OFFICE OF THE ADVISORY COMMITTEE ON BUSINESS APPOINTMENTS
Room G/08, 1 Horse Guards Road, London, SW1A 2HQ
Telephone: 020 7271 0839
Email: acoba@acoba.gov.uk
Website: http://www.gov.uk/acoba

27 November 2018

Dear Mr Prince,

You sought the Committee's advice about taking up a commission under your independent consultancy with BAE Systems Applied Intelligence. The Committee has now considered your application.

Commission details

You informed the Committee that BAE Systems Applied Intelligence (BAE AI) is the division of BAE Systems that is responsible for products and services relating to cyber security and data analytics.

The commission would be to:

- advise on strategy for BAE AI's work with foreign governments, including, for example, reviewing their country strategies;
- support senior customer engagement with foreign governments, including by participating in engagements with foreign governmental customers; and
- support the development of the wider BAE AI products and services 'offer' as regards foreign governmental customers, including reviewing solutions and providing feedback.

You confirmed the commission would solely relate to BAE AI's international work. You said you would not advise on BAE AI's provision of more general cyber products and services to the financial services sector. You also said you would not get involved in any BAE AI sales to or contracts with the UK Government. Neither would you be involved in lobbying the UK Government nor advising BAE AI on any bid or contract directly relating to the work of the UK Government.

The commission would be for up to 70 days a year, for two years.

You informed the Committee that in your capacity as Cyber Security Ambassador, you met a wide range of UK cyber companies to talk about the UK Government's cyber exports strategy and export opportunities.

You said you held formal meetings with BAE AI on half a dozen occasions over the last two years of your government service. These meetings were to discuss the UK Government's cyber exports strategy, learn in broad terms about BAE AI's thinking as regards export, and to discuss particular opportunities. You also spoke at two BAE AI conferences at which you presented on the UK National Cyber Security Strategy and the UK Government's approach to cyber exports.

You said you participated in international UK Government-to-Government engagements on cyber capacity building, particularly in the Gulf. In a number of the countries concerned BAE AI has contracts with the government in question, or has had discussions about potential contracts.

You had contact with a number of competitors of BAE AI, including BT, their main UK competitor. You met BT and other UK cyber companies on a number of occasions to discuss the UK Government's cyber exports strategy and to hear in broad terms about the companies' thinking on cyber exports.

You informed the Committee you had no direct contractual dealings with BAE AI, nor were you responsible for those carrying out any such dealings. You said you were not involved in the award of grants or contracts, or in regulatory work, regarding BAE AI, its competitors, or the UK cyber industry sector as a whole. You have been involved in the UK Government's policy thinking on the UK cyber industry sector in that you provided input to the UK cyber exports strategy (designed to benefit all UK cyber companies). You also said you advised DCMS on that part of the National Cyber Security Strategy designed to encourage the growth of the UK cyber sector. You said this is not relevant to well-established companies such as BAE AI.

As regards access to relevant privileged information in your Government role, you said you received very little privileged information from your interactions with UK cyber companies. UK cyber companies sometimes shared top-level information on their export strategies with you but you said this has been of a very generic nature..

You said your personal discussions with foreign governments on cyber were mostly at a strategic level, generally involving you explaining the UK Government's National Cyber Security Strategy and exploring lessons that might be relevant to the foreign governments' own cyber strategies and programmes. Where foreign governments shared their thinking as to future acquisition of cyber capability, the Department of International Trade shared that information with relevant UK cyber companies, including BAE AI and its competitors. In all respects BAE AI was treated no differently to any other UK cyber company.

Your former department, the Department of International Trade (DIT) was consulted on the commission and provided the information below. DIT confirmed that the Permanent Secretary, Antonia Romeo, had agreed the Department's advice to the Committee.

- There are no contractual arrangements between DIT's Defence and Security Organisation (DSO)[1] and BAE AI. The relationship between DSO and BAE AI is the normal relationship held with any UK company that is seeking to export.
- BAE AI is one of the two main/ largest cyber security companies (the other is BT).
- The Interim Head of DSO is not aware that you have access to any unannounced UK Government policy. He confirmed you would have known about other UK company export successes.
- The Interim Head of DSO is of the view that, having worked closely with companies, you have the knowledge of an industry insider - but he does not believe this included having access to privileged information.
- DSO consider your role with BAE AI as '...generally having a clear benefit to the UK's cyber security industry as revenue will flow to companies in addition to BAE AI. When prime contractors such as BAE AI and BT are delivering capability for overseas governments they often include technology provided by UK cyber SMEs and, as subcontractors, the SMEs receive a share of the contract revenue from the prime contractor.'
- DSO added: '...to address cyber security challenges there is a trend for increasing cooperation across national borders and also between public and private sector actors. In recognition of this, the HMG cyber security strategy supports and encourages the growth of the commercial cyber security ecosystem in the UK to ensure that there will be an increase in the number of UK based cyber security technology providers which can protect the UK in the future. It is commonplace for HMG staff who have experience of cyber security operations gained during government service to join companies such as BAE AI or BT Security. Many also join, and sometimes lead, a growing number of cyber start-ups and cyber SMEs. Delivering technically complex cyber security contracts for overseas government clients often requires UK cyber companies to work together.'
- DIT recommended that you should be precluded from engaging on BAE AI business with any Government in the Gulf region for fixed period of time, with the exception of a specific contract supported by a UK Government-to-Government agreement on cyber security. DIT has stated that there would be a huge benefit to HMG and the wider sector if you were permitted to be involved in this contract. They consider that because the contract is being bid for via a consortium of UK companies, this manages the risk of any perceived (or actual) conflict as there is no single benefit to BAE AI.

