

**SBRI: Quantifying Insider Risk based on Public Information**

**BRIEF**

**AN INTRODUCTION TO SBRI**

SBRI is a mechanism which enables public sector bodies to connect with innovative ideas and technology businesses to provide innovative solutions to specific Public Sector challenges and needs.

The Public sector is able to find innovative solutions by reaching out to organisations from different sectors including small and emerging businesses. New technical solutions are created through accelerated technology development, whilst risk is reduced through a phased development programme. SBRI also provides applicants with a transparent competitive and a reliable source of early-stage funding.

SBRI competitions are open to all organisations that can demonstrate a route to market for their solution. The SBRI scheme is particularly suited to small and medium-sized business, as the contracts are of relatively small value and operate on short timescales. Developments are 100% funded and focus on specific identified needs, increasing the chance of exploitation. Suppliers for each project will be selected by an open competition process and retain the intellectual property generated from the project, with certain rights of use retained by the contracting Authority. This is an excellent opportunity to establish an early customer for a new technology and to fund its development.

**SUMMARY**

## Funding Body

UK Cabinet Office

## Background and Challenge

### Policy Background

* Security is seen as complicated or confusing by many people, or even as a blocker or impediment to working. Security is rarely promoted as an enabler or core business outside the security practitioner community.
* Government needs to **better enable our people to reduce and manage risk,** where ‘our people’ are defined as **users** (anyone who uses government official IT) and **practitioners** (those responsible for managing and delivering security in an organisation), and ‘**risk**’ is defined as "the harm arising from potential loss, damage or compromise of government assets."

### Goal of the project

* We know that organisational cultures can be a powerful influence on how people act in the workplace, where ‘culture’ is defined as “shared **values (what is important)** and **beliefs** **(how things work)** that interact with an organisation’s structures and control systems to produce **behavioural norms** **(the way we do things around here).**”
* We want to validate or disprove the following hypotheses:
	1. Promotingappropriate culture(s) **is an effective lever in reducing risk;**
	2. Human Factors —including organizational climate and culture— play a critical role in our cross government **risk posture** today;
	3. It is feasible to develop a holistic methodology or capability that can assess and monitor the health of the Human Factors landscape - including organizational climate and culture - **across a public sector organisation** in near real time;
	4. It is feasible to develop a single methodology or capability to assess and monitor the health of the Human Factors landscape - including organizational climate and culture - **across government** in near real time;
	5. Although several aspects of culture are interrelated, it adds value to target ‘**cyber culture**’ separately from **‘organisational culture’ or** ‘**security culture’** (where “security culture” is defined as including physical, personnel, technical and cyber culture)**;**
	6. Leadership (senior leaders as well as local line managers) attitudes and behaviours are the **single greatest factor** which drive an **organisation’s risk posture**, and therefore represents the greatest value for risk interventions;
	7. Risk interventions applicable to government departments are also applicable to other **public sector organisations such as local authorities, education and healthcare arm lengths bodies**;
	8. Appropriate security cultures require the organisation to improve people's **capability and opportunity** to work securely, as well as their **attitudes and motivation.**
	9. **Interventions which** reduce high risk behaviours (e.g. reduced IT security violations) can **be measured in near real-time, quantitatively and qualitatively.**
* We hypothesise that third party suppliers might validate or disprove our hypotheses through **Human Factor interventions, bespoke technology application or nudge learning**, but welcome innovative alternative approaches.
* Over 12 weeks, Phase One invites potentially multiple suppliers to:
	1. validate or disprove **as many of our hypotheses as possible** and;
	2. develop, prototype and test systematic interventions or groups of **interventions to reduce risk**, and;
	3. propose implementation measures and **outcome measures of the effectiveness** for these intervention(s).

