Submission 1

SENETAS
trusted to secure critical information

MELBOURNE
Level 1/11 Queens Road
Melbourne VIC 3004
Australia
Phone: +61 3 9868 4555
Fax: +61 3 9821 4899

SYDNEY
Suite 5, Level 13
327 Pitt Street
Sydney NSW 2000
Australia
Phone: +61 2 9283 2333
Fax: +61 2 9283 7558

corporate@senetas.com
www.senetas.com

Mr Andrew McGowan
Secretary
House of Representatives Standing Committee on
Infrastructure and Communications
PO Box 6021, Parliament House,
Canberra ACT 2600.

Re: Invitation to comment on the National Broadband Network

Dear Mr McGowan,

Senetas believes, as the only Australian manufacturer and exporter of high speed network encryption hardware that secures critical local and international data networks, that its expertise developed in this sector over the past 12 years, makes us well-qualified to comment.
The new economic model that is at the heart of the NBN, will deliver economic benefits across indicated areas (a) through (e), however we are most concerned that the network is essentially not secure and this will impact its ability to effectively deliver (f) through (i).

As a high speed, high bandwidth, globally-connected information conduit, the NBN leaves Australia's individuals and businesses open to the growing international threat posed by cybercriminals. Without a properly designed security focus, deployed through dedicated encryption hardware, communications from and to governments, enterprises, small businesses, researchers/innovators and individuals poses a significant risk.

The risk is not only that government information transmitted over fibre optic cable is not secured – and I remind the Committee that the ICON dark fibre network in Canberra remains unencrypted – but organisations looking to take advantage of the new opportunities the NBN will present must accept the risk their IP (Intellectual Property) will be transmitted over the fibre optic NBN "in the clear" and therefore at risk of data interception.

We recognise that information security is analogous to insurance – many people do not think about it until there has been a breach. But should there be a breach of the NBN, it will result in massive data loss. Assuming the average size of a data packet is 6 Kb per personal record, an accidental leak or a deliberate act such as a fibre optic tap on NBN traffic travelling at 10 Gigabits per second could result in the loss of 1.04 million unencrypted records every five seconds, 12 million records a minute, or one billion pieces of information in 90 minutes.

I do not need to remind the committee that the massive Wikileaks data-breach apparently involved only one CD (740 Mb) to steal hundreds of thousands of classified documents.

The Federal Government should not allow the NBN to effectively become an uninsured vehicle on the global superhighway. Data travelling over the NBN should be risk-managed through mandatory information security and compulsory reporting of data breaches - whether government information, business or financial reports, intellectual property or personally identifiable information, such as health records.

Likewise data at rest in storage area networks, backup and disaster recovery sites associated with the NBN should also be secured through globally certified high speed encryption solutions.

We remain ready to give evidence or provide further technical information to the Standing Committee, either in Melbourne or Canberra.
We appreciate the opportunity to comment and look forward to your response.

Sincerely,

John H DuBois
Chief Executive Officer