

**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

We are looking to test our hypothesis that the quantification of insider risk can add unique value to people risk management, based on public information.

Insider risk is defined as ‘An insider is someone who (knowingly or unknowingly) misuses legitimate access to commit a malicious act or damage their employer.

A recent report assessed that the insider threat to government has likely increased in the last three years; hostile states almost certainly possess the greatest intent and capability to recruit HMG staff. The threat from serious and organised criminals is focused on HMG staff working at the borders, in law enforcement and in prisons, but capability levels vary.

There are live cases of espionage conducted against government departments, with some in the courts. The vast majority of civil servants, contractors and private sector employees are loyal and scrupulous but an individual with the right access can do immense damage; financially, reputationally and with regards to Civil Service morale.

A recent assessment indicated that HMG may be insufficiently agile, flexible or consistent to mitigate insider risk effectively. The current Covid-19 crisis risks exacerbating these issues as our workforce is under significant emotional stress, added financial pressures, reduced supervision, meaning our risk profile is likely to change in unpredictable ways as a result of greater ongoing use of remote working.

We are looking to learn how we can use public information to quantify potential insider risk for existing and prospective employees. We would like to assess the extent to which public information or open source online content provides relevant, unique, legally compliant and potentially actionable information for people risk management purposes, with a focus on (but not limited to); access to data; identity resolution; application of business rules (including business rules to restrict the collection of protected information e.g. LGBTQ+ status); scalability;delivery of alerts to end users; usability of the user interfaces; platform security and access.

We will do this by prototyping systems that collect, analyse and present this data to potential users.

### Goal of the project

The work supports the policy goal to deliver inclusive, supportive on-going people risk management throughout an employee’s life cycle. Public information will be treated like any other investigative lead before negative clearance action is initiated. The subject/ applicant will be provided an opportunity to refute or mitigate the content, and will also be afforded due process.

### Key policy priorities

Go beyond national security by applying people risk management to a wider range of sensitive roles, enabled by an overhaul of the security clearance system;

Move beyond a focus on point-in-time vetting to a cross-functional approach to assurance that manages risks throughout an individual’s employment; and

Deliver a new relationship of support and advice between employer and staff based on trust, integrity, wellbeing and a vibrant security culture.

### Key User Needs

The user needs to decide, using public information, whether a security clearance applicant is likely to fall into a defined list of risk categories.

These risk categories include unintentional or non-malicious risk, e.g., open source indicators that an employee may be experiencing alcohol, drug or other serious life stressors that could potentially affect their workplace reliability and wellbeing.

## Scope

The Cabinet Office is looking to partner with a third party supplier to assess the extent to which public information or open source online content provides relevant, lawfully and ethically defensible, unique and potentially actionable information for people risk management purposes, with a focus on (but not limited to); access to data, identity resolution, application of business rules, scalability, delivery of alerts to end users, usability of the user interfaces and platform security and access. We intend to research and test interfaces that collect information from the public web, cluster and analyse the information, possibly with the use of supervised or unsupervised machine learning algorithms, and present relevant information to users.

Phase one is focused on the assessment of the individual mechanisms (e.g. identity resolution) that make up the total capability.

In phase two, we target providing personally identifiable information (PII) from a subset of our population to the two successful vendors in order to assess the validity and reliability of their overall capability.

## 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.

### Phase 1:

Phase 1 involves research and development contracts being awarded to demonstrate technical feasibility of the proposed project.

A total of up to £250,000k (inc VAT) is allocated to phase 1 of the competition and it is anticipated that the feasibility study contracts will be in the region of up to £50,000k (inc VAT) per project for up to 8 weeks. The assessors will consider fair value in making their evaluation.

We would welcome bids from organisations that bring together a consortium of sectorial specialists to work together to provide a solution to the challenge set.

### Phase 2:

Phase 2 involves research and development contracts being awarded to businesses chosen from the successful Phase 1 applicants, to develop a prototype and undertake field-testing. It is anticipated that up to two phase 2 contracts, up to £150k (Inc. VAT) will be awarded for up to 12 months.

The contract will terminate at the end of Phase 2, and the chosen business will be expected to pursue commercialisation of their solution.

**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)