15th November 2018

Freedom of Information Request Reference No: FOI 003719/18

I write in connection with your request for information received by the Norfolk and Suffolk Constabularies on the 10th October 2018 in which you sought access to the following information:

> I am currently embarking on a research project around Cyber Security and was hoping you could provide me with some contract information relating to following information:
>
> 1 Standard Firewall (Network) - Firewall service protects your corporate Network from unauthorised access and other Internet security threats
>
> 2 Anti-virus Software Application - Anti-virus software is a program or set of programs that are designed to prevent, search for, detect, and remove software viruses, and other malicious software like worms, trojans, adware, and more.
>
> 3 Microsoft Enterprise Agreement - is a volume licensing package offered by Microsoft.
>
> The information I require is around the procurement side and we do not require any specifics (serial numbers, models, location) that could bring threat/harm to the organisation. For each of the different types of cyber security services can you please provide me with:
>
> 1 Who is the existing supplier for this contract?
> 2 What does the organisation spend for each of contract?
> 3 What is the description of the services provided for each contract? Please do not just state firewall.
> 4 Primary Brand (ONLY APPLIES TO CONTRACT 1&2)
> 5 What is the expiry date of each contract?
> 6 What is the start date of each contract?
> 7 What is the contract duration of contract?
> 8 The responsible contract officer for each of the contracts above? Full name, job title, contact number and direct email address.
> 9 Number of License (ONLY APPLIES TO CONTRACT 3)

Response to your Request

The response provided below is correct as of 6th November 2018.

Norfolk and Suffolk Constabularies have located the following information as relevant to your request.

Q1 The Constabularies do not have a contract for network firewalls.

Q2 The security environment covers all aspects of business and confidential matters. Any details regarding the Constabularies anti-virus software could be used to attempt an attack on the Constabularies infrastructure. Information has therefore not been provided due to exemptions within the Act.

Section 1 of the Freedom of Information Act 2000 (FOIA) places two duties on public authorities. Unless exemptions apply, the first duty at section 1(1)(a) is to confirm or deny whether the information specified in a request is held. The second duty at section 1(1)(b) is to disclose information that has been confirmed as being held.

Section 17 of the Freedom of Information Act 2000 requires that Norfolk and Suffolk Constabularies, when refusing to provide such information (because the information is exempt) is to provide you, the applicant, with a notice ban, which:-

(a) States that fact
(b) Specifies the exemptions in question, and
(c) States (if that would not otherwise be apparent) why the exemptions apply

The information is exempt from disclosure by virtue of the following exemptions:-

- **Section 24(1) National Security**
- **Section 31(1)(a)(b) Law Enforcement**

Sections 24 and 31 are qualified prejudice based exemptions and therefore we are obliged to consider the harm in disclosure and conduct a public interest test.

Evidence of Harm

Disclosure of information under the Freedom of Information Act 2000 (FOIA) is considered to be a release to the world, as once the information has been published on the Disclosure Log pages of the Constabularies external websites, the Constabularies have no control over access to that information. Whilst not questioning an applicant's motive for requesting information, it could be of use to persons who are involved in criminal activity, including terrorism related offences.

Although there is a call for openness and transparency, this needs to be balanced against the harm in disclosure of the requested information. The Police Service has a clear responsibility to prevent and detect crime and disorder and to protect the communities we serve.

Disclosing the details of Norfolk and Suffolk Constabularies' security products could assist those who plan to attempt an attack on force systems and infrastructure. It is essential that Police systems are secure as they contain a variety of information which relates to policing activities, including investigations, police intelligence and personal information. Such attacks could take the form of data theft, denial of service and other deliberate disruptions. This would have the effect of reducing the ability of the Police to undertaken relevant activities.

There would be a significantly increased risk of a security compromise, undertaken by a malicious act against our infrastructure. Should a security compromise actually be successful, the harm would be a compromise of the forces' ability to use its own ICT (including radio and telephony), potentially leading to direct harm to the public, as a result of not being able to access systems and data. Also, a compromise of the forces' data, could result in information being released into the public domain.

The Constabularies have a duty to enforce the law and protect the public. Disclosure under the Freedom of Information Act could be used to identify if there are any areas of potential weaknesses in security products. This would lead to a security risk to systems. This would consequently undermine the Police Services' law enforcement ability and this would be harmful.

The prevention and detection of crime is the foundation upon which policing it built and the threat from terrorism cannot be ignored. It is generally recognised, in this current environment, that the international security landscape is increasingly complex and unpredictable. The current UK threat level from international terrorism, based on intelligence, is assessed as 'severe' which means that a terrorist attack is highly likely. Please see below:-
https://www.mi5.gov.uk/threat-levels

Providing any information regarding the Constabularies' anti-virus products could assist individuals who are involved in the planning of terrorist activity.

Public Interest Test

Section 24 – factors favouring disclosure
Releasing the details would provide reassurance to the public that the Constabularies are taking all steps possible to combat terrorist activity, and international criminal activity, against our National Security. The public are entitled to know how public funds are spent. In the current financial climate, and with the call for transparency of public spending, this would enable improved public debate.

