FREEDOM OF INFORMATION REQUEST

FREEDOM OF INFORMATION REQUEST 2024/27591

Dear requester,

Thank you for your recent request under the Freedom of Information Act 2000.

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, **Section1 (1) (b)**, is to disclose information that has been confirmed as being held.

The information that you are seeking is in relation to the following:

REQUEST

Please may you provide some information on the following areas:

Networks

1. What network vendor(s) / service provider does your emergency service currently use for their LAN, WAN,, wireless and core network (e.g., BT, Virgin, Cisco)?
2. Is the network managed / run internally, or is the network managed and/or supplied by a third party? Please specify which elements of the network are outsourced and to which companies.
3. Please may you provide an indication of the size of the network (e.g., number of switches, routers, access points etc.)?
4. How much money was spent on the last major network refresh (referring to replacement of the LAN / WAN / core network)?
5. When was the last major network refresh (month & year)?
6. When is the next major network refresh likely to take place (month & year)?
7. What frameworks are likely to be used when releasing a tender for a network refresh?

Cyber Security

1. Which cyber security providers / vendors are used, and for what technologies (e.g., firewalls, SOC etc.)?
2. When is your service due for a renewal of these technologies (month & year)?
3. Is all cyber security managed in-house, or is it / parts of it outsourced to a third party? Please specify which elements are outsourced and to which companies.

Command and Control

1. Which technology suppliers / vendors are used in your command and control rooms?
2. Is your command and control room managed in-house, or is it / parts of it outsourced to a third party? Please specify which elements are outsourced and to which companies.
3. How much was spent on the last major command and control technology refresh (referring to the replacement of the CAD / ICCS)?
4. When was the last command and control technology refresh (month & year)?
5. When is the next command and control technology refresh likely to take place (month & year)?

RESPONSE

Networks

1. What network vendor(s) / service provider does your emergency service currently use for their LAN, WAN,, wireless and core network (e.g., BT, Virgin, Cisco)?

Information Withheld * Please see exemption Section 24(1) below.

2. Is the network managed / run internally, or is the network managed and/or supplied by a third party? Please specify which elements of the network are outsourced and to which companies.

The WAN is provided and managed by the PSBA which is a Welsh Government initiative delivered by BT.

3. Please may you provide an indication of the size of the network (e.g., number of switches, routers, access points etc.)?

Information Withheld * Please see exemption Section 24(1) below.

4. How much money was spent on the last major network refresh (referring to replacement of the LAN / WAN / core network)?

The last major LAN network refresh was for the new HQ building costing approx. £643,981 and also replacement LAN network equipment across the estate costing approx. £145,524.

5. When was the last major network refresh (month & year)?

New HQ LAN ordered in two parts during May & July 2021 and the replacement LAN equipment across the estate ordered in May 2024.

6. When is the next major network refresh likely to take place (month & year)?

A rolling programme of equipment refresh is maintained with all equipment supplied via conformant tendering process.

7. What frameworks are likely to be used when releasing a tender for a network refresh?

As above.

Cyber Security

Due to the sensitivity of this information the following exemptions has been applied:

Harm

Release of this information into the public domain would highlight to cyber-criminals the specific brand of protection and supplier used by the force. This would allow individuals wishing to perpetrate cybercrime the opportunity to conduct research into any known weaknesses in this brand or with the supplier and would highlight any vulnerabilities to those wishing to exploit these. This could have a huge impact on the effective delivery of operational law enforcement as it would leave the forces open to cyberattack which could render computer devices obsolete.

Furthermore, release of this information would allow comparisons to be drawn between the software used by various police forces allowing criminals to compile national information upon weaknesses which could identify areas of weakness which could then be exploited. This type of information would be extremely beneficial to offenders, including terrorists and terrorist organisations.
It is vitally important that information sharing takes place with other law enforcement agencies within the UK to support counterterrorism in the fight to deprive terrorist networks of the ability to commit crime. To disclose information on the cyber-security solution including providers/vendors, would be extremely useful to those involved in terrorist activity as it would enable them to map vulnerable information upon security databases.

Public Interest Considerations

Section 24(1) National Security Factors favouring disclosure.

The public are entitled to know how public funds are spent and how resources are distributed within an area of policing. To confirm this information would highlight to the public that the Police are using the most appropriate methods to protect sensitive

information. In the current financial climate of cuts and with the call for transparency of public spending this would enable improved public debate into this subject.

Section 24(1) National Security Factors opposing disclosure.

Security measures are put in place to protect the community we serve. As evidenced within the harm this information would highlight to terrorists and individuals' intent on carrying out criminal activity, vulnerabilities with policing. Disclosure of this sensitive information may allow individuals to research known weaknesses of any solution/supplier/vendor disclosed that a cyber-criminal could then use to attack the force's IT infrastructure.

A cyber-attack could negatively affect the infrastructure of policing and undermine national security in relation to terrorism. 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 become more impactful when linked to other information gathered 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 country as a whole.

Section 31(1) Law Enforcement Factors favouring disclosure.

The public are entitled to know how public funds are spent and how resources are distributed within an area of policing. To confirm this information would highlight to the public that the Police are using the most appropriate methods to protect sensitive information.

Section 31(1) Law Enforcement Factors opposing disclosure.

Disclosure of this information due to its sensitive nature would affect operational policing. The release of this type of information would better inform criminals on the protection we use and how best to perform a cyber-attack on the force to negate these protections. Should this be successful it may lead to IT systems not working efficiently and a negative impact would occur on the prevention or detection of crime. This would lead to the force being unable to carry out its primary duty of protecting the public and detecting and preventing crime. It would also lead to criminals being better informed on any vulnerabilities of the force.

Balancing Test

The points above highlight the merits of providing the information requested and weigh these against the potential harm of disclosure. The police service is charged with enforcing the law, preventing and detecting crime and protecting the communities we serve. As part of that policing purpose, information is gathered which can be highly sensitive relating to high profile investigative activity. Weakening the mechanisms used to monitor any type of criminal activity and protect this

information, specifically terrorist activity would place the security of the country at an increased level of danger.

Having considered the public interest test factors, we are required to determine whether, on balance, the factors favouring disclosure outweigh those which are against disclosure. At this time, it is our opinion that for the issues highlighted above, the balance test favours non-disclosure of this information.

Command and Control

1. Which technology suppliers / vendors are used in your command-and-control rooms?

Information Withheld * Please see exemption Section 24(1) above.

2. Is your command-and-control room managed in-house, or is it / parts of it outsourced to a third party? Please specify which elements are outsourced and to which companies.

Information Withheld * Please see exemption Section 24(1) above.

3. How much was spent on the last major command and control technology refresh (referring to the replacement of the CAD / ICCS)?

£356k

4. When was the last command and control technology refresh (month & year)?

This would be when HQ was occupied – Nov 2022

5. When is the next command and control technology refresh likely to take place (month & year)?

No date has been confirmed currently.

Freedom of Information Act is a public disclosure regime, not a private regime. Any information disclosed under the Act is thereafter deemed to be in the public domain, and therefore freely available to the public and will be published on the Gwent Police website.

If, upon receiving a response to a freedom of information request, you are unhappy with the outcome, you may request an internal review**. This should be made within 40 working days of the initial response.**

Please direct any internal review requests to FOI@gwent.police.uk

You have the right to request an appeal from the Information Commissioners Office about your Freedom of Information request, if you are dissatisfied with your internal review response.

ICO Contact Details:

The Information Commissioner's Office, Wycliffe House, Wilmslow, Cheshire, SK9 5AF

Tel: 0303 123 1113

Web: www.ico.org.uk

Thank you for your interest in Gwent Police.