**Freedom of Information Request Reference Nº: FOI 003477-20**

I write in connection with your request for information received by Suffolk and Norfolk Constabularies on 15 October 2020 which you sought access to the following information:

*"Under the Freedom of Information Act 2000 may I kindly request the following information about your IT Infrastructure Information. The information needed is as follows:*

*SECURITY / CYBERSECURITY:*

1. *What SEIM (Security Event and Incident Management) solution is used by your organisation?*

2. *When does your SEIM (Security Event and Incident Management) platform license subscription come up for renewal?*

3. *If the SEIM (Security Event and Incident Management) solution was purchased via third party please disclose the contracting party's details?*

4. *Do you outsource your security management to a third party (managed security service provider)? If so can you disclose the name of the managed security service provider.*

5. *When does the current service contract from the current managed security service provider end?*

6. *Can you provide the email address of the individual that is responsible for your IT Security?*

*ICO - breaches:*

7. *How many cyber security breaches has your organisation had over the past 2 yrs?"*

**Response to your Request**

The response provided below is correct as of 19 October 2020

Suffolk and Norfolk Constabularies have considered your request for information and the response is below.

1. Suffolk and Norfolk Constabularies are using the services of a nationally provided solution, the name of which has not been disclosed as a result of exemptions within the Act.

   Section 17 of the Freedom of Information Act 2000 requires that Suffolk and Norfolk 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 exemption(s) in question and
   (c) States (if that would not otherwise be apparent) why the exemption(s) applies.

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

   **Section 24(1) – National Security**
   **Section 31(1) – Law Enforcement**

   Sections 24 and 31 are qualified and prejudice-based exemptions and I am therefore obliged to consider the harm in providing the information and conduct a public interest test.

   **Harm**

   Provision of information concerning the versions we are utilising for Security Event and Incident Management (SEIM), would provide actual knowledge of the systems in use and could identify vulnerable computer systems. This information would be of significant interest to those involved in criminal and terrorist activity as it could indicate any forces and systems that may be more vulnerable to a cyber-attack. This could result in the loss of Police information, intelligence and tactics.

   The Constabularies have a duty to enforce the law and protect the public. Disclosure under the Freedom of Information Act (FOIA) could be used to identify where there are potential weaknesses in security products and target specific areas, this could lead to a security risk to systems. This would consequently undermine the Police Service's law enforcement capability.

   If the Police Service are subject to a cyber-attack, this would affect the Country on a national scale and could therefore affect National Security, as well as undermining law enforcement.

   The loss of data from national databases would impact on the Constabularies partnership working. It is vitally important that information sharing takes place with security bodies within the UK to support counter-terrorism measures in the fight to deprive terrorist networks of their ability to commit crime.

   An attack on Police systems could place the safety of officers and members of the public at risk.

In order to comply with statutory requirements and to meet National Police Chiefs' Council of the Police Service, with regard to the management of information security, a national policy approved by the College of Policing, titled National Policing Community Security Policy, has been put in place. This policy has been construed to ensure the delivery of core operational policing by providing appropriate and consistent protection for the information assets of member organisations. A copy of this can be found at the below link:-

http://library.college.police.uk/docs/APP-Community-Security-Policy-2014.pdf

In addition, anything that places that confidence at risk, no matter how generic, would undermine any trust or confidence individuals have in the Police Service.

**Public Interest Test**

Factors favouring disclosure – Section 24

The public are entitled to know how public funds are spent. To confirm what versions we have would enable the general public to determine whether Norfolk and Suffolk Constabularies are managing resources appropriate when it comes to ICT systems. In the current financial climate of cuts, and with the call for transparency of public spending, this would enable improved public debate.

Provision of the installation dates would also ensure we are maintaining adequate storage solutions and providing additional information for transparency.

Factors against disclosure – Section 24

Security measures are put in place to protect the communities that we serve. As evidenced within the harm, to confirm what Security Event and Incident Management solution is used, would highlight to terrorists and individual's intent on carrying out criminal activity, any potential vulnerabilities within Norfolk and Suffolk.

Considering the current security climate within the UK, no information, which may aid a terrorist, should be disclosed. To what extent this information may aid a terrorist is unknown, but it is clear that it would have an impact on a forces' ability to monitor terrorist activity.

The public entrust 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 is placed into the public domain.

The cumulative effect of terrorists gathering information from various sources would be even more impactive when linked to other information from various sources about terrorism. The more information disclosed over time will give a more detailed account of the tactical infrastructure of not only a force area but also the County as a whole.

Any incident that results from such a disclosure would, by default, affect National Security.

Factors favouring disclosure – Section 31

Provision of the information would allow a greater understanding of where public funds are being allocated. For the Police Service to be fully transparent and open, it is appreciated that there is a public interest in providing information that infers where public money may be spent.

Confirming that information exists, relevant to this request, would lead to a better-informed public which may encourage individuals to provide intelligence in order to reduce attacks.

Factors against disclosure – Section 31

Whilst we are not questioning the motive of the applicant, provision of such information would allow individuals to utilise the data in a discovery phase of a potential attack, which would leave the Constabularies network vulnerable. The public entrust 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 is placed into the public domain. the information we supply will be published on the website available for any person to review and use to their advantage.

The IT infrastructure is vital to the ability of the Constabularies to effectively prevent and detect crime, share data and maintain a proficient law enforcement capacity. Information will not be disclosed if it such would compromise that capability in any way and expose the Constabularies to 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.

Policing resources and the police capability would be negatively affected, and manipulated by those with criminal intent, to obtain an advantage over any potential police tactics and capabilities. In a world where cybercrime is ever increasing it is of paramount importance to protect such sensitive information.

Provision of the information would suggest that Norfolk and Suffolk Constabularies take their responsibility to protect information and information systems from unauthorised access, destruction, etc, dismissively and inappropriately.

**Balance Test**

The Police Service is charged with enforcing the law, preventing and detecting crime and protecting the communities we serve. 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.

Whilst there is a public interest in the transparency and accountability, there is a very strong public interest in safeguarding information that may imply vulnerabilities or weaknesses that individuals may use to try and focus efforts on to attack the Constabulary IT Infrastructure

Any disclosure that places the confidence of the Constabularies ICT infrastructure at risk, no matter how generic, would undermine any trust or confidence individuals have in the Police Service. 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, at this moment in time, it is our opinion that the balance test for the information requested is not provided and the exemption at Sections 24 and 31 are engaged.

2. This is an ongoing service.

3. This service has been provided by a central solution as per question 1.

4. Only the 'SEIM' solution is 'outsourced' to the centrally provided solution.

5. This is an ongoing service.

6. The Information Security Advisors email address is InformationSecurity@suffolk.pnn.police.uk

7. The definition of a cyber-attack is an attempt by hackers to damage or destroy a computer network or system.

   There have been no cyber security breaches within Norfolk and Suffolk Constabularies over the past 2 years.

Should you have any further queries concerning this request, please contact Clair Pack, 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 20 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*
*Suffolk Constabulary*
*Police Headquarters*
*Martlesham Heath*
*Ipswich*
*Suffolk*
*IP5 3QS*
*OR*
Email: information@suffolk.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 40 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