Early Market Engagement (EME)

CONTRACTING AUTHORITY: GOVERNMENT DIGITAL SERVICE (GDS) on behalf of CABINET OFFICE.

REFERENCE: SMS for GOV.UK Notify 23/24 (please include on all correspondence)

DATE RESPONSE REQUIRED: 06/11/2023

RESPOND VIA EMAIL to: gds-digital-buyer@digital.cabinet-office.gov.uk

Dear Supplier,

We would like to notify you of an upcoming requirement, and by doing so we are keen to understand the market.

We are looking to understand;

(1) Which suppliers can fulfil the requirements.
(2) Your capabilities.
(3) What routes to market are available to GDS.
(4) The current commercial offerings available on the market (price).

This engagement seeks information relating to the provision of SMS services to the public sector via GOV.UK Notify, the Government Digital Service's digital communications platform.

The Government Digital Service (GDS) is part of the Cabinet Office.

The Contracting Authority (GDS) seeks information relating to Technical competence, Information Assurance, Financial Stability and Innovation aspects as well as potential routes to market and Commercial offering (Price).

Please note the following general conditions:

- This engagement will help us to refine the requirements.
- We reserve the right not to proceed with a further competition. Nothing shall constitute a commitment to ordering unless we undertake a further competition that results in the award of a Call-Off Contract.
- Should a Call-Off Agreement be awarded following a further competition, the Potential Provider agrees to supply the services in accordance with the Call-Off Terms contained within the relevant framework agreement or otherwise.
- Any and all costs associated with the production of such a response either to this EME or a further competition must be borne by the Supplier. We will not contribute in any way to meeting production costs of any response.
- We expect that all responses to this EME will be provided by Potential Providers in good faith to the best of their ability in the light of information available at the time of their response.

CURRENT SITUATION

GOV.UK Notify is a digital communications platform, developed and run by the Government Digital Service (GDS). Notify allows public sector service teams to send notifications (text message, email and post) to their users.

The notifications are typically status updates, requests for action, MFA codes, receipts of applications or supporting information, and reminders. The messages are sent via an API or manually through a web interface.

Currently there are over 7,100 service teams using GOV.UK Notify, from over 1,300 public sector organisations across central and local government and the NHS.
Notify's daily total SMS average is around 2 million, achieving peaks of 7 million.

Current forecasting work indicates that Notify will send 1.5 billion SMS fragments during FY24/25, however this figure may vary significantly due to changes in demand.

Many Notify services send messages that are longer than one fragment and the average message sent via Notify is 4 fragments long. Notify SMS messages have a high average delivery rate of 96.5%.

Notify uses two concurrently integrated SMS suppliers to ensure a resilient service. Typically, traffic is shared between the two based on supplier performance (speed of processing) and load. Ultimately GDS reserves the right to allocate work between suppliers at its absolute discretion and there is no guarantee of volume as it's influenced by both government policy and how the services choose to use Notify.

OUR AIMS – WHAT WE WANT TO ACHIEVE

The Contracting Authority are looking for two Suppliers to deliver on the following:

We're looking to procure 2 SMS suppliers for 12 months, with options for contract extension (12+ 12). The unit price for a single SMS ***fragment** will be **fixed** throughout the duration of the contract and any subsequent extensions, independent of volume.

To meet Notify's SMS redundancy requirements the suppliers should utilise independent computing and network infrastructures throughout their respective end to end services, avoiding any single points of failure that could simultaneously impact both providers. Suppliers are asked to provide sufficient information in their responses to enable GDS to evaluate this.

***If a text message is longer than 160 characters (including spaces) then it counts as more than one message i.e. more than one fragment.**

WHAT WE ARE LOOKING FOR

We would like to understand your capabilities against our SMS service requirements listed in the table below.

A yes/no response is sufficient against many of the requirements - please provide additional detail where requested. Please respond to every question and clearly identify the question number against your response.

Supplier Name:	
Registered Company Number:	
Contact Name: **Title/Role:**	
Contact Email:	
Contact Telephone:	

		Yes	**No**
Pre-condition(s)	Notify requires two **independent**, concurrently integrated SMS suppliers to ensure a resilient service. i. Are you an Affiliate of any other entity that has submitted a response to this Early Market Engagement.. Where: “Affiliate” means in relation to a body corporate, any other entity which directly or indirectly Controls, is Controlled by, or is under direct or indirect common Control with, that body corporate from time to time; and “Control” means the possession by any person, directly or indirectly, of the power to direct or cause the direction of the management and policies of the other person (whether through the ownership of voting shares, by contract or otherwise) and “**Controls**” and “**Controlled**” shall be interpreted accordingly		
	ii. Do you share any infrastructure which would be utilised for the delivery of the Services with any other entity/respondent to this EME? If you have answered yes to either, or both, Pre-conditions i and ii, please only submit a response for the service that you would like to be considered, should we proceed to tender.		

