OFFICE OF THE ADVISORY COMMITTEE ON BUSINESS APPOINTMENTS
G/7 Ground Floor, 1 Horse Guards Road SW1A 2HQ
Telephone: 020 7271 0839
Email: acoba@acoba.gov.uk
Website: http://www.gov.uk/acoba

April 2022

BUSINESS APPOINTMENT APPLICATION: Dominic Fortescue, former Government Chief Security Officer, application to establish an independent consultancy, KeyHaven Advisory.

1. Mr Fortescue, former Government Chief Security Officer, sought advice from the Advisory Committee on Business Appointments (the Committee) under the government's Business Appointments Rules for former Crown servants (the Rules) on his proposal to establish an independent consultancy, KeyHaven Advisory. The material information taken into consideration by the Committee is set out in the below annex.

2. The purpose of the Rules is to protect the integrity of the government. Under the Rules, the Committee's remit is to consider the risks associated with the actions and decisions made during Mr Fortescue's time in office, alongside the information and influence a former Crown servant may offer his consultancy and its future clients.

3. The Committee considered whether this consultancy was unsuitable given that in Mr Fortescue's former role as Government Chief Security Officer, he will have access to a wide range of information in the security and cyber space. The Committee will also consider the information provided by the department.

4. The Committee has advised that a number of conditions be imposed to mitigate the potential risks to the government associated with this appointment under the Rules; this does not imply the Committee has taken a view on the appropriateness of this consultancy for a former Government Chief Security Officer in any other respect.

5. The Rules set out that Crown servants must abide by the Committee's advice[1]. It is an applicant's personal responsibility to manage the propriety of any appointment. Former Crown servants are expected to uphold the highest standards of propriety and act in accordance with the 7 Principles of Public Life.

[1] Which apply by virtue of the Civil Service Management Code, The Code of Conduct for Special Advisers, The Queen's Regulations and the Diplomatic Service Code

The Committee's Consideration

Consultancy

6. In his application Mr Fortescue said he proposes to set up a consultancy defined as helping '...*company boards understand the nature of cyber risk and threat and the strategies they will need to adopt to mitigate that risk'*. It will also *'help cyber security companies best position themselves in what is a very crowded market…'*. The Committee[2] considered the broad nature of the consultancy to raise potential risks.

7. Although it is not improper for Mr Fortescue to operate a consultancy which draws on generic skills and experience he gained from his time in government, there are risks that arise under the government's Business Appointment Rules, where work is related to his time in office. As the Government Chief Security Officer, he would have had oversight of a wide range of security information and policy that may provide an unfair advantage to a range of organisations. There are also risks attached with his access to contacts within government and his potential to offer unfair influence.

8. The Committee considered the information provided about the broadly transparent nature of Mr Fortescue's responsibilities in office - building security capability and capacity within government departments. However, the Committee would remind Mr Fortescue that he must not draw on privileged insight from his time in office, generally or more specifically - for example around security and cyber security. It is important to note that alongside the Committee's advice, Mr Fortescue is also bound by the Official Secrets Act and an ongoing duty of confidentiality.

9. As well as imposing conditions on the consultancy itself, Mr Fortescue will be required to seek advice in relation to each individual client, so that risks can be assessed. The broad risks can be mitigated through conditions which: prevent individuals from drawing on privileged information; lobbying the UK government; and providing advice in relation to working with the UK government.

10. As the former Government Chief Security Officer, there is a risk associated with his potential influence and contacts within the security sector gained in office. Therefore the Committee would draw Mr Fortescue's attention to the restriction which makes it clear he should not use contacts he has developed in the security sector and other organisations whilst he was in government service, for the purpose of securing business for any company or organisation.

Future commissions

[2] This application for advice was considered by Jonathan Baume; Andrew Cumpsty; Isabel Doverty; Sarah de Gay; Dr Susan Liautaud; The Rt Hon Lord Pickles; Richard Thomas; Mike Weir and Lord Larry Whitty.

11. Mr Fortescue must seek advice from the Committee for each commission he wishes to accept. Whether the conditions set out below can sufficiently mitigate the risks presented by any future commission he proposes to take up will depend on the specific details of each piece of work. Any failure to seek advice before accepting work would be a breach of the Rules and treated as such - including reporting any breach to the government.

12. As Mr Fortescue seeks to provide advice on matters where he had insight or access to sensitive information in office this work will be more likely to give rise to risks under the Rules and applications will need close scrutiny. For example, should Mr Fortescue seek to provide advice on matters where he had insight or access to sensitive information in office, conditions alone may not be sufficient to mitigate the risks presented. The Committee will therefore want to carefully consider the suitability of this work, and may advise that a further waiting period is required. Where conditions and a suitable waiting period cannot appropriately mitigate the risks, the Committee may advise the work is unsuitable[3] to take up within the two years the Rules apply. The Committee will consider such risks on a case by case basis.

13. All potential clients must be notified of this advice; and when seeking work/new clients Mr Fortsecue should adhere to the conditions below. Under the Government's Business Appointment Rules, the Committee advises that this **Independent Consultancy - KeyHaven Advisory,** should be subject to the following conditions:

- he should not draw on (disclose or use for the benefit of himself or the persons or organisations to which this advice refers) any privileged information available to him from his time in Crown service;

- for two years from his last day in Crown service, he should not become personally involved in lobbying the UK government or any of its Arm's Length Bodies on behalf of those he advises under his independent consultancy (including parent companies, subsidiaries, partners and clients); nor should he make use, directly or indirectly, of his contacts in the government and/or Crown service contacts to influence policy, secure business/funding or otherwise unfairly advantage those he advises under his independent consultancy (including parent companies, subsidiaries, partners and clients);

- for two years from his last day in Crown service, he should not provide advice to on behalf of those he advises under his independent consultancy (including parent companies, subsidiaries, partners and clients) on the terms of, or with regard to the subject matter of, a bid with, or contract relating directly to the work of the UK government or any of its Arm's Length Bodies;

- for two years from his last day in Crown service, he should not become personally involved in lobbying contacts he has developed during his time in office and in other governments and organisations for the purpose of securing

[3] Should an applicant subsequently take up or announce this work ACOBA will publish relevant information.

business for any company or organisation (including parent companies, subsidiaries and partners); and

- for two years from his last day in Crown service, before accepting any commissions for his independent consultancy and or/before extending or otherwise changing the nature of his commissions, he should seek advice from the Committee. The Committee will decide whether each commission is consistent with the terms of the consultancy and consider any relevant factors under the Business Appointment Rules.

14. By 'privileged information' we mean official information to which a minister or Crown servant has had access as a consequence of his or her office or employment and which has not been made publicly available. Applicants are also reminded that they may be subject to other duties of confidentiality, whether under the Official Secrets Act, the Civil Service Code or otherwise.

15. The Business Appointment Rules explain that the restriction on lobbying means that the former Crown servant/Minister *"should not engage in communication with government (Ministers, civil servants, including special advisers, and other relevant officials/public office holders) – wherever it takes place - with a view to influencing a government decision, policy or contract award/grant in relation to their own interests or the interests of the organisation by which they are employed, or to whom they are contracted or with which they hold office."*

16. I should be grateful if you would inform us as soon as Mr Fortescue takes up employment with this organisation, or if it is announced that Mr Fortescue will do so, either by returning the enclosed form or by emailing the office at the above address. We shall otherwise not be able to deal with any enquiries, since we do not release information about appointments that have not been taken up or announced. This could lead to a false assumption being made about whether Mr Fortescue has complied with the Rules.

17. Please also inform us if Mr Fortescue proposes to extend or otherwise change the nature of his role as, depending on the circumstances, it may be necessary for him to make a fresh application.

18. Once the appointment has been publicly announced or taken up, we will publish this letter on the Committee's website, and where appropriate, refer to it in the relevant annual report.

Yours Sincerely,

Isabella Wynn
Committee Secretariat

Annex - Material information

1. Mr Fortescue said KeyHaven Advisory will:

- Help company boards understand the nature of current cyber risk and threat and the strategies they will need to adopt to mitigate that risk.
- Help cyber security companies best position themselves in what is a very crowded market, by thinking harder about what aspect of the cyber threat their product mitigates, and why security organisations should prioritise their product over others.
- Provide other ad hoc security advisory as required.

2. Mr Fortescue said this work will reflect his experience in government as leader of a large security function, and draw on the credibility of that role, but it will not draw on specific government knowledge. He said '...*the cyber world moves at great speed and the open-source insight from the big security companies, NCSC, and other cyber security experts, is immense. New cyber threat and vulnerability experience is generated every day and it is this corpus of material that [*he] *will need to stay current with'*.

3. Mr Fortescue said there is no lobbying component to this work and said seeking to sell anything to, or lobby government, is '...*a red-line for me: I would find it professionally demeaning'*

4. Mr Fortescue provided some general context around his time as Chief Security Officer:

   'Government Security sounds highly sensitive. In fact, the vast majority of our work is not. Government security is focussed on protecting government, and the challenges in that and the mitigations are familiar to security practitioners across all other sectors, across the globe. There is nothing special, or uniquely sensitive about Government Security, other than its prominence when things go wrong. In particular, Government Security is NOT national security, as practiced by the National Security Secretariat – which looks at threats to the UK from terrorists or hostile states, and is heavily involved with the intelligence and defence world and their capabilities, and constitutes some of the most sensitive work conducted by HMG.'

   '*Unlike the big policy departments in HMG, Government Security does not develop sensitive, let alone market or commercially sensitive policies or strategies (unlike HMT, DfT, etc). Nor does it have a regulatory role. Like the other Functions, the Security Standard is published on gov.uk. Our new Government Cyber Security Strategy will be published in early January, after the publication of the National Cyber Security Strategy. Many of our other broader policies are also publicly available on gov.uk. None of this is sensitive and because one of the ambitions, backed by Ministers, is that Government Security, our policies and practices, should become an exemplar for other sectors in the UK, we give them prominence.*'

'*There is nothing sensitive, for the most part, about Government Security capabilities either. Government overwhelmingly uses commercial tools from the big security providers. We deploy one bespoke platform for more sensitive material, but the fact of this has long been in the public domain. The providers are from the private sector.*'

5. He noted there may be some limited information he would have had access to in relation to general security threats. However, he also noted the government's work to publicly attribute cyber-attacks to those responsible, referring to the example of the SolarWinds attacks earlier this year. He said any access he did have to sensitive information was subject to the Official Secrets Act. Mr Fortescue noted he had held the highest level of security clearance for 31 years and said he recognised his '.....*life-long obligations under the OSA, of course, and have made the necessary undertakings to* [his]*parent department.* [He] *spent a career using what* [he] *know*[s] *with different audiences in different ways, carefully adhering to protective caveats….'*

6. The Cabinet Office provided their views on this application. The Cabinet Office confirmed Mr Fortescue's information above and added:

- the government security function seeks to build the capacity and capabilities of security professionals across UK government departments, covering physical, human and information security.
- as Director General of the Government Security Group within the Cabinet Office, he was also responsible for the oversight, coordination and delivery of protective security within all central government departments, their agencies and arm's-length bodies.
- he was also responsible for the Government Security Profession, bringing together security professionals from across government in supporting them gain skills and knowledge to fulfil their roles.
- The role was primarily focused on building capability and capacity as opposed to developing policy or regulatory in nature and the protective security knowledge and information is shared widely across sectors.

7. The Cabinet Office acknowledged there is a risk that his seniority and role within government could be perceived to unfairly assist organisations in influencing government, but noted Mr Fortescue ceased to his role in October 2021 so has already observed a 3 month waiting period. It also said that all sensitive national security and other information that DF had access to/ knowledge of will be protected under the terms of the OSA and noted his ongoing duty of confidentiality means he is obligated to '*to ensure that all information surrounding Government business, whether secret or not, is protected and kept confidential following departure from the department….*'. The department also noted:

- '*Protective security knowledge and information, particularly in relation to techniques, are no different to those used by industry and in fact we share and draw on much knowledge and information gleaned from industry partners and wider sectors.*'

- ‘*Techniques and understanding of protective security move fast and much innovation and development in this space is available from open sources*.’

8. The Cabinet Office confirmed it had no concerns with this appointment and recommended the standard conditions.