Prospectus Introducing the National Cyber Security Centre

ICAEW welcomes the opportunity to comment on the *Prospectus Introducing the National Cyber Security Centre* published by National Cyber Security Centre on 25 May 2016, a copy of which is available from this link.

This response of 31 August 2016 has been prepared on behalf of ICAEW by the Information Technology Faculty. Recognised internationally for its thought leadership, the Faculty is responsible for ICAEW policy on issues relating to technology and the digital economy. The Faculty draws on expertise from the accountancy profession, the technology industry and other interested parties to respond to consultations from governments and international bodies.

The Institute of Chartered Accountants in England and Wales
Chartered Accountants' Hall
Moorgate Place
London
EC2R 6EA UK

T +44 (0)20 7920 8100
F +44 (0)20 7920 0547
DX 877 London/City
icaew.com

ICAEW is a world-leading professional accountancy body. We operate under a Royal Charter, working in the public interest. ICAEW's regulation of its members, in particular its responsibilities in respect of auditors, is overseen by the UK Financial Reporting Council. We provide leadership and practical support to over 145,000 member chartered accountants in more than 160 countries, working with governments, regulators and industry in order to ensure that the highest standards are maintained.

ICAEW members operate across a wide range of areas in business, practice and the public sector. They provide financial expertise and guidance based on the highest professional, technical and ethical standards. They are trained to provide clarity and apply rigour, and so help create long-term sustainable economic value.

For more information, please contact representations@icaew.com

icaew.com

MAJOR POINTS

Overall aims

1. We strongly support the unifying aim of the National Cyber Security Centre. There have been a number of government bodies involved in providing cyber security advice and support to date, which has been confusing for users of the services. Having a single structure that brings together elements such as CESG, CISP and CERT should make it easier for businesses to find the right support.

2. The principles identified as a basis for working, such as collaboration, international co-operation and diversity, are all reasonable and appropriate. Further definition of what these mean in practice, though, is needed, as they are currently vague.

3. Partnership is a particularly important element to the approach and we are pleased to offer our help and support to the Centre wherever we can. We worked successfully with the Department for Business, Innovation and Skills and the Cabinet Office during the previous Cyber Security Strategy, inputting the experience of our members into initiatives such as Cyber Essentials, and acting as a communication channel to the business and professional services community. We are keen for this engagement to continue with the new Centre.

4. Accountability is also key to building relationships with the business community. Enabling more effective working between the security and intelligence agencies and the private sector may provide benefits, but care needs to be taken to ensure trust is built and nurtured. Clear responsibilities, appropriate transparency and accountability around actions will underpin trusted relationships and we recommend that the Centre puts significant thought into how this interaction will work in practice.

Scope and priorities

5. It is unclear how much budget and resource will be available to the Centre. While we welcome the fact that the government is investing record sums in cyber security, history shows that the vast majority of money typically goes to the Ministry of Defence and GCHQ, rather than business-support activities. We hope that the Centre will receive substantial enough resources to deliver on its mission to provide useful support to businesses, without undue reliance on large private sector organisations.

6. Regardless of resources, though, it is crucial to provide real clarity on the priorities of the new organisation. Most activities in the Prospectus focus on supporting large businesses within the Critical National Infrastructure sector, and key areas of government. The support to other businesses appears primarily limited to good practice guides and potential membership of the CISP.

7. While this may be appropriate, given limited government resources and the highest risk areas of the economy, the Centre needs to take care not to oversell itself to the private sector more generally. Anecdotal advice suggests some frustration to date with the lack of information and proactive support given to businesses outside of the CNI sector, and therefore clear and realistic expectations need to be set.

8. We also note that everyday support to individuals and other businesses will continue to be through Action Fraud. We hope that this service will be closely linked into the Centre and will receive increased resources to improve its services. Again, we note again frustration with the lack of response from Action Fraud to small businesses who suffer continual attempts at fraud. Few prosecutions appear to flow from reporting these kinds of attacks, reducing confidence in the ability and determination of government to help small businesses here. Therefore the Centre should work with other agencies to ensure that cyber attacks on small businesses are taken

seriously by relevant authorities, and to build confidence in the business community that action is being taken where possible.

Effective support to business

9. The simple provision of good practice guidance is unlikely to lead to significant changes in behaviour in the private sector, especially in small to medium sized businesses. This approach has had little impact in practice to date and the Centre needs to be realistic about how much change this approach will achieve.

10. We suggest that more research is undertaken on small businesses in particular to identify what support would be useful for them and how government can encourage them to improve their practices. Based on our experience with this sector, we recommend focusing on simple messages, sharing case studies to make the risks real to them, and building a network of trusted suppliers. Our roundtable discussion on cyber security in SMEs highlighted many issues related to trust. Small businesses struggle with knowing where to turn when they do have issues, and better credentialing of suppliers for the small end of the market, for example, would be very helpful.

11. We also await the outcome of the Department of Culture, Media and Sport project on regulation and incentives around cyber security, and hope that the outcome of this study will inform the work of the Centre. We note, for example, that the incentives offered by the insurance market are not yet working as intended, and identifying how to improve the provision of services, e.g. through common standards, should be considered.

12. Furthermore, it is surprising to see no mention of Cyber Essentials, given the significant investment and emphasis put on it to date. We strongly support the standard and encourage our members to adopt it, although we recognise that further work is needed to drive adoption, update it and potentially raise the standard. If Cyber Essentials is believed to be a key part of improving cyber hygiene in the private sector, we would expect it to feature strongly in the activities of the Centre.

13. Finally, our forthcoming *Audit Insights Cyber Security* update will focus on the need for cultural transformation and behavioural change. Embedding changes in an organisation's DNA will be far more effective than adopting a tick-box approach. However, the Centre seems heavily focused on technical controls and practices. We would like to see greater emphasis on the people, cultural and organisational elements of cyber security. All of our cyber security materials can be found at icaew.com/cyber