HMGCC Co-Creation

Challenge: Detecting changes in authorship within online communication

Summary of the challenge

When talking online, how do we know that the person we're talking to is who we think they are? Can we tell if a piece of writing has been changed by a different author?

These questions are at the heart of the latest national security challenge launched by HMGCC Co-Creation, which is looking for tech solutions founded in forensic linguistics, to help ensure the identity of online authors. A key requirement is to automate processes with explainable and defensible decisions.

HMGCC Co-Creation will provide funding for time, materials, overheads and other indirect expenses for applicants successful in phase 2 of the competition.

Technology themes

Artificial intelligence, behavioural and social sciences, communication systems, data science and engineering, machine learning, software development.

Key information

HMGCC Co-Creation will be hosting a two-stage competition process.

1) Phase 1. The objective is to rapidly assess brief proposals. Those unsuccessful will be informed with feedback. Successful applicants will be invited to phase 2. For further information please see **How to apply – Phase 1.**
2) Phase 2. Following a feedback phase, successful phase 1 applicants will be requested to submit a proposal directly to cocreation@hmgcc.gov.uk. For further information please see **How to apply – Phase 2.**

Total budget (excluding VAT)	£60,000
Project duration	12 weeks
Phase 1 Competition opens	Monday 1 September 2025

Phase 1 competition closes	Thursday 25 September 2025 at 5pm
Assessment and feedback window	6 working days
Phase 2 competition opens	Tuesday 7 October 2025
Phase 2 competition closes	Friday 24 October 2025 at 5pm

Context of the challenge

HMGCC Co-Creation is launching a challenge on behalf of national security to find a solution that detects changes in authorship within online communications and provide a detailed explanation of the detected differences.

UK government departments, like many private sector organisations with a global reach, conduct significant communication online. By communicating only via online text, there is a need for assurance that the person being messaged is the intended recipient, using writing style, motivation, mood and attitude changes as clues to their identity, with any changes needing to be understood in the context of national security concerns.

The gap

Specialists can analyse written online communication and may be able to spot inconsistencies across multiple messages from an individual, for example changes in linguistic style, tone, mood and motivations. However, this can be labour intensive and does not scale for many different online interactions.

It is believed that writing patterns of an individual can be learnt by a machine, giving the capability of automated anomaly detection. The machine’s explanation of why a change has been detected can then be investigated further.

Example use case

Javier is an operational officer investigating serious and organised crime gangs. He often communicates with different suspected criminals to gain evidence.

These communications are mainly in an email style layout; typically including a greeting, one or more paragraphs of text and a sign-off. They can be written in English and foreign languages including non-Latin.

Javier is wary when dealing with the suspected criminals. He rarely meets his contacts in person, to ensure everyone’s safety. He feels he may be unaware if he is being deceived.

This information may be exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to the originating department.

From his first communication with his contact, Javier logs all of his interactions in a central repository. The number of communications received can vary considerably, with the minimum total length being about two short paragraphs. He spots subtle changes across communications from the same contact, and it is difficult for Javier to note if the content changes are significant or not. He flags this to a central forensic linguist team to analyse and to also check if two supposedly different contacts show common communication styles.

As Javier and his colleagues have multiple contacts in the criminal world, they would like a tool to automatically flag authorship inconsistencies.

Project scope

Applicants should aim to deliver a demonstrator in this 12-week project, to at least Technology Readiness Level (TRL) 6. A developed model is required that can be transferred to the sponsor for initial trials. Essential and desirable requirements are listed below, along with constraints and elements which would not be required for this challenge.

Essential requirements:

- Authorship analysis of the writing style of an online contact to detect changes over time, and identify if changes relate to new authors, additional authors, or use of generative AI.
- Ability to assess in English and foreign languages including non-Latin.
- Ability to assess authorship of email-style layout, typically a greeting, one or more paragraphs and sign-off.
- Ability to provide a detailed explanation of why an authorship change has been detected.
- Solution architecture is expected to comprise n-tier architecture, with a minimum of two tiers, user interface and application. Additionally, the solution should be self-contained or ‘black-box’ with integration capabilities, for example APIs, to allow ingest of data, models, languages, and egress of outputs.
- Authentication and authorisation for roles, for example user and administrator.
- Model provided in either safetensor format or containerised in Docker or Kubernetes, likewise the solution as a whole will be containerised or capable of being built and deployed as a container.
- Design patterns that will allow to deploy anywhere (on-prem, on cloud infrastructure, or in a data centre) and can work off-line.
- Good documentation along with example code used.

