Statement of Requirement (SoR)

Purpose

This document is for new Extra-Mural (EMR) Contracts. Use the Request for Contract Action (RCA) Guidance for EMR page on WikiD when filling out this SoR and a supporting RCA. Please seek assistance if desired from Commercial or your Divisional Procurement Representative.

This document is supplier facing and the RCA is an internal document. Please delete non-essential grey text before issuing externally/ to suppliers.

Reference Number	1000166761
Version Number	**V1.0**
Date	**07/7/21**

1.	**Requirement**
1.1	**Title**
	Harnessing influential online content creators to inform or influence audiences of interest to UK Defence
1.2	**Summary**
	This research is intended to develop practical guidance that will aid information activity practitioners on how to identify, engage with, and harness online content creators in order to help to spread or reinforce messages to overseas audiences of interest to UK Defence.

1.3	**Background**
	"We live in a data-rich information age in which the combined power of exponential growth in computer capability, data, and digital connectivity is fundamentally shaping almost every facet of modern life. Those who could adapt have thrived, others have clung to old methods and withered. Information, in all its manifestations, must change the way Defence execute business and prosecute warfare, both at home and overseas in an era of constant competition. Defence must harness this digital horsepower or be left behind; we have reached the tipping point. Information is no longer just an enabler, it is a fully-fledged national lever of power, a critical enabler to understanding, decision-making and tempo, and a 'weapon' to be used from strategic to tactical level for advantage. *The smart use of information through the mass customisation of messaging, narrative and persuasion, can vastly extend reach and deliver disproportionate influence on targeted audiences. It is underpinned by core digital technologies and digitally savvy people. This digital race – human and machine – is increasingly geopolitical in nature. Currently we are being challenged in a 'grey-zone' short of armed conflict by agile state and non-state actors – notably Russia – who understand our vulnerabilities and seek to exploit them through multifarious asymmetric approaches and the flouting of rules-based norms.* *Central to these strategic contests are 'information battles'; battles in which information is 'weaponised' and ones in which we increasingly lack the initiative. To regain the initiative and achieve information advantage we must rapidly up our digital game, fundamentally shift the way we think, act, invest, and move with pace through the incremental development of new capabilities. Defence, as part of a national and allied effort, must become a potent and resilient strategic actor; postured for constant competition both home and away. This requires a cultural transformation and a conceptual foundation that puts information advantage at the heart of 21st Century deterrence and campaign design. Information advantage must become part of our doctrinal lexicon and joint action practice; a bedrock upon which a range of physical, virtual and cognitive effects will be built, including the use of information as an effecter in its own right."* Air Marshal E J Stringer CB CBE Director General Joint Force Development and Defence Academy **- Joint Concept Note 2/18 Information Advantage** https://www.gov.uk/government/publications/information-advantage-jcn-218 In order to maximise the effectiveness of influence campaigns and messaging, Defence needs to ensure it can successfully reach, inform and/or influence overseas audiences of interest via online channels. However, for numerous reasons, examples being the congested and face-paced nature of the online domain, audience disinterest or hostility etc. it can be difficult to reach audiences of interest directly. One way, potentially, to support the dissemination of messaging and influence to audiences, could be to use influential online content creators to spread or reinforce our messaging or narratives.
1.4	**Requirement**

Research Scope

The research will provide practical guidance that will aid information activity practitioners in identifying influential and suitable online content creators, and how we can harness these creators to propagate and reinforce our messages. The guidance will be used to support the design and delivery of a range of information operations effects aimed at a range of overseas audiences.

Annex A provides a high-level overview of Defence Information Activities requirements at the Strategic, Operational and Tactical levels, and provides an analysis of regions / countries of interest taken from the Integrated Review of Security, Defence Development and Foreign Policy. The Annex also contains a list of information and influence Effects UK Defence may wish to achieve.

The contractor shall:

1. Design a framework and approach for **identifying** influential online content creators

2. Design a framework and approach for **assessing the suitability** of such content creators

3. Design a framework and approach for **utilising** suitable content creators to support the above

The frameworks and guidance will be designed considering the specific context within which the communications activities are to be conducted. For example:

- The **specific type of target audience** we are trying to inform or influence e.g. whether it is a national population as whole versus a specific population segment or demographic group, or a smaller group versus an individual etc.

- The **geographical location of audience** i.e. in which region or country the audience is located etc.

The contractor will also consider the various ways content creators can be utilised in practice. For example either via directly engaging and working with such content creators but also potential covert approaches where content creators can be specifically targeted via other influence activities to support UK Defence objectives without asking them to do it.

The contractor shall also consider whether the objectives of the information activities impact on the suitability of different content creators. For example whether the messaging and communications is to simply inform audiences or where the intent is to influence i.e. is the primary objective to reach more people in order to inform them rather than create a specific influence effect e.g. to Convince or Reassure (see Annex A).

The contractor will also identify, assess and include any other important factors in the development of frameworks and approaches.

Research Approach

The Contractor shall design a research approach to achieve the stated requirements.

This could include analysis of secondary sources, primary qualitative or quantitative data collection and experimentation.

