Submission to Australian Cyber Security Strategy Discussion Paper

Enea AB

Date: **April 14, 2023**

Australian Cyber Security Expert Advisory Board

Australian Ministry for Home Affairs

Via: https://www.homeaffairs.gov.au

April 14th, 2023

Dear chairperson and members of the Expert Advisory Board,

Enea AB commends the Australian Government and Minister for Cyber Security, the Hon. Clare O'Neil MP for an inclusive and comprehensive approach to the development of 2023-2030 Australian Cyber Security Strategy.

As an acknowledged world leader in software for telecoms and cybersecurity, we appreciate the opportunity to contribute our international perspectives on the security of mobile networks and mobile communications.

Enea is frequently called on to share insights and expertise with governments, regulators and at industry events, and we are pleased to make our team available for follow up briefings or clarifications at the pleasure of the Expert Advisory Board.

Sincerely,

Joseph Habib, Regional Director Sales APAC, Enea

[redacted]

Rowland Corr, VP Government Relations, Enea

[redacted]

CORPORATE HEADQUARTERS
P.O. Box 1033
Jan Stenbecks Torg 17
SE-164 21 Kista
Sweden
Phone: +46 8 507 140 00

www.enea.com

Table of Contents

1. About Enea AB

Enea is a world-leading specialist in software for telecom and cybersecurity. The company's cloud-native solutions connect, optimize, and secure services for mobile subscribers, enterprises, and the Internet of Things. More than 100 communication service providers and 4.5 billion people rely on Enea technologies every day. Enea has strengthened its product portfolio and global market position by integrating a number of acquisitions, including Qosmos, Openwave Mobility, Aptilo Networks, and AdaptiveMobile Security. Enea is headquartered in Stockholm, Sweden, and is listed on Nasdaq Stockholm.

Enea's software portfolio includes:

• Signalling, messaging and voice protection trusted by the world's largest Mobile Network Operators and CPaaS providers to secure communications infrastructure and services. The portfolio includes signalling, messaging, and voice managed firewalls, A2P (application to person) revenue protection and commercial traffic management solutions, as well as signalling & messaging intelligence services.

• 5G Data Management solutions to unify subscriber and session data across network functions, and policy and access control products for efficient utilization of network resources and authentication of subscribers. The portfolio includes the Enea Stratum Cloud Data Manager, the Enea Unified Data Manager, the Enea Policy Manager, and the Enea Access Manager.

• Traffic Management – Enea mobile video traffic management solutions alleviate radio network congestion, accelerate video delivery, reduce network energy consumption, and improve subscribers' quality of experience. The portfolio supports 5G and includes the Enea Encrypted Video Manager, the Enea RAN Congestion Manager, and the Enea TCP Accelerator.

• Enea's embedded traffic intelligence products classify traffic in real-time and provide granular information about network activities. The portfolio includes the Enea Qosmos ixEngine and the Enea Qosmos Probe. The products support a wide range of protocols and are delivered as software development kits or standalone network sensors to network equipment manufacturers, telecom suppliers, and vendors of cybersecurity software.

Enea's industry leadership in mobile network security

Enea is an active member of the GSMA Fraud and Security Working Group, and key contributor to development of industry standards including the GSMA Fraud and Security Group's (FASG's) FS.36 "5G Interconnect Security" reference document for GSMA members, as well as FASG's FS.11 "SS7 Interconnect Security Monitoring and Firewall Guidelines".

In March 2023, Enea was invited to present to the European parliamentary enquiry into Pegasus Spyware. The representation by VP Government Relations Rowland Corr can be viewed here https://multimedia.europarl.europa.eu/en/webstreaming/committee-of-inquiry-to-investigate-use-of-pegasus-and-equivalent-surveillance-spyware_20230316-0900-COMMITTEE-PEGA

Recent white papers and research publications include:

https://info.adaptivemobile.com/defending-telecoms-against-nation-state-cyber-threats

https://info.adaptivemobile.com/mobile-network-enabled-attacks-in-hybrid-warfare

Further reports and insights can be found on www.enea.com and www.adaptivemobile.com

2. Introduction : Enea's response to the Discussion Paper

Enea submits the following recommendations in respect of mobile telecommunications signalling security for consideration by the Expert Advisory Board and Panels. The submission outlines how the integration of mobile network signalling protection into the Strategy might offer a means to further: harmonize regulatory frameworks, provide a sovereign capability to counter threats, and demonstrate international leadership based on assured resilience.

While achieving resilience is not about reducing cyber risk to zero as the Minister for Cyber Security has made clear[1], the priority is to address security gaps in frameworks and capabilities to identify and mitigate risks, and to ensure trust in the security of personal data and critical infrastructure. As stated in the Discussion Paper:

"[t]he transition to a digital economy relies on the ability to trust that our personal data, infrastructure, and underpinning systems are secure, even as the cyber threat landscape evolves."

The foundation for this trust cannot be confined to conventional cybersecurity frameworks focused on computer-based systems and IT environments, since the threat to data privacy and digital sovereignty already extends beyond these contexts.

Access to mobile signalling systems is abused by threat actors to remotely exfiltrate personal information in the form of unique identifiers for subscribers and other exploitable information. The signalling threat landscape is dynamic in nature and global in scope. All too often it is also an unreported and, worse, an uncontested landscape as threat actors exploit access to signalling resources to manipulate network operations in international targeting activities. Australia's Cyber Security Strategy 2020[2] highlights the possibility for individuals to play their part in reducing their personal risk. When it comes to signalling-enabled threats however, individuals are powerless to mitigate their personal risk as attacks occur at the network level.

Mobile subscribers take for granted that phones can seamlessly switch between 3G, 4G and 5G, however a downside of this layered approach is that some legacy vulnerabilities persist. A signalling system (SS7) deployed since the 70's for legacy networks, is notoriously open to abuse and remains in operation and targeted by newer surveillance tools. Other signalling protocols too such as Diameter and GTP are also at risk. Indeed, advanced attackers have the ability to conduct cross-protocol attacks. While 5G networks are designed to be more secure across network interfaces and with user identity management, the upcoming ubiquity of 5G means the attack surface has drastically spread. Malicious inbound signalling could penetrate the core or "brain" of networks, leading to user meta-data theft, call rerouting, or even hijacking location tracking services.

The global nature of the attack surface is owed to the fact that signalling infrastructures enable, support, and control interconnection between networks nationally and internationally, primarily governed by commercial agreements where security has not been a primary focus.

---

[1] https://clareoneil.com/media-centre/speeches/australian-information-security-association-s-aisa-australian-cyber-conference-2023/

[2] https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy/australias-cyber-security-strategy-2020

This was the natural result of deregulation and opening of the telecom markets wherein the ability for operators to open their networks and to partner with multiple service providers served as an important business enabler for operators, and service enabler for consumers. The exploitation of this openness, and an absence of protective measures to mitigate the technical vulnerabilities to attack have made the interconnect environment perilous, particularly for countries at significant risk of hostile targeting efforts by external state-level threat actors.

Examples of currently known attack scenarios include:

Network Reconnaissance

Scanning and probing of networks to gather information (including network element and personal information in the form of unique identifiers) which can be used to conduct subsequent attacks, including focused surveillance operations.

Location Acquisition and Tracking Attacks

Targeting subscribers or connected devices / equipment (e.g. vehicles, or cargo).

Interception and Diversion of Communications

Interception of calls or messages including One Time Passcodes (OTPs), and other data.

Harvesting of Credentials

Subscriber Authentication Vectors/Keys, for example, can be obtained.

Fraud

Modification of subscriber or network data causing revenue loss to networks.

Denial of Service (DoS)

Network or subscriber data modified to remove access to services.

Enabling/supporting the delivery of malware:

Signalling vectors can be used in phased attacks which culminate in the deployment of malware to subscribers' devices (e.g. delivery of a message containing malicious links).

Other combined attacks:

Signalling capabilities can be used in combination with other forms of attack over telecoms networks. For example, we have detected the combined use of 'IMSI Catcher'[3] tools and signalling attacks.

Advanced attackers have the ability to combine or switch between signalling protocols taking advantage of the fact that different signalling protocol sets require their own particular protection, and operators often lack protection across multiple signalling interfaces.

3. Enhancing and harmonising regulatory frameworks

An assured capability to detect and respond to state-level signalling attacks must recognise the vital interconnection between networks nationally and internationally, as well as the

[3] https://blog.adaptivemobile.com/adaptive-mobile-imsi-catchers

requisite interworking between protocols and across generations of mobile telecommunications technology which underpins the continuous, seamless connectivity that so much societal and economic activity relies upon today.

The mobile interconnect environment comprises a global threat landscape that has historically remained beyond the scope of national cybersecurity frameworks, and beyond the visibility of many mobile network operators whose security obligations have traditionally focused on service availability.

As the Discussion Paper highlights, data breaches impact both companies and their end customers who face continued risk with their personal information potentially in the hands of nefarious actors. Indeed, where customers' mobile numbers and identities are exfiltrated in such breaches, such information can be sufficient to enable targeting by threat actors equipped with signalling attack capabilities.

Placing primary emphasis on protection of privacy is vital to ensure that the new Strategy proves "adaptable to account for changes in the strategic and technological environment in the coming years".

In addition to the kind of data breaches highlighted by the Discussion Paper, mobile subscribers are exposed to the privacy risk of data leaks which can be deliberately induced from networks by attackers. Exploiting access to signalling systems, threat actors targeting inadequately protected networks can exfiltrate information pertaining to subscribers and the network equipment serving them on an ongoing basis with impunity. While such breaches are typically much smaller in scale in any single instance than the likes of the Optus breach, signalling attacks can impact multiple thousands of subscribers in a single instance, and in the case of global network reconnaissance, potentially tens or hundreds of thousands of subscribers at a time.

Moreover, mobile network security and users' data privacy can be compromised by attackers without causing a service disruption. Indeed, the core value of weaponising signalling is in being able to execute real-time surveillance and targeting of individuals and networks.

4. Measurement and reporting

If the new Strategy is to look beyond operational disruptions, as the Discussion Paper suggests it might, the new frameworks it supports must move beyond outage-focused metrics when assessing impact. This would not only be an innovative expansion of scope, it would arguably represent a natural evolution of existing frameworks, particularly where confidentiality and integrity of information are already acknowledged as areas of relevant and significant impact.

Signalling attacks encompass fundamental elements of phased malicious activity by threat actors as recognised in existing frameworks such as the Security of Critical Infrastructure Act (SOCI) 2018[4], including:

- The conduct of reconnaissance or network scanning activity;
- Exploitation of unauthorised access;
- Undertaking of subsequent malicious actions including further theft of data and altering how systems operate.

[4] CISC Factsheet - Cyber Security Incident Reporting

Despite this fundamental consistency in the nature of the threat presented, the narrow focus of current cybersecurity incident reporting on computer data, systems, programs and communications has the effect of excluding the telecoms network attack surface presented by signalling infrastructure and systems.

The combination of the nature of non-disruptive intrusions (which elicit no complaints, for example, from customers oblivious to its occurrence) and non-requirement for reporting results in operators having little to no external incentive to resource signalling protection.

Incident reporting requirements therefore effectively determine and at the same time delimit the development by operators of threat detection capabilities. Accordingly, this is precisely where regulatory harmonisation and enhancement might be achieved. To begin with, this might require that signalling systems are included in the Register of Critical Infrastructure Assets.

The criteria for incident reporting should not be overly weighted towards quantitative metrics such as an arbitrary absolute number of subscribers impacted by a single breach. Rather, the relative severity of any single incident might reflect the level of certainty for example that the intrusion constitutes deliberate state-level targeting (i.e. surveillance) of the individual(s) involved, not least because a single case of targeting could present a potential national security threat.

Consideration should be given to the inclusion of signalling infrastructure among designated systems of national significance due to the potential risk to national security posed by the manipulation of such assets by threat actors. This may require adapted provisions in respect of the application of hazards to telecoms assets.

Consideration might also be given to adapting the application of terms such as cybersecurity incident, relevant impact, and significant impact to account for the nature of the interconnect environment in which the long-term compromise of network security involves repeated intrusions by attackers exposing data to cumulative exfiltration over time. Such an approach could address the potential national security impact posed by such intrusions over time.

An enhanced regulatory framework could also reflect the need to ensure sufficient resourcing of protective monitoring of the signalling interconnect environment. This is essential to enable a meaningfully comprehensive evaluation of resilience to unauthorised intrusions and other anomalous network behaviour resulting in (or risking) data leakage, and to support the ongoing monitoring of risk over time. Towards this end, the potential relevance of interdependencies between critical assets within Australia and operators' infrastructure located in the surrounding region might also be considered.

This would enable response to possible regulatory provision enabling, for example:

- Reporting by providers/operators to the relevant national competent authority of unauthorised intrusions (these to be defined, for example, in amendment to SOCI Act).
- Compliance by network operators (or other service providers controlling the relevant telecoms signalling assets) with requests for information from national competent authorities pursuant to the relevant framework (e.g., national security investigation).

Incorporating mobile signalling security is thus consistent with the Discussion Paper's call for greater recognition in legal frameworks that data collection efforts by attackers are widespread, and that "[t]he Strategy must reflect the importance of protecting customer data". This provides the basis for an assured and sovereign capability to underpin Australia's cyber resilience against unauthorised mobile network intrusions into the foreseeable future.

5. Moving from acute uncertainty to assured capability.

Mitigation of an evolving cross-domain threat calls for evolved cross-domain cooperation between key stakeholders, public and private, beyond the scope of conventional cybersecurity.

Sufficiently resourced and strategically leveraged signalling security can offer national-level threat detection and defence which might be readily integrated into a unified approach that "move[s] cyber security beyond a niche technical field to a strategic national security capability". The integration of signalling threat detection and defence measures could support a capability to recognise and respond to possible hostile targeting activities of state-level adversaries that might otherwise represent a strategic blind spot in Australian cybersecurity.

This would require transformative partnerships as envisaged and called for in the Discussion Paper. New partnerships in multiple contexts between mobile network operators and telecoms regulators, cybersecurity authorities, law enforcement agencies, and national intelligence services are imperative.

The potential benefits would otherwise be lost, for example, even were operators to deploy advanced signalling firewalls in their networks, if such deployments and the security insights they generate remained ultimately siloed within each operator environment.

Signalling firewall deployments must be adequately resourced to ensure that sufficient security insight can be generated. The ability to do so will be dependent upon the level of protection implemented, and upon the level of analysis (threat detection) supported by the software in use. A potentially useful proxy measure for determining the level of capability of operators in this regard could be the level of GSMA recommendations on interconnect security implemented across operators. At a very high level, this might be used to determine, for example:

- What levels of filtering (based on GSMA Categories 1 – 3) are present;
- Which signalling protocols are / are not covered;
- Whether cross-protocol correlation is possible;
- Whether protection is passive or active (i.e. enabling blocking of malicious traffic);
- What direction (e.g. bi-directional or inbound only) of traffic is covered.

GSMA recommendations may also serve as a benchmark to guide improvement and to measure progress into the future. At the same time, through new cooperative arrangements, key security insights might be made available to the relevant government stakeholders as appropriate for investigation, assessment, and response.

Resourcing the requisite threat detection and defensive capabilities in this regard may rely on burden sharing between stakeholders. This would be consistent with recognition expressed in the Discussion Paper that lifting and sustaining cyber resilience will require an "integrated whole-of-nation endeavour" in the form of concerted efforts across public and private sectors.

Such partnerships would provide a foundation for an assured collective capability based on the production and provision of signalling threat intelligence without prejudice to privacy of subscribers.

6. International leadership in cybersecurity and critical infrastructure protection.

As the Discussion Paper highlights, we live in a cyber environment that is increasingly contested by threat actors. At the same time, it is also one of increasingly convergent attack surfaces created by the growing digital connectivity at the centre of Australians' lives.

The importance of having a national capability encompassing conventional cybersecurity and mobile signalling together in a 'whole of nation' defensive endeavour is nowhere better demonstrated than by Ukraine's defence against the ongoing invasion by Russia.

Clear recognition of the effects of mobile signalling attacks is referenced[5] in articles quoting Natalia Tkachuk, Head of Ukraine's Information Security and Cybersecurity Service, describing attempts by Russian forces to use captured telecoms infrastructure to execute attacks over SS7 signalling.

Ukraine's defenders have demonstrated to the world the importance of securing control of telecoms infrastructure in order to prevent it being weaponised by adversaries.

The incorporation of signalling protection into the Strategy not only supports Australia's objective of becoming the world's most cyber secure country by 2030, it presents an opportunity for Australia to become a leader in the leveraging of signalling protection as part of a strategic national cyber security capability.

This is because the gaps in cybersecurity and critical infrastructure protection frameworks highlighted in this submission tend to be the rule rather than the exception among national frameworks. In recent times, the potential extent of the risk attached to such attacks has been reflected in media reporting[6] indicating that signalling capabilities form part of the cyber arsenal of a company allegedly engaged in worldwide election interference and disinformation campaigns as a service.

Mobile signalling threat intelligence can enhance counterintelligence capabilities to support Australia's National Intelligence Community. Dedicated protective measures for at-risk persons is also possible with the right integration between operators and national competent authorities. It merits highlighting here that signalling protection and intelligence provision may be implemented without adversely affecting individuals' privacy and the confidentiality of their communications.

Such a capability would help to further the objective identified in the Cyber Security Strategy 2020 of strengthening the capacity of the Australian government to prevent and respond to malicious cyber activity of sophisticated threat actors through a "classified national situational awareness capability to better enable government to understand and respond to cyber threats to critical infrastructure".

As a strategic capability, signalling threat detection and defence might complement classified national situational awareness and at the same time enable proactive protection through:

- Real-time detection of remote intrusions targeting subscribers;
- Adaptive defence against advanced attacks aimed at bypassing protection;

[5] From the front lines of 'the first real cyberwar' (therecord.media)
[6] Revealed: the hacking and disinformation team meddling in elections | Technology | The Guardian

- Victim identification and incident response;
- Evaluation of level of resilience nationally and regionally to intrusions;
- Identification of specific network vulnerabilities over time;
- Tracking of trends in threat levels and types of attack over time;
- Knowledge of innovation and adaptation of attackers' techniques;
- Tracking of changes in attack group composition (infrastructure used) over time;
- Detection of globally significant attacks such as mass network reconnaissance.

Australia's development of a new Cyber Security Strategy presents an opportunity to "lead on safety and security while respecting basic rights" by turning digital connectivity into a tool for assurance and true national security capability without prejudice to the privacy and confidentiality of individuals' digital communications.

The strategic integration of signalling capabilities can thus provide a crucial pillar of assurance for the security of personal data and critical infrastructure upon which the trust of people and international partners alike can be strengthened.

ENDS.

About Enea

Enea is a world-leading specialist in software for telecom and cybersecurity. The company's cloud-native solutions connect, optimize, and secure services for mobile subscribers, enterprises, and the Internet of Things. More than 100 communication service providers and 4.5 billion people rely on Enea technologies every day. Enea has strengthened its product portfolio and global market position by integrating a number of acquisitions, including Qosmos, Openwave Mobility, Aptilo Networks, and AdaptiveMobile Security. Enea is headquartered in Stockholm, Sweden, and is listed on Nasdaq Stockholm. For more information: www.enea.com

CORPORATE HEADQUARTERS
P.O. Box 1033
Jan Stenbecks Torg 17
SE-164 21 Kista
Sweden
Phone: +46 8 507 140 00

www.enea.com