Government Cyber Security Advisory Board

The Government Cyber Security Strategy (GCSS) was launched in January 2022 outlining the vision to ensure that core government functions are resilient to cyber attack, strengthening the UK as a sovereign nation and cementing its authority as a democratic and responsible cyber power.

Please note we are no longer accepting Expressions of Interest (EoI) for membership of the Government Cyber Security Advisory Board (GCSAB). GCSAB will build on the success of the External Challenge Panel that brought industry and academic perspectives to support the development of the GCSS.

GCSAB will be a body comprised of independent external experts to build better links between government, the private sector and academia. It will provide independent perspectives and input from experts across industry and academia into providing solutions to the challenges of government cyber security, through rigorous challenge and driving best practices across government.

The objectives of the GCSAB will be to:

- support the government to keep on track to achieve the GCSS aim of ensuring all government organisations across the whole public sector being resilient to known vulnerabilities and attack methods no later than 2030
- aid the long-term improvement of government cyber security by providing advice, expertise and guidance, and where required additional programme resource
- bring depth and experience across multiple fields with a diversity of viewpoints to improve policy making by providing solutions to particular problems and challenges
- identify solutions and proposals on how to achieve the 24 GCSS outcomes
- ensure government is leveraging industry expertise to deliver on the goals of the strategy

Membership Requirements

Eligibility

The Government Cyber Security Advisory Board will gather individual expertise in cyber security from industry and academia. We are not seeking expressions of interest from organisations, although we welcome candidates who can leverage the knowledge and experience that comes from their organisations themselves.

Candidates must have specific cyber security professional expertise, competence or knowledge with regard to areas covered in the GCSS, including:

- cyber security strategy, standards and assurance
- governance, risk and management
- programme delivery
- cyber detection and response
- technology
- cyber skills and culture

The GCSAB will meet once every two months, excluding August, virtually, but there may be requirements to attend in person in London.

Diversity

HMG embraces and values diversity in all forms. We welcome and pride ourselves on the positive impact diversity has on the work we do, and we promote equality of opportunity throughout the organisation. We therefore encourage applications from the widest range of qualified groups.

Selection process

Applications are now closed.

In the cover letter, candidates should set out their reasons for applying for the Government Cyber Security Advisory Board, their suitability for membership and how they meet the requirements set out in Eligibility.

Applications are now closed. The deadline for receipt of applications was 11.59pm 6 June 2022.

Any queries about this process, should be sent to gsgcyber@cabinetoffice.gov.uk.

Next steps

Following the EoI campaign, we will determine membership while ensuring that membership is representative of the diversity of the United Kingdom.

We will publish the outcome of the EoI campaign as soon as possible and in any event ahead of the first meeting of the Government Cyber Security Advisory Board.