Ministry of Housing, Communities & Local Government

Pre-Tender Market Engagement

Smart Cities Cyber Resilience
CPD/004/119/129

Authority: Ministry for Housing, Communities and Local Government (MHCLG) (**"the Authority"**).

Date Response required: **11:00am GMT on 22 March 2019**

1 PURPOSE

1.1 This Pre-Tender Market Engagement (PTME) seeks information in preparation for the potential procurement of a Supplier (from herein referred to as a "**Potential Supplier**"). The purpose of this PTME is to:

1.1.1 help define the requirement;
1.1.2 help provide a better understanding of the feasibility of the requirement;
1.1.3 understand the capacity of the market to deliver and possible risks involved; and
1.1.4 provide the market with an opportunity to ask questions, raise queries and any issues to be addressed at an early stage.

1.2 The Authority shall maintain commercial confidentiality of information received during the PTME.

2 INTRODUCTION

2.1 Smart infrastructure – infrastructure managed with data and digital connectivity – is already in use around the UK , and deployment is increasing. Local government is a key owner and operator of systems, which offer sustainable, cost-saving solutions and better integration between domains (e.g. transport, planning and health). Smart systems can be subject to disruption, whether through technical failure, human error or attack. As the scale and complexity of connected networks increases, so does the risk. Therefore, local government increasingly needs to be able to make effective decisions on purchasing, deploying and operating smart systems. In particular, local government needs guidance and capability to deliver cybersecurity of data and systems, as the necessary basis for using the systems to deliver safely and effectively for citizens and local businesses.

2.2 The aim of this project is to identify the key cyber resilience and security challenges for local government in the deployment and use of smart Internet of Things (IoT) infrastructure and systems, and to provide a high-level account of what the sector needs in practice to address these challenges successfully. The focus is on practical needs in the medium term, therefore the scope includes applications that are already in use or are market-ready, that are purchased and/or operated by the local public sector. It specifically excludes technology that is currently far from market or technology such as smart transport systems, smart grid or other power systems or networks, autonomous vehicles, drones or other systemic technology that would require national policy decisions to enable deployment, where cyber security is engineered into the system by necessity.

The case for local knowledge & capability

2.3 Cities and city agencies across the UK are already making purchasing decisions and deploying IoT and smart technology, including TfL, the Manchester CityVerve IoT demonstrator programme, Glasgow control centre & field operations; Bristol is Open; Milton Keynes MK Smart; Leeds; WMCA. This is cost effective for local authorities, and provides sustainable solutions for maintaining local services, including smart lighting, waste management, traffic and logistics management, CCTV and online digital services.

2.4 Local-level tech solutions are already available and maturing rapidly, and it is anticipated that purchasing decisions will increasingly favour digital and IoT solutions over more expensive traditional infrastructure-only investments. This eventuality would present both savings for councils working in partnership with government, public, private and voluntary sector partners in a place, to join up around their shared customers and communities and promote more sustainable, energy efficient solutions. One existing barrier to realising this is the lack of confidence in IoT solutions, their availability and resilience.

2.5 To address this BSI PD8100 has outlined the benefits of becoming a smarter city for city leaders, and outlines a process to do so, providing practical recommendations and highlighting how standards can help eliminate risks, provide consistency that can lower costs and stimulate innovation, and reduce effort required to manage cities effectively. The growing portfolio of BSI guidance, notably including recent material on city data and resilience, offers a route to a more fluid and productive market.

2.6 More could be achieved in terms of providing education and training to enhance confidence in technology that is not widely understood by local-level procurement decision makers. Especially in the face of evidence suggesting that hacks of industrial control systems continue to rise steadily[1], and serious ransomware incidents with city information systems have been reported[2].

2.7 Enabling a more mature understanding of available technology and its associated risks would empower a generation of local government procurement decision makers to deliver cost-saving efficient local infrastructure and services at a time when the risk to such systems is increasing.

2.8 City service and infrastructure disruptions through cyber attacks have been observed abroad, though are fortunately not as yet a reality in the UK. However, as city systems come to rely more on digital solutions, for instance connected and automated city control systems, the consequences of failure become more prominent. And as digital solutions for cities become more interlinked, complex and multi-layered, cities will no longer be able to rely simply upon updates or patches.

2.9 Instead of waiting until such events become a reality, and retro-engineering costly cyber resilience solutions into city IoT systems (or simply replacing or ignoring the problem) it, local leaders and decision makers should be equipped with more profound understanding of consequence and risk relating to IoT purchasing and data management, and be empowered to understand and demand cyber resilient products from the market.

[1] IBM – https://securityintelligence.com/outsmarting-the-smart-city/- The Dangers of Smart City Hacking
[2] Reuters June 7, 2018, 'Atlanta officials reveal worsening effects of cyber attack' https://www.reuters.com/article/us-usa-cyber-atlanta-budget/atlanta-officials-reveal-worsening-effects-of-cyber-attack-idUSKCN1J231M

Privacy and continuity of service

2.10 Local level smart tech is highly likely to/ will make of and gather personal data. It is also likely to drive privacy concerns through the use of devices that mine the use of personal data, such as CCTV systems running facial recognition software.

2.11 The owners of such personal information are legally bound to protect it. Should such systems not be fully protected this could present a vulnerability for sensitive data, equally if such systems are not resilient this could cause continuity of services or in extreme cases, crime prevention issues. Services managed by local IoT may in some cases rely on personal data for effective functioning.

