The Institution of **Engineering and Technology**
Michael Faraday House
Six Hills Way, Stevenage
Hertfordshire, SG1 2AY
United Kingdom
T +44 (0) 1438 313311
F +44 (0) 1438 765526
www.theiet.org

Ref: Snnn/ab

Privacy and Security Inquiry
Intelligence and Security Committee of Parliament
35 Great Smith Street
London, SW1P 3BQ.

4th February 2014

Re: Privacy and Security Inquiry

Please find attached the Institution of Engineering and Technology's written evidence in the form requested.

About the IET

The IET is one of the world's leading professional societies for the engineering and technology community, with more than 150,000 members in 127 countries and offices in Europe, North America and Asia-Pacific. The IET provides a global knowledge network to facilitate the exchange of ideas and promote the positive role of science, engineering and technology in the world.

This submission has been approved on behalf of the IET's Board of Trustees, and takes into account the views of IET Members under the guidance of the IET's Information Technology Policy Panel.

The IET is happy to discuss these points with the Ministers or Officials.

Yours sincerely,

Paul Davies
Head of Policy
Tel: 01438 765687 Email: pdavies@theiet.org

Enc.

About the IET

i) Your details:

Name:	Paul Davies
Position:	Head Of Policy
Name of organisation (if applicable):	The Institution of Engineering and Technology
Address:	Policy Dept Michael Faraday House Six Hills Way Stevenage SG1 2AY United Kingdom
Email:	pdavies@theiet.org
Telephone number:	01438 765687

1. The IET is a professional engineering institution and we have therefore strictly limited this evidence to the technical and engineering points that are implicit in your call for evidence, illuminated by the material released by Edward Snowden.

Balancing security and intelligence issues against the wider public good

2. Edward Snowden reveals that the Security and Intelligence Agencies (hereafter SIA's) knew about security vulnerabilities in widely distributed software and that they did not notify these to Computer Emergency Response Teams or otherwise arrange that they would be patched urgently. It has also been claimed that the SIA's or their international partners acted to weaken cryptography that is widely used for private communications including financial transactions.

3. If this is true, then the IET believes that there is a significant risk that these security vulnerabilities would become known to some criminals or overseas SIA's and exploited against the interests of the UK and its citizens or damage the economic and social value of the internet. Unpatched vulnerabilities have a value in criminal markets and are widely searched for; there is also the obvious insider threat of disclosure.

4. The IET does not wish to express an opinion on whether the intelligence benefits outweigh these risks, as this is not a strictly technical matter. We do, however, wish to raise the question of whether the SIAs always take the negative externalities into account appropriately when deciding what security vulnerabilities they will create or leave unpatched, and whether the oversight regime of which the ISC is a part has the remit, breadth of knowledge and technical expertise to ensure that they do so.

5. With hindsight, to some security experts it appears that GCHQ has not always balanced security risks appropriately against other considerations, and consequently there is insufficient public confidence in their attention to this aspect of their remit.

The oversight regime

6. It appears from press reports that the SIAs' programmes revealed by Snowden were not known to Cabinet ministers or discussed in the National Security Council, which (if it is true) implies that some Government Departments that have a legitimate interest in the integrity and security of internet communications were not consulted when the decisions were taken within the SIAs to weaken such integrity and security.

7. The continuing rapid expansion of use of the Internet has made it part of the UK and the world's critical infrastructure. We would ask the ISC to consider whether the SIA oversight regime is adequate to protect such a vital asset and, if not, how it should be improved.

8. The IET would be happy to give oral evidence if that would assist the Committee.

End Of response