Response to 2023 – 2030 Australian Cyber Security Strategy: Legislative Reforms

Table of Contents

Group Country Manager Letter

1 March 2024

Department of Home Affairs
PO Box 25
BELCONNEN ACT 2616

Via email: ci.reforms@homeaffairs.gov.au

Dear Department of Home Affairs representative,

Visa's response to the 2023-2030 Australian Cyber Security Strategy: Legislative Reforms Consultation Paper

Visa welcomes the opportunity to provide its perspectives on the 2023-2030 Australian Cyber Security Strategy: Legislative Reforms Consultation Paper (the Paper).

We share the Government's commitment to make Australia a world leader in cyber security, which is particularly important given the recent cyber incidents that have impacted supply chains and infrastructure, governments, and large and small businesses in various parts of the world.

In responding to this consultation, we provide our perspectives on a number of specific questions in the Paper, such as actions which would assist in making Australia a world leader in cyber security by 2030.

Visa is available to provide further details on our submission if helpful.

Yours sincerely,

Julian Potter
Group Country Manager, Australia, New Zealand & South Pacific

Overview

Cyber security is a top concern for both the private and public sectors, driven in large part by an increasingly connected and digital world. According to the Australian Signals Directorate (ASD), in fiscal year 2022-23, the number of total cybercrime reports was up 23% and the average cost of cybercrime per report was up 14%.[1] As ASD notes, cybercrimes "have caused harm and continue to impose significant costs on all Australians," particularly small businesses and individuals.

For Visa specifically, cyber security is a top priority – so we can ensure that consumers and businesses can pay and be paid with confidence. Visa invests heavily in our cyber security program, including ensuring we have the talent, tools, and state of the art technological capabilities to detect and prevent cyber attacks on our systems. We build and use AI to detect and secure cyber threats and approach cyber security with a layered defence-in-depth strategy. The strategy includes policy and training, adaptive resiliency, audits and third-party certifications. Beyond our risk products and services, we work with industry organisations to develop and support standards for payment data security. In addition, we partner with clients, businesses, governments, and law enforcement agencies to help identify and prevent fraud and share security best practices and threat intelligence.

In addition, governments play an important role in ensuring cyber security. In this regard, Visa supports a cyber security policy environment that promotes a flexible and risk-based approach to cyber security and that encourages close collaboration between the private and public sectors. Given the importance of public-private cooperation in ensuring the security of the global payments ecosystem, we endorse the World Economic Forum's (WEF) Cyber Resilience Playbook for Public-Private Collaboration as a basis for evaluating the impact of policy options for cyber security.

Beyond engagement with individual governments and law enforcement agencies on cyber issues, Visa experiences first-hand the benefits of international collaboration in cyber security, leading to fast and frictionless information sharing across borders, for the benefit of all ecosystem participants and the customers they serve. Initiatives such as the European Cyber Resilience Board (ECRB) and the Financial Services Information Sharing and Analysis Center (FS-ISAC) in the United States involve multiple organisations working together through formal contractual arrangements and informal partnerships – across both the public and private sectors – to achieve greater global resilience to cyber attacks and to promote best practices in deterring cyber threats.

Visa provides below its responses to specific questions in the Paper.

[1] ASD Cyber Threat Report (2022-2023), https://www.cyber.gov.au/sites/default/files/2023-11/asd-cyber-threat-report-2023.pdf

Response to specific questions

Measure 2: Further understanding cyber incidents – Ransomware reporting for businesses

8. What mandatory information, if any, should be reported if an entity has been subject to a ransomware or cyber extortion incident?

Visa believes that voluntary information sharing generally best preserves the collaborative partnership between government and industry. However, if a ransomware or cyber extortion requirement is introduced, the information required should be focused on what is necessary to counter criminal actors and prevent further harm to others. For example, the Government may benefit from technical indicators (such as IP addresses associated with the criminal actor) digital currency account identifiers of the criminals (e.g., Bitcoin wallet addresses included in the extortion demand) or a summary of observed tactics, techniques, and procedures (such as malware type used and vulnerability targeted). In other words, the information required should centre around threat-focused information rather than sensitive information about the targeted entity.

