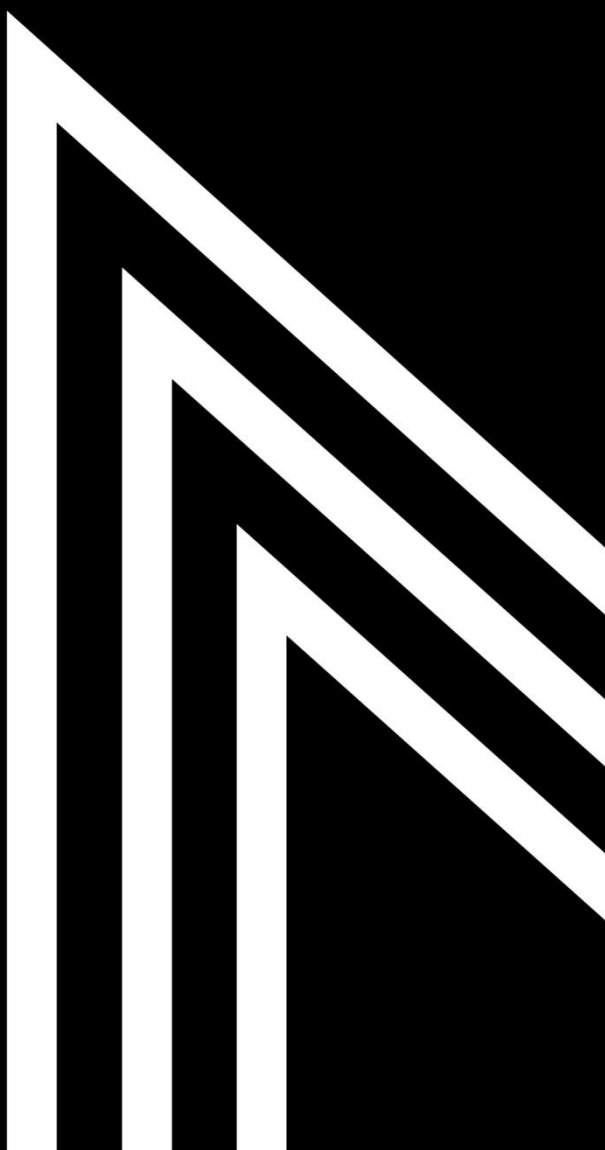
Department of the Treasury

Crypto asset secondary service providers: Licensing and custody requirements

McGrathNicol submission

May 2022



McGrathNicol

Contents

Executive Summary

McGrathNicol is a specialist advisory and restructuring firm operating in Australia and New Zealand. Our services include large and complex insolvencies, forensic investigations, cyber security, data analytics, forensic technology and governance, risk and compliance advisory. In addition to our own Digital Asset advisory services, we are also the Strategic Partner of Chainalysis, the blockchain analytics company.

McGrathNicol considers that CASSPrs represent critical infrastructure which Australians and others around the world rely on to engage in the crypto asset economy. As such, our submission centres on supporting a regulatory framework which protects this critical infrastructure from a security perspective by addressing Questions 19 through 23 of the consultation paper.

Our fundamental view is to advocate for a separation between the concepts of mandatory regulation and the principle-based management described in the consultation paper. We contend:

- Obligations relating to custody should have a regulatory focus and must be capable of regulatory assessment and enforcement;
- Principles should provide a goal state that practitioners should aim to achieve as best practice and describe broader behavioural expectations in their scope and definition;
- A tiered regulatory regime should be developed which is proportional to risk;
- Existing legislation and discussion papers need to be considered due to the potential overlap of regulation across data security, privacy, cyber security, financial services and critical infrastructure; and
- The harmonisation of legislation and policy across government between crypto assets, digital, cyber and financial strategy is critical.

Enquiries in respect of this submission or McGrathNicol's digital asset services should be directed to: digitalassets@mcgrathnicol.com.

Introduction

McGrathNicol is pleased to provide a submission to the Department of the Treasury's (the Treasury) consultation on crypto asset secondary service providers: licensing and custody requirements.

