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

June 2022

BUSINESS APPOINTMENT APPLICATION: Dominic Fortescue, former Government Chief Security Officer, application to work with EY.

1. Dominic 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 an appointment with EY as a Cyber Security Partner. 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 EY.

3. 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 appointment for a former Government Chief Security Officer.

4. 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.

<u>The Committee's Consideration of the risks presented</u>

5. Mr Fortescue did not meet with EY while in government and did not make any policy or commercial decisions specific to EY. The risk this appointment was offered as a reward for decisions or actions taken in office is low.

[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

6. The Committee[2] noted the information provided about the broadly transparent nature of Mr Fortescue's responsibilities in office - building security capability and capacity within government departments. However, there are inherent risks associated with his access to information in office, including some sensitive security matters, though the Committee recognised this is limited.

7. There are also risks associated with Mr Fortescue's network gained in government service which could lead to the perception his influence might assist EY unfairly. The Committee noted Mr Fortescue has confirmed his role will not involve any contact with government so this risk is limited.

8. EY's clients are unknown; it is therefore possible Mr Fortescue is asked to advise clients who were affected by matters he had direct involvement in.

The Committee's advice

9. There is an overlap in the sector he is working in - security. However, Mr Fortescue will be working with EY in financial services and has confirmed he will have no involvement in its public sector division. The risks above in relation to his access to information and influence are therefore limited.

10. The conditions below which seek to prevent any improper use of privileged information and influence gained from his time in office. Alongside these conditions, the Cabinet Office notes Mr Fortescue is bound by on ongoing duty of confidentiality and the Official Secrets Act.

11. To mitigate the inherent risks associated with the unknown nature of EY's clients the Committee has also imposed a condition which makes it clear Mr Fortescue must not advise EY or its clients on policy he had specific involvement in or responsibility for as Government Chief Security Officer at the Cabinet Office. The Committee notes these conditions are in keeping with his role as described.

12. The Committee's advice, under the Government's Business Appointment Rules, that this appointment with **EY** 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 EY (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

[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; and Mike Weir. Richard Thomas and Lord Larry Whitty were unavailable.

business/funding or otherwise unfairly advantage EY (including parent companies, subsidiaries, partners and clients);

- for two years from his last day in Crown service, he should not provide advice to EY (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 advise EY or its clients on work with regard to any policy he had specific involvement or responsibility for as Government Chief Security Officer at the Cabinet Office, or where he had a relationship with the company or organisation during his time as Government Chief Security Officer at the Cabinet Office; and

- 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 business for EY (including parent companies, subsidiaries and partners).

13. 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.

14. 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.*'

15. Please inform us as soon as Mr Fortescue takes up employment with this organisation, or if it is announced that he will do so, 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.

16. Please also inform us if he 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.

17. 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

The role

1. Mr Fortescue said EY is one of the "Big 4" global audit/consultancy firms. The website states EY is a multinational professional services network with headquarters in London, England. EY is one of the largest professional services networks in the world.

2. Mr Fortescue said he will be joining the EMIA Financial Services practice as a partner with a remit to build EY's cyber security effort in Financial Services, and particularly the insurance sector. EY's Financial Services division's focus is to '*...build a better financial services industry, one that is stronger, fairer and more sustainable'*.

3. Mr Fortescue informed the Committee he will '*...not be working anywhere near the EY public sector practice and would emphatically not wish to'*. Further, he said this role will not include any contact or dealings with government.

Dealings in office

4. Mr Fortescue said he did not meet with EY.

5. Mr Fortescue confirmed his role in government had no direct crossover with EY or this role. He said he has no role in regulation or work specific to EY. He also confirmed he had no involvement in commercial or contracting decisions more generally, as above this was the responsibility of the cyber team.

6. He 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.*'

7. 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….'*

<u>Departmental assessment</u>

8. The Cabinet Office confirmed the details provided by Mr Fortescue.

9. The Cabinet Office has also previously confirmed:

- 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, Mr Fortescue were also responsible for the oversight, coordination and delivery of protective security within all central government departments, their agencies and arm's-length bodies; and 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.
- The Cabinet Office said that Mr Fortescue notionally oversaw contracting within your team as the responsible DG but that Mr Fortescue was far enough removed from them for the Permanent Secretary to be confident that this would not present a conflict of interest in these applications.
- All sensitive national security and other information that he had access to/ knowledge of will be protected under the terms of the OSA and your 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….*'
- '*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*.'

10. The department had no concerns with this work, identifying no specific risks and recommended it be subject to the conditions which prevent lobbying and use of privileged information.