9. What additional mandatory information should be reported if a payment is made?

Regardless of whether payment is made, the focus of any reporting requirement should be on information helpful to the Government and others in countering the criminal actors, such as the method of payment demanded and information that would help identify the criminal actors.

10. What is the appropriate scope of a ransomware reporting obligation to increase visibility of ransomware and cyber extortion threats, whilst minimising the regulatory burden on entities with less capacity to fulfil these obligations?

Any new ransomware reporting obligation should be scoped to larger entities or those particularly critical to Australia's essential national functions. It should also apply only to successful deployment of ransomware or authentic cyber extortion demands relating to a confirmed data breach. For other events, reporting should be encouraged, but not mandated. This tailoring will help increase visibility into the threats while minimising any additional burdens on Australian businesses least able to bear them.

11. Should the scope of the ransomware reporting obligation be limited to larger businesses, such as those with an annual turnover of more than $10 million per year?

While a voluntary reporting model is preferred, if a new ransomware reporting obligation is imposed, it should not be limited solely based on the size of the business. It is important to consider that smaller businesses often require substantial operational support in the event of a cyber attack. Therefore, the threshold for reporting obligations should be determined not just

by the size of the business, but also by its potential impact on critical infrastructure (e.g., if the impacted system is one of national significance operated by a smaller business). Although the regulatory burden disproportionately affects smaller businesses, if those businesses can obtain operational support from relevant agencies in response to and recovery from a cyber attack, the additional burden may be justified.

12. What is an appropriate time period to require reports to be provided after an entity experiences a ransomware or cyber extortion attack, or after an entity makes a payment?

A business suffering a ransomware or cyber extortion attack should focus its time and resources on remediating the threat and protecting its data, particularly in the challenging early hours and days after an attack. In addition, aligning incident reporting timeframes helps avoid unnecessary costs in tracking divergent regulatory requirements. Therefore, it would be appropriate for a new ransomware reporting period to match that currently in the Security of Critical Infrastructure (SOCI) Act —i.e., 72 hours. Furthermore, the Government could consider including provisions that would allow the targeted entity to prioritise threat remediation and data protection by permitting additional details to be furnished after the formal reporting timeframe. For instance, if the targeted entity is unable to provide the full set of initial reporting data due to resources being focused on remediation efforts, a grace period of, say, an additional 48 hours could be given for the submission of the remaining information.

Lastly, it is important for the ransomware notification to be kept strictly confidential to protect the entity that was targeted.

13. To what extent would the no-fault and no-liability principles provide more confidence for entities reporting a ransomware or cyber extortion incident?

The no-fault and no-liability principles would provide more confidence for entities reporting a ransomware or cyber extortion incident that they can focus on providing information useful in countering cyber criminals rather than being concerned that any information disclosed could be used against the target of criminal activity. It is also critical that there be strict confidentiality associated with reporting of this information. That will encourage more organisations to report ransomware incidents.

14. How can the Government ensure that no-fault and no-liability principles balance public expectations that businesses should take accountability for their cyber security?

Accountability for sensible security is an important goal, but cyber criminals and government actors are capable of breaching even companies with world-class security that comply with stringent security standards. Therefore, accountability should be based on non-compliance with applicable legal and regulatory standards rather than whether a company has suffered and reported a ransomware attack or breach. No-fault and no-liability principles applied to information reported under the SOCI Act and any new ransomware reporting regime would

help balance the need for transparency with the need for accountability. As noted in the Paper, such principles would not prevent regulators from holding businesses accountable for their existing regulatory obligations.

15. What is an appropriate enforcement mechanism for a ransomware reporting obligation?

Ransomware reporting obligations should be enforced through existing regulatory mechanisms, such as those in Part 5 of the SOCI Act, rather than via a new mechanism.

16. What types of anonymised information about ransomware incidents would be most helpful for industry to receive? How frequently should reporting information be shared, and with whom?

Technical indicators and summaries of criminal actors' tactics, techniques, and procedures, particularly any novel techniques, would be helpful for industry to receive. However, not all industry entities are equally able to ingest, understand, and action this type of information. Therefore, there should be a voluntary mechanism whereby entities can request to receive this information, if not published through mechanisms like the Australian Signals Directorate (ASD)/Australian Cyber Security Centre (ACSC) public threat advisories. Anonymised information about the threats should be made available as quickly as practicable after the Government receives it.

Measure 3: Encouraging engagement during cyber incidents – Limited use obligation on the Australian Signals Directorate and the National Cyber Security Coordinator

17. What should be included in the 'prescribed cyber security purposes' for a limited use obligation on cyber incident information shared with ASD and the Cyber Coordinator?

A limited use obligation on cyber incident information should permit ASD and the Cyber Coordinator to use the information solely for the purposes of identifying and countering cyber threats to the individual victim and the broader community and assisting victims of malicious or criminal cyber activity. Such uses should include sharing incident information with other law enforcement, intelligence, or national security agencies to enable actions to identify, disrupt or deter cyber threat actors. Any use of the information to provide advice to industry or the public should not identify the targeted entity without that entity's consent.

18. What restrictions, if any, should apply to the use or sharing of cyber incident information provided to ASD or the Cyber Coordinator?

While a restriction on use of reported information for regulatory enforcement is helpful, a restriction on sharing such information with regulatory agencies would better preserve the trusted, collaborative partnership between ASD, the Cyber Coordinator, and industry and

address the reduced engagement identified in the Paper[2] and in ASD's recent submission to the Parliamentary Joint Committee on Law Enforcement.[3] A restriction on sharing information attributable to a specific entity would maintain a clear distinction between sharing for regulatory purposes and sharing for purposes of threat intelligence and threat response actions. Regulators seeking information about a cyber incident can and should do so through the standard regulatory mechanisms.

19. What else can Government do to promote and incentivise entities to share information and collaborate with ASD and the Cyber Coordinator in the aftermath of a cyber incident?

Government agencies, such as the ASD and the Cyber Coordinator, play a crucial role in managing cyber threats during an ongoing cyber attack and mitigating its aftermath. However, effectiveness largely depends on the timely and accurate information received about these threats.

One significant incentive is the operational support that these (government) agencies can provide to targeted entities, for instance, the availability of 24/7 hotlines for immediate reporting and support. During a ransomware attack, these hotlines can provide entities with direct access to technical assistance to help identify the source and nature of the attack, guidance on how to limit its spread, and advice on preserving evidence for a potential criminal investigation.

Continuous operational support should be rendered in the aftermath of a cyber incident. These may include further technical assistance to ensure the threat is fully eliminated, support in recovery efforts, and guidance on improving cyber security measures to prevent future attacks.

By clearly articulating the range and nature of this operational support, the Government can demonstrate to entities that reporting a cyber incident serves not only as a regulatory obligation, but a pathway to valuable assistance.

In addition, the Government needs to assure entities that the information they provide will be protected appropriately. This includes safeguarding the confidentiality of sensitive information and ensuring that it is used primarily for the purpose of enhancing cyber security, rather than for regulatory enforcement or public disclosure.

By providing these incentives and assurances, the Government can foster a more collaborative and effective approach to manage cyber threats, benefiting not just individual entities, but the entire critical structure ecosystem.

---

[2] Home Affairs (2023), 2023-2030 Australian Cyber Security Strategy: Legislative Reforms, p18
[3] Australian Signals Directorate (2023), ASD Submission, Parliamentary Joint Committee on Law Enforcement Inquiry- the capability of law enforcement to respond to cybercrime, p4

Measure 4: Learning lessons after cyber incidents – A Cyber Incident Review Board

20. What should be the purpose and scope of the proposed Cyber Incident Review Board (CIRB)?

The purpose of the CIRB should be to identify lessons learned from major cyber incidents that will help entities improve their cyber security posture. To avoid duplicating effort, the CIRB should be focused on incidents that have had a major impact on the public and that have not been well studied elsewhere. CIRB reports should focus on identifying the criminal actors' tactics, techniques, and procedures as well as the lessons learned and recommendations to other entities from those lessons. As noted in the Paper, it is important that the CIRB focus not on blame, but on helping the cyber security ecosystem improve[4]. It is also crucial that sensitive company information, such as trade secrets, be protected from public disclosure.

21. What limitations should be imposed on a CIRB to ensure that it does not interfere with law enforcement, national security, intelligence and regulatory activities?

The CIRB should limit its inquiries to incidents where the immediate threat has been resolved, including any pending law enforcement, national security, or intelligence activities. If a regulatory enforcement action is to be taken, the CIRB should delay its inquiry until such action is complete to avoid unintentionally interfering with a regulatory investigation or putting the targeted company in the position of having to answer CIRB questions while still facing the prospect of legal action. This is particularly important if any information provided, or conclusions reached by the CIRB could be used against the company in a regulatory setting. A restriction on the use of information gathered by or conclusions reached by the CIRB in regulator or legal proceedings could help mitigate this concern.

22. How should a CIRB ensure that it adopts a 'no-fault' approach when reviewing cyber incidents?

Consistent with best practices for identifying lessons learned in an incident response, it is critical that the CIRB adopt a 'no-fault' approach when reviewing cyber incidents. This approach can be built into both the review and reporting stages. At the review stage, the focus should be on what happened, rather than on the actions of an individual. For example, it may be significant that a user with privileged access clicked on a phishing link; it is likely not significant who that user is. At the reporting stage, the CIRB should be careful to avoid language implying blame or fault, such as 'negligent', and focus on the 'what' rather than the 'who'. Visa, therefore, supports the CIRB adopting the Australian Transport Safety Board approach noted in the Paper[5].

---

[4] Home Affairs (2023), 2023-2030 Australian Cyber Security Strategy: Legislative Reforms, p24
[5] Home Affairs (2023), 2023-2030 Australian Cyber Security Strategy: Legislative Reforms, p22

23. What factors would make a cyber incident worth reviewing by a CIRB?

A cyber incident may be worth reviewing by a CIRB if it had a significant impact on the public or involved novel adversary tactics and has not been otherwise thoroughly studied elsewhere, such as by the U.S. Cyber Safety Review Board.

24. Who should be a member of a CIRB? How should these members be appointed?

CIRB members should be government officials with expertise in cyber security and experience in industry or former, retired industry experts no longer associated with a specific company. The members should be appointed by the Government in a transparent, public manner. It is important that the board members bring real-world experience with managing cyber risks, including in an industry setting. However, appointing currently serving corporate cyber security representatives risks the appearance of a conflict of interest, such as when a board member is overseeing a review of his or her company's competitor. These conflicts — perceived or real — would likely make companies less willing to participate fully in the process.

25. What level of proven independent expertise should CIRB members bring to reviews? What domains of expertise would need to be represented on the board?

The CIRB members should have some expertise in cyber security risk management and incident response. They ideally would represent a diverse range of domains within the cyber security ecosystem, including cyber security operations/incident response, architecture, intelligence, and legal/compliance. But the members cannot reasonably be experts in all domains, so they must be supported by a professional staff and external experts as needed.

26. How should the Government manage issues of personnel security and conflicts of interest?

The Government should manage personnel security issues consistently with any other prominent national security position — CIRB members should have (or be granted) security clearances in order to receive the fullest picture possible from the intelligence and national security community, where relevant. Granting security clearances to only some members of the CIRB would potentially result in an imbalance of information, inhibiting the value of a multi-member board able to bring different perspectives to bear on a common set of data.

Conflicts of interest, similarly, should be managed consistent with general standards for ethics across the Government, such as the Australian Public Service Code of Conduct. Conflict of interest issues are significantly more challenging if the board members are currently serving employees of a private company, as noted above.

27. Who should chair a CIRB?

The CIRB should be chaired by a senior government official from a relevant department with cyber security expertise, such as the Cyber Coordinator.

28. Who should be responsible for initiating reviews to be undertaken by a CIRB?

The CIRB itself should be responsible for initiating reviews, based on transparent, public standards articulated in law and policy.

29. What powers should a CIRB be given to effectively perform its functions?

The CIRB should have the authority to receive evidence from all relevant government departments and voluntary information contributions from relevant industry entities. For a no-blame, lessons-learned process, empowering the CIRB to compel the provision of evidence does not appear necessary when such powers are already vested in law enforcement and regulatory authorities. This approach could be subject to re-evaluation based on the practical experience of the CIRB after a few years of operation.

30. To what extent should the CIRB be covered by a 'limited use obligation', similar to that proposed for ASD and the Cyber Coordinator?

The CIRB is far more likely to receive robust cooperation if it is subject to a 'limited use obligation,' particularly one that prohibits regulatory use of any information provided to the CIRB or conclusions reached by the CIRB.

31. What enforcement mechanism(s) should apply for failure to comply with the information gathering powers of the CIRB?

As noted above, law enforcement and regulatory authorities already have the ability to compel provision of information. The CIRB should base its reviews on that information and any supplemental information voluntarily provided by industry. As a result, additional enforcement mechanisms to compel the provision of information is not necessary and would likely duplicate information already available to the Government.

32. What design features are required to ensure that a CIRB remains impartial and maintains credibility when conducting reviews of cyber incidents?

Please see the responses above to Questions 22-26 concerning composition of the CIRB membership and the 'no—blame' approach.

33. What design features are required to ensure a CIRB can maintain the integrity of and protection over sensitive information?

In addition to the personnel security, limited use obligations, and conflict of interest measures noted above, the CIRB should have the legal authority to protect information it acquires from compelled public disclosure. For example, documentation provided to the CIRB should be exempt documents under Division 2, Part IV, of the Freedom of Information Act 1982.

Measure 5: Protecting critical infrastructure – Data storage systems and business critical data

34. How are you currently managing risks to your corporate networks and systems holding business critical data?

Visa takes an all-hazards, risk-based approach to managing security of our corporate networks and systems holding business critical data. Visa has designed and implemented a comprehensive information security policy based on global standards, such as ISO 27002, and the Payment Card Industry Data Security Standard, and reviewed by external assessors against widely accepted frameworks, such as the U.S. National Institute of Standards and Technology Cybersecurity Framework. Visa assesses the criticality of its systems and applications based on their importance to core business functions and the nature of the data they store (such as personal information) and implements controls as directed by our policy appropriate to the risk of the system or application.

To verify that these policies are implemented appropriately, Visa uses a three-lines-of-defence model, with both internal and external oversight, to track compliance with our policy, identify gaps, and address them. We also operate a 24x7 cyber security operations centre across three cyber fusion centres to continually monitor Visa's network security posture. Finally, we are continually reviewing the latest cyber threat intelligence, vulnerabilities, and threats (cyber, physical, and insider) that may affect the company and its systems, and regularly update our information security policy and practices based on these evolving threats and changes in technology.

35. How can the proposed amendments to the SOCI Act address the risk to data storage systems held by critical infrastructure while balancing regulatory burden?

The SOCI Act, when amended, should continue to reference global, accepted standards for managing cyber security risks, including for on-premises and cloud-based data storage systems. Relying on global standards can help balance the regulatory burden of compliance with the need to articulate baseline requirements.

36. What would be the financial and non-financial impacts of the proposed amendments? To what extent would the proposed obligations impact the ability to effectively use data for business purposes?

Given the data-driven nature of Visa's business and our commitment to world-class security, Visa already implements the risk management measures contained in the amendments for

systems containing business critical data. However, the proposed amendments would also expand the incident reporting requirements to include these systems, which may already be subject to other Privacy Act and Australian Prudential Regulation Authority (APRA) reporting requirements, as noted in the Paper[6]. So, to the extent the amendments add another duplicative reporting requirement, that would impose financial and non-financial impacts regarding the time and resources necessary to ensure Visa has the appropriate processes in place to comply with the reporting requirement.

Measure 6: Improving our national response to the consequences of significant incidents – Consequence management powers

37. How would the proposed directions power assist you in taking action to address the consequences of an incident, such as a major cyber attack on your critical infrastructure asset?

