ABN 33 006 067 607

SENETAS CORPORATION LIMITED

312 Kings Way, South Melbourne, VIC 3205, Australia

T +61 (03) 9868 4555 F +61 (03) 9821 4899 E info@senetas.com

www.senetas.com

26/02/2024

**To Whom It May Concern,**

**Re: Submission to the Australian Cyber Security Strategy 2023-2030**

## Introduction

We fully support the government's aims set out for the 2023-2030 Australian Cyber Security Strategy.

Specifically, we:

- Welcome and strongly support the consideration being given to legislating a Cybersecurity Act. We see this as an urgent priority that would set the foundations for a successful national cybersecurity strategy.
- Support the initiatives for a more secure national infrastructure sector through regulatory alignment/s, and the "…possibility of a new Cybersecurity Act and developments to the Security of Critical Infrastructure Act.".

The strategy's aim of "enhancing and harmonizing regulatory frameworks" has become urgent as Australian (government, commercial and industrial) organisations have rapidly become increasing targets for both state-sponsored and other cyber-criminal attacks. The planned legislative and regulatory alignment initiatives, including a holistic national Cybersecurity Act, will highlight to our international trade partners, Australians and business sectors within the Australian economy the importance and seriousness of cybersecurity.

Robust national cybersecurity governance will send a clear message that Australia is no longer a vulnerable target, similar to the effectiveness of Europe's implementation of the General Data Protection Regulation (GDPR) since 2018.

### Submission Purpose

Senetas' submission addresses the cybersecurity strategy's planned legislative and regulatory actions. Our purpose is to contribute our 25-year international cybersecurity expertise - working with government and defence force agencies; major commercial, industrial, critical infrastructure, data centre, telecommunications, and cloud organisations.

As a recognised leader in cybersecurity solutions, we appreciate the opportunity to contribute input to the Australian Government's 2023-2030 Cyber Security Strategy. Our international expertise in developing high assurance encryption and anti-malware cybersecurity technologies, meeting the highest security standards of government, defence, commercial, cloud and industrial customers positions us well to contribute to this critical dialogue.

Our submission reflects our cybersecurity expertise in:

- more than 50 countries (Americas, Europe, Middle East, and Asia Pacific regions).
- enterprise and government vertical sectors.
- the legislative and regulatory frameworks under which our customers are governed.
- international data security certification standards and requirements.
- the security threats faced by enterprises and government agencies.

### Credentials

Senetas is an Australian listed public company (ASX:SEN) specialising in cybersecurity hardware and software solutions for more than 25 years. These solutions are used across most government, commercial/industrial and IT/telecommunications service provider verticals around the world.

We develop and manufacture in Australia the leading multi-certified and quantum-resistant network encryption security products (CypherNET) for: public and private data networks; communications to/within/from the cloud; operational networks and control systems for critical infrastructure and in-field communications (e.g. land, sea and air defence forces and civil applications).

Senetas was the first cybersecurity manufacturer to implement quantum-resistant encryption security for high-speed data networks.

Our network encryption products hold the leading international cybersecurity certifications: FIPS (142 Level 3), Common Criteria (EAL4+ international and Europe), NATO (Green Restricted) and ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information - France).

Additionally, our secure cloud file sharing and storage solution, SureDrop, enables encryption security for workgroup collaboration and file sharing. It is the only of its type providing 100% data location and sovereignty control.

Senetas's subsidiary, Votiro, provides patented anti malware/ransomware protection against known, unknown and zero-day exploit file born cyberattacks. Votiro Zero Trust's advanced CDR technology is not malware signature dependent to identify and eliminate malicious content.

## Senetas Submission

We support and address the following key elements of the proposed legislation and national infrastructure regulation actions planned:

A National Cybersecurity Act mandating:

- Consolidation of various privacy and corporate responsibilities legislation and regulations into a single comprehensive Cybersecurity Act
- 'Data protection' beyond (mandated) requirements to 'prevent successful cyber-attacks' – thus mandating encryption of sensitive data (government and commercial as defined) throughout its lifecycle
- Proper and secure use and storage of data
- Whole of data lifecycle security responsibilities – when at rest (stored), in use and in motion across networks and in use
- Government agencies' and (selected) commercial sector businesses' migration to 'quantum-safe' cybersecurity (e.g. critical infrastructure, intellectual property, citizen identity, other valuable sovereign data).

