28 October 2022

General Manager, Policy

Australian Prudential Regulation Authority

I thank the Australian Prudential Regulation Authority ('APRA') for the opportunity to make this submission on the Discussion Paper on *Strengthening Operational Risk Management*.[1]

I am a PhD Scholar at the University of Sydney in the Discipline of Business Law. My project will answer the following research question:

> How should the development and deployment of critical software be regulated as part of the regulation of the cyber resilience of critical infrastructure assets?

Given my research area, this submission is focused on the parts of the *Discussion Paper* that concern cyber supply chain risk management, a term which refers to 'the discipline of addressing cybersecurity risks stemming from extended supply chains and supply ecosystems', encompassing functions like 'third-party risk management and external dependency management'.[2]

Therefore, this submission responds to the following consultation questions together:

2. *Are there specific topics or areas on which guidance would be particularly useful to assist in implementation?*
5. *How could APRA improve the definitions of critical operations, tolerance levels and material service providers?*
6. *What additions or amendments should be made to the lists of specified critical operations and material service providers?*

This submission will outline its recommendations first and then explain the rationale for those recommendations.

---

[1] Australian Prudential Regulation Authority, Commonwealth, 'Strengthening Operational Risk Management' (Discussion Paper, July 2022) ('*Discussion Paper*').

[2] Jon Boyens et al, National Institute of Standards and Technology, *Key Practices in Cyber Supply Chain Risk Management: Observations from Industry* (Report No NISTIR 8276, February 2021) 3.

1. Recommendations

This submission recommends that APRA:

1. *specifically require APRA-regulated entities to manage operational risks that stem from, or are otherwise affected by, their deployment of open source software ('OSS'). APRA should amend the definitions and list of critical operations to reflect the reliance by APRA-regulated entities on OSS to carry out their business models; and*

The deployment of OSS[3] by APRA-regulated entities can be both: direct, for instance, when entities' employees or third party service providers directly incorporate OSS as end-user developed or configured software; and indirect, for instance, when entities deploy software which is licensed from third-party vendors and service providers, and incorporates OSS, making the OSS a nested dependency within the information assets[4] of entities. Specifically requiring entities to manage OSS-driven operational risks could be performed through inclusion in the Prudential Practice Guide for the proposed Prudential Standard or by amending *CPS 234* to specifically refer to OSS.

2. *work through the Council of Financial Regulators ('CFR'), with the financial sector broadly and under the leadership of the OSS community to ensure that the deployment of OSS in the financial sector more broadly is the subject of greater (regulatory) scrutiny.*

It is recommended that any black-letter law within the context of this scrutiny be confined to entities directly regulated by CFR members and the *first*-tier suppliers of those entities. This is

---

[3] This submission adopts the definition of OSS from the National Institute of Standards and Technology:

> Software that can be accessed, used, modified, and shared by anyone. OSS is often distributed under licenses that comply with the definition of "Open Source" provided by the Open Source Initiative and/or that meet the definition of "Free Software" provided by the Free Software Foundation.

National Institute of Standards and Technology, U.S. Department of Commerce, *Open Source Code* (Directive No NIST S 6106.01, 6 December 2018) 1.

OSS is contrasted with proprietary software 'which restricts who can access, use, and change the source code': U.S. Department of Commerce and U.S. Department of Homeland Security, United States, *Assessment of the Critical Supply Chains Supporting the U.S. Information and Communications Technology Industry* (Report, 24 February 2022) 36 ('*ICT Supply Chains Report*').

[4] This submission adopts the definition of 'information assets' from APRA's Prudential Standard on Information Security: Australian Prudential Regulation Authority, Commonwealth, *Information Security* (Prudential Standard No CPS 234, July 2019) s 12(d) ('*CPS 234*').

because of (as will be detailed below) the inherently decentralised and global nature of the OSS community, particularly the developers and maintainers of OSS. Rather, to operationalise Recommendation 2, members of the CFR should work together and with the financial sector broadly, *and under the leadership of the OSS community*, towards:

(a) identifying OSS packages that are the most critical to the operational resilience of the financial sector because they are deployed in the manner described under Recommendation 1 ('Critical OSS'); and

(b) contributing to efforts, led by the OSS community, that assure that the development and maintenance of Critical OSS occurs in line with best practice — such as those recommended by the Australian Cyber Security Centre and the National Institute of Standards and Technology ('NIST') — in addition to the security measures recommended by NIST for 'EO-Critical Software'.[5]

To be clear, Recommendation 2 is neither suggesting amendment of the proposed Prudential Standard nor guidance which APRA may issue for the latter. Rather, Recommendation 2 seeks the CFR to work with the financial sector and the OSS community as an enabler of the sound development and maintenance of Critical OSS.

