Harm

Identifying the specific solution which is used has potential to undermine law enforcement and threaten national security by providing an awareness of exactly what software is actually used by individual forces in the identification and management of security breaches. Release of this information would help build a national picture of how police forces identify and manage such risks which would, in turn, highlight to hackers intent on carrying out cyber-attacks on police systems, potential vulnerabilities which would ultimately allow them to evade or circumvent detection.

Public Interest Considerations

Section 24 National Security

Factors favouring release

The public are entitled to know how public funds are spent and how resources are distributed within an area of policing. In the current financial climate of cuts and with the call for transparency of public spending this would enable improved public debate.

Factors against release

Security measures are put in place to protect the community we serve. As evidenced within the harm to confirm details of suppliers used by West Midlands Police could highlight to individuals intent on carrying out criminal activity vulnerabilities within WMP.

If WMP were to fall subject to a cyber-attack, the implications would affect the country on a national scale and therefore could adversely affect national security as well as undermine policing.

The release of the requested information could lead to sensitive information going into the public domain that a cyber-criminal could use to attack West Midlands Police. The information is sensitive in nature if it would highlight vulnerabilities. For instance, if it is known that a particular piece of software has weaknesses and a force was to disclose they use this then those weaknesses could be exploited. A cyber-attack could negatively affect the infrastructure of policing. By affecting the infrastructure of policing the nation’s security will be more vulnerable 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.

Police information, intelligence and tactics could be obtained from a cyber-attack resulting in the criminal fraternity including terrorists gaining knowledge that will assist in the planning of offences and evading detection. It is also possible the sharing of information and the updating of multiagency databases such as PNC are affected, which could jeopardise officer safety as well as that of the public.

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

Section 31(3) Law Enforcement

Factors favouring release

Disclosing information relevant to this request would lead to a better informed public which may encourage individuals to provide intelligence in order to reduce these attacks. Factors against release Disclosure of the withheld information would suggest West Midlands Police take their responsibility to protect information and information systems from unauthorised access, destruction, etc., dismissively and inappropriately.

The information requested is sensitive in nature to the extent it would affect operational policing. Sensitive information could be if a force was using a particular programme that had known vulnerabilities. The release of this type of information would better inform a criminal on how to cyber-attack the police. If a force was hacked and this lead to their IT systems not working efficiently then a negative impact would occur on the prevention or detection of crime. Cyber-crime can lead to forces being unable to carry out their objectives which is why you would not want to provide information that could lead to criminals being better informed on the vulnerabilities a force has.

Balancing Test

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

In order to comply with statutory requirements and to meet NPCC expectation 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 constructed 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. Therefore, at this moment in time, it is our opinion that for these issues the balance test favours withholding this information.