McGrathNicol is a specialist advisory and restructuring firm operating in Australia and New Zealand. Our services include large and complex insolvencies, forensic investigations, data analytics, forensic technology and governance, risk and compliance advisory. We regularly work in conjunction with law enforcement bodies, law firms, regulators and other government agencies to provide subject matter expertise in respect of digital assets, cyber security and national security risk across public and private sectors to manage risk and drive performance. We equip our clients with the information they need to manage risk, protect people and for informed decision making.

In addition to our own Digital Asset advisory services, we are also the Strategic Partner of Chainalysis, the blockchain analytics company. Chainalysis provides data, software, services, and research to government agencies, crypto asset exchanges, financial institutions, and insurance and cybersecurity companies in over 70 countries. As Chainalysis' Strategic Partner our experts have obtained qualifications in blockchain based investigations and related advisory services.

Our interest in providing crypto asset advisory services stems from a recognition of its emergence as disruptive financial technology which has the potential to impact the way in which our clients and broader society conduct business, exchange goods and services and store value. As noted by the Treasury in this consultation paper, the market capitalisation of the crypto asset ecosystem exceeded $2.6 trillion US dollars in 2021. This market capitalisation has since eroded, undermining consumer confidence and leaving many with significant losses to their investments or lifetime savings. Although this erosion has resulted from a combination of factors, including the crypto asset market structure and products available to consumers, we believe that implementing a regulatory framework for *Crypto Asset Secondary Service Providers* (CASSPrs) is a necessary step towards a robust and resilient digital economy.

We have read the consultation paper and welcome the Treasury's focus on enhanced and appropriate levels of regulation safeguards consumers from significant loss. However, we also recognise the need to balance consumer protection with domestic and global financial stability, and the growth of a thriving crypto asset economy in Australia.

McGrathNicol considers that CASSPrs represent critical infrastructure which Australians and others around the world rely on to engage in the crypto asset economy. As such, our submission centres on supporting a regulatory framework which protects this critical infrastructure from a security perspective by addressing Questions 19 through 23 of the consultation paper.

Our fundamental view is to advocate for a separation between the concepts of mandatory regulation and the principle-based management described in the consultation paper. We contend:

- Mandatory regulation should be clearly defined, based on industry agreed frameworks that can be independently assessed or audited, and provide a mechanism for policing; and
- Principles should provide a goal state that practitioners should aim to achieve as best practice and describe broader behavioural expectations in their scope and definition.

We believe a combination of mandatory regulation and principles is critical to a successful framework and that distinguishing between these two concepts provides clarity to governance efforts and ensures consistency across industry.

Enquiries in respect of this submission or McGrathNicol's digital asset services should be directed to: digitalassets@mcgrathnicol.com.

Q 19. Are there any proposed obligations that are not appropriate in relation to the custody of crypto assets?

It is our view that:

- The proposed custody obligations currently contained in the consultation paper are best described as custody security principles, to reflect that they do not dictate specific or measurable goals or outcomes in their current form.
- Clear obligations should be developed as minimum standards to reinforce these principles. Obligations relating to custody should have a regulatory focus and must be capable of regulatory assessment and enforcement. Regulators need to be empowered to appropriately enforce regulations or it is unlikely the obligations will lead to the desired effect. Regulation requires that assessments or audits can be conducted which are standardised and clearly communicated.
- Custody security obligations and custody security principles can then be published together, setting both a minimum standard for regulation and aspirational goals to guide desired behaviour.

Proposed custody obligation (4) *'ensuring that the custodian of private keys has the requisite expertise and infrastructure'* infers that there is a standardised and accessible training and certification process for CASSPrs to measure expertise, and that there is a common definition or measurement of an appropriate asset and infrastructure profile. These fundamental precursors do not currently exist in a standardised manner.

If such obligations were included, there would need to be supporting guidance to enable training, certification and infrastructure architecture development. Currently, crypto asset businesses and infrastructure can be managed by people who do not need any form of qualifications relating to technology, infrastructure, finance, or other relevant disciplines to participate in the crypto asset economy. If a certification process was developed it would need strong industry involvement and consultation to ensure it is relevant and effective, without creating unnatural barriers to adoption or unfair barriers to entry into the industry.