This submission will refer to Recommendations 1 and 2 collectively as 'Recommendations'.

2. Rationale

The rationale for the Recommendations is two-fold. Firstly, OSS poses several risks to the operational resilience of APRA-regulated entities. Secondly, both Recommendations are synchronous with APRA's regulatory approach when it comes to cyber resilience, one of the 'longer-term objectives' of APRA's *2020-2024 Corporate Plan* as well as its *2020-2024 Cyber Security Strategy*.[6] These points will now be explained.

---

[5] Australian Cyber Security Centre, Commonwealth, *Information Security Manual* (Manual, September 2022) 103-7; Murugiah Souppaya, Karen Scarfone and Donna Dodson, National Institute of Standards and Technology, *Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities* (NIST Special Publication No SP 800-218, February 2022). To understand the security measures recommended by NIST for 'EO-Critical Software', see National Institute of Standards and Technology, United States, *Security Measures for "EO-Critical Software" Use under Executive Order (EO) 14028* (Document, 9 July 2021).

[6] Australian Prudential Regulation Authority, Commonwealth, *Corporate Plan: 2020/24* (Report, August 2020) 16 ('*APRA Corporate Plan'*); Geoff Summerhayes, Australian Prudential Regulation Authority, 'Strengthening the Chain' (Speech, Financial Services Assurance Forum, 26 November 2020) [5].

2.A. Risks from OSS for Operational Resilience

The risks from OSS for the operational resilience of APRA-regulated entities primarily stem from how pervasively deployed OSS is in modern computing, not just in technological systems that underpin the functioning of the Australian financial sector.[7] The European Commission captured this pervasiveness when introducing the European Union's OSS strategy:

> *Open source is present everywhere*… It powers the cloud and provides professional tools for big data and for information and knowledge management. It is in supercomputers, blockchain, the internet of things and artificial intelligence. It is in the internet. It is in our phones and our TVs… The chances are that, in any new project involving software, … most of the code will be based on open source.[8]

The United States Departments of Commerce and Homeland Security similarly wrote of the 'critical role [of OSS] in today's software ecosystem' and how modern computing displays a 'critical dependence on OSS libraries borrowed from third-party ecosystems'.[9] Out of 2,409 commercial codebases[10] across seventeen industries in 2021 that were surveyed by the software composition analysis firm, Synopsys, 97% of the number of codebases contained OSS and 78% of the content of the codebases was comprised of OSS.[11] All the codebases belonging to the categories, 'Computer Hardware and Semiconductors', 'Cybersecurity', 'Energy and Clean Tech' and 'Internet of Things', contained OSS.[12] The equivalent figure was 98% for codebases belonging to the 'Internet and Software Infrastructure' category.[13]

This saturated deployment of OSS — the 'reusable building blocks' of computing — is indeed a driver of the deep interconnectivity of our digital infrastructure.[14] Little wonder that OSS is

---

[7] See, eg, Chinmayi Sharma, 'Open-Source Security: How Digital Infrastructure Is Built on a House of Cards', *Lawfare* (Blog Post, 25 July 2022) [5] <https://www.lawfareblog.com/open-source-security-how-digital-infrastructure-built-house-cards>.

[8] European Commission, European Union, *Communication to the Commission: Open Source Software Strategy 2020-2023* (Communication No C(2020) 7149, 21 October 2020) 2.

[9] *ICT Supply Chains Report* (n 3) 36.

[10] A codebase is the 'code and associated libraries that make up an application or service': Synopsys, *2022 Open Source Security and Risk Analysis Report* (Report, 2022) 7 ('*Synopsys Report*').

[11] Ibid 4, 6.

[12] Ibid 8.

[13] Ibid.

