Bond University

Bond Law Review

Volume 37 Issue 1

2025

Complex Regimes – Regulatory Overlap in Australia's Cloud Services Sector

Susanne Lloyd - Jones
University of Technology Sydney

Kayleen Manwaring
University of New South Wales

Tyrone Berger
Monash University

COMPLEX REGIMES – REGULATORY OVERLAP IN AUSTRALIA'S CLOUD SERVICES SECTOR

SUSANNE LLOYD-JONES,* KAYLEEN MANWARING,◊ TYRONE BERGER∠

Abstract

Robust cyber security protection is essential to cloud services and government and private sector customers. In Australia, cloud services have undergone a significant regulatory reset, in part due to reforms to the critical infrastructure ('CI') legislative framework, including amendments to the Security of Critical Infrastructure Act 2018 (Cth) ('SOCI Act'). Shifts in industry practice, such as the increased uptake of cloud services by businesses and government agencies and the advent of new security threats, have accentuated these changes.

While Australian governments and regulators have implemented numerous legislative, policy, and guidance instruments to bolster cyber security measures, many of these attempts are not well-aligned. The outcome is an unclear and difficult-to-navigate regulatory ecosystem. We argue this complex regulatory landscape will likely result in increased costs, variable compliance, and decreased confidence in providing cyber security services unless careful attention is paid to mitigating the detrimental effects of 'regulatory overlap'.

This article identifies and critically examines key elements of existing statutory, regulatory and guidance instruments imposing cyber security and CI obligations on cloud services providers, as well as agencies and institutions holding key regulatory roles. These elements are examined in the context of cloud services providers subject to direct legal obligations, such as being responsible entities for CI assets and/or systems of national significance under the SOCI Act and other cloud services entities that form part of the supply chain for other providers with such obligations.

* PhD LLM LLB BEc (SocSci) (Hons) GD Legal Practice, Lecturer, Faculty of Law, University of Technology, Sydney. Dr Lloyd-Jones undertook most of her work on this piece during her appointment as a Cyber Security Cooperative Research Centre Postdoctoral Fellow, Faculty of Law & Justice, UNSW, 2021-2024.

◊ PhD LLM BA LLB (Hons) GD Legal Practice GD Communications, Associate Professor and Director of Undergraduate Studies (Law), Faculty of Law & Justice, UNSW.

∠ PhD JD BA BCom GD Legal Practice, Lecturer, Faculty of Law, Monash University.

I Introduction

Cloud services in Australia operate within multiple, complex, and evolving regulatory regimes. These intersecting sectoral and cross-sectoral regimes do not always provide industry participants and customers with certainty due to the array of statutory and contractual obligations, and policy and guidance frameworks, that do not always work well together. This situation is highly risky as the cloud services sector is uniquely positioned in Australia's cyber security landscape. Cloud platform businesses participate in every sector of the economy and have a national and international footprint. Moreover, cloud services providers have close relationships with government agencies, providing both business-as-usual services and strategic providers of specialised, confidential and/or secret services.[1] In this article, we examine a key barrier to effective governance of the Australian cloud services sector, 'regulatory overlap', from the perspective of cloud services providers. Regulatory overlap describes a situation where multiple regulatory frameworks interact over the same or similar aspects of cloud services, leading to potential conflicts or redundancies in regulation. This situation creates significant challenges for cloud services providers and their clients.

Appropriate regulation of the cloud services industry is vital in creating and maintaining resilient cyber security practices in Australia. Yet regulatory overlap can be found 'in virtually every sphere of social and economic regulation, in contexts ranging from border security to food safety to financial regulation'.[2] Our analysis demonstrates the extent to which the cloud services sector is subject to fragmented, overlapping, and sometimes conflicting regulation relating to data protection and critical infrastructure ('CI') assets. Multiple government agencies (federal and state) have issued guidance on cyber security management along with mandatory requirements when providing services to government. This practice has increased rather than reduced complexity. For cloud services providers, the complexity is compounded by additional or conflicting contractual obligations imposed by both customers and service providers.

The expansion of cloud computing has rapidly increased worldwide. Consequently, cloud services providers have emerged as a regulatory object in Australia,[3] the European Union ('EU'),[4] and the United States ('US').[5] While critical literature relating to cyber security regulation of the cloud services sector exists in other jurisdictions,[6] in Australia, the literature is sparse.[7] In light of this and the sector's complexity, we attempt to map and analyse the legal and regulatory environment from the perspective of cloud services providers, focusing on those engaged in Software as a Service ('SaaS'). We focus on SaaS because, as we outline in Section III(b) below, SaaS is the largest cloud services section of the market globally. Its place in the 'stack'[8] means it is especially prone to overlapping regulation. It operates more commonly as a third and fourth party in industry and business supply chains – a system of systems – for which there is limited transparency.[9]

The article focuses on three areas of inquiry: In what ways and to what extent is the current regulatory regime under the *Security of Critical Infrastructure Act 2018* (Cth) ('*SOCI Act*') inconsistent, overlapping or

---

1 See The Hon Anthony Albanese and The Hon Richard Marles, 'Australian Government partners with Amazon Web Services to bolster national defence and security' (Joint Media Release, 4 July 2024) <https://www.minister.defence.gov.au/media-releases/2024-07-04/australian-government-partners-amazon-web-services-bolster-national-defence-and-security>. See also Justin Hendry, 'Accenture lands $14m to Prep Defence for "Secret" Cloud', *InnovationAus* (Web Page, 17 March 2023) <www.innovationaus.com/accenture-lands-14m-to-prep-defence-for-secret-cloud>.

