**Public Interest Test**

**Applicable Exemptions** Section 31 – Law Enforcement

**Harm**

The disclosure of the requested information would provide the public at large with details of force systems which are intended to be secure. These systems are secure because they contain a variety of information which relates to policing activities. This information might include data relating to investigations, police intelligence and personal information. The requested information could be used by a hostile party to plan and execute an attack on force systems. Such attacks could take the form of data theft, denial of service or other deliberate disruptions. This could not help but have the effect of reducing the ability of the police to undertake relevant activities.

**Reasons for Disclosure**

The disclosure of the requested information would show which software/hardware is used by the police service and reassure the public that these systems are up to date and secure.

**Reasons for Non-Disclosure**

Disclosure would provide those intent on disrupting police activities with enough information to plan and execute a targeted attack. This would be detrimental to the effective operation of police activities. Additional resources would be required to counter the attack and this would also have financial implications. Where systems were compromised, there is also the potential for sensitive information such as personal data, security information and other data to be made public.

**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 the NPCC's expectations of the Police Service with regard to the management of information security a national policy created by the College of Policing titled Information Assurance 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:

https://www.app.college.police.uk/app-content/information-management/information-assurance/

This is linked to the old ACPO Information Systems Community Security Policy:

http://library.college.police.uk/docs/APPref/ACPO-ACPOS-2009-Information-Systems.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.