Proposed custody obligations (5) *'private keys used to access the consumer's crypto assets must be generated and stored in a way that minimises the risk of loss and unauthorised access'* and (6) *'adopt signing approaches that minimise 'single point of failure' risk'* imply the conduct of a formal risk assessment, as a means of identifying specific risks relevant to a CASSPr. A holistic security risk assessment with mandated minimum requirements relating to physical, personnel and cyber security aspects should provide a foundational view of risk, preferably accompanied by an independent assessment or review. The utility of a risk management program as an obligation under legislation has been demonstrated in the recent *Security Legislation Amendment (Critical Infrastructure Protection) Act 2022* (SLACIP Act). A risk-

based approach would provide each CASSPr with the opportunity to contextualise risk in respect of its own business and operations. Although this approach is harder to regulate through simple regulatory terms, it is more likely to enable the balance between innovation and security, as well as facilitating updates as new vulnerabilities and threats emerge which may outpace specific regulatory obligations.

Proposed custody obligations (7) *'robust cyber and physical security practices'* and (8) *'independent verification of cybersecurity practices'* should also incorporate personnel risk and the need to understand the ongoing suitability of personnel and persons holding critical positions. The definition of 'robust' is subject to significant interpretation. Principle-led statements such as these are useful to convey intended behaviours. However, it is not adequate from a regulatory perspective. When describing mandatory requirements, these should be aligned to specific industry standards, thereby supporting the conduct of independent verification and consistent application. Independent verification of cybersecurity practices should also seek to adopt an agreed standardised approach, to prevent inexperienced and/or unqualified parties from conducting the verification.

Cyber security controls and the security posture of each CASSPr should be proportionate to the risk faced. For example, a small low-volume and low-value exchange should not be required to maintain a full 24/7 incident response capability and top-tier cyber-security capabilities. On the other hand, an exchange dealing with very large value transactions should have a strong security posture.

There is a cost associated with robust security controls. A lack of standardisation in how controls are mandated could result in significant cost penalties for some CASSPrs, as those CASSPrs who seek to meet a higher standard are likely to incur relatively higher costs than those who do not.

Noting the rapidly changing cyber security environment and evolving regulatory environment, a balance must be struck between agility within the industry to keep up with relevant threats and address vulnerabilities, the encouragement of innovation and international cross-border competition, and the need for regulatory and governance certainty for CASSPr operations.

Q 20. Are there any additional obligations that need to be imposed in relation to crypto assets that are not identified above?

- We believe that the custody obligations proposed in the consultation paper are appropriate as behavioural expectations or principles to be applied to CASSPrs. However, we do not believe that these obligations are sufficient to describe the regulatory minimum standards for CASSPrs.
- A more nuanced and tiered regulatory regime is proposed below, which is proportional to risk.
- There is a significant risk that innovation and the development of Australian industry will be hampered by over-regulation. However, there is also a significant need for regulation in the operation of crypto assets and the risks they present to the community.

We propose the development of tiered risk levels used to categorise CASSPrs, with corresponding security obligations imposed based on the perceived risks associated with each CASSPr category.