[14] Cyber Safety Review Board, United States, *Review of the December 2021 Log4j Event* (Report, 11 July 2022) ii, iv ('*CSRB Report*').

accepted as having had a 'tremendous impact on the development and distribution of the software we depend on today' and that 'much of that software supply chain consists of [OSS]'.[15]

In this regard, vulnerabilities in OSS ought to be a major cause for concern for governments generally, not just individual regulators like APRA.

Firstly, malicious cyber actors can exploit vulnerabilities in OSS to cause harm across economic sectors and geographies. Given the entrenched dependencies of organisations — including software vendors and critical infrastructure asset operators — on OSS to deliver their business models, the exploitation of vulnerabilities in OSS can yield serious negative externalities, including the manifestation of systemic risk, for societies as a whole.[16] A recent example of said manifestation was the exploitation of a critical vulnerability in a ubiquitous piece of OSS called Log4j, which resulted in significant efforts across borders to develop a patch for the vulnerability and then assure the installation of the patch on systems running Log4j.[17] In general, the exploitation of vulnerabilities in OSS is enabled by the attractiveness of the (open source) software supply chain as an 'entry point for people and organizations interested in theft, disruption, or exploitation for economic or political gain'.[18] In providing attack vectors for malicious cyber actors seeking to access their networks, OSS and the software supply chains that it feeds into are thus major sources of operational risk for APRA-regulated entities, like all organisations that are dependent on digital technologies to operate.

Secondly, the risk of widespread harm from the exploitation of vulnerabilities in OSS is magnified by the sheer number of these vulnerabilities. The *Synopsys Report* found at least one vulnerability in 71% of the codebases examined and OSS which was more than four years out of date in 85%.[19] When broken down by sector, 64% of codebases belonging to the 'Internet of Things' category contained OSS vulnerabilities, 60% for 'Aerospace, Aviation, Automotive, Transportation, and Logistics', and 56% for 'Internet and Mobile Apps'.[20] It should thus come as no surprise that

---

[15] Stephen Hendrick and Martin Mckeay, *Addressing Cybersecurity Challenges in Open Source Software* (Report, 2022) 3.

[16] 'Open Source Supply, Demand, and Security', *Sonatype* (online report, 2022) [20] <https://www.sonatype.com/state-of-the-software-supply-chain/open-source-supply-demand-security> ('*Sonatype Report*'); Federal Financial Institutions Examination Council, United States, *Risk Management of Free and Open Source Software* (Financial Institution Letter No FIL-114-2004, 26 May 2005) [3] ('*FFIEC Letter*'). See also Sharma (n 7).

[17] *Sonatype Report* (n 16) [19]. For an explanation of the vulnerability in Log4j and the aftermath of its discovery, see the *CSRB Report* (n 14).

[18] Hendrick and Mckeay (n 15) 3.

[19] *Synopsys Report* (n 10) 6.

[20] Ibid 12.

the Cyber Safety Review Board ('CSRB') warned just in July: 'While the computing industry is maturing, our ability to handle risk and incidents in our digital ecosystems is not keeping pace'.[21]

Indeed, the very nature of the OSS community makes the occurrence of these vulnerabilities more likely. As Hendrick and Mckeay wrote in a report sponsored by The Linux Foundation and Open Source Security Foundation, 'The more loosely structured and community focused nature of OSS development presents a more challenging environment for addressing software security'.[22] The CSRB pointed to the 'thinly-resourced, volunteer-based open source community…[, which] is not adequately resourced to ensure that code is developed and maintained pursuant to industry-recognized secure coding practices and audited by experts'.[23] 30% of all OSS packages have one maintainer, though, 'in practice many have zero', which makes it ever more likely that those packages will have vulnerabilities in them and patches for those vulnerabilities will not be developed (expeditiously).[24] These factors make worldwide dependence on OSS a major liability for worldwide cyber resilience, and governments need to work towards ensuring that OSS developers and maintainers receive the resources they require for developing and maintaining OSS in line with best practice, which is core to Recommendation 2.[25]

In addition to upholding the need for APRA-regulated entities to recognise and tackle risks to their operational resilience from OSS, the Recommendations are backed by APRA's regulatory approach when it comes to the cyber resilience of the financial sector, which will now be explored.[26]

2.B. Intersection with APRA's Regulatory Approach for Cyber Resilience

Given the very real, pervasive risk to the cyber resilience of the financial sector from OSS (as per Section 2.A.), incentivising APRA-regulated entities to manage OSS-induced risk to their operational resilience would help meet one of the 'longer-term objectives' of the *APRA Corporate Plan* as well as APRA's *2020-24 Cyber Security Strategy*; especially when APRA made clear that it 'will seek to drive *significant* improvement in the Australian financial system's cyber resilience'.[27]

---

[21] *CSRB Report* (n 14) ii.

