Ministry of Defence

Ministry of Defence
D3, Building 405
Corsham
Wiltshire SN13 9NR
United Kingdom

Ref. FOI2015/11501

E-mail: ISS-SecretariatGpMbx@mod.uk

[redacted]

[redacted]

11 February 2016

Dear [redacted]

FREEDOM OF INFORMATION REQUEST

Your correspondence dated 14 December 2015 is considered to be a request for information in accordance with the Freedom of Information Act (FOIA) 2000. You requested the following information:

> *"How many breaches of security have taken place at RAF Shawbury, RAF Cosford, MOD Donnington in Telford, Copthorne Barracks in Shrewsbury, Nesscliffe Army Camp, and Clive Barracks in Tern Hill in the last 10 years.*
>
> *Can you provide me with a year by year break down of figures for each base and give details of the type of breach of security there has been.*
>
> *Can you also provide me with a quote in relation to the figures."*

I wrote to you on 13 January 2016 advising that I believed the information you requested would be subject to an exemption under section 31 (Law Enforcement) and that a public interest test would need to be carried out.

A search for the the information you requested has now been completed within the Ministry of Defence (MOD) and I can confirm that information in scope of your request is held. However I can confirm that some of the information is subject to the following exemptions:

Section 24 (National Security)
Section 26 (Defence)
Section 31 (Law Enforcement)

Information that does not fall within scope of the exemptions listed above is provided at Annex A to this letter.

Please note that no Information Assurance Security breaches were found for Clive Barracks or Nesscliffe Army Camp.

Sections 24, 26, and 31 are qualified exemptions and are subject to public interest testing which means that the information requested can only be withheld if the public interest in doing so outweighs the public interest in disclosure.

Section 24(1) has been applied because it would not be in the interest of the UK's national security for departments to provide information about the specific number or type of cyber attacks being detected. Nor would it be in the interest of the UK's national security to release information relating to internal procedures which may be invoked in the event of a cyber attack or suspected cyber attack. Release of any of this information could reveal to an adversary the comprehensive cyber defence capabilities employed by the MOD. This is not in the public interest. Release of such information could enable adversaries to deduce how to potentially circumvent our cyber defence capabilities and their ability to conduct damage assessments on any attacks they might have conducted would be enhanced, as would evaluation of the effectiveness of UK defences, or components of those defences, against cyber threats. Release of such material could thus increase the risk of a successful attack on MOD computers, with the concomitant risk of further information being consequently released which could further compromise national security.

Sections 26(1)(a) and (b) have been applied because knowledge of the type of cyber attacks being detected could reveal to an adversary the cyber defence capabilities employed by the MOD. Release of such information could enable adversaries to deduce how to potentially circumvent our cyber defence capabilities and their ability to conduct damage assessments on any attacks they might have conducted would be enhanced, as would evaluation of the effectiveness of UK defences, or components of those defences, against cyber threats. Release of such material could thus increase the risk of a successful attack on MOD computers, with the risk of further information being consequently released which could further compromise the defence of the UK. For these reasons I have set the level of prejudice against release of the exempted information at the higher level of “would” rather than “would be likely to”.

Additionally, section 31(1)(a) has been applied because disclosure of any information relating to the number or types of cyber attacks and processes followed in the event of a cyber attack or suspected cyber attack would aid a criminal intent on launching a cyber attack on Departmental IT systems. Knowledge of the cyber attacks against MOD systems would provide an adversary with details on the level of protection employed by the MOD, therefore, giving them an insight in to how to perform malicious activity against the MOD. For these reasons I have set the level of prejudice against release of the exempted information at the higher level of “would” rather than “would be likely to”.

In favour of release is the presumption towards disclosure under the FOIA as answering this question would increase transparency of the level of IT security employed by MOD.

On balance, I consider the public interest favours maintaining the exemptions and withholding some of the information you have requested.

With reference to your request for a quote, I would advise you to call the press office on:
0207 218 7907.

If you are not satisfied with this response or you wish to complain about any aspect of the handling of your request, then you should contact me in the first instance. If informal resolution is not possible and you are still dissatisfied, then you may apply for an independent internal review by contacting the Deputy Chief Information Officer, 2nd Floor, MOD Main Building, Whitehall, SW1A 2HB (e-mail CIO-FOI-IR@mod.uk). Please note that any request for an internal review must be made within 40 working days of the date on which the attempt to reach informal resolution has come to an end.

If you remain dissatisfied following an internal review, you may take your complaint to the Information Commissioner under the provisions of Section 50 of the Freedom of Information Act. Please note that the Information Commissioner will not investigate your case until the MOD internal review process has been completed. Further details of the role and powers of the Information Commissioner can be found on the Commissioner's website, http://www.ico.gov.uk.

Yours sincerely,

Information Systems and Services (ISS) Secretariat