Figure 1: Proposed risk-based regulatory model

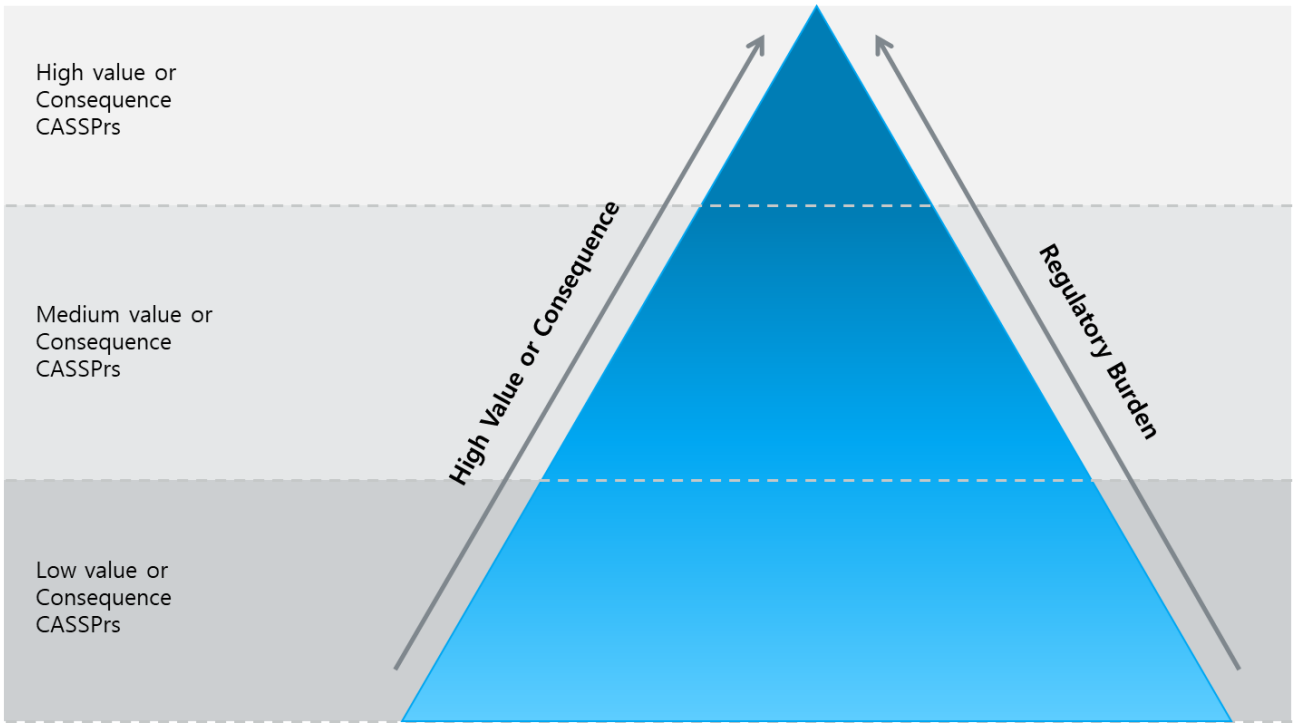


Figure 1 depicts a three-tiered regulatory model. The regulation applied is proportional to the respective metrics associated of a respective CASSPr. The exact means of identifying and determining what metrics would be applied to a CASSPr is not defined within this submission. However, it is intended that risk is classified based on the inherited consequence on third parties dealing with and through the CASSPr.

We believe the risk calculus for categorising CASSPr should be focused on consequence to consumers and crypto asset trading, not necessarily based solely on the direct impact to the CASSPr. For example, an attack exposing private keys may not directly impact the financial assets of the CASSPr; but would have a significant resulting impact on asset owners whose private keys are exposed.

By describing risk as a combination of likelihood and consequence, we propose that the likelihood aspect is dealt with by the combination of regulation and the application of desired behaviours expressed through principles. From a simplified perspective, the greater the security posture of the CASSPr the lower the likelihood (and potentially consequence) of an adverse security event or compromise. Therefore, the focus on consequence in the tiered model is based on the premise that the security controls applied will have the effect of reducing likelihood; which is why enhanced controls and regulation are needed as the consequence increases.

We propose that a tiered regulatory model is defined as follows:

- High value CASSPRs are those that facilitate large volume and/or value transactions. The consequence of a security incident upon a high value CASSPr exposes large numbers of high value consumers and users to inherited (second and third order) impacts.
- Medium value CASSPrs are likely to have a reduced impact on specific groups of asset owners and represent an undetermined middle class to distinguish between low and high value CASSPrs.
- Low value CASSPrs provide a means of encouraging innovation and reducing the regulatory burden associated with operating small-scale operations that cannot afford significant security investment or even independent assessment.

The lowest level CASSPrs would only be required to conduct a risk self-assessment with executive sign off. This reflects the limited capacity for the smallest-sized CASSPrs to undertake audits, third party assessments or invest in significant security outlays.

The medium value CASSPrs requires board–level (or equivalent) risk assessments, and third-party expert audit or certification against a recognised standard. We propose ISO27001 as an appropriate framework based on its international nature and the potential for broader comparison with cross-border CASSPr and those outside of Australian jurisdictions.

The high value tier of CASSPrs would have the additional obligations of vulnerability and penetration testing, as well as the provision of a detection, monitoring and incident response capability 24/7. This is considered proportional based on the high values and potential impact of a cyber security event on a high value CASSPr. The ability to rapidly detect, respond and recover from an adverse cyber security event could significantly reduce third party losses associated with this type of CASSPr. However, such capabilities require investment that may not be feasible for a medium or low tier CASSPr.

Q 21. There are no specific domestic location requirements for custodians. Do you think this is something that needs to be mandated? If so, what would this requirement consist of?