Reporting Requirements

	Table 1.6 provides a breakdown on Deliverables for this research. Key deliverables are described below: Guidance and supporting framework The key output is the development of a framework(s) and supporting guidance aimed at both those new to information operations and current practitioners. The outputs must therefore provide concise, clear and non-technical as far as possible. The framework should follow a step-by-step process and be illustrated with real-world case studies with demonstrable relevance to UK Defence information activities and audiences. The guidance and framework should be provided in MS Word, MS Power Point or PDF format, and may also be supplemented by a simple searchable Excel database that can be used by practitioners in real-time information operations. Two-page summaries A number of two-page non-technical summaries will be produced. As a minimum the two-pagers will cover the three research requirement i.e. Identification, Suitability and Utility. However, contractors are free to propose additional summaries as part of their proposal.

1.5	**Options or follow on work** *(if none, write 'Not applicable')*
	Not Applicable

1.6	Deliverables & Intellectual Property Rights (IPR)						
Ref.	**Title**	**Due by**	**Format**	**TRL***	**Expected classification (subject to change)**	**What information is required in the deliverable**	**IPR DEFCON/ Condition** *(Commercial to enter later)*
1	Start-up Meeting Presentation	Presentation 2 working days prior to meeting Meeting within 2 weeks of contract award (CA).	MS PowerPoint	Redacted under FOIA Section 23 - National Security		Presentation pack to include but not limited to: • Proposed activity, resourcing and timelines. • Review of risk management plan. • Review of intended deliverables and deadlines.	DEFCON 705 Wish to circulate across Govt. Suggest we clarify "Authority" is UK Govt. not just MoD
2	Technical Report	T+5 Months	MS Word	Redacted under FOIA Section 23 - National Security		A short technical report (no more than 40 pages). To include, though not limited to: a. Introduction and background to the research b. The overview of methodology used c. High level findings from the research d. Overview of case studies e. A standalone Executive Summary f. Conclusions and recommendations, where appropriate, for further research and development within this area.	As above

3	Framework and guidance	T+5 Months	MS Word / MS Power Point, Excel	Redacted under FOIA Section 23 - National Security	As specified within 1.4. Requirement	As above
4	Two-page summaries	T+5 Months	To be confirmed	Redacted under FOIA Section 23 - National Security	As specified within 1.4. Requirement	As above
5	Customer Presentation /& Closure Meeting	Presentation 5 working days prior to meeting. Meeting held by T+6 months Post meeting slides 5 working days post Start-up meeting.	MS PowerPoint	Redacted under FOIA Section 23 - National Security	To include, though not limited to: a. Introduction and background to the research b. The overview of methodology used c. High level findings from the research d. Overview of case studies e. A standalone Executive Summary f. Conclusions and recommendations, where appropriate, for further research and development within this area. g. Demonstration of the framework/guide	As above

***Technology Readiness Level required**

Notes- IPR should be inserted / checked by commercial staff before sharing with the supplier(s) to ensure accuracy.

1.7	**Standard Deliverable Acceptance Criteria**
	All Reports included as Deliverables under the Contract e.g. Progress and/or Final Reports etc. must comply with the Defence Research Reports Specification (DRRS) which defines the requirements for the presentation, format and production of scientific and technical reports prepared for MoD. Final Reports: shall describe the entire work performed under the Contract in sufficient detail to explain comprehensively the work undertaken and results achieved including all relevant technical details of any hardware, software, process or system developed there under. The technical detail shall be sufficient to permit independent reproduction of any such process or system. All Reports shall be free from spelling and grammatical errors and shall be set out in accordance with the Statement Of Requirement above. Failure to comply with the above may result in the Authority rejecting the deliverables and requesting re-work before final acceptance.
1.8	**Specific Deliverable Acceptance Criteria**
	Not Applicable

2.	Quality Control and Assurance
2.1	**Quality Control and Quality Assurance processes and standards that must be met by the contractor**
	Redacted under FOIA Section 26 – Defence
2.2	**Safety, Environmental, Social, Ethical, Regulatory or Legislative aspects of the requirement**
	There is no requirement to work from a Dstl or other Defence site.

3.	Security	
3.1	**Highest security classification**	
	Of the work	Redacted under FOIA Section 23 - National Security
	Of the Deliverables/ Output	Redacted under FOIA Section 23 - National Security
3.2	**Security Aspects Letter (SAL)**	
	Redacted under FOIA Section 23 - National Security	
3.3	**Cyber Risk Level**	
	Redacted under FOIA Section 26 – Defence	
3.4	**Cyber Risk Assessment (RA) Reference**	
	Redacted under FOIA Section 26 – Defence If stated, this must be completed by the contractor before a contract can be awarded. In accordance with the Supplier Cyber Protection Risk Assessment (RA) Workflow please complete the Cyber Risk Assessment available at https://suppliercyberprotection.service.xgov.uk/	

4.	Government Furnished Assets (GFA)

GFA to be Issued - No

If 'yes' – add details below. If 'supplier to specify' or 'no,' delete all cells below.

GFA No.	Unique Identifier/ Serial No	Description: *Classification, type of GFA (GFE for equipment for example), previous MOD Contracts and link to deliverables*	Available Date	Issued by	Return Date or Disposal Date (T0+) *Please specify which*

5.	Proposal Evaluation criteria
5.1	Technical Evaluation Criteria
5.2	Commercial Evaluation Criteria