.
Communal Establishment Questionnaire	A questionnaire for a communal establishment, about the establishment itself, for a Communal Establishment Manager to complete.
Communal Establishment Individual Questionnaire	A questionnaire for an individual living in a communal establishment.
Centre for the Protection of National	The United Kingdom government authority which provides protective security advice to businesses and organisations across the UK national infrastructure.

Infrastructure (CPNI)	
Data Collect (Phase)	The phase in the Census Operation where data is collected, before it is statistically processed.
Data Collection Operational Management System (DCOMS)	DCOMS is an interactive, response and tracking system that supports Data Collection.
Decommissioning (Phase)	The phase in the Census Operation when all data that is required to be kept is extracted for future processing and all data and systems that are no longer used are stood down and purged.
Disaster Recovery	A set of policies and procedures to enable the recovery or continuation of vital technology infrastructure and systems following a natural or human-induced disaster.
DTMF Tone	DTMF (dual tone multi frequency) is the signal to the phone company that is generated when an ordinary telephone's touch keys are pressed.
eForm	An eForm (electronic form) is an online form accessed from a website which can be completed by a user or customer and sent direct to an organisation in the same format as an email.
Enumeration Address Register (EAR)	A register of enumeration addresses, their sub-addresses and associated information created for the data collection operation and maintained throughout the census operation.
ESPD(Scotland)	European Single Procurement Document (ESPD) Scotland is a self-declaration of the businesses' financial status, abilities and suitability for a public procurement procedure.
Field Force	Individuals working as part of a team who deliver census enumeration strategy and encourage and assist members of the public to complete the census.
Field Worker	A member of the Field Force.
First Contact Resolution (FCR)	First Contact Resolution is the number of contacts that properly address the customer's need the first time they contact an organisation thereby eliminating the need for the customer to follow up with a second contact.
Frequently Asked Questions (FAQs)	Frequently asked questions or Questions and Answers (Q&A), are listed questions and answers commonly asked in some context, and pertaining to a particular topic. The format is commonly used on websites and online forums, where certain common questions tend to recur.
General Data Protection Regulation (GDPR)	A legal framework that sets guidelines for the collection and processing of personal information of individuals within the European Union (EU). GDPR sets out the principles for data management and the rights of the individual, while also imposing fines that can be revenue based.

Geography	For the purposes of this document Geography refers to the Geography team within NRS. This team shall provide the initial addresses for the Census Address Register.
Hosting Environment	The technical environment where the data and system reside.
HMG	Her Majesty's Government.
Household	• One person living alone, or • A group of people (not necessarily related) living at the same address who share cooking facilities and share a living room, sitting room, or dining area. A household may also be: • a person or a group of people living in sheltered housing or very sheltered housing (irrespective of whether there are other communal facilities), • a person or a group of people living in a temporary or mobile structure (for example a caravan, mobile home or boat) on any type of site that is their usual place of residence.
Household Individual Questionnaire	A questionnaire for an individual in a household offered on request. Guidance: A separate IAC will be allocated for these, linked to the appropriate address.
Household Questionnaire	A questionnaire for a householder to complete.
Interactive Voice Response (IVR)	An IVR system is a technology that allows a computer to interact with humans through the use of voice and DTMF tones input via keypad. In telecommunications, IVR allows customers to interact with a company's host system via a telephone keypad or by speech recognition, after which services can be inquired about through the IVR dialogue. IVR systems can respond with pre-recorded or dynamically generated audio to direct users on how to proceed further.
Internet Access Code (IAC)	An Internet Access Code is linked to a census address or census sub-address and is provided to the respondent. This can be either a household or a communal establishment census address or census sub-address. The IAC is used by the respondent when they log into the online instrument and associates the response with a census address or census sub-address. A census address or census sub-address can have more than one IAC.
Iterative Development	Iterative development is a way of breaking down the software development of a large application into smaller chunks. In iterative development, feature code is designed, developed and tested in repeated cycles.
Metadata	Data that defines and/or describes other data.
Non-response Return	A non-response return is a rules-generated return based on information provided by field force during follow-up fieldwork. Non response returns will be created for every census enumeration