The imposition of domestic location requirements would be difficult to police; particularly given the following considerations:

- cloud backups are unlikely to be located in the same datacentres, meaning they are often deployed overseas;
- the CASSPr transactions in question could involve parties who are not themselves located in Australia;
- the transaction itself could be made by a CASSPr employee outside of Australia, using equipment that is not located in Australia;
- most of the infrastructure supporting digital currency transactions and processing is not located within Australia.

The application of the *Privacy Act 1988* and associated *Australian Privacy Principles* to cross-border information exchange is relevant to the security of client information. Equally, the *European Union General Data Protection Regulation* may apply to transactions between jurisdictions. Location and jurisdictional regulation and management requires significant analysis prior to the publication of regulation. We suggest expert legal opinion is applied to consider these aspects prior to development of the final regulation.

Q 22. Are the principles detailed above sufficient to appropriately safeguard client crypto assets?

- We believe that the custody obligations, as they are currently described, provide a useful set of desired behaviours but should be reframed as principles.
- The custody obligations are unlikely to provide sufficient regulatory certainty to improve the current cyber-security landscape for CASSPrs.
- The regulations described should provide a foundational set of expectations which can be policed, overlaid with a higher-order set of principles to drive enhanced outcomes.

For example, independent verification in Principle (8) could mean anything from an ISO27001 audit to a penetration test. If a specific verification approach is employed, it does not follow that remediation work will then be undertaken to rectify any deficiencies identified unless there is close regulatory scrutiny, or an event causes the entity to take action to address the issue.

In many cases within other industry sectors, vulnerability activities lack consistency and quality between providers and the issues they identify are often not subsequently adequately addressed. Each year the same issues are identified without follow up action.

We propose an alternative approach, using the tiered model shown at Figure 1, to regulate the minimum expected standard of security for CASSPrs. All CASSPrs regardless of size would require a risk management plan, risk register and remediation plan. Higher tiered CASSPrs would require additional governance, such as independent third-party assessment and the demonstration that efforts have been undertaken between reports to improve the overall security of the CASSPr and address identified vulnerabilities.

Although the goal should always be to have robust cyber-security controls, regulation should also ensure the minimum standards are defined and policed. The existing principles do not provide any guidance on what that minimum standard is, or how it will be policed and standardised across CASSPrs.

Q 23. Should further standards be prescribed? If so, please provide details.

- There are several relevant cyber security standards. Whatever standard is selected, the international nature of CASSPr transactions and alignment between jurisdictions should be considered.
- Existing legislation and discussion papers need to be considered due to the potential overlap of regulation across data security, privacy, cyber security, financial services and critical infrastructure.
- The harmonisation of legislation and policy across government between crypto assets, digital, cyber and financial strategy is critical.

ISO27001 provides the best global coverage, integration with other ISO standards such as risk management (ISO31000) and utilises a policy-driven baseline with a common international vocabulary. However, the *National Institute of Standards and Technology* (NIST) *Cyber Security Framework* (CSF), *Centre for Internet Security* (CIS) *Critical Security Controls, Open Web Application Security Project* (OWASP) *Top 10, Essential Eight,* and the Australian *Information Security Manual* (ISM) should all be considered relevant and could be applied.

Given the tiered model presented within this proposal, additional alternative regulatory and principle-based models could be adapted from examples such as the *Cybersecurity Maturity Model Certification* (CMMC), *Capability Maturity Model Integration* (CMMI) *Cybermaturity, and Program Review for Information Security Assistance* (PRISMA).

A variety of parallel legislation and policy should be considered as part of the CASSPr regulation. For example, small business operators with annual turnover of less than $3 million are generally exempt under the *Australian Privacy Principles*. This has implications under the *Notifiable Data Breach Scheme*. Where legislation has differentiated between mandatory obligations for Australian businesses, it should be considered in any CASSPr legislation.

Discussion papers such as the *National Data Security Action Plan* should be considered in parallel with this consultancy effort. In addition, existing legislation should be considered such as the Australian government's *Digital Economy Strategy*, *Consumer Data Right, Cyber Security Strategy,* and *Security Legislation Amendment (Critical Infrastructure Protection) Act 2022* (SLACIP Act). The SLACIP Act includes obligations for entities to establish, maintain and comply with a risk management program, together with annual reporting obligations to government. The expansion of the *Security of Critical Infrastructure Act 2018* to incorporate financial services and markets may mean inclusion of some or all CASSPrs, depending on interpretation and evolution of the crypto asset market.

