Open Source Software and Security

December 2011

This note, developed in consultation with CESG, highlights some of the key security considerations for the use of open source software in Government, and their implications for procurement practice.

It focuses on dispelling common security myths about open source software which prevent a level playing field for its evaluation and use in Government. It is published in recognition that a wider audience wish to understand the UK Government's position on open source software and security.

Public sector customers can obtain further information from CESG in GPG38.

1. Open source, as a category, is no more or less secure than closed proprietary software.

All software, including open source and closed proprietary, will have vulnerabilities. Individual software products, regardless of category, will have strengths and weaknesses in security characteristics such as provenance, quality, support, and vulnerability management. Given the range of vulnerabilities and diversity of exploits, on balance, neither category is considered more or less secure than the other.

2. Therefore, open source software cannot be excluded from an options analysis for Government IT.

Given that no one type of software is inherently more secure than another, neither open source nor closed proprietary software should be excluded from an options analysis for security reasons.

It is Government policy for open source software to be evaluated in an options analysis, and for suppliers to provide appropriately detailed evidence of the reasoning behind their selection.

It is entirely possible that an open source option is not selected for valid reasons, such as insufficient functional fit, inability to meet performance requirements, or higher cost of ownership due to more expensive security controls. It is important that the same selection criteria are applied to all options. It is also important that requirements are not exaggerated, unnecessarily inflating costs.

3. CESG does not accredit software products. Departments accredit their own ICT solutions.

It is a myth that some software products are "accredited" for use in Government. This is a misunderstanding of the security framework and accreditation process. Departmental accreditation of their own IT solutions is a sophisticated and rigorous process encompassing business benefit, threat and risk assessment, hardware, software, communications, and human factors.

CESG does operate assurance schemes through which security enforcing products, both open source and closed proprietary, can be evaluated and certified. Such certification assures the public sector that security enforcing products, such as firewalls and cryptography tools, can mitigate various risks to its information. The large majority of software used to build Government IT solutions does not fall into this category. Furthermore, the risk managed decision whether or not to use such software remains with the Department's information risk owner.