Desirable:

- Cross-case writing analysis enabling comparison of writing styles across online conversations with different individuals to detect authorship matches.
- Cross-genre writing style analysis using additional genres such as SMS, social media and formal documents.
- Ability to assess authorship using message content that is not just writing style, but could include, for example, meta-data analysis, and behavioural science characteristics.
- The model could be plugged into a corporate knowledge base, with the ability to search on historical information.

Constraints:

- Training data sets must be compliant with UK law, including GDPR. Use of already developed algorithms, anonymised datasets or synthetic training data should be considered.
- Capable of functioning even with a small number of words.

Not required:

- No requirement for audio and visual genres.
- Analysis of handwritten communications.
- Digital forensic analysis of AI watermarks.
- Cloud-only based solutions.
- Horizon scanning only.

Dates

Phase 1 competition opens	Monday 1 September 2025
Clarifying questions published	Friday 19 September 2025
Phase 1 competition closes	Thursday 25 September 2025 at 5pm
Applicants notified with feedback	Monday 6 October 2025
Phase 2 competition opens	Tuesday 7 October 2025
Phase 2 competition closes	Friday 24 October 2025 at 5pm

Applicant notified	Tuesday 4 November 2025
Pitch day in Milton Keynes	Wednesday 12 November 2025
Commercial onboarding begins*	Wednesday 19 November 2025
Target project kick-off	Late November/ early December 2025

*Please note, the successful solution provider will be expected to have availability for a one-hour onboarding call via MS Teams on the date specified, to begin the onboarding/contractual process.

Eligibility

This challenge is open to sole innovators, industry, academic and research organisations of all types and sizes. There is no requirement for security clearances.

Solution providers or direct collaboration from countries listed by the UK government under trade sanctions and/or arms embargoes, are not eligible for HMGCC Co-Creation challenges.

Clarifying questions

Clarifying questions or general requests for assistance can be submitted directly to cocreation@hmgcc.gov.uk before the deadline with the challenge title as the subject. These clarifying questions may be technical, procedural, or commercial in subject, or anything else where assistance is required. Please note that answered questions will be published to facilitate a fair and open competition.

Application and evaluation criteria – Phase 1

Please send applications directly to cocreation@hmgcc.gov.uk including the challenge title with a note of the collaborator network where this challenge was first viewed.

Applications must be no more than one page or one slide in length. The assessment panel will only read the first page or slides if the page limit is exceeded.

All proposals will be assessed by the HMGCC Co-Creation team. Proposals must include the following criteria, and will be scored 1 - 5:

Applicant details	Contact name, organisation details and registration number.
Scope	Does the proposal fit within the challenge scope, taking into consideration cost and benefit?
Innovation	Is the technical solution credible, will it create new knowledge and IP, or use existing IP?
Deliverables	Will the proposal deliver a full or partial solution, if a partial solution, are there collaborations identified?

Following assessments, the successful applicants will be invited to submit a more in-depth proposal in phase 2. There will be feedback given to the successful applicants to aid their full proposal submission.

Application and evaluation criteria – Phase 2

Applications must be no more than six pages or six slides in length. The assessment panel will only read the first six pages or slides if the page limit is exceeded. The page/slide limit **excludes** personnel CVs and organisational profiles.

All proposals will be assessed by the HMGCC Co-Creation team. Proposals must include the following criteria, and will be scored 1 - 5:

Applicant details	Contact name, organisation details and registration number.
Scope	Does the proposal fit within the challenge scope, taking into consideration cost and benefit?
Innovation	Is the technical solution credible, will it create new knowledge and IP, or use existing IP?
Deliverables	Will the proposal deliver a full or partial solution, if a partial solution, are there collaborations identified?
Timescale	Will the proposal deliver a minimum viable product within the project duration?
Budget	Are the project finances within the competition scope?
Team	Are the organisation / delivery team credible in this technical area?