The following are a non-exhaustive list of essential requirements. We would like to understand your capacity and capability to deliver against these specific requirements, should we proceed to tender.			
1. Functionality	a. Inbound and outbound text messages		
	b. International text message sending		
	c. Delivery receipts for sent messages		
	d. Restful API		
	e. Zero downtime API key rotations via self-service API key management		
	f. Do you support Multi-Factor Authentication (MFA) and if so, which method?		
2. Performance	a. Message sending rate of 1000/s or above for 6 fragment messages		
	b. Failover capability to maintain message sending rates in a-d		
	c. Delivery receipt matches message sending rate		
	d. What is your maximum sending rate per second of 1 fragment messages?		
	e. 24/7 support		
	f. SLAs for response and resolution times		
3. Information Assurance	a. Do you hold current Cyber Essentials Plus and / or ISO/IEC 27001 certifications of scopes that include all the people, places, equipment, IT systems and any cloud services that are involved in the provision of your SMS service?		
	b. Are you a member of the Mobile Ecosystem Forum (MEF)? If you are, we would expect to see your name on the MEF website.		
	c. i) Do you actively take part in MEF's SMS SenderID Protection Registry?		
	ii) Please describe your involvement.		

	d. Are you a signatory to the MEF Business SMS Code of Conduct? If you are, we would expect to see your name on the MEF website.		
	e. i) Do you offer direct routing of SMS messages to MNOs exclusively via Tier One connections?		
	ii) Please describe any exceptions that may apply.		
	f. Please describe what tools and support you offer to reduce SMS Artificial Traffic Inflation (ATI) fraud.		
	g. Please provide a high-level architecture diagram that shows your SMS service end-end, including any aspects that are provided by other companies, such as SMS aggregators and cloud service providers.		
	h. Please describe the service model and deployment model used for your SMS service, for example: Is your service provided as software-as-a-service (SaaS) which you manage, is it part of a communications-platform-as-a-service (CPaaS) managed by another provider? Is your service multi-tenanted - multiple customers accessing a shared instance, or is your service a dedicated instance accessed by a single customer? Please indicate whether the service is hosted at your premises, third party data centres, or on a cloud infrastructure-as-a-service (IaaS) or a communications-platform-as-a-service (CPaaS). Please indicate whether the underlying hardware is dedicated to your service or shared with others.		
	i. What are the locations of the physical sites involved in providing your SMS service? Please include: - sites hosting IT systems, facilities, networks and processes delivering the service. - sites that could be used as part of a fail-over solution.		

	Please include your own sites and those of your supply chain. If you are using cloud-hosted infrastructure, please provide the name of your cloud service provider and identify the regions and availability zones used to host both the production and fail-over instances.		
	j. For these physical sites, please describe, in outline, what physical controls are in place to protect IT systems, data, and networks. Please include if these controls were designed with any particular standard in mind, such as CSA CCM v3.0.1 or ISAE 3402?		
	k. Please describe the supply chain involved in your SMS service, to include any SMS aggregators, delivery partners, cloud service providers and outsourced functions you may be using. Please identify each supplier, their physical location and their role. Please identify any use of offshoring by your service, such as for data storage, data processing, support, development or maintenance.		
	l. Please identify and give the location of groups of people that could have access to our data, or are in a role that could directly affect the operation or integrity of the SMS service, such as those who support IT systems / cloud services / network equipment and those who can check in code.		
	m. i) Please describe what background checks you and your supply chain carry out on employees and contractors.		
	ii) Do these include verifying their identity, their right to work, and identifying any unspent criminal convictions?		
	iii) Do you provide security awareness training, covering common attacks on users, such as phishing and other means of enticing users to disclose sensitive information, or download unauthorised code?		
	iv) How do you encourage a positive security culture? For example, do you encourage users to report suspected or actual incidents promptly in		