The inclusion of miners and validators as CASSPrs could have regulatory impacts on a broad variety of individuals who run their own small-scale miners at home, through to businesses using Hyperledger Validating Peers to facilitate the Hyperledger network. The scale of operators, impact on the integrity of

the network, the relative financial value to consumers, and the distinction between permissioned and permissionless crypto assets are all important distinctions that should impact any regulation and be carefully considered prior to any regulatory decisions. A clear taxonomy and classification system is needed to facilitate regulation whilst enabling continued growth of the Australian digital economy through crypto asset innovation. Three different examples are provided below to facilitate discussion about the different use cases regulation would need to consider. These are not exhaustive:

- An individual running an altcoin miner at home could be considered a CASSPr. They may have minimal asset investment and little understanding of legislative requirements. They both mine and facilitate transactions through their proof of work on the permissionless network.
- Mining pools allow individual crypto miners to combine computational resources to increase their collective hash rate. Mining pools operate across jurisdictions, with rewards for block hash identification shared between miners, based on their respective contribution.
- A business running Hyperledger could use crypto assets for a wide variety of use cases, from document record management through to supply chain integrity, digital smart contracts and decentralized finance (DeFi) applications. The Hyperledger technology may simply be used to facilitate business functions, or it could enable the transfer of assets between businesses and/or consumers.

The broad range of potential use cases and the prospect of new technological developments relating to crypto assets means that broad regulation could restrict innovation within Australia. A thorough analysis and impact study is needed to facilitate legislative development for crypto assets and CASSPr.

Conclusion

McGrathNicol appreciates the opportunity to provide a submission to the Treasury consultation on crypto asset secondary service providers. Our submission supports a robust regulatory framework proportional to risk, enforceable, and harmonised with international standards and Australian legislation. We also support custody principles, for encouraging desired behaviours above and beyond the regulatory regime.

Yours faithfully,

McGrathNicol Advisory

Jamie Norton
Partner
McGrathNicol

Joss Howard
Partner
McGrathNicol

Jamie Norton
Partner

Jamie specialises in assisting organisations with their cybersecurity strategy, program development, governance, risk, and operations. He has over 20 years experience in managing security resilience for State and Federal Government agencies and commercial organisations.

Jamie is an established leader in the security field and former Chief Information and Security Officer (CSIO) with the Australian Taxation Office. He has been a member of the global CISM Certification Working Group for ISACA and co-chair of the Cyber Security Stakeholders Group (CSSG) with Chartered Accountants Australia and the CPA. He has been involved in several senior government committees on cyber resilience, including contributing to the Australian Cyber Security Strategy 2020 and the ASD IRAP and Cloud programs.

As an experienced CISO, Jamie regularly works with boards, executives, and security leaders to advocate the business case for better security, improve reporting and metrics, and refine organisational security strategy. Leveraging his real-word experience, Jamie offers guidance and mentoring to business leaders and organisations seeking security leadership advice.

Areas of expertise

- Cyber Awareness
- Cyber Risk
- Digital Forensics
- EDiscovery

Joss Howard
Partner

Joss has led teams in delivery of technical, information security and cyber resilience projects for over 25 years. She has held senior security management positions in industry and professional services, advising companies globally. Her career has seen her work in aerospace, defence, finance, government, healthcare, leisure and retail, transport, telecommunications, and utilities sectors.

Her professional services career has included working with an extensive number of clients globally, helping to tackle cyber risk and increase their security resilience. She specialises in assessing security posture, developing strategies, and identifying investments, resources, and initiatives to achieve optimal cyber security growth for her clients. Further, Joss advises boards and senior management on initiatives to improve their business resiliency against cyber threats, reduce risks and protect profitability.

An authentic security professional, her experience is relied upon at the board, senior management, and operational level of a business. She is regarded by clients as a 'trusted advisor' and a cyber leader providing genuine insight and innovation on information risk and cyber-security matters.

Areas of expertise

- Cyber Security Strategy
- Cyber Governance and Information Security
- Cyber Risk and Performance
- Incident Handling and Breach Response