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

May 2022

BUSINESS APPOINTMENT APPLICATION: Dominic Fortescue, former Government Chief Security Officer, commission with Netacea, under the consultancy - KeyHaven Advisory.

1. You 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 a commission you wish to take up with Netacea under your independent consultancy, KeyHaven Advisory. The material information taken into consideration by the Committee is set out in the 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 your time in office, alongside the information and influence you may offer Netacea.

3. When the Committee advised on your consultancy (this advice is available here: [link]), the Committee made it clear that where the work overlaps with his responsibilities in office the potential risks will need close scrutiny. The Committee has advised that a number of conditions be imposed to mitigate the potential risks to the government associated with this work under the Rules; this does not imply the Committee has taken a view on the appropriateness of this work 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>

[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

5. The Committee[2] considered this commission to be consistent with the description of your consultancy, KeyHaven Advisory, which you said will help'...*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…'*.

6. The website states Netacea Bot management takes a '...*new approach'* to bot detection, spotting known and evolving attacks to ensure that the maximum number of bots are detected with a minimum number of false positives. You had a private meeting with Netacea whilst still in post at the Cabinet Office - though not in your official capacity as Government Chief Security Officer but as part of your consideration for what you would do after leaving office. The Committee noted you did not make any policy or commercial decisions specific to Netacea and therefore. There is no evidence this appointment was offered as a reward for decisions or actions taken in office.

7. The Committee took into account the information provided about the broadly transparent nature of your responsibilities in office - building security capability and capacity within government departments. There remain inherent risks associated with your access to information in office, including some sensitive security matters, though the Committee recognised this is limited.

8. There are also risks associated with your network gained in government service which could lead to the perception your influence might assist Netacea unfairly. The Committee considered this to be limited given your role does not involve contact with the government.

<u>The Committee's advice</u>

9. The Committee noted this work fits within the description of your consultancy and the conditions applied to your consultancy (below) will sufficiently mitigate the risks associated with your access to information and potential influence.

10. The Committee advises, under the government's Business Appointment Rules, that this commission, with **Netacea** should be subject to the same conditions which apply to your independent consultancy:

- You should not draw on (disclose or use for the benefit of yourself or the persons or organisations to which this advice refers) any privileged information available to you from your time in Crown service;

- for two years from your last day in Crown service, you should not become personally involved in lobbying the UK government or any of its Arm's Length Bodies on behalf of those you advise under your independent consultancy (including parent companies, subsidiaries, partners and clients); nor should you make use, directly or indirectly, of your contacts in the government and/or

[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. Lord Larry Whitty was unavailable.

Crown service contacts to influence policy, secure business/funding or otherwise unfairly advantage those you advise under your independent consultancy (including parent companies, subsidiaries, partners and clients);

- for two years from your last day in Crown service, you should not provide advice to on behalf of those you advise under your 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 your last day in Crown service, you should not become personally involved in lobbying contacts you have developed during your time in office and in other governments and organisations for the purpose of securing business for any company or organisation (including parent companies, subsidiaries and partners); and

- for two years from your last day in Crown service, before accepting any commissions for your independent consultancy and or/before extending or otherwise changing the nature of your commissions, you 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.

11. The advice and the conditions under the government's Business Appointment Rules relate to your previous role in government only; they are separate to rules administered by other bodies such as the Office of the Registrar of Consultant Lobbyists or the Parliamentary Commissioner for Standards. It is an applicant's personal responsibility to understand any other rules and regulations they may be subject to in parallel with this Committee's advice.

12. 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.

13. 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."*

14. I should be grateful if you would inform us as soon as you take up employment with this organisation, or if it is announced that you 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 you have complied with the Rules.

15. Please also inform us if you propose to extend or otherwise change the nature of your role as, depending on the circumstances, it may be necessary for you to make a fresh application.

16. 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

<u>The role</u>

1. You seek to take up work with Netacea**.** The website states websites are often targets for malicious attacks by automated bots. It states Netacea Bot management takes a '...*new approach'* to bot detection, spotting known and evolving attacks to ensure that the maximum number of bots are detected with a minimum number of false positives. It states it helps protect customers, data etc.

2. You said you will advise on a Go to Market strategy for their bot management defensive tool. You said Netacea needs help best positioning themselves in what is a very crowded market, and thinking harder about what aspect of the cyber threat their product mitigates, and why security organisations should prioritise their product over others. You do not propose your role will have any contact with government.

<u>Dealings in office</u>

3. You said you had a meeting with Netacea whilst still employed at the Cabinet Office. This meeting was in a private capacity when you were considering what you would do in your post government career.

4. You said your role in government had no direct crossover with Netacea or this role and you had no role in work specific to Netacea. You also confirmed you had no involvement in commercial or contracting decisions.

5. You provided some general context around your 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.*'

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

<u>Department Assessment</u>

7. The Cabinet Office confirmed the details provided by you.

8. 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, you 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 you notionally oversaw contracting within your team as the responsible DG but that you were 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 you had access to/ knowledge of will be protected under the terms of the OSA and your ongoing duty of confidentiality means you are 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*.'

9. 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.