Submission No 2**37**

Inquiry into potential reforms of National Security Legislation

Organisation: Senetas Corporation

30 November 2011

Registered Office

Level 1/11 Queens Road
Melbourne VIC 3004
Australia

Phone +61 3 9868 4555
Fax: +61 3 9521 4899

corporate@senetas.com
www.senetas.com

The Chair, Joint Intelligence & Security Committee
The Hon. Anthony Byrne MP
Parliament House
Canberra ACT 2600

Dear Anthony,

Please find below Senetas Corporation Limited's Parliamentary Joint Committee on Intelligence and Security Committee submission.

CONSIDERATION – PROTECTING THE NATION'S DATA THROUGH DATA ENCRYPTION

The Parliamentary Joint Committee on Intelligence and Security (PJCIS) is considering a package of national security ideas comprising proposals for telecommunications interception reform and Australia intelligence community legislation reform as released in the "Equipping Australia against emerging and evolving threats" discussion paper.

One of the proposed reforms relates to the collection and retention of communications associated data. Should the telecommunications sector be required to collect and retain data based on new legislation, a critical question arises.

"How is this data protected from unauthorised access, modification and misuse, whether intentionally or inadvertently?"

This is a global concern faced by governments worldwide and is causing a rethink in the approach to data security as evidenced below.

> *"As cybercriminals have become more skillful and sophisticated, they have eroded the effectiveness of our traditional perimeter-based security controls. The constantly mutating threat landscape requires new defensive measures, one of which is the pervasive use of data encryption technologies. In the future, you will encrypt data — both in motion and at rest — by default. This data-centric approach to security is a much more effective way to keep up with determined cybercriminals. By encrypting, and thereby devaluing, your sensitive data, you can make cybercriminals bypass your networks and look for less robustly protected targets. Encryption will become a strategic cornerstone for security and risk (S&R) executives responsible for their organization's data security and privacy efforts."*
>
> *FORRESTER RESEARCH INC, JULY 2012*[1]

In addition to the technical considerations it is recommended that the government mandate how collected and retained data is secured – both in motion (when moving between locations) and at rest (when stored) through certified encryption technology and a regime for data breach notification to ensure the interest of all stakeholders is aligned.

[1] Kill Your Data To Protect It From Cybercriminals, 12 July 2012 – by John Kindervag, Forrester Research Inc

Duty of care
If legislation requires personally identifiable data to be captured and retained it represents a security and privacy issue for every Australian - In essence this process captures and retains the nation's data. It is therefore incumbent on the custodians to take every step to ensure important data is protected and the privacy of its citizens upheld.

Risk-based approach
Carriers and carriage service providers (C/CSPs) will be high value targets for criminal organisations, terrorists and state based espionage. Despite every protection effort, it must be assumed that this data will be lost, stolen and/or compromised. The consequence of that data loss is so great that the highest levels of security must be employed to protect it. Part of that optimal security solution is through the use of certified encryption technology.

The levels of security
Because the C/CSPs are responsible for the collection and retention of data it follows that they are obliged to take reasonable steps to protect it whilst it is under their control. Additionally parties seeking access to the retained data have the same responsibilities.

Ideally the legislation to protect this data will provide clear guidance as to how that data will be secured. This will address both the securing of that data while in motion and at rest.

Conclusion
This data collected and retained and the substantial nature and volume of it make it valuable. Therefore it is at extremely high risk of attack by cybercriminals. If legislation is enacted it is imperative that mandatory compliance standards of encrypting data be set by government to protect the data.

Senetas Corporation Limited's (Senetas) submission is that a critical issue is the protection of that data from theft, misuse and interference by certified encryption, therefore we recommend:

1. Mandatory certified encryption of the data – both in motion and at rest
2. Mandatory data breach regime

The certified encryption of the data ensures that any data accessed is of no value to cybercriminals.

Yours Sincerely,

Andrew Wilson CEO
About Senetas
Senetas Corporation Limited (ASX Code: SEN) is an Australian ASX-listed public company and is the world's leading developer and supplier of high speed network encryption hardware products.
Senetas encryption technology has been independently tested and accredited by the world's leading agencies and now offers the only certified encryption hardware - certified to FIPS 140-2 Level 3 (US), Common Criteria EAL4+ (AUS) and CESG CAPS Baseline certification (UK). Senetas is now represented in more than 40 countries. Customers include Government, military, law enforcement agencies plus leading financial and banking institutions in Australia, USA, Middle East, Asia, and the EU.