	a no-blame environment?		
	v) Have you performed a risk assessment to understand your insider threat?		
	n. i) Please list your SMS service's customer-facing interfaces and describe how access to these is controlled. For example, you might offer a web console and a REST API. If applicable: ii) Does your web console support MFA? If so which types? iii) Does your web console support SSO integration with an external identity provider such as Google Workspace or Azure Active Directory? iv) Does your web console enforce a password policy? If so, please provide details.		
	o. i) Does your service protect data at rest and data in transit? ii) Please describe how and where this is achieved within your SMS service.		
	p. Do you have a GDPR compliance statement you can share with us that describes how you manage personal data and meet the ICO's GDPR security principles? This might be part of a terms of service or privacy policy document.		
	q. Do you have a formal process for assessing the cyber security posture of products and services before using them?		
	r. i) Are the applications and infrastructure used to deliver your end-end service, including those of any SMS aggregators you may use, subject to independent security assessments at least annually?		
	ii) Are those performing the assessments members of CREST, Cyber Scheme or CHECK?		
	iii) Are the findings remediated?		
	s. i) Are all the end-user devices that you and your supply chain use to provide your SMS service corporately-managed?		
	ii) Is the data stored on these devices encrypted in case of loss or theft?		

	iii) Do you know what devices connect to your network and who has access to them?		
	t. Do you have plans and processes in place to cope with a cyber security incident (e.g. a ransomware attack) and recover from it?		
Sub-processor information: For resilience our suppliers should work with different sub-processors.			
4. **Sub-processor(s)**	a. Please confirm the names of any sub-processors that you would be working with to deliver our SMS service requirements.		
	b. If you use an SMS aggregator, where is their platform physically hosted? i.e. what is the physical location of the data centres that host the platform? Please include both production and any fail-over instances		
Commercial requirements:			
5. **Financial Stability**	If GDS proceed with this requirement, we will carry out a number of financial checks on suppliers to ensure that your financial standing is sufficient for a contract of this scope and value: 1. GDS will check the Companies House website to see whether each potential supplier has filed audited company accounts for the past three (3) years. If there is no record of the potential supplier having filed its accounts with Companies House, you need to provide a written explanation. ***Please confirm that you understand and are fully compliant with this requirement***		
6. Unit price (Please provide a sustainable price for 01/04/2024 to 31/03/25, including scope for 12 month extension)	a. UK rate for single text message fragment		
	b. International rate for single text message fragment (by country)		
	c. Inbound text messages received		
	d. Non-delivered message rate for single text message		
7. Additional costs - UK and International	a. Virtual mobile numbers		
	b. Licence / API usage fees		
	c. Setup and monthly fees, including any specific		

	costs for International SMS delivery	
	d. Support charges	
	e. Any other costs	
	f. Price stability - please confirm if you can sustain this service at the costs shared in your response, for the duration of a minimum 1 year contract term + 1 year optional extension?	
	g. Do you offer service credits, for example for incidents impacting message sending rates?	
8. CCS Frameworks	Are you registered on any CCS' Commercial Agreements (frameworks) that would enable you to deliver on the specified requirements - please list the available CCS frameworks.	
9. Innovation	The Contracting Authority would like to engage with potential suppliers on innovation and discuss what the future might look like with regards to the service we offer. Do you offer any other notification services aside from provision of SMS? If yes, please provide a list of services and short case studies of how you have implemented them (up to 200 words) for each additional service. Would you be happy for us to contact you? If so, please provide details of the contact within your organisation. We will only contact suppliers that can meet all of our essential criteria.	

OUR TIMETABLE

DATE	ACTIVITY
16/10/2023	Publication of the Early Market Engagement
16/10/2023	Clarification period starts
23/10/2023	Clarification period closes
25/10/2023	Deadline for the publication of responses to EME Clarification questions.
06/11/2023	Deadline for submission of an EME Response

QUESTIONS AND CLARIFICATIONS

- Suppliers may raise questions or seek clarification regarding any aspect of this EME document at any time during the clarification window. Please submit any questions to gds-digital-buyer@digital.cabinet-office.co.uk referencing the requirement in the subject line.
- This Early Market Engagement document and your responses to it are intended to facilitate GDS in developing contractual requirements for a potential future re-procurement of the SMS for GOV.UK Notify Service. As we may use the results of this process to develop our future requirements, you should not provide any commercially sensitive information, confidential information or trade secrets in your response.

GENERAL CONTACT POINT FOR THIS EARLY MARKET ENGAGEMENT;
Please reference "SMS for GOV.UK Notify 23/24" in the subject line.
Name: COMMERCIAL TEAM
Email: gds-digital-buyer@digital.cabinet-office.gov.uk