Direct alignment of the secure national infrastructure regulatory framework with the Cybersecurity Act (such as above).

## Australian Cybersecurity Act

As new technologies continue to evolve, such as AI and quantum-computing, a national Cybersecurity Act should focus business and government organisations on preparedness as well as responsibility requirements.

Organisations must actively reduce the cyber-risks threatening IT/OT (Information Technology/Operational Technologies), cloud, Internet and data/voice/video network infrastructures and maintain the secure privacy of their data and their critical activities. Privacy requirements should not be limited to individual citizens' data. Commercial data, whether business secrets, financial or business identity, should be afforded the same confidentiality.

## Legislative and Regulatory Consolidation and Clarity

Currently, laws governing cybersecurity – data privacy, use, retention and responsibilities - may be found in a variety of federal Acts, such as in the Corporations Act, Privacy Act, telecommunications Act, and Security of Critical Infrastructure Act… This legislative situation needs urgent consolidation into a single national Cybersecurity Act, necessary to ensure:

- A single holistic legislative framework providing consistency, unambiguity, and easier administration
- One Act dealing with all aspects of cybersecurity EG:
    - Responsibilities - cyber defences, data protection, data use, data retention, data breaches, data classifications
    - Specific vertical requirements/regulations
    - Security standards required – cyber-strategy, IT systems and infrastructure, and data security (throughout the data life cycle)
    - Specific data protection classification standards based on the type of data being protected – e.g. FIPS or Common Criteria and levels of certification.

Significantly, cybersecurity legislative clarity is crucial to optimal compliance and effective regulatory administration. European research into GDPR's cybersecurity impact (cyber-threats and data breaches) highlights concerns GDPR's benefits have been limited by areas of unclear complexities. Non-compliant organisations point to a lack of technical clarity.

## Prevention and Protection Cybersecurity Requirements

Experience with many of the most secure government and commercial organisations highlights the need for cybersecurity legislation/regulation to differentiate two critical cybersecurity elements:

1. *Prevention* – of cyberattacks wherever, whenever, and however they occur. Prevention technologies (e.g. anti-malware, firewalls, digital identity security) aim to resist the most persistent and malicious attacks through all attack vectors

2. *Protection* – of data itself (e.g. citizen identities, intellectual property, financial transactions…) and systems (e.g. critical infrastructure control systems) that cybercriminals seek to steal, harm, or eavesdrop. Protection technologies are encryption – of data: at rest; in use; and in motion across networks.

Prevention technologies are the front line of cyber defences. Data *protection* is encryption. Protection is referred to as "the last line of defence". The distinction is crucial. In the former case, technologies push to keep pace with cybercriminals' attack technologies and new threats. Like other forms of crimes, preventing cybercrime is largely a matter of catch-up.

Therefore, effective cybersecurity strategies must include protection technologies – encryption. Only when strong encryption is used will data remain safe in the hands of criminals. Data – at rest (stored), in use and in motion across networks - must be encrypted to be secure in the event of a successful cyberattack.

## Encryption for Data Protection

Data protection should apply throughout data's life-cycle – when at rest (stored), in use and in motion across data networks. At each stage data is a risk of a cybersecurity attack and a successful data breach. Of course, not all data is the same, nor does all data require encryption security. We are not suggesting all data be encrypted at all times in its life cycle.

However, A Cybersecurity Act should require organisations to identify and classify their data assets – from not sensitive to sensitive and even highly sensitive. Government agencies adopt such risk assessment practices – so too should businesses. At some level of sensitivity/confidentiality data should require encryption security.

Under Europe's GDPR, organisations successfully attacked that have encrypted data are exempt from mandatory breach notifications and any consequential penalties. Cybersecurity professionals generally

consider Europe's GDPR as the current legislative 'gold standard' since it was proclaimed in 2018 and has seen amendments since.

Significantly, successful major Australian cyberattacks have too often involved unencrypted sensitive data. It's not good enough to claim: "malicious and sophisticated cyberattacks", "our defences failed" and "we took reasonable steps" when unencrypted legal, medical, intellectual property, citizen identity or financial data is stolen or held to ransom.