	address that has not returned a census questionnaire. In addition to the unique address identifier, it will contain the perceived reason for non-response along with field force responses to significant questions relating to the address.
Occupancy Rate	Occupancy is the percentage of time agents spend handling calls and wrap time (completing other tasks associated with the call such as updating a database, sending emails etc) compared with the total amount of time they are logged in and ready, waiting for calls to arrive.
Online Return	The return for an online questionnaire, which is stored in an electronic format.
Online Collection Instrument (OCI)	The online web developed system for completing the online census. The system must work across multi device types, multi browser types, multi operating systems.
Operational Information	All Census Data used for running the Census Collection process excluding Census Record Data.
Paradata	Data about the process by which raw survey data are collected, such as how long it took a respondent to complete a questionnaire.
Product Owner	The product owner is the person with clear vision of what he or she wishes to build, and convey that vision to the development team.
Public Assistance	Services provided to the respondents by Scotland's Census 2021 to assist them in completing the census either online or on paper. For example, language translations and Contact Centre help.
Questionnaire	A questionnaire is a linked, routed set of questions, the purpose of which is to gather information from respondent(s) in a digital or paper format.
Quality Gate	A milestone in a software project, located before a phase that is strongly dependent on the outcome of a previous phase. They are especially useful between phases in which breaches in disciplines must be overcome.
Return	An individual, communal establishment, household or enumerator response to a questionnaire, which may be stored in electronic or paper format.
Security Governance	A process of establishing and maintaining a framework to provide assurance that information security strategies are aligned with and support business objectives, are consistent with applicable laws and regulations through adherence to policies and internal controls.
Service Levels (SLs)	Service levels for the duration of the operation that have been agreed by the Authority and the Supplier.
Schedule Adherence	The adherence of advisors to their shift and breaks schedule that has been developed to maintain service levels.

Shrinkage	Contact centre shrinkage is a measure of how much time is lost in the call centre to things like vacation, breaks, meetings, lunch, holidays, sick time, training etc.
Speech Recognition	A telephony system that recognises the human voice and is able to carry out spoken commands.
Support Hub	A Support Hub is part of a network of locations, for example a library, where members of the public can go for support with their census questionnaire, either to complete their questionnaire online using the Hub's equipment or to ask questions and receive general help and support.
Telephone Data Capture (TDC)	Telephone Data Capture is where an advisor completes a census questionnaire on behalf of a member of the public online during a live call.
User Acceptance Testing (UAT)	Software users testing a system to ensure it can handle required tasks in real world scenarios prior to going live.
User Experience (UX)	User experience refers to a person's emotions and attitudes about using a particular system or service. It includes the practical, experiential, affective, meaningful and valuable aspects of human–computer interaction and product ownership.
User Journeys	A path that a user may take to reach their goal when using a particular website or IT system. Used in designing websites to identify the different ways to enable the user to achieve their goal as quickly and easily as possible.
User Needs	User needs are the needs that members of the public, businesses or customers have of the census, including how to complete it and support to complete it.
Web Chat	Web Chat is a type of internet online chat that allows users to communicate in real time using an easily accessible web interface. It is usually simple to use and accessible through a web page as no software download is required.
General Correspondence	Unsolicited mail from members of the public.
Wrap Time	Wrap time refers to the amount of time an advisor spends on after call work once they have finished the call with a customer, for example adding data to a system, recording outcomes or completing paperwork. Sometimes referred to as after call work.

APPENDIX EIGHT: TENDER EVALUATION

1. PURPOSE

In order to ensure that National Records of Scotland (NRS) appoint a Supplier that can meet our requirements in relation to security, as well as demonstrating best overall value for money, Suppliers will be required to respond to the statements and questions contained within this document.

There are three sections within this document:

- **Security Requirements/Questions** – Responses to the mandatory questions in this section will be assessed as Yes / No / Willing to Obtain answers;
- **Technical Questions** – Responses to these questions will be evaluated by the NRS Technical Evaluation Team and scored in accordance with the scoring criteria listed below each question;
- **Pricing Schedule** – pricing will be evaluated as detailed below at 2. Weightings and Evaluation Process.

In submitting a tender in response to this procurement exercise you are confirming that you have read, understood, and are able to deliver all requirements detailed within the Statement of Requirements (SoR) fully.

2. WEIGHTINGS AND EVALUATION PROCESS

The Quality / Cost weighting that will be applied to evaluation of the tenders received will be 70% Quality / 30% Price.

The following (Quality) weightings will be applied to each question:

Security Requirements				
Question No	**Yes**	**No**	**Willing to Obtain**	**Mandatory**
3,1,2				
3.2.1				
3.2.2				
3.3.1				
3.3.2				
3.3.3				
3.3.4				
3.3.5				
3.4.1				
3.5.1				
3.6.1				
3.6.2				
3.6.3				
3.7.1				
3.8.1				
3.9.1				
3.9.2				
3.10.1				
3.11.1				
3.12.1				
3.12.2				
3.12.3				
3.12.4				
3.13.1				
3.14.1				
3.15.1				
3.16.1				
3.17.1				
3.18.1				
3.18.2				
3.19.1				
3.19.2				
3.19.3				
3.19.4				

Technical Questions		
Question No	**Question Weighting**	**Section Weighting**
4.1	20%	70%
4.2	20%	
4.3	15%	
4.4	10%	
4.5	10%	
4.6	5%	
4.7	15%	
4.8	5%	
Total Quality Weighting		**70%**

NRS Technical evaluators will undertake evaluation of the tenders received independently of each other and apply a score to each question response based on the scoring criteria detailed beside each question.

3. SECURITY REQUIREMENTS/QUESTIONS

Data Security Requirements. Please note these requirements are all mandatory and any 'No' response will be deemed non-compliant and your bid will be rejected.

Standards and Compliance	
3.1	Standards
3.1.1 Critical	The service and component services or products must be compliant with the UK Government's Minimum Cyber Security Standard (v1.0 issued June 2018). Compliance requirements with any updates or revisions will be managed through revisions of the Technical Security Standard (Appendix I). Please confirm that you understand and are compliant with this requirement.
Please answer Yes, No or Willing to Obtain in the box opposite	
3.1.2 Critical	Bidders are required to be compliant with the UK Government's Cyber Essentials Scheme and either be certified to the scheme (or Cyber Essentials Plus). Bidders who are not currently certified may submit their plan to be certified to the scheme with a target date no later than 31 July 2019. Please confirm that you are or will be compliant by 31 July 2020.
Please answer Yes, No or Willing to Obtain in the box opposite	
3.2	**Cloud Security Principles**
3.2.1 Critical	Where any service is provided using public, hybrid or private cloud instances, or where cloud technologies are used to provide or support elements of the Service, the Supplier must meet the requirements detailed in the HMG Cloud Security Principles.

	Security reporting and alerting thresholds must be agreed with the Authority and documented. The Supplier will be required to document all Logging and Monitoring capabilities within component applications and infrastructure, even if these are not proposed to be implemented in the service delivered for the Authority. The Supplier shall state clearly, for any public, hybrid or private cloud data hosting services utilised in the provision of the Services, that their solutions comply with and which of the designated levels of assurance they will provide for each of the Principles within the relevant NCSC Cloud Security Guidance referenced below: i. Cloud Standards and Definitions ii. Implementing Cloud Security Principles iii. Having confidence in cyber security. Please confirm that you are, or will be, compliant with this requirement by 31 July 2020.
Please answer Yes, No or Willing to Obtain in the box opposite	
3.2.2	Please indicate your solutions and services meet the applicable good practice measures outlined in the NCSC Protecting Bulk Personal Data guidance. Please confirm that you are, or will be, compliant with this requirement by 31 July 2020.
Please answer Yes, No or Willing to Obtain in the box opposite	
Data Protection	

3.3	Data Protection
3.3.1 Critical	The Supplier (including their Sub-contractors) will need to ensure that any proposed solution is both compliant with their obligations under Data Protection Act 2018 (DPA 2018) and Regulation (EU) 2016/679 (the General Data Protection Regulation / GDPR) and enables Scotland's Census 2021 to comply fully with its obligations under DPA 2018 and GDPR. Particularly, suitable and sufficient records should be kept, and made available to the Authority on request, of design and implementation criteria, evidence and decisions for any functionality affecting personally identifiable data processing to meet both parties' obligations under GDPR Article 5 Para 2 and Article 25. The Supplier should describe their DPA 2018 and GDPR compliance regime and how they intend to assure the operational use of the Service complies with their, and the Authority's, responsibilities under Articles 34(3) (Controller Responsibilities and Compliance) and Articles 57 and 103 (Data Protection by Design). Please confirm that you are, or will be, compliant with this requirement by 31 July 2020.
Please answer Yes, No or Willing to Obtain in the box opposite	
3.3.2 Critical	To comply with legal obligations only certain development and operational activities will be permitted outside of the UK. Where a Supplier is proposing to host any data or provide development or operational activities concerned with their solution or service out with the United Kingdom, the Supplier should note that any such solution may require external approval by Central Government. Such approval may be out with the control of the Authority and the Supplier should be aware that approval may not be granted automatically. Please confirm your acceptance of this requirement.
Please answer Yes, No or	

Willing to Obtain in the box opposite	
3.3.3 Critical	Please confirm that all data will be hosted within the European Economic Area.
Please answer Yes, No or Willing to Obtain in the box opposite	
3.3.4 Critical	Census data must be stored in a manner that allows secure migration to systems or locations specified by the Authority and are securely retained until its secure deletion and/or destruction is ordered by the Authority. Any storage media which is used for non-ephemeral storage of census record data will either require transferring to Scottish Government custody when no longer required for the delivery of the service or product or be destroyed in accordance with the HMG destruction requirements in force at time of disposal. For information, current requirements can be found in the CPNI "Secure Destruction Standard." The Supplier must confirm that their pricing model reflects this requirement, including for the appropriate disposal of storage media that develops faults during use. Please confirm your acceptance of this requirement.
Please answer Yes, No or Willing to Obtain in the box opposite	
3.3.5 Critical	The Supplier is required to protect Census data even when legislation (either from the country in which they, or their parent company, work or the jurisdiction in which they reside) exists which

	may compromise confidentiality by requiring them to disclose information of a confidential nature and with which they must comply. Example of such legislation would be the US CLOUD and PATRIOT Acts. Where relevant please confirm: - the proposed solution avoids a conflict between non-UK legislation and the confidentiality requirements as expressed in this SOR and/or UK legislation (e.g. The Census Act 1920 as amended or the Data Protection Act 2018); - you would jointly work with the Authority to manage the public perception of the risk to data confidentiality presented by such external legislation, including example key messages. The Supplier must confirm they will provide a solution whereby any Census Data able to be related to specific individuals will never be held or controlled by employees of companies who are subject to the Patriot Act, or similar legislative requirements. The Authority reserves the right only to award a contract that meets this requirement. Please confirm your acceptance of this requirement.
Please answer Yes, No or Willing to Obtain in the box opposite	
3.4	Data Confidentiality & Classification
3.4.1	All Census data is subject to the confidentiality and retention requirements of the Census Act 1920. Census record data and some census data will contain Sensitive Personal Data in accordance with Section 42 of the DPA 2018. Census record data has been classified as OFFICIAL SENSITIVE in accordance with the **HMG** Security Classification Policy. In addition, a local descriptor of CENSUS will be used to differentiate those data sets to which Section 8.2 of the Census Act 1920 applies. Other data sets or elements will be treated either as OFFICIAL SENSITIVE or OFFICIAL.

	Please confirm your acceptance of this requirement.
Please answer Yes, No or Willing to Obtain in the box opposite	
3.5	Security Governance
3.5.1 Critical	The Authority security requirements differ from and, in many cases exceed, those for other government services operating at the same classification. As such, all services and products will require the validation of security controls implementation and efficacy via the governance process before they can be used to support the Census in 2021. The Authority is establishing a rigorous Information Security Governance and management Framework programme to provide assurance of the solutions and activities undertaken to deliver the Census in 2021. Formal Accreditation of the systems, services or products supplied for the use of the Census 2021 Programme is mandatory and will be owned and facilitated by the Authority's in-house Security and Assurance Team. It will be the responsibility of the Technical Representative and/or Subject Matter Expert to manage the progress of the systems, services or products through the Formal Accreditation Process to gain accreditation. Successful completion of this process shall be one of the factors contributing to the successful delivery and completion of contractual milestones. The Formal Accreditation process will involve the signed approval from various business teams including, but not limited to, Architecture, Security, Testing and specific Subject Matter teams. This signed approval will attest to the satisfactory completion of deliverables and any associated remediation activities for the Governance arrangements under their specific remit e.g. formal acceptance of security Health Checks etc. Please confirm you will comply with the policies, standards, processes and any other measures involved in the Governance Framework Programme.

Please answer Yes, No or Willing to Obtain in the box opposite	
3.5.2 Critical	Please confirm you will be fully engaged with the Security and Privacy team throughout the Contract duration.
Please answer Yes, No or Willing to Obtain in the box opposite	
3.5.3 Critical	The Supplier must ensure and confirm that any sub-contracts involving the transmission, processing or storage of data on behalf of the Authority contain appropriate clauses to cover the Authorities and Suppliers responsibilities as detailed in this Section and the supporting Schedules.
Please answer Yes, No or Willing to Obtain in the box opposite	
3.6	Security Documentation
3.6.1 Critical	The Supplier must produce design and operational documentation to allow the Authority to assess the level of security designed in to and implemented within the product or service properly. Please confirm your acceptance of this requirement.
Please answer Yes, No or Willing to Obtain in	

the box opposite	
3.7	**Risk Assessment**
3.7.1 Critical	Information Risk Assessments will be conducted to the multi-stage Census 2021 "Attack Tree" Risk Assessment methodology. Support will be provided from the Authority and its independent security advisors to enable the Supplier to conduct and document the Risk Assessment for the service. The Supplier must be aware that a separate security risk assessment will be conducted, by the Authority, on the Supplier's corporate presence and capabilities. The scope of the assessment will depend on the delivery model that the Supplier is proposing and will include relevant sub-contractors. Please confirm your acceptance of this requirement.
Please answer Yes, No or Willing to Obtain in the box opposite	
3.8	**Accreditation**
3.8.1	A full Accreditation Documentation Set will be required for each separate system supporting the Service Provision. This will include the following items, as well as any documentation specific to the system: • System Description • Privacy Impact Assessment (completed by the Authority requiring co-operation from the Supplier and, if appropriate, their sub-contractors). PIAs will require to cover DPA 2018 Section 34(3) (Accountability and Compliance) and, DPA 2018 Sections 57 and 103 (Data Protection by Design) issues in detail. • Risk and Issues Register • Controls Statements – aligned to ISO27001:2013 • Business Continuity Plan – aligned to ISO22301:2012 • Forensics Readiness Pack – aligned to Census 2021 standards.

3.8.2 Critical	A penetration test, covering both infrastructure and application testing, to at least the standard of the NCSC CHECK scheme, and the subsequent risk managed remediation of identified defects will be required as a pre-requisite for security accreditation (see also 3.19.2). Please confirm your acceptance of this requirement.
Please answer Yes, No or Willing to Obtain in the box opposite	
Security Management	
3.9	Information Security Management System
3.9.1 Critical	The Supplier must develop and maintain an Information Security Management System (ISMS) and ensure alignment of their technical controls with both the Cyber Essentials scheme and the specific Census technical security controls. Please confirm your acceptance of this requirement.
Please answer Yes, No or Willing to Obtain in the box opposite	
3.10	Security Working Group
3.10.1 Critical	The Supplier will be required to participate in the monthly Security Working Group. This group will focus on a common understanding and implementation of "good commercial security practice"[3] throughout the Census supporting infrastructure and will lead on the Technical Security Standard reviews. Although it may be practical for some attendees to join by remote means, physical attendance at the Authority's premises or another Edinburgh location will normally be required.

[3] As stated in the Cabinet Office "Managing Information Riskat OFFICIAL".

	Please confirm your acceptance of this requirement.
Please answer Yes, No or Willing to Obtain in the box opposite	
Security Operations	
3.11	Overview
3.11.1	The Authority requires a consistent and effective view of security status and exposure across the range of systems and services that will support Census Operations. The Supplier and, where appropriate, their sub-contractors, must provide the Authority with comprehensive data on a range of security relevant statuses. Full details are provided in the "Technical Security Controls" section below and in the Technical Security Standard.
3.11.2 Critical	The Supplier (including their Sub-contractors) must ensure that all supporting infrastructure and applications are subject to a formal change and patch management process. This is to include standard and emergency change procedures, regression testing and compliance reporting. Please confirm your acceptance of these requirements.
Please answer Yes, No or Willing to Obtain in the box opposite	
3.11.3 Critical	Census requires a comprehensive and effective view of security relevant events in order to detect and respond appropriately to security events and issues. Full details are provided in the Technical Security Standard (Appendix G). Please confirm your acceptance of these requirements.

Please answer Yes, No or Willing to Obtain in the box opposite	
3.11.4 Critical	Whenever the Authority supporting infrastructure is exposed to the internet or to other uncontrolled or untrusted networks, full network and security event data must be provided to the Security Operations Centre (SOC). Please confirm your acceptance of this requirement.
Please answer Yes, No or Willing to Obtain in the box opposite	
3.12	Security Incident Management
3.12.1 Critical	Suppliers must co-operate, and ensure that their subcontractors are required to, and do co-operate, throughout the duration of the service provision, with the Authority and Scottish Government Security Incident Management frameworks and processes. This may include, but is not limited to: • Attendance at incident management meetings, including outside normal working hours. • Provision of, or co-operation in the delivery of, ad-hoc vulnerability assessments of exposed or potentially exposed services. • Ensuring that supplier contacts are available to conduct investigation and / or mitigation actions upstream of the Census contracted Service. • Shutting down or restricting access to affected or potentially affected systems. • Making available suspected compromised systems for digital forensic analysis. The Supplier will be expected to take part in Incident Management exercises and Red / Blue Team exercises.

	Please confirm your acceptance of this requirement.
Please answer Yes, No or Willing to Obtain in the box opposite	
Technical Security Controls	
3.13	Security Working Group
3.13.1	The appropriate level of technical security controls will be set and managed by an Authority-led Security Working Group, with planned meetings monthly and, if necessary, on an ad-hoc basis. Please confirm your acceptance of this requirement.
Please answer Yes, No or Willing to Obtain in the box opposite	
3.14	Anti-Malware Protection
3.14.1 Critical	As an extension to the requirements in Section 4 of Cyber Essentials, the Supplier should be able to provide, for each anti-virus product involved in the solution and in any support system on which the solution depends: i. the frequency with which they provide anti-virus updates or, ii. whether they are accepting updates on push from the vendor and how they ensure those updates are delivered in a timely fashion to the supported systems. Please confirm you can provide these details.
Please answer Yes, No or Willing to Obtain in the box opposite	

3.15	Technical Security Standard
3.15.1	The Authority is aware that security standards will continue to evolve during the life-time of this procurement and where it expects standards or industry practice to change; detailed requirements will be published in the "Technical Security Standard". As the service or solution will need to be live at various periods throughout the Census lifecycle and maintain security, the published specifications for core security controls and techniques will be reviewed by the Authority at various points throughout the lifecycle. Interim reviews may be necessary in response to significant threat or security environment changes. Reviews of the Standard will be managed by the Security Working Group. The current version of the Technical Security Standard is published as an appendix to this document. The Supplier (including their Sub-contractors) must comply with all relevant aspects of this and future Technical Security Standards at the "minimum" and should comply at the "desirable" level. Where it is impractical for a supplier to comply at the "desirable" level, the non-compliance must be managed through the Census Risk Management Process. Please confirm your acceptance of this requirement.
Please answer Yes, No or Willing to Obtain in the box opposite	
3.16	Personnel Security
3.16.1 Critical	The UK Government Baseline Personnel Security Standard will be considered the minimum necessary for any supplier staff that will have access to Census data. The Supplier must ensure that the nominated personnel have undertaken the UK Government pre-employment process known as the Baseline Personnel Security Standard (Baseline Standard) and that this is currently valid.

	Where, due to nationality or residence issues, it is not practical to obtain BPSS, vetting to BS 8758:2012 will be required. The Supplier (and their Sub-Contractors) should be aware that some roles, particularly where bulk access to Census data is required or involving Security Operations or investigations functions, may be required to undergo UK Security Vetting. The Authority will facilitate the sponsorship of security vetting clearances where these are not already held at cost to the Supplier. The Supplier (and their Sub-Contractors) should be aware that any role which may require the employee to be in contact with potentially vulnerable individuals will require vetting under the Disclosure Scotland "Protecting Vulnerable Groups" scheme. Please confirm your acceptance of this requirement.
Please answer Yes, No or Willing to Obtain in the box opposite	
3.17	Physical Security
3.17.1	Standards and Specifications Good commercial security practice is considered appropriate for working at OFFICIAL SENSITIVE; therefore there are no specific HMG or Authority requirements for physical security measures in administration and operational areas.
3.17.2 Critical	Data Centres are to comply with TIA-942 at the Rating 3 or Rating 4 levels (or Uptime Institute Tier 3 or 4) and compliance with EN-50600-2-5 is recommended. Other hosting environments will require to be secured to an appropriate level, dependant on the nature of the data being processed or stored. Please confirm your acceptance of this requirement.
Please answer Yes, No or	

Willing to Obtain in the box opposite	
3.18	Security Audit
3.18.1 Critical	In accordance with Clause 36.11 of the contract Agreement the Supplier must co-operate with the Authority and its agents and suppliers in the conduct of Audits to ensure the security of the solution or service, including those hosted by sub-contractors and other suppliers. Where any element of the proposed architecture will include cloud services to be procured as a commodity purchase, the Supplier should detail how they intend to enable functionality to provide equivalent audit capabilities. Information Security Audit will include, but not be limited to, • the conduct of Penetration Testing (including formal IT Health Checks), • Red-Team / Blue-Team testing, • physical security audits of locations where census data is held or services are provided from, and • regular and ad-hoc vulnerability assessment of services. For clarity, 'regular' vulnerability assessment is considered to be monthly outside of Census operations periods for the service provided and weekly during active operations. Please confirm your acceptance of these requirements.
Please answer Yes, No or Willing to Obtain in the box opposite	
3.18.2 Critical	The formal IT Health Check, and any necessary checks on remediation actions, shall be conducted by the Authority and its suppliers. There is no restriction on the Supplier conducting its own penetration tests on the service or supporting systems. Any such reports are to be made available in full (with redactions where necessary to protect the commercial confidentiality of users of

	shared services other than the Supplier and the Authority) to the Authority. Please confirm your acceptance of this requirement.
Please answer Yes, No or Willing to Obtain in the box opposite	
3.18.3 Critical	The Authority will manage business continuity plans across the census operation and feeding into this will be both fully resourced and tested disaster recovery and service continuity plans and capabilities provided as part of the solutions developed by the Supplier. The Supplier shall have in place detailed disaster recovery and business continuity plans and procedures in respect of any applicable services provided under this contract. These plans and procedures must be made available to the Authority for agreement following the award of the contract. It is then up to the Supplier to maintain appropriate technology, processes, procedures, security and testing to ensure that the Return to Operation (RTO) and Recovery Point Objective (RPO) expectations are achievable in the event of foreseeable events. Please confirm your acceptance of this requirement.
Please answer Yes, No or Willing to Obtain in the box opposite	
3.18.4 Critical	As a minimum the Supplier (including their Sub-contractors) must adopt to an auditable approach to ISO 22301:2012 (Business Continuity Management) to their entire dealings with the Census programme and will work with the Authority to understand any trade-offs to that standard for instance between the standard and