### Key policy priorities

**We would like your Phase One feasibility assessment to demonstrate consideration of some or all of the following:**

* How to support different professional **roles and disciplines** across government to reduce risk, including but not limited to [Analysis](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/941369/Analysis-Function-Career-Framework.pdf), [Government Commercial](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/697452/Commercial_Career_Framework_V2.0__2_.pdf) & Procurement, [Government Communications](https://3x7ip91ron4ju9ehf2unqrm1-wpengine.netdna-ssl.com/wp-content/uploads/2020/03/Government-Communication-Service-Career-Framework.pdf), [Digital, Data & Technology](https://www.gov.uk/government/collections/digital-data-and-technology-profession-capability-framework?_ga=2.174318693.692969177.1633704697-1568500685.1633704697), [Human Resources,](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/958120/HR_Career_Frameworks-A4_v0l.pdf) [Knowledge & Information Management](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/931963/Onion-diagram.jpg), [Operational Delivery](https://odp-proto.herokuapp.com/career_framework?utm_source=govuk), [Project Management & Delivery](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/755783/PDCF.pdf), [Property](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/862583/Government_Property_Career_Framework.pdf), [Government Security](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/864752/Government_Security_Profession_career_framework.pdf), [Counter Fraud](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/730050/Annex_B_-_GCFP_Brochure.pdf), [Finance](https://www.gov.uk/guidance/government-finance-academy?_ga=2.195365739.692969177.1633704697-1568500685.1633704697), [International Trade & Negotiation](https://www.civil-service-careers.gov.uk/professions/working-in-international-trade-and-negotiation/), [Legal](https://www.civil-service-careers.gov.uk/professions/working-in-legal/) & [Policy](https://www.gov.uk/government/organisations/civil-service-policy-profession/about?_ga=2.164890616.692969177.1633704697-1568500685.1633704697).
* How to support government organisations to identify what interventions should be **prioritised** to reduce risk;
* How to support both the **user** (anyone who uses government official IT) and the **practitioner** (those responsible for managing and delivering security in a government organisation) to reduce risk; whilst suppliers are welcome to target a specific user group for the intervention(s) e.g. system administrators, senior executives, suppliers should target the user groups which have the **greatest influence over the organisation’s risk posture**;
* How to evolve interventions to reflect the **changing risk landscape** over the long term;
* How your intervention prototype could **scale** across multiple public sector organisations, whilst maintaining a holistic methodology or capability that can assess and monitor the health of the Human Factors landscape;
* The extent to which your tests and proposed interventions draw on relevant published scientific research and/or independently validated “best practice” solutions used in similar organizations.

### Key User Needs

* Our users need to be able to:
	+ implement your intervention(s) **quickly, cheaply and easily;**
	+ measure the effectiveness of your intervention(s) on reducing risk in **near real time**;
	+ **integrate** your intervention(s) seamlessly with existing business processes and initiatives;
	+ **monitor** the impact of your intervention(s) on risk across diverse public sector organisations.

## Outcomes

The overall programme will be delivered over two phases. This is phase 1 of a potential 2-phase competition. A decision to proceed with phase 2 will depend on the outcomes from phase 1. Only successful applicants from phase 1 will be able to take part in phase 2.

The Contracting Authority reserve the right to adjust the provisional funding allocations between the phases. The total funding available for the competition may be subject to change.

* The overall programme will be delivered over two phases; this contract is for the first phase (Phase One).
* Up to £400,000 (including VAT) is allocated to Phase One of the competition, with potentially a number of simultaneous technical feasibility study contracts awarded of **up to £60,000k** (including VAT) per project **for up to 12 weeks**.
* Phase Two will award research and development contracts to Phase One project partners to deliver a “private beta” or field testing of the prototype developed in phase one with a small group of controlled users.
* The intended outcome of Phase Two is that we have field tested what will turn into a centrally delivered service that improves delivery in departments/ public sector organisations.
* We target awarding **up to three Phase Two contracts of up to £200,000 each** (including VAT) for **up to 6 months of research, development and prototyping**.
* The contract will terminate at the end of Phase Two, and the chosen business will be expected to pursue commercialisation of their solution.
* Suppliers will retain intellectual property developed during the contract, but foreground and necessary background IP to exploit the solution must be available to license on equitable, non-royalty terms by the government.

**APPLICATION PROCESS**

Directions on how to enter this competition can be found in the Invitation to Tender.

More information on this and other competitions may be obtained at [www.innovateuk.gov.uk](http://www.innovateuk.gov.uk)