[22] Hendrick and Mckeay (n 15) 3.

[23] *CSRB Report* (n 14) v.

[24] Eric Brewer, 'The Consequence of Success: OSS is Critical Infrastructure' (Speech, Open Source Summit North America, 21 June 2022) 7.

[25] See, eg, *CSRB Report* (n 14) v, 25-6.

[26] *APRA Corporate Plan* (n 6) 16; Summerhayes (n 6) [5].

[27] *APRA Corporate Plan* (n 6) 16, 21 (emphasis added); Summerhayes (n 6) [5].

Mandating OSS risk management as well as working with the financial sector, under the leadership of the OSS community and through the CFR, to improve the overall hygiene of Critical OSS would certainly go towards achieving that goal, given that it would help: map out supply chain dependencies and vulnerabilities; and 'address weak links within the broader financial eco-system and supply chain'.[28] Given that OSS has not received specific attention in *CPS 234*, the Recommendations would also achieve APRA's objective of '[innovating] using impactful regulatory tools and approaches by… dialling-up supervision scrutiny and intensity'.[29]

Specifically requiring APRA-regulated entities to manage risks to their operational resilience from OSS, especially Critical OSS, would also be consonant with the requirements of *CPS 234*. As per Section 2.A., OSS can provide an attack vector for threat actors to leverage in compromising an APRA-regulated entity's information security, as defined by *CPS 234* s 12(e). Mitigating cyber risks borne from OSS is already required as part of an entity's 'information security capability' — as defined by *CPS 234* s 12(f) — because the capability must be 'commensurate with the size and extent of threats to its information security' as well as responsive to said threats.[30] The requirement for the entity to 'classify its information assets [defined by *CPS 234* s 12(d) to include software]… by criticality and sensitivity' would extend to OSS which is deployed directly by the entity.[31] The entity's obligation to implement controls for cyber resilience would also extend to safeguarding the hygiene of that OSS.[32] These factors reinforce the cogency of the Recommendations because said factors are directly taken from APRA's regulatory instrument on *cyber resilience*, *CPS 234*.

The alignment of the Recommendations with APRA's regulatory approach is also evident in the content of Prudential Practice Guide *CPG 234.*[33] Paragraph [40] flags cyber risks for APRA-regulated entities from 'software which is outdated or has limited or no support'. Given that several OSS projects are no longer maintained and/or are otherwise not subject to uniform, professional support from their developers in the same way as proprietary software (as described in Section 2.A.), there is a very real risk that APRA-regulated entities' information assets are running software which is outdated or not supported in an appropriate fashion. The warning of paragraph [40] of *CPG 234* is engaged in the context of risks to the cyber resilience, as well as operational resilience more generally, of entities from OSS. Therefore, APRA's expectations for

---

[28] *APRA Corporate Plan* (n 6) 22.

[29] Ibid.

[30] *CPS 234* (n 4) s 15.

[31] Ibid s 20.

[32] Ibid s 21.

[33] Australian Prudential Regulatory Authority, Commonwealth, *Prudential Practice Guide: CPG 234 Information Security* (June 2019) ('*CPG 234*').

how entities mitigate these risks — as communicated through paragraphs [41]-[43] of *CPG 234* — are to a great extent applicable to the management of risks from OSS. One should note, however, that paragraph [43] may not perfectly apply to mitigating risks from OSS because of the sheer criticality of certain OSS packages to the software which entities rely on to undertake their critical operations.[34] That reality actually strengthens the case for implementing Recommendation 2, including the call for APRA to work with partner regulators and the financial sector, and under the leadership of the OSS community, to uplift the hygiene of the development and maintenance of Critical OSS and assure that the deployment of Critical OSS in the sector is more robust and the subject of greater (regulatory) scrutiny.

