HM Treasury

Information Rights Unit
HM Treasury
1 Horse Guards Road
London
SW1A 2HQ

Mr Don Priest

020 7270 5000
foirequests@hmtreasury.gov.uk
www.gov.uk/hm-treasury

15 April 2019

Dear Mr Priest

Ref: FOI2019/04423

Freedom of Information Act 2000: Cyber security

Thank you for your enquiry of 19 March 2019, which we have considered under the terms of the Freedom of Information Act 2000 (the FOI Act).

You asked for the following information:

> *Qu 1 What security rules, codes, protocols, procedures and precautions are taken to ensure that the CIA, GCHQ /Cabinet office are not eavesdropping / spying on staff, officials and ministers in your Department with social media eg Google, Facebook as a conduit?*
>
> *Qu 2 What summaries / reports does the department have about its cyber security? Please indicate the public facing reports.*
>
> *Qu 3 Has the Department risk assessed the threat posed by social media, especially that owned by foreign corporations and countries and especially US and CIA? What summaries does the department have of this information, including any public facing ones?*
>
> *Qu 4 What social media apps are allowed on the Departments phones and computers?*
> *Which are installed?*
>
> *Qu 5 Are Facebook, Google and Twitter apps allowed to be installed and or used on Department computers and mobile phones?*
>
> *Qu 6 Are private, ie individually owned, mobile phones and computers with social media apps installed such as Facebook, Google and Twitter allowed in Department meetings, committees, and in the office environment?*
>
> *Qu 7 If the answer to Qu 5 and Qu 6 are yes, how does the Department stop companies / CIA spying utilising microphones, cameras, and GPS data on those devices?*
>
> *Qu 8 Has the department informed staff of the risk of spying and eavesdropping via social media apps? If so please send a copy of the memo / paper.*
>
> *Qu 9 Has the Department contributed material to the Cabinet Office as part of the cyber security strategy? If so what?*
>
> *Questions on Q sometimes written as QAnon, #Q #QAnon*

(Background information on Q follows the questions)

Qu 10 Has the Secretary, Ministers or the top 3 civil servants in the Department been briefed about QAnon?

Qu 11 If so please indicate the date and the type of recorded information that has been briefed so that any future request may be narrowed down, as per Section 16 of the UK freedom of Information Act and Information Commissioner Guidance.

Qu 12 Has the Department any other recorded information on Q / QAnon ? If so please indicate the date and the type of recorded information that has been briefed so that any future request may be narrowed down, as per Section 16 of the UK freedom of Information Act and Information Commissioner Guidance. (If there is a mass of information that will take the request over the time limit, please disregard this question)

I can confirm that HM Treasury does hold information within the scope of your request, except where clearly stated in the answers, which I have set out below:

Qu 1

In the security rules, codes, protocols and procedures and precautions that we apply and maintain in relation to any aspect of eavesdropping and social media we are guided by the expertise and published guidance of central government authorities. These include, by way of example:

- UK National Authority for Counter Eavesdropping (UK NACE) (https://www.fcoservices.gov.uk/products-and-services/global-digital-technology/technical-security-cyber-services-uk-nace/) and
- Centre for the Protection of National Infrastructure (CPNI) Guidance: My Digital Footprint (https://www.cpni.gov.uk/my-digital-footprint)

Qu 2, 3, 4, and 5

Any reports that we hold, or threat assessments we have made, in relation to our cyber security, or threats related to possible attack through social media form part of our protection against organised crime. Similarly, while we do allow some specific social media apps on the Department's smartphones, our policy of not disclosing which specific apps we allow, also forms part of our protection against organised crime. We therefore consider that disclosing such information engages the exemption at section 31(1)(a) of the FOI Act which is engaged when release of that information would, or would be likely to, prejudice the prevention or detection of crime.

Section 31 is a prejudice based exemption and is subject to the public interest test. In applying this exemption, we are required to consider whether, in all the circumstances of the case, the public interest in maintaining the exemption outweighs the public interest in disclosing the information. This is set out below.

In favour of disclosure, we acknowledge that disclosure of this information might provide some assurance on the extent to which the department has assessed the likelihood of cyber-attacks against its IT systems, or social media attacks against its staff.

However, balanced against this, is the public interest in not prejudicing law enforcement by aiding a criminal intent on launching attacks on the department's IT systems and/or staff. We consider that, in this case, disclosure of the information requested would be likely to create a vulnerability to criminal activity. Therefore, on balance we believe that the public interest is in favour of not disclosing the information.

Qu 6 and Qu 7

I can confirm that we do allow privately owned mobile phones and computers (some of which may contain social media apps installed such as Facebook, Google and Twitter) in most areas of our building including in meetings held within those areas. However, some areas of the building and certain meeting rooms restrict the use of private and departmental mobile phones and computers.

Qu 8

The guidance that we provide to our staff in relation to spying and/or eavesdropping relate primarily to those handling information of a higher government security classification, and to specific areas of our building. We consider that disclosing such information engages the exemption at section 24(1) of the FOI Act which is engaged when release of that information would, or would be likely to, undermine national security and section 31(1)(a) of the FOI Act as release of that information would, or would be likely to, prejudice the prevention or detection of crime.

These are prejudice based exemptions and subject to the public interest test. In applying the exemptions, we are required to consider whether, in all the circumstances of the case, the public interest in maintaining the exemption outweighs the public interest in disclosing the information. This is set out below.

In favour of disclosure, we acknowledge that disclosure of this information might provide some assurance on the extent to which the department has provided adequate guidance to its staff in relation to the risk of spying and eavesdropping via social media apps.

However, balanced against this, is the public interest in not aiding those intent on spying or eavesdropping on the department's staff. We consider that, in this case, disclosure of the information requested would be likely to undermine national security and prejudice law enforcement by aiding a criminal intent on launching attacks. We consider that, in this case, disclosure of the information requested would be likely to create a vulnerability to criminal activity. Therefore, on balance we believe that the public interest is in favour of not disclosing the information.

Qu 9, 10, 11 and 12

I can confirm that we do not hold any information in relation to these four questions.

If you have any queries about this letter, please contact us. Please quote the reference number above in any future communications.

Yours sincerely

Information Rights Unit

Copyright notice

Your right to complain under the Freedom of Information Act 2000

If you are not happy with this reply, you can request a review by writing to HM Treasury, Information Rights Unit, 1 Horse Guards Road, London SW1A 2HQ or by emailing us at the address below. Any review request must be made within 2 months of the date of this letter.

Email: foirequests@hmtreasury.gov.uk

It would assist our review if you set out which aspects of the reply concern you and why you are dissatisfied.

If you are not content with the outcome of the review, you may apply directly to the Information Commissioner for a decision. Generally, the Commissioner will not make a decision unless you have exhausted the complaints procedure provided by HM Treasury which is outlined above.

The Information Commissioner can be contacted at: The Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF (or via their website at: https://ico.org.uk).