Department for Business Innovation & Skills

CALL FOR EVIDENCE ON A PREFERRED STANDARD IN CYBER SECURITY

Government Response

NOVEMBER 2013

Contents

Key Conclusions: **3**

Outcome: **4**

Useful Links: **5**

We are helping businesses better understand the cyber security standards landscape to:

- Offer clarity to businesses in what is a complex and confused standards landscape, by supporting standards that are accessible and fit-for-purpose;
- Help businesses follow best practice in basic cyber hygiene and mitigate cyber risks at the low-threat level e.g. hacking and phishing;
- Offer a voluntary alternative to a legislative approach;
- Enable businesses that are cyber secure to differentiate themselves in the marketplace.

Key Conclusions:

The feedback we received from industry through the Call for Evidence was that none of the standards or approaches fully met our requirements, but that industry are keen to help us develop something new that would meet our requirements. We anticipated that we would back which ever came the closest and work with the supporting bodies to develop it further. We recognise that this is a challenging journey and value this support from industry.

The backing of a preferred standard is intended to help businesses navigate what is a complex standards landscape and offer clarity to organisations on how to implement basic cyber hygiene to mitigate cyber risks at the low-threat level. With regard to the legislative approach being taken in the EU, our approach will inform the voluntary and collaborative UK position. It will also give customers and investors a clear indicator of whether a business is taking their cyber risk seriously and enable those businesses that are cyber secure to differentiate themselves and make it a selling point.

The greatest volume of support from industry was in favour of the ISO27000-series of standards, which offers a management framework for managing information security risk and is well-established, relatively widely used and internationally recognised. However the ISO27000-series of standards have perceived weaknesses in that implementation costs are high and that due to their complexity SMEs sometimes experience difficulties with implementation. The fact that in the previous version businesses were free to define their own scope for which area of their business should be covered by the standard can also make auditing ineffective and inconsistent.

Industry were also supportive of two additional publications - IASME (Information Security for SMEs) and the ISF (Information Security Forum) Standard of Good Practice for Information Security. As you would expect the main strengths of IASME are that it is easy to understand and used, and designed around small businesses. The contrasting strengths of the ISF's Standard of Good Practice for Information Security are that it is comprehensive and is typically used by larger businesses. We heard from industry that both IASME and the ISF's Standard of Good Practice for Information Security were good at helping businesses implement good practice in the relevant parts of their organisation. However, both these standards have common weaknesses in that, compared to ISO27000-series standards, they have limited take-up in the market and limited international recognition.

Outcome:

Government will now work with industry to develop a new implementation profile, which will become the Government's preferred standard. This profile will be based upon key ISO27000-series standards and will focus on basic cyber hygiene.

Government will work with the **ISF,** who will be the lead author of the project, and with **IASME** to ensure that the new profile will be simple, SME-friendly, and will have a trustworthy audit framework. We will also be working with the **British Standards Institution (BSI)** as the national standards body and UK copyright custodians for ISO standards.

We will aim for this new profile to be launched in early 2014. This will do more than fill the accessible cyber hygiene gap that industry has identified in the standards landscape; it will be a significant improvement to the standards currently available in the UK. We view the use of an organisational standard for cyber security as the next stage on from the 10 Steps to Cyber Security guidance - enabling businesses, and their clients and partners, to have greater confidence in their own cyber risk management, independently tested where necessary.

The consultation has also highlighted that demand exists in the market for additional cyber security profiles covering areas other than basic cyber hygiene. It is possible that Government could develop additional profiles in the future by working along the same lines with industry partners.

In parallel to developing the cyber hygiene profile, we plan to work with industry to develop an assurance framework to support the profile. Once businesses have 'passed' their audit they would be able to state publicly that they were properly managing their basic cyber risk and they had achieved the Government's preferred standard. Businesses that conform to the standard will be able to use some form of 'badge' when promoting themselves, stating they have achieved a certain level of cyber security.

Industry was very clear in the consultation that there is both a need and a growing demand for a standard such as this. The consultation has significantly raised awareness of cyber security standards in general, particularly with businesses outside of the ICT sector.

The Government's work to stimulate the use of cyber security standards continues. The preferred standard will be applicable to all organisations, of all sizes, and in all sectors. We want to encourage all organisations to use the preferred standard. This will not be limited to companies in the private sector, but will be applicable to universities, charities, public sector organisations, and Government departments. We will be making it as accessible as possible: it will be free to download from .GOV. UK so that all organisations, at the very minimum, can self-certify themselves.

Several businesses including the members of the Defence Cyber Protection Partnership (the DCPP - BAE Systems, BT, EADS Cassidian, CGI, General Dynamics, HP, Lockheed Martin UK, QinetiQ, Raytheon, Rolls Royce, Selex ES, Thales UK) have agreed to use the Government's preferred standard, as the foundation for standards meeting the defence and security sector needs. Other businesses in UK industry including Dell, Nexor, EADS (soon to be Airbus Group), Astrium (soon to be Airbus Defence and Space) have agreed to use the preferred standard in their own business and supply chains.

Additionally, audit firms including Ernst & Young and Grant Thornton, law firms including Linklaters and Allen & Overy, companies such as GlaxoSmithKline, and industry bodies, such as the Institute of Chartered Accountants for England and Wales (ICAEW), the Law Society, the British Bankers' Association (BBA), the Telecommunications Industry Security Advisory Council (TISAC), Universities UK (UUK), techUK, and the Information Assurance Advisory Council (IAAC), have offered their public support to the standard. These public statements of support create momentum in the market which helps our ongoing efforts to find more businesses willing to state that they will adopt the standard. The Government itself will also be using the standard in its own procurement, where relevant and proportionate.

Useful Links:

10 Steps to Cyber Security Guidance:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/73128/12-1120-10-steps-to-cyber-security-executive.pdf

Small Business Cyber Security Guidance:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/197177/bis-13-780-small-business-cyber-security-guidance.pdf

Innovation Vouchers for Cyber Security:

https://vouchers.innovateuk.org/cyber-security

PwC Cyber Security Standards Research November 2013:
https://www.gov.uk/government/publications/uk-cyber-security-standards-research

For further information please contact cybersecurity@bis.gsi.gov.uk.

This publication available from www.gov.uk/bis

Any enquiries regarding this publication should be sent to:

Department for Business, Innovation and Skills
1 Victoria Street
London SW1H 0ET
Tel: 020 7215 5000

If you require this publication in an alternative format, email enquiries@bis.gsi.gov.uk, or call 020 7215 5000.
BIS/13/1308