The specific sections of *CPG 234* on 'software security' and 'end-user developed/configured software' are also applicable to OSS risk management, making clearer the alignment of the Recommendations with APRA's regulatory approach.[35] Several risks to the operational resilience of APRA-regulated entities are invited by failing to perform sufficient due diligence on OSS packages simply acquired via the Internet, not vetted vendor relationships, and incorporated by vendors or personnel of APRA-regulated entities into code running on the information assets operated by entities.[36] As a result, paragraphs [48]-[49] of *CPG 234*, concerning 'secure software development and acquisition', are engaged. As outlined in Section 1, one of the ways in which OSS packages are deployed in the computing environments of entities is via end-user configured software. Therefore, paragraphs [57]-[59] of *CPG 234* — that pertain to the management of risks to life-cycle management from end-user developed or configured software — are engaged.

Given these elements of *CPG 234* and the nature of (risks to the cyber and operational resilience of APRA-regulated entities from) OSS, Attachment D of *CPG 234* is also engaged. The thrust of Attachment D — the formal inclusion of cyber risk management 'throughout the software delivery life-cycle' — is aligned with the Recommendations.[37] Also relevant are the 'typical factors' for entities to consider when seeking to assure the '[o]ngoing security of existing software', including: the explicit identification of cyber resilience requirements for any software being used; testing of code procured from vendors (which can easily be applied to OSS); and having a concrete framework of standards and guidelines for secure software development.[38] Similarly, APRA's expectation that an entity 'maintain a register of approved software development tools and

---

[34] For an exploration of the most important OSS packages, see Frank Nagle et al, *Census II of Free and Open Source Software — Application Libraries* (Report, January 2022).

[35] *CPG 234* (n 33) [48]-[49], Attachment D.

[36] The Federal Financial Institutions Examination Council warns about such risks in the *FFIEC Letter* (n 16).

[37] *CPG 234* (n 33) Attachment D [1].

[38] Ibid Attachment D [2].

associated usage' easily applies to how the entity's personnel configure and incorporate OSS into the entity's information assets.[39] Therefore, the components of *CPG 234* that pertain to software hygiene make clear how the Recommendations represent a continuation of APRA's regulatory approach.

That the Recommendations are aligned with APRA's regulatory approach is also evident in the *Discussion Paper* and the proposed Prudential Standard themselves.

The inclusion of 'technology risk' in the definition of operational risk in the *Discussion Paper* highlights that APRA considers operational risk to include that which stems from OSS incorporated into proprietary software licensed by an APRA-regulated entity and/or configured by the entity to run directly on the entity's information assets.[40] The definition of operational resilience would capture the operation of controls for risk stemming from OSS.[41] APRA's reference to entities' 'increasing reliance on service providers', though a reliance on vendors of proprietary code, can arguably apply to OSS developers and maintainers, given the dependence of modern computing generally on OSS packages supported by the latter.[42] This is because entities and their vendors (almost always) do not develop these packages themselves, rather download them from the Internet (as above) and incorporate them into applications running on networks that entities use to deliver their critical operations.

As with vendors of proprietary code, 'problems in [OSS communities]… can quickly impact on the availability and level of service of an [entity]… with flow-on impacts to the broader financial system'.[43] Indeed, the extraordinary growth in the use of OSS packages 'is [also] giving rise to longer and more complex supply chains, often involving a reliance on fourth parties and other downstream providers', to borrow the language of the *Discussion Paper*.[44] This makes the Recommendations all the more important to implement, considering the already complex, long software supply chains that are serving APRA-regulated entities, as flagged in the *Discussion Paper*. Additionally, while the reliance on service providers and vendors of proprietary code is 'increasing', one should note that world computing — like digitalised financial services sectors — *continues* to be dependent on OSS as alluded to by Section 2.A..[45]

---

[39] Ibid Attachment D [3].

[40] *Discussion Paper* (n 1) 10.

[41] Ibid.

[42] Ibid 11.

[43] Ibid.

[44] Ibid; *Sonatype Report* (n 16) [6]-[7].

[45] *Discussion Paper* (n 1) 11.