	security implications or cost. ISO 27031:2011 (Guidelines for information and communication technology readiness for business continuity) should be used for further guidance. A full disaster recovery test will be required as part of the Security Governance validation process. The Supplier should note that malicious (or suspected malicious) events will be handled within the Information Security Incident Management framework and should not be incorporated in the answer to this section. Please confirm your acceptance of this requirement.
Please answer Yes, No or Willing to Obtain in the box opposite	
3.18.5 Critical	The Supplier (including their Sub-contractors) must implement a backup/recovery and restore strategy that, as well as meeting the business continuity requirements, is resilient to equipment failure, and to loss or denial of access to any relevant location. The Supplier must provide the right and any assistance required by the Authority to question, test and assure the quality of any proposed and implemented solutions and shall be responsible for rectification on demand in the run up to Census 2021. Please confirm your acceptance of this requirement.
Please answer Yes, No or Willing to Obtain in the box opposite	

4. TECHNICAL QUESTIONS - Weighting 70%

Please answer each question as fully as possible.

Question 1: Customer Contact - 20%

Provide details on how you will deliver the core requirements:

- A multi-channel service that will support and manage customer contact by phone, email, direct messages on social media and webchat
- An automated solution (eg IVR) for customers to request a paper questionnaire (through validation of their unique code), get answers to most common questions and interface with the Authority's main database (DCOMS)
- A call management system to:
  - Receive calls from four different numbers
  - Queue calls, play messages and music to customers
  - Allow certain groups to skip call queues
  - Inform the public how long it will take for their call to be answered or their queue position
  - Provide reporting on customer calls
- Advisor access to the Authority's web based systems and browsers used

Response:

Question 2: Personnel – 20%

1. Provide details on how you will onboard and manage staff including:
   - Recruitment (internal and external if appropriate)
   - BPSS and Disclosure Scotland certification
   - Training (including but not limited to):
     - Census specific material – knowledge, processes etc
     - Census confidentiality requirements
     - FAQs and common questions
     - Systems training
     - Sensitivity training
     - Customer service
     - Medium specific: Calls, Email, Webchat, Social Media
   - In life management and measurement
   - Staff scheduling and adherence
   - Location

2. Describe your staff succession plan and any other measures in place to ensure the continued provision of appropriately skilled and experienced personnel to your Census delivery proposal.

Response:

Question 3: Reporting and Service Levels - 15%

Provide details on how you will deliver the required KPI reporting and maintain the required service levels throughout the operation. Please include details of how you:

- Intend to manage the peaks and troughs of demand to ensure you maintain service levels and also provide value for money
- Intend to report on the required KPIs and contact types

Response:

Question 4: Operational Security – 10%

1. Describe how you will achieve and maintain the levels of security required in the requirements section including:
   - Data security (including CCS paper questionnaires)
   - Personnel security
   - Segregation of personnel (overheard and overlooked)
   - Limiting visitor / staff entry to your premises
   - Decommissioning on completion of the operation:
     a. Secure return of all census data and material to the Authority
     b. Secure destruction of all census material on completion of the collect phase
   - Location(s) security including:
     - Data centres or other locations where census data will be stored
     - Operational premises that will be used to support census live operations and any other premises that will be used for the delivery of the service or product
     - Perimeter security, access control, visitor entry, intrusion detection, limited access areas and secure segregated security for sensitive material and systems
   - Patch Management, including:
     - standard patch processes including timescales and regression testing
     - emergency patch processes
     - any different processes for security-related patching
     - how you provide compliance status monitoring for patch status
     - what data you would provide to Census to enable our whole-environment awareness

2. Describe how you will demonstrate how you will comply with the NCSC guidance for securing End-User Devices. This is available from the Guidance section of the NCSC website.

3. Please also confirm you have procedures in place to ensure continuity of service and protection against cyber-attacks including:
   - Details of processes followed for assessing future risks
   - Testing of Disaster Recovery policies and procedures, including the dates, duration and frequency
   - Methods in place to mitigate against cyber-attack and crime using online technologies including processes relating to Boundary Firewalls and Internet Gateways, Secure Configuration, Access Control, Malware Protection and Patch Management
   - Details of Security Monitoring and Incident Response policies and procedures
   - Describe your GDPR and your DPA 2018 compliance regime

4. As an extension to the requirements in Section 4 of Cyber Essentials, the Supplier should indicate, for each anti-virus product involved in the solution and in any support system on which the solution depends:
   - the frequency with which they provide anti-virus updates or,
   - whether they are accepting updates on push from the vendor and how they ensure those updates are delivered in a timely fashion to the supported systems
   - how you provide compliance status monitoring for anti-virus patch levels and activity and
   - what data you would provide to Census to enable our whole-environment awareness.