Therefore, we recommend a federal Australian Cybersecurity Act address:

Cybersecurity Act

Data is an asset – data is among the highest intangible assets possessed by organisations. A national Act would seek to protect such an asset from:

- Access and misuse by cyber-criminals and other unauthorised parties
- Misuse in the hands of organisations holding data on behalf of third parties – consumers, employees, supply chain members and customers

The importance of 'data protection' and difference to 'cyber-attack prevention'

- Responsibilities beyond simple "reasonable prevention steps" (defending IT and communications systems)
- Responsibilities to protect data in the event of successful cyberattacks (data breaches) and data theft (encryption)
- Responsibilities to protect sensitive (as defined) data throughout its lifecycle)
- Security responsibilities for data transmitted across international borders

Data definitions/classifications

"Sensitive data" definition (government and commercial - shelf life, value, citizen information…)

Data sovereignty – types of data requiring location control on sovereign Australian soil

Government sector application of the Act – Federal, State, Local

Future threats – preparedness requirements – e.g. for quantum computing

Data usage – rules requiring:

- Removal of customer proof of identity data obtained at the time of becoming customers - within a period after the identity data has been used for the purpose for which it was given.
- Use, retention and possession of data provisions - deletion of individual and company contact data used in marketing after a period of non-engagement (e.g. 18 months as required under GDPR) however obtained.

Lessons learned – need to reflect legislative achievements in other jurisdictions:

- Europe – General Data Protection Regulation 2018 and as amended (GDPR):
    - Strong statistical improvement in successful cyber-attacks and reduction in breaches of unencrypted data
    - Significant improvement in 'cross-border' cybersecurity compliance
    - Weaknesses identified e.g. clarity/complexities impacting compliance and administration of the Act.
- USA:
    - Significant improvement in government agencies' 'quantum-threat readiness' since legislated
    - General statistical decline in successful breaches of unencrypted data and the strongest cybersecurity performance since the Cybersecurity and Infrastructure Security Agency Act of 2018 was proclaimed and establishment of the Cybersecurity and Infrastructure Security Agency under the Department of Homeland Security.

Infrastructure

- Data, communications, and control systems protection through the use of 'authenticated network encryption'. Prevention of Denial-of-Service and similar 'hacking attacks' on data networks (including those used for operational and command/control systems) used to manage critical infrastructure may be prevented by the encryption of those links.
- Classification of critical verticals within the Australian economy (primary, secondary and tertiary sectors).

## Conclusion - Core principles of data protection

### Securing the Economy and Cyber Ecosystem

Senetas' advanced encryption solutions play a pivotal role in securing the digital ecosystem. Our commitment to innovation ensures that Australian businesses and government entities have access to state-of-the-art security technologies, crucial for protecting sensitive data and maintaining economic stability.

### Resilient Critical Infrastructure

We recognize the emphasis on protecting Australia's critical infrastructure from cyber threats. Senetas' encryption products are designed to safeguard critical data transmitted across networks, thus ensuring the operational continuity of vital services like defence, energy, transport, and healthcare.

### Sovereign Capability in Cybersecurity

Senetas is dedicated to enhancing Australia's sovereign capabilities in cybersecurity. Our research and development efforts are focused on creating resilient technologies that can withstand emerging cyber threats, thereby contributing to national security.

### Policy and Legislative Frameworks

We welcome the initiative to develop a Cybersecurity Act. Such legislation will simplify legal requirements for businesses and government agencies alike thus better meeting their respective regulatory compliance requirements. Further, we support the proposed developments in the SOCI Act.

### International Strategy and Government Systems

As an Australian company with global reach, Senetas is well-placed to contribute to the country's cyber leadership on the international stage. Additionally, we advocate for a robust framework to secure business and government systems, leveraging our expertise in high-assurance encryption.

Addressing Specific Challenges and Threats Our solutions are specifically designed to address the unique challenges faced by critical infrastructure sectors. We emphasize the need for heightened security in data protection through data encryption and network encryption technologies for secure IT/OT operating environments, areas increasingly targeted by cyber adversaries.

### Public-Private Collaboration

Senetas strongly believes in the value of collaboration between the public and private sectors. We are keen to engage in information sharing initiatives and contribute to the formulation of effective cyber threat response strategies.

### Engagement in Policy Development:

Senetas is willing to participate in further policy development forums and welcome the opportunity to share our experiences.

Senetas Corporation Limited is committed to supporting the Australian Government in elevating the nation's cybersecurity posture. We look forward to ongoing engagement and collaboration, offering our expertise to help shape a resilient and secure digital future for Australia.

Sincerely,

Simon P Galbally, CMO

And on behalf of Andrew R Wilson, CEO.