Given the nature of Visa's business and the global, redundant nature of our infrastructure, it is unlikely the proposed directions power would assist Visa in taking action to address the consequences of an incident, except in the context of sharing personal information. Visa's contracts and privacy policies generally permit the sharing of information necessary for fraud prevention, particularly with affected financial institutions. However, if there were a scenario where contracts or the Privacy Act itself would otherwise prohibit sharing of such personal information, it is possible that the Privacy Act power to direct sharing of information, along with the immunity provisions, could assist with information-sharing efforts.

38. What other legislation or policy frameworks (e.g., at a state and territory level) would interact with the proposed consequence management power and should be considered prior to its use?

Other than the Privacy Act provisions noted in the Paper, we are not aware of other legislation or policy frameworks in Australia that would interact with the proposed power in a manner relevant to Visa.

39. What principles, safeguards and oversight mechanisms should Government establish to manage the use of a consequence management power?

The safeguards and oversight mechanisms proposed in the Paper are appropriate, particularly the last resort nature of the power and the requirement to consult the impacted entity.

Measure 7: Simplifying how government and industry shares information in crisis situations – Protected information provisions

[6] Home Affairs (2023), 2023-2030 Australian Cyber Security Strategy: Legislative Reforms, p36

40. How can the current information sharing regime under the SOCI Act be improved?

The proposed clarifications and amendments to the SOCI Act 'protected information' provisions are welcome improvements to the current information sharing regime.

41. How would a move towards a 'harm-based' threshold for information disclosure impact your decision-making? Would this change make it easier or more difficult to determine if information held by your asset should be disclosed?

The harms-based approach to sharing 'protected information' would make it easier to determine if information under the SOCI Act should be disclosed.

Measure 8: Enforcing critical infrastructure risk management obligations – Review and remedy powers

42. How would the proposed review and remedy power impact your approach to preventative risk?

Visa is committed to championing cyber security within our operations. We use an established risk assessment methodology and framework based on global standards to identify cyber security risks and associated business impacts. Visa operates in a highly regulated global industry in which operational resilience and cyber security risk management is already subject to robust regulatory oversight. As a result, the proposed review and remedy power is unlikely to impact our approach to preventive risk.

About Visa

Visa's mission is to connect the world through the most secure, reliable, and innovative payment network – enabling individuals, businesses, and economies to thrive. Our advanced global processing network, VisaNet, provides secure and reliable payments around the world, and is capable of handling more than 65,000 transaction messages a second.

In Australia, Visa has offices in Sydney and Melbourne. Together with our Australian financial institutions, fintech and business clients, and our technology partners, we are committed to building a future of commerce that fosters Australian economic growth, security and innovation. Visa continues to expand acceptance across the payments ecosystem, ensuring that every Australian can not only pay, but also be paid in a convenient and secure way. Visa invested US$10 billion (A$14.95 billion) in technology over the past five years, including to reduce fraud and improve security. Visa's Advanced Authorisation (VAA), an AI-based real-time payment fraud monitoring solution, has helped Australian financial institutions prevent $714 million[7] in fraud from disrupting Australian businesses in a year[8].

As commerce moves rapidly online, Visa recently released its updated Australian Security Roadmap 2021-23[9] in response to the increasing risk of cybercrime and scams facing Australian businesses and consumers. The roadmap highlights the steps that Visa, together with industry, are taking to continue to secure digital payments in Australia, including:

- Preventing enumeration attacks through new ecommerce requirements
- Driving adoption of secure technologies
- Securing digital first payment experiences, including contactless ATM access
- Enhancing the cyber security posture of payments ecosystem participants
- Preventing Australian consumers and businesses from becoming victims of scams
- Ensuring payments ecosystem resilience through real-time AI solutions.

[7] Visa (2024) https://www.visa.com.au/about-visa/newsroom/press-releases/visa-prevents-more-than-700-million-in-fraud-from-disrupting-australian-businesses.html
[8] 12 months ending March 2023, VisaNet (April 2022 – March 2023)
[9] Visa (2021) https://www.visa.com.au/pay-with-visa/security/future-of-security-roadmap.html