Section 24 – factors against disclosure
Security measures are put in place to protect the communities we serve. The public entrusts the Police Service to make appropriate decisions with regard to their safety and protection and the only way of reducing risk is to be cautious with what information is placed into the public domain.

Any specific details of software that is used by the Constabularies could be used in order to plan a cyber-attack on force systems. Where the same requests have been submitted to all force areas, releasing information would allow for planning to disrupt policing activity on a national basis. Any incident which results from such a disclosure would, by default, affect National Security.

Section 31 – factors favouring disclosure
The provision of this information would reassure the public that the Constabularies are taking steps to ensure that systems are appropriately protected and that sufficient public funds are being allocated for this purpose. There is a public interest in how the Police protect personal data and providing the full details of the products used would ensure accurate public debate, regarding security matters, and what is in place to prevent cyber-attacks.

Section 31 – factors favouring non-disclosure
The IT infrastructure is vital to the ability of the Constabularies to effectively prevent and detect crime, share information and maintain a proficient law enforcement capability. Details of security products which are in place to protect our systems, could be used by individuals to identify potential vulnerabilities which they could use to plan a cyber-attack. Any disruption to Constabulary systems would result in the need for additional resources and increased expenditure to ensure that policing activities are not compromised or data

lost. There would also be a requirement for additional funds to carry out repairs and system recovery.

For every piece of security infrastructure there is a list of known vulnerabilities or loopholes. No piece of security software is infallible, they all have weaknesses, and those weaknesses can be exploited. By detailing exactly what security products we use, we would be advertising the Constabularies vulnerabilities. This would be useful information for individuals planning to attempt to bypass security software.

Balance Test

The points above highlight the merits for and against disclosure of the requested information. Disclosure would undoubtedly provide a greater openness and transparency to the community at large. Whilst there is a public interest in the transparency in how the Police Service delivers effective law enforcement and ensures information security, there is a strong public interest in safeguarding police systems and information.

Additionally, we also need to take into account the safety of the public and the impact on National Security. This would be severely compromised if an attack was successful and police systems compromised.

The security of force systems is of paramount importance and this should not be jeopardised by the any release of information under the Freedom of Information Act. Therefore it is our opinion that the balance lies in favour of non-disclosure and this letter serves as a refusal notice under section 17(1) of the Act.

Q3 Details of the Microsoft Enterprise Agreement are published on the Bluelight Procurement Database website under reference SOFT003. A link has been provided below:-

https://www.blpd.gov.uk/foi/foicontractview.aspx?contractid=35677

Under Section 21(1) of the Freedom of Information Act (2000), public authorities are not required to provide information that is reasonably accessible to the public by other means, in this case via the BLPD website, therefore in accordance with Section 17 of the Freedom of Information Act (2000), this serves as a Refusal Notice for this part of your request.

This response will be published on the Constabularies web-site under the Freedom of Information pages:-

https://www.norfolk.police.uk/about-us/our-data/disclosure-log
https://www.suffolk.police.uk/services/freedom-information/disclosure-logs

Should you have any further queries concerning this request, please contact Amanda Gibson, FOI Decision Maker, quoting the reference number shown above.

A full copy of the Freedom of Information Act (2000) can be viewed on the 'Office of Public Sector Information' web-site;
http://www.opsi.gov.uk/

Norfolk and Suffolk Constabularies are not responsible for the content, or the reliability, of the website referenced. The Constabulary cannot guarantee that this link will work all of the time, and we have no control over the availability of the linked pages.

Your Right to Request a Review of Decisions Made Under the Terms of the Freedom of Information Act (2000).

If you are unhappy with how your request has been handled, or if you think the decision is incorrect, you have the right to ask the Norfolk and Suffolk Constabulary to review their decision.

Ask Norfolk and Suffolk Constabularies to look at the decision again.

If you are dissatisfied with the decision made by Norfolk and Suffolk Constabularies under the Freedom of Information Act (2000), regarding access to information, you must notify the Norfolk and Suffolk Constabulary that you are requesting a review within 40 days of the date of its response to your Freedom of Information request. Requests for a review should be made in writing and addressed to:

Freedom of Information Decision Maker
Information Management Department
Norfolk Constabulary
Operations and Communications Centre
Jubilee House
Falconers Chase
Wymondham
Norfolk NR18 0WW
OR
Email: freedomofinformation@norfolk.pnn.police.uk

In all possible circumstances Norfolk and Suffolk Constabulary will aim to respond to your request for us to look at our decision again within 20 working days of receipt of your request for an internal review.

The Information Commissioner.

After lodging a request for a review with Norfolk and Suffolk Constabulary, if you are still dissatisfied with the decision, you can apply to the Information Commissioner for a decision on whether the request for information has been dealt with in accordance with the requirements of the Act.

For information on how to make application to the Information Commissioner please visit their website at www.ico.org.uk or contact them at the address shown below:

The Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Telephone: 01625 545 700