Besides, APRA has stated that the proposed Prudential Standard reflects a 'principles-based approach with a focus on outcomes rather than process'.[46] Coupled with APRA's seeking to be innovative when it comes to policing the cyber resilience of its regulated population,[47] the Recommendations certainly follow a principles-based, outcomes-focused approach. They are directed at managing risks to the operational resilience of the financial sector from OSS, risks that have most likely never received explicit attention under Australian financial services law. The Recommendations envisage APRA following a flexible, non-prescriptive approach when it comes to supervision of management of OSS risks as well as assuring — in partnership with the financial sector and through the CFR, and under the leadership of the OSS community — that Critical OSS is developed and maintained appropriately.

Furthermore, the Recommendations are also synchronous with APRA's regulatory approach as disclosed by the proposed Prudential Standard.[48] APRA proposes that APRA-regulated entities: assess the impacts of new products on their operational risk profile (section 25); 'identify and document processes and resources needed to deliver critical operations, including… technology…' (section 26(b)) and 'maintain the capabilities required to execute [their business continuity plans]' (section 40).[49] Given the preceding analysis, *Draft CPS 230* would require entities to: monitor risk stemming from OSS, identify OSS packages that their personnel configure to be, or vendors incorporate into software which is, used in undertaking critical operations; and see to it that neither OSS vulnerabilities nor the deployment of OSS thwarts the ability of entities to implement business continuity plans. Indeed, critical operations, as defined by proposed section 34, would include the deployment of controls by entities to ensure the safe deployment of OSS, particularly Critical OSS, on their systems; certainly since the definition of critical operations is inclusive (section 35).[50]

Besides, APRA's intent to uplift the quality of cyber supply chain risk management in the financial sector is evident in proposed sections 46, 48, 52 that pertain to entities: 'maintain[ing] a comprehensive service provider management policy'; tracking their material service providers and '[managing] risks associated with using these [providers]'; and assessing risks from reliance with material service providers and reasonably 'assess[ing] whether the provider is systemically important in Australia', respectively.[51] Material service providers are proposed to be defined as

---

[46] Ibid 13.

[47] *APRA Corporate Plan* (n 6) 22.

[48] Australian Prudential Regulation Authority, Commonwealth, *Prudential Standard CPS 230: Operational Risk Management* (Draft Prudential Standard, July 2022) ('*Draft CPS 230*').

[49] Ibid 6, 9.

[50] Ibid 8.

[51] Ibid 9-11.

'those on which the entity relies to undertake a critical operation or that expose it to material operational risk' and may be third parties, related parties or connected entities (section 48).[52] *Conceptually* speaking at least, developers and maintainers of Critical OSS packages are material service providers. Similarly, the policy underpinning of proposed sections 46, 48 and 52 can be extended to the management of material operational risks stemming from the actions of the developers and maintainers of Critical OSS packages, certainly for packages on which software or services provided by other material service providers (such as vendors of security software or cloud service providers) are dependent. It could be argued that the developers and maintainers of Critical OSS packages are 'systemically important in Australia' because of the sheer (nested) dependence or dependencies of the financial sector on these pieces of software to function.[53]

Nonetheless, given the nature of the OSS community, as flagged in Section 2.A., the Recommendations do not propose that, *legally* speaking, developers and maintainers of Critical OSS packages be defined as material service providers. Rather, this submission calls on APRA — under the auspices of both Recommendations — to work with the financial sector and through the CFR, as well as under the leadership of the OSS community, to develop workable solutions that assure: the sound management of operational risks by APRA-regulated entities that stem from, or are otherwise affected by, their deployment of OSS; and the sound development and maintenance of Critical OSS.

Conclusion

This submission highlighted the need for APRA to act and thus the cogency of both Recommendations. It did so by pointing to the real risks to the operational resilience of APRA-regulated entities via their entrenched dependencies on OSS, be it as end-user configured or developed software, or through OSS incorporated into proprietary software which entities license from vendors. This submission also used APRA's own regulatory approach to make the case for APRA to implement both Recommendations.

I thank you again for the opportunity to make this submission.

Yours sincerely,

[redacted]

[redacted]

PhD Scholar at the University of Sydney

[52] Ibid 10.

[53] Ibid 11.