3 HIGH LEVEL OUTLINE PROJECT OUTCOMES REQUIRED

3.1 Unless decisions are made that prioritise security in smart city technology purchasing, this will render future cities less resilient to cyber events.

3.2 To ensure cyber resilience for future cities it is critical to understand how to empower and equip local decision makers to prioritise resilient and secure cyber solutions from the market, within the framework of making decisions on digital technology to benefit cities.

3.3 The tangible benefits of this will be:

- 3.3.1 Local leaders, decisions makers will have skillset to make intelligent decisions on cyber secure and resilient IoT technology for cities
- 3.3.2 Cities will understand more the systemic nature of their city systems and will have a better understanding of the implications of interconnectedness within their cities
- 3.3.3 Purchasing decisions that prioritise security will help the market develop and prioritise cyber security and resilience; including budgeting for cyber security operational management (such as monitoring and response capacity) and understanding the consequences of large-scale use and collection of data
- 3.3.4 Local leaders will be enabled to take responsibility for professional and thoroughly-exercised emergency and risk management that can respond to city level cyber-incidents.
- 3.3.5 Making private-public collaboration for cybersecurity prevention, response and recovery explicit and understood.

4 OUTPUTS/DELIVERABLES

4.1 Potential Products & Outputs from Research

- 4.1.1 Guidance
- 4.1.2 Standards
- 4.1.3 Training and supporting tools
- 4.1.4 Capability model for local government – what is out there and can be adapted for local government

4.2 Indicative Research Approach

- 4.2.1 Literature review of existing studies and guidance
- 4.2.2 Interview and discuss current arrangements in place
- 4.2.3 Development of case studies to bring issues to life
- 4.2.4 Development of principles and outline products
- 4.2.5 Test principles and products with councils and local resilience partners
- 4.2.6 Development of detailed products
- 4.2.7 Test products with stakeholders
- 4.2.8 Publish findings and products
- 4.2.9 Outline areas of risk / uncertainty where further work may be beneficial

5 KEY DATES & TENDERING PROCESS

5.1 If it is decided this service is required, it is anticipated that a procurement may start in late March/early April 2019 with the contract to commence June 2019. These indicative dates are for information purposes only. The Authority reserves the right to amend these dates at any time, and Potential Suppliers rely on them entirely at their own risk.

5.2 The contract is expected to be for a period of 6 months.

5.3 The tender is likely to be commissioned through the Crown Commercial Service (CCS) Dynamic Purchasing System (DPS) - RM6018 Research Market Place.

5.4 Suppliers are able to apply to join the DPS at any time. During application to join the DPS, suppliers indicate which services they may be able to provide under the DPS.

5.5 Please note that new suppliers are able to register with the DPS via the following link and that this process can take around 2 weeks: https://supplierregistration.cabinetoffice.gov.uk/dps#research

5.6 If you have any questions about the DPS and would like to contact a member of the CCS team, please email: researchmarketplace@crowncommercial.gov.uk

6 RESPONSE

6.1 Please respond via Bravo Solution with the following by 11:00am GMT on 22 March 2019 (the "Response Deadline").

Q1 Would you be interested in bidding for this project?

Q2 Is this project deliverable in the timeframe proposed?

Q3 Is what the Authority asking for clear?

Q4 What, if anything, has the Authority missed or overlooked in setting out their requirement?

Q5 Is there anything here which is irrelevant, outdated or unnecessary?

Q6 What would the indicative cost be for this piece of work?]

7 QUESTIONS AND CLARIFICATIONS

7.1 Potential Suppliers may raise questions or seek clarification regarding any aspect of this PTME document at any time prior to the Response Deadline. Questions must be submitted via Bravo Solution only.

7.2 To ensure that all Potential Suppliers have equal access to information regarding this PTME exercise, responses to questions raised by Potential Suppliers will be published in a "Questions and Answers" document, which will also be circulated by email, with updates appearing at regular intervals (approximately two to three working days).

7.3 Responses to questions will not identify the originator of the question.

7.4 If a Potential Supplier wishes to ask a question or seek clarification without the question and answer being revealed, then the Potential Supplier must state this in their email and provide its justification for withholding the question and any response. If the Authority does not consider that there is sufficient justification for withholding the question and the corresponding response, the Potential Supplier will be invited to decide whether:

7.4.1 the question/clarification and the response should in fact be published; or
7.4.2 it wishes to withdraw the question/clarification.

8 GENERAL CONDITIONS

8.1 This PTME will help the Authority to refine the requirements and to understand the potential level of interest in the delivering requirements. It will also aid Potential Supplier's understanding of the requirements in advance of any formal competitive tender exercise.

8.2 The Authority reserves the right to change any information contained within this PTME at any time, and Potential Suppliers rely upon it entirely at their own risk.

8.3 The Authority reserves the right not to proceed with a competitive tender exercise after this PTME or to award any contract.

8.4 Any and all costs associated with the production of such a response to this PTME must be borne by the Potential Supplier.

8.5 No down-selection of Potential Suppliers will take place as a consequence of any responses or interactions relating to this PTME.

8.6 The Authority expects that all responses to this PTME will be provided by Potential Suppliers in good faith to the best of their ability in the light of information available at the time of their response.

8.7 No information provided by a Potential Supplier in response to this PTME will be carried forward, used or acknowledged in any way for the purpose of evaluating the Potential Supplier, in any subsequent formal procurement process.