**Anomaly Detection RFI**

Summary

The Protective Security Co-Creation Programme is part of the National Security Technology and Innovation Exchange (NSTIx) network. We are exploring how anomaly detection algorithms could be best used across and beyond government to help examine, identify and then detect concealed threat and contraband items in baggage, vehicles and cargo.

Our aim is to build a better understanding of current market capability and to drive innovation and progress by bringing together the supplier and customer community. The specific focus of this project is data, and to address some of the challenges associated with it. We want to engage suppliers that have experience in anomaly detection to: understand what suppliers require to enable them to meet threat detection and security screening requirements; understand what data would be useful to share; and develop strategies as to how best to facilitate data sharing. The information you provide will assist in forming the basis of an in-person event designed to discuss these issues and challenges across the community and in developing a statement of requirements for potential future activities (such as data sharing agreements).

We are seeking submissions from individuals / organisations that have experience in anomaly detection, irrespective of the market sector they are currently working in.

Please note that this Request for Information (RFI) is not a commitment to any subsequent development.

Background

The Protective Security Co-Creation Programme is part of the National Security Technology and Innovation Exchange (NSTIx) network. NSTIx is a government-led science, technology and innovation partnership that supports the development of innovation and technology in areas that are critical to national security.

Automated Threat Detection (ATD) algorithms for detection of threat items in X-ray screening have developed and improved over recent years. However, further development of these algorithms has proven challenging due to the difficulty of access to large representative X-ray datasets, and in particular, images of threat items, which can be very challenging to collect.

One area of future development is anomaly detection, whereby an algorithm is trained to recognise what is ‘normal’ so that it can detect what is ‘abnormal’. Anomaly detection has the potential to provide a capability that detects a wide range of threats and contraband, while not being reliant on images of those items of interest being available for training. However, development of this type of software still requires access to very large amounts of benign yet representative data. As such, there is significant value in facilitating access for developers to large quantities of relevant operational images for the purposes of algorithm development.

Our initial focus is on algorithms that could be trained to assist in the detection of concealed threat and contraband items in X-ray screening of baggage (both 'hold' and 'cabin' baggage), but we would also be interested in anomaly detection that could be used for screening vehicles and cargo.

We are specifically focused on the use of operational data to train algorithms for threat detection. However we are also very interested in the potential use of synthetic data in the future, and are therefore interested in any requirements and/or developments relating to the use and/or creation of such data.

We are intending to hold an in-person collaboration event in London on **28th February 2023** to bring together:

* Cross-government security stakeholders that have a requirement for threat and contraband detection;
* Operational stakeholders who own datasets associated with security screening;
* Supplier teams that are developing anomaly detection.

The event will consider the practicalities of sharing data and images to support algorithm development, as well as the arrangements needed to help enable data and images to be shared. At the event, government organisations (such as the Department for Transport and Border Force) will brief on their security screening and threat detection requirements, together with constraints and challenges for operational use. Organisations that own datasets associated with security screening will present an overview of the data and images that they hold (including metadata) and the constraints and limitations associated with any sharing of such data for training anomaly detection systems.

If chosen to attend the event, you will be invited to present a short brief on:

* Your background and experiences in the area of anomaly detection, and how that could be applied to security screening and threat detection applications;
* The datasets that you would ideally require for training and trialling anomaly detection algorithms for detection of concealed threat and contraband items. This would need to include your requirements to increase your capability, such as the quantity of data required, the image file types, and the data transfer media.

We will **not** require you to share any unique intellectual property with the other attendees.

What we want

We are looking for individuals / organisations that have anomaly detection capability that could credibly result in the detection of threat and contraband items, even if those algorithms are not currently trained to detect such items. We welcome responses from any sector, not solely aviation.

What we don’t want

We are not interested in individuals / organisations that have no experience in anomaly detection.

This is not a competition and therefore we are not asking for costed proposals. Please note that these requests for information do not form a commitment to any subsequent development.

How to submit a response

Responses to this RFI should be submitted using the attached form and uploaded to the Defence Sourcing Portal or emailed to **acork@dstl.gov.uk**.

Submissions must be submitted by 18:00 on Friday 10th February 2023. Unfortunately, we are unable to accept any submissions after this point.

Selection for the collaboration event will take place week commencing the 13th February and we will let you know whether you have been selected for the event on Friday 17th February 2023, at which point further details will be provided.

The collaboration event is subject to receipt of an appropriate number of responses.

If you have any questions or require further information regarding this RFI, then please email **acork@dstl.gov.uk** with “Anomaly Detection RFI Question” in the subject line. Any further information will only be shared with organisations who can credibly contribute to a UK security capability.

How we use your information

Information you provide to us in an RFI submission, that is not already available to us from other sources, will be handled in confidence. By submitting this RFI, you are giving us permission to keep and use the information for internal purposes, including to inform the creation of a list of data challenges, and to provide the information onwards, in confidence, within UK Government.

The information you provide will be included in the NSTIx Protective Security Anomaly Detection Phase 1 Final Report. This will be used to inform potential future activities, with the ability to share within UK Government.