The Committee's consideration

The Committee[2] is satisfied this role is consistent with the terms of your consultancy, which you described as providing strategic advice around cyber security, as well as on wider risk and organisational strategy issues in a way that supports the UK's security and prosperity.

The Committee has considered whether this commission raises concerns under the Government's Business Appointment Rules.

---

[1] The Defence & Security Organisation (DSO) is an organisation within the Department for International Trade providing specialist export advice and practical assistance to the UK defence and security industries.

[2] This application for advice was considered by Sir Alex Allan; Jonathan Baume; Baroness Browning; Lord Michael German; Dr Susan Liautaud; Baroness Helen Liddell and John Wood. Terence Jagger and Richard Thomas were unavailable.

The Committee noted that during your role as Cyber Security Ambassador you engaged with BAE AI on multiple occasions. Given this, there is a risk it could appear this work is a reward for actions taken while you were in office. However, this is balanced by the fact that, as Cyber Security Ambassador, it was an integral part of your role to engage with UK industry on cyber exports. The objective evidence provided by DIT is that your actions were entirely in keeping with your role at DIT and for the UK's economic benefit. Therefore the Committee concluded the risk your actions were motivated by the expectation of future work is low.

Your commission will involve supporting senior customer engagement with foreign governments, including by participating in engagements with foreign governmental customers. As Cyber Security Ambassador you played a key role in government-to-government engagements on cyber capability. This saw you developing trusted relationships with Ministers and senior officials in Governments in the Gulf. You have therefore developed connections in post that it would be reasonable to think could benefit BAE AI. The Committee has, therefore, considered whether a 12-month, or longer, waiting period is required to mitigate this. However, it also took into account DIT's confirmation that most of your work as Cyber Security Ambassador focused on the Gulf. The Committee concluded that the risk of providing BAE AI with an unfair advantage is largely addressed by imposing a condition precluding you from working in the Gulf (subject to the caveat below) and the nine months that have passed since your last day in office.

In light of the public interest in you working on a specific contract supported by a UK Government-to-Government agreement on cyber security (as explained by DIT), the Committee is content to make an exception to the restriction on you working in the Gulf, in relation to securing the specific contract, and ensuring it delivers effective capability.

Conditions applied to the commission

Under the Government's Business Appointment Rules, the Committee's advice is that this commission with BAE AI should be subject to the following conditions:

- you should not draw on (disclose or use for the benefit of yourself or the organisations to which this advice refers) any privileged information available to you from your time in Crown office;
- for two years from your last day in Crown service you should not engage on BAE Systems' business with any Government in the Gulf region (defined as Bahrain, KSA, Kuwait, Oman, Qatar and UAE)*.
- for two years from your last day in Crown service, you should not provide advice to any company or organisation on the terms of, or with regard to the subject matter of, a bid or contract relating directly to the work of the UK Government*;
- for two years from your last day of service you should not become personally involved in lobbying the UK Government on behalf of BAE Systems or its subsidiaries, partners or clients. Nor should you make use, directly or indirectly, of your Government and/or Crown Service contacts to influence policy or secure business or funding on their behalf;
- for two years from your last day in Crown service, you should not become personally involved in lobbying contacts developed during Crown service in other Governments or organisations, for the purpose of securing business for BAE Systems or its subsidiaries, partners or clients*; and

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

*These conditions are not intended to prevent you from working on a specific contract supported by a UK Government-to-Government agreement on cyber security. However, the Committee would expect you to adhere to the remaining conditions in doing so.

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.

The Business Appointment Rules explain that the restriction on lobbying means that the former Crown servant "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."

I should be grateful if you would let me know when you take up this commission, or if it is announced that you are to do so. This will enable the Committee to publish this letter on the Committee's website, and where appropriate, refer to it in the relevant annual report.

Yours sincerely,

Nicola Richardson
Committee Secretariat