2 Jody Freeman and Jim Rossi, 'Agency Coordination in Shared Regulatory Space' (2012) 125(5) *Harvard Law Review* 1131, 1134-5.

3 Cloud services are a listed CI sector (as the 'data processing and storage' sector) under the *SOCI Act* with the potential for significant additional obligations in relation to cyber security practices and reporting.

4 See, eg, Mar Negreiro, 'The NIS2 Directive: A High Common Level of Cybersecurity in the EU' (European Parliament Briefing, February 2023) <www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf≥ discussing the Network and Information Security Directive 2.0 (NIS2) ; *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)* [2016] OJ L 119/1 ('GDPR').

5 See, eg, Cybersecurity & Infrastructure Security Agency, 'Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience', *Critical Infrastructure Sectors* (Web Page) <https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors>, which advances a national policy to strengthen and maintain secure, functioning, and resilient critical infrastructure.

6 See, eg, ibid; Paul T Jaeger, Jimmy Lin and Justin M Grimes, 'Cloud Computing and Information Policy: Computing in a Policy Cloud?' (2008) 5 *Journal of Information Technology & Politics* 269 (US); Kenji E Kushida, Jonathan Murray and John Zysman, 'Diffusing the Cloud: Cloud Computing and Implications for Public Policy' (2011) 11 *Journal of Industry, Competition and Trade* 209; Chris Reed, 'Governance in Cloud Computing' [2013] Queen Mary School of Law Legal Studies Research Paper No. 157/2013 <https://papers.ssrn.com/abstract=2353764>; Nir Kshetri, 'Blockchain's Roles in Strengthening Cybersecurity and Protecting Privacy' (2017) 41 *Telecommunications Policy* 1027, 1027-38.

7 See, eg, Rebecca Iglesias, Rob Nicholls, and Anisha Travis, 'Private Clouds with No Silver Lining: Legal Risk in Private Cloud Services' [2012] *Communications & Strategies* 125; Kim-Kwang Raymond Choo, 'Legal Issues in the Cloud' (2014) 1 *IEEE Cloud Computing* 94; George Yijun Tian, 'Cloud Computing and Cross-Border Transfer Pricing: Implications of Recent OECD and Australian Transfer Pricing Laws on Cloud Related Multinational Enterprises and Possible Solutions' (2018) 44 *Rutgers Computer & Technology Law Journal* 33.

8 See Figure 1.

9 See, Jennifer Cobbe, Chris Norval and Jatinder Singh, 'What Lies Beneath: Transparency in Online Service Supply Chains' (2020) 5(1) *Journal of Cyber Policy* 65, 66. Cobbe et al study market consolidation in online service supply chains, in which SaaS providers and cloud platforms operate, noting the lack of transparency in the supply chains (69) and that a failure in one infrastructural component of the supply chain can lead to problems affecting other components that rely on the failing infrastructure. The concentration of infrastructure providers, such as cloud platforms, means a failure will impact other entities operating in the supply chain and in the 'stack' (70).

duplicative? To what extent might any overlap, inconsistency and/or duplication be detrimental to the growth of the cloud sector in Australia? How can any such detriments be mitigated?

This article identifies broad instances of regulatory overlap in the cloud services sector, focusing on SaaS. Analysing the entire Australian regulatory landscape would not be feasible in a single article, so we have limited our analysis to the most critical areas of Commonwealth regulation of general application. However, due to Australia's federal system and the application of sector-specific and cross-sectoral regulation to cloud services, this would give an insufficient view of regulatory overlap. Therefore, we have also selected examples from two states (New South Wales ('NSW') and Queensland ('Qld')) and from two sectors, Energy (Electricity) and Financial Services.

The concept of regulation, at its broadest, is used to describe all forms of social, economic, and legal influence.[10] Freiberg, quoting Philip Selznick, notes that regulation is the 'means of bringing about some desired social outcome.'[11] Julia Black provides a detailed definition that encompasses the broad scope of regulation, defining it as the sustained and focused attempt to alter the behaviour of others according to defined standards and purposes with the intention of producing a broadly identified outcome or outcomes, which may involve mechanisms of standard-setting, information-gathering and behaviour modification.[12]

Regulation includes specific commands, as set out in legislation, or deliberate interventions by the State, such as taxes, subsidies or funding arrangements.[13] We use the term regulation to mean instances of specific state influence, including 'any rule endorsed by government where there is an expectation of compliance'.[14] Not only does this include legislation, regulations and other subordinate legislation, government procurement requirements, mandatory codes of practice, and guidance notes, it may also include governance arrangements, control of information and other techniques, such as collaboration and negotiation.[15]

Governance is an equally broad concept used to examine the role of the state and the role of institutions. It entails the use of mechanisms other than formal structures such as law, and hierarchies, such as those found in government portfolio departments, to make decisions or effect outcomes. Governance accounts for shifts in the style and order of governing.[16] It also encompasses the practice and processes for decision-making in economic, legal and regulatory settings. In this article, we use 'governance' to mean 'the systems, processes and institutions which govern, run, protect and regulate … activity.'[17]

In Part II, we begin by utilising a taxonomy developed by Robb, Candy, and Deane, that provides an identification framework for approaching regulatory overlap.[18] Additionally, we analyse and extend the existing literature on the harms caused by regulatory overlap. Part III provides an overview of the cloud services sector and the threat environment in Australia. Part IV maps the regulatory framework governing cyber security and CