5 September 2025

Australian Government
Department of Home Affairs
GPO Box 9984
Sydney NSW 2001

By electronic submission only at: *homeaffairs.gov.au*

Australian Payments Network (AusPayNet) welcomes the opportunity to respond to the consultation on developing Horizon 2 of the *2023-2030 Australian Cyber Security Strategy*.

AusPayNet is the industry association and self-regulatory body for the Australian payments industry. We manage and develop standards and guidelines governing payments in Australia. Our purpose is to create confidence in payments by: setting enforceable industry standards for a safe, reliable and effective payments system; leading transformation in payments to drive efficiency, innovation and choice; and being the home for ecosystem collaboration and strategic insight. AusPayNet currently has more than 160 members including financial institutions, payment system operators, major retailers and financial technology companies.[1]

Introduction

The Australian payments ecosystem provides the critical infrastructure that underpins the smooth functioning of the economy, enabling the safe and efficient transfer of funds between individuals, businesses and institutions.

Recent innovation in the payments sector has enabled Australian consumers to pay for goods and services in increasingly efficient and diverse ways. In addition to more traditional payment methods such as cash, cheques, and physical debit and credit cards, Australian consumers can now choose from an increasing range of convenient and secure digital payment options, including digital wallets, mobile banking apps, and wearable payment devices.

The introduction of some of these new payment technologies in recent years has supported continued growth in the Australian card market, with debit and credit cards now being the most common method of retail payments in Australia.[2] Over 15 billion card payments were made in 2024, up from 9.8 billion in 2018/19, with the total value of card payments increasing from $635 billion to almost $1 trillion in the same time period.[3]

Concurrently, the power of computer processing has increased significantly due to technological advances in both classical and quantum computing. While supporting the rapid expansion of the digital payments ecosystem, this is simultaneously enabling bad actors to harness more powerful computer processing to carry out more potent and wider scale cyberattacks, including on payments data.

---

1 The views expressed in this submission are those of AusPayNet Management and may not necessarily represent the views of all of our members.
2 Reserve Bank of Australia retail payments statistics.
3 Reserve Bank of Australia retail payments statistics, Payments System Board Annual Report 2019.

The Triple Data Encryption Standard (TDES) and Advanced Encryption Standard (AES) are cryptographic algorithms that are used in card payment systems to protect sensitive card payment data during transmission and storage. TDES is currently widely used in the Australian payments ecosystem. However, ongoing advances in computing technology present a material risk to the effectiveness of TDES. To ensure the ongoing safety of Australian card payments, since late 2022, AusPayNet has been planning and designing an industry-wide program to migrate the Australian card payments system to AES, which is widely recognised as a more secure quantum resistant and quantum safe cryptographic algorithm.

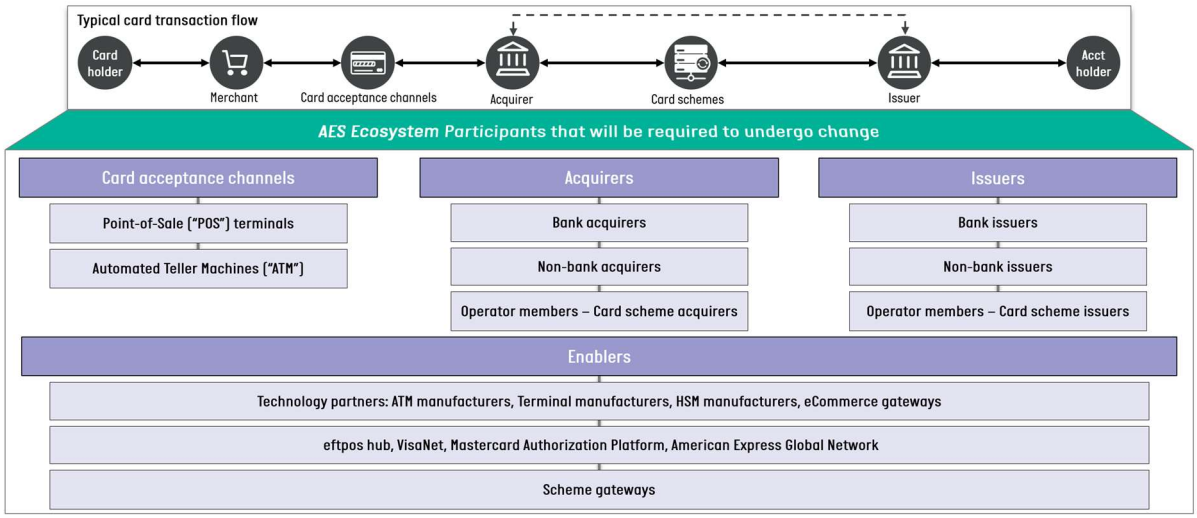
The program is in line with, and supported by, the Australian Government's *Strategic Plan for Australia's Payment System*, which calls for 'a safe and resilient system'.[4] The Reserve Bank of Australia (RBA) has also expressed support for the industry to ensure encryption standards continue to meet the standards expected by the Australian public.[5]

This submission focuses on providing insights on the issues relevant to the critical infrastructure that is the card payments system, and the challenges that are presented by the networked nature of these assets.

The AES Migration Program

The Australian card payments ecosystem is extensive, and almost every part of the ecosystem will be impacted by the AES Migration Program. The Program will require the upgrade of all functions, processes and infrastructure that rely on the existing data security standards, including point-of-sale systems, ATMs, and the payments networks that enable card payments. To give an indication of the scale involved in this upgrade, there are currently 1,030,000 point-of-sale terminals and 23,700 ATMs that will require upgrades. All payments made using the international and domestic card schemes will be in scope.

This ecosystem is illustrated in the diagram below.



4 Australian Government's Strategic Plan for Australia's Payment System.
5 Reserve Bank of Australia media release, February 2024.

The AES Migration Program will substantially reduce the likelihood of an attack on Australian payments data and ensure that Australia adopts the heightened security standards that leading Australian and international agencies have already adopted to defend against the threats facing TDES.

Risks & Challenges

Given the size, scale and criticality of the card payments system, its owners and operators are obliged to prevent and mitigate material risks under the *Security of Critical Infrastructure Act 2018* (SOCI Act). Migration to AES is consistent with these obligations, given the materiality of the security risk. However, it is not at this stage a specific requirement.

Due to the networked nature of the card payments system, the risk of compromise of TDES is significant. Should TDES be compromised in one location, it is compromised everywhere across the system. To the extent that assets in the card payments system have not removed TDES, they would therefore all be considered vulnerable. For example, should an acquirer be compromised, this has the potential to expose cardholder data for all cardholders, irrespective of whichever financial institution has issued those cards. This exposes all issuing banks to risks that are not under their own direct control, even if the issuer has already migrated their own systems to AES.

Furthermore, it may not be apparent that the system has been compromised. The Australian Signals Directorate's (ASD) Annual Cyber Threat Report 2023-2024 highlights a particular concern of state actors compromising systems without being detected:

> *In February 2024, ASD joined the US and other international partners in releasing an advisory that assessed the People's Republic of China (PRC) is leveraging living off the land techniques that abuse native tools and processes on systems. The PRC's choice of targets and pattern of behaviour is consistent with pre-positioning for disruptive effects rather than traditional cyber espionage operations.*[6]

Additionally, with the potential for 'Store Now, Decrypt Later' attacks, data that has already been exfiltrated may be accessible and used for malicious purposes in the future, before the breach has even been detected.

The potential consequences of these risks are material. Whilst an individual hacker may seek to use compromised data for personal gain (e.g. through fraudulent transactions), national state actors are considered more likely to see the opportunity to disrupt the payments system as a whole, causing widespread disruption to the Australian economy. Once compromised, it would be nearly impossible to know which credentials are valid, thus likely causing a wholesale shutdown of the card payments system until it can be secured and all cards are reissued.

The SOCI Act obliges certain critical infrastructure owners to adopt, maintain and comply with a written risk management program. However, these risk management programs are subject to the risk appetite of each asset owner. This is consistent with the prevailing view that industry is best placed to identify hazards and determine how to minimise or eliminate material risks.

However, one limitation of this approach in a payments ecosystem is that it does not ensure sufficiency of system-wide risk management, instead relying on the adequacy of individual risk-

---

6 Australian Signals Directorate's Annual Cyber Threat Report 2023-2024.

management efforts within the broad range of industry standards that apply. In the case of the card payments system, this means that issuing banks will continue to be reliant on the adequacy of risk management at each acquiring bank and payment scheme.

A Preferred Future

A preferred alternative approach would be to seek to establish minimum standards across the card payments system that are appropriate for the system as a whole. These standards would set the baseline for the adequacy of risk management plans for each entity within the system, in addition to the current requirements of the Critical Infrastructure Risk Management Program.

Such an approach would require a number of changes to the current framework, including:

- The establishment of a standards setting body with appropriate authority and responsibility for setting relevant standards.
- A requirement within the SOCI Act that risk management plans meet the standards set.
- Disclosure provisions to enable the relevant regulator (in this case, the RBA) to review the risk management plans and assess adequacy and compliance to the standard.
- Broader enforcement powers to act on non-compliance, noting that current enforcement powers are limited to seriously deficient risk management plans.

Noting that this approach may take some time to establish, in the short term, it may be appropriate for AES-128 be set as a minimum standard for card payment systems identified as critical infrastructure and/or prominent payment systems.

Responses to Specific Consultation Questions

Q1: What trends or technology developments will shape the outlook over the next few years and what other strategic factors should Government be exploring for cyber security under Horizon 2?

The consultation paper outlines the main developments that need to be considered. The developments that are of specific concern for the card payments system are advances in classical and quantum computing, ongoing threats from state actors, and the security of data subject to "store now, decrypt later" risks.

Q33: How effective do you consider the SOCI Act at protecting Australia's critical infrastructure? Are the current obligations proportionate, well-understood, and enforceable?

Q34. Are there significant cyber security risks that are not adequately addressed under the current framework?

As noted above, whilst the SOCI Act provides a good basis for the security of individual assets, it is not sufficient to address counterparty risks in networked infrastructure. Consideration should be made as to how to address system-wide security, as well as security of individual assets.

Furthermore, the enforcement powers are primarily limited to seriously deficient risk management. A broader perspective which seeks compliance with established standards may be preferable.

Q38: How are Australian Government security requirements or frameworks being considered or adopted among private sector partners, including in critical infrastructure?

The ASD's Information Security Manual[7] is a useful resource providing guidance to industry on minimum standards. This manual has been used as a reference point for the technical blueprint developed for the AES Migration Program.

Please contact [redacted] if you have any questions related to this submission.

Yours sincerely,

[redacted]

[redacted]

Australian Payments Network

[7] Australian Signals Directorate's Information Security Manual.