5. The Supplier must co-operate with the Authority and its agents and suppliers in the conduct of Audits to ensure the security of the solution or service, including those hosted by sub-contractors and other suppliers. Where any element of the proposed architecture will include cloud services to be procured as a commodity purchase, the Supplier should detail how they intend to enable functionality to provide equivalent audit capabilities. Information Security Audit will include, but not be limited to:
   - the conduct of Penetration Testing (including formal IT Health Checks),
   - a Red-Team / Blue-Team test,
   - physical security audits of locations where census data is held or services are provided from, and
   - regular and ad-hoc vulnerability assessment of services.

Response:

Question 5: Denial of Service, Business Continuity and Disaster Recovery – 10%

The Contact Centre and its supporting services is designated as 'Essential' in accordance with the Census 2021 Business Continuity (BC) and Disaster Recovery (DR) Strategy. The recovery time objective is 4 hours during opening times and by 7.30 am next day during non-opening hours.

1. Denial of Service
   Describe how you intend to secure the service or product, and any other aspects of your, and your supply chain network, on which the service or product depends, against cyber-attack, Denial of Service and Distributed Denial of Service attacks.
2. Business Continuity
   Describe the controls in place, or you intend to have in place, to maintain services in the event of systems and utility failures and temporary denial of access to facilities. Where any business continuity or disaster recovery measures are implemented and managed in compliance with British, European or International standards, please provide details.
3. Disaster Recovery
   Briefly describe the controls in place, or you intend to have in place, to maintain or, if stopped, recover services in the event of large scale incident, catastrophic failure of systems or utilities or long-term (> 48 hours) denial of access to facilities.

Response:

Question 6: Planning and Testing - 5%

Provide details on what approach and what steps you will take to create and develop your implementation plan, ensuring its fit for purpose including the execution of full system, operational and user acceptance testing to ensure smooth operational running of the operation and to provide confidence to the Authority prior to going live.

Response:

Question 7: Requirements – 15%

With regard to the Functional and Non-Functional Requirements in Section 6, if you have not addressed and answered all of these requirements in your responses, please add further details below.

Response:

Question 8: Sustainability – 5%

Section 9 of the Public Procurement Reform (Scotland) Act 2014 places a sustainable procurement duty on a Contracting Authority (public body) before carrying out a regulated procurement to consider how in conducting the procurement process it can improve the economic, social and environmental wellbeing of the Contracting Authority's area.

Wellbeing of the Authority's area includes in particular, reducing inequality in the area. The Authority is contributing towards improving the social wellbeing element of its sustainable procurement duty by adopting a policy to promote fair work practices in relevant public contracts,which include:

- a fair and equal pay policy that includes a commitment to supporting the Living Wage, including for example being a Living Wage Accredited Employer
- clear managerial responsibility to nurture talent and help individuals fulfil their potential, including for example, a strong commitment to Modern Apprenticeships and the development of Scotland's young workforce
- promoting equality of opportunity and developing a workforce which reflects the population of Scotland in terms of characteristics such as age, gender, religion or belief, race, sexual orientation and disability
- support for learning and development
- stability of employment and hours of work, and avoiding exploitative employment practices, including for example no inappropriate use of zero-hours contracts
- flexible working (including for example practices such as flexi-time and career breaks) and support for family friendly working and wider work life balance
- support progressive workforce engagement, for example Trade Union recognition and representation where possible, otherwise alternative arrangements to give staff an effective voice

In order to ensure the highest standards of service quality in this contract we expect contractors to take a similarly positive approach to fair work practices as part of a fair and equitable employment and reward package.

Please describe how you will commit to fair work practices for workers (including any agency or sub-contractor workers) engaged in the delivery of this contract.

Answers need not be constrained to, or be reflective of, any examples given alongside this question. Good answers will reassure evaluators that your company takes a positive approach to rewarding staff at a level that helps tackle inequality (e.g. through a commitment to paying at least the Living Wage); improves the wider diversity of your staff; provides skills and training, and opportunities to use skills which help staff fulfil their potential; avoids exploitative employment practices (e.g. in relation to matters such as the inappropriate use of zero-hours contracts); takes the engagement and empowerment of staff engaged on this contract seriously, including having arrangements in place to ensure trade union representation where possible; otherwise alternative arrangements to give staff an effective voice and that your company will demonstrate organisational integrity with regards to the delivery of those policies. This reassurance can include a variety of practices which demonstrate your approach to fair work and should be tangible and measurable examples that can be monitored and reported during contract management procedures.
Response:

PRICING SCHEDULE

Please provide details on the implications for the Authority should there be a change in the requirement for a fully operational contact centre to be ready for the census in March 2021 (any costs implications should be included within the Pricing Schedule) as well as the detailed key milestones.

APPENDIX NINE: PROGRAMME TEST STRATEGY

The Authority's Programme Test Strategy is enclosed in the below embedded document.

Scotlands Census 2021 - IT Services Tes