This information may be exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to the originating department.

Invitation to present

Successful phase 2 applicants will be invited to a pitch day, giving them a chance to meet the HMGCC Co-Creation team and pitch the proposal during a 20-minute presentation, followed by questions.

After the pitch day, a final funding decision will be made. For unsuccessful applicants, feedback will be given in a timely manner.

Co-Creation terms and conditions

Proposals must be compliant with the HMGCC Co-Creation terms and conditions; by submitting your proposal you are confirming your organisation's unqualified acceptance of Co-Creation terms and conditions.

Commercial contracts and funding of successful applications will be engaged via our commercial collaborator, Cranfield University.

HMGCC Co-Creation supporting information

HMGCC works with the national security community, UK government, academia, private sector partners and international allies to bring engineering ingenuity to the national security mission, creating tools and technologies that drive us ahead and help to protect the nation.

HMGCC Co-Creation is a partnership between HMGCC and Dstl (Defence Science and Technology Laboratory), created to deliver a new, bold and innovative way of working with the wider UK science and technology community. We bring together the best in class across industry, academia, and government, to work collaboratively on national security engineering challenges and accelerate innovation.

HMGCC Co-Creation aims to work collaboratively with the successful solution providers by utilising in-house delivery managers working Agile by default. This process will involve access to HMGCC Co-Creation's technical expertise and facilities to bring a product to market more effectively than traditional customer-supplier relationships.

FAQs

1. Who owns the intellectual property?

As per the HMGCC Co-Creation terms and conditions, project IP shall belong exclusively to the solution provider, granting the Authority a non-exclusive, royalty free licence.

2. **Who are the end customers?**

National security users include a wide range of different UK government departments which varies from challenge to challenge. This is a modest mark and so we would encourage solution providers to consider dual use and commercial exploitation.

3. **What funding is eligible?** This is not grant funding, so HMGCC Co-Creation funds all time, materials, overheads and indirect costs.

4. **How many projects are funded for each challenge?**

On average we fund two solution providers per challenge, but it does come down to the merit and strength of the received proposals.

5. **Do you expect to get a full product by the end of the funding?**

It changes from challenge to challenge, but it's unlikely. We typically see this initial funding as a feasibility or prototyping activity.

6. **Is there the possibility for follow-on funding beyond project timescale?**

Yes, it is possible, if the solution delivered by the end of the project is judged by the HMGCC Co-Creation team as feasible, viable and desirable, then phase 2 funding may be made available.

7. **Can we collaborate with other organisations to form a consortium?**

Yes, in fact this is encouraged. Please see the maximum budget of the individual challenge.

I can't attend the online briefing event, can I still access this?

If a briefing event is held, which varies challenge to challenge, then yes. Either the recording or the transcript will be made available to view at your leisure after it has been broadcasted. This will be made available via the HMGCC Co-Creation community collaborators.

8. **Do we need security clearances to work with HMGCC Co-Creation?**

Our preference is work to be conducted at OFFICIAL, we may however, request the project team undertake BPSS checks or equivalent.

9. **We think we have already solved this challenge, can we still apply?**

That would be welcomed. If your product fits our needs, then we would like to hear about it.

10. **Can you explain the Technology Readiness Level (TRL)?**Please see the UKRI definition for further detail.

This information may be exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to the originating department.

11. Can I source components from the list of restricted countries, e.g. electronic components?

Yes, that is acceptable under phase 1 - feasibility, as long as it doesn't break UK government trade restrictions and/or arms embargoes.

Further considerations

Solution providers should also consider their business development and supply chains are in-line with the National Security and Investment Act and the National Protective Security Authority's (NPSA) and National Cyber Security Centre's (NCSC) Trusted Research and Secure Innovation guidance. NPSA and NCSC's Secure Innovation Action Plan provides businesses with bespoke guidance on how to protect their business from security threats, and NPSA and NCSC's Core Security Measures for Early-Stage Technology Businesses provides a list of suggested protective security measures aimed at helping early-stage technology businesses protect their intellectual property, information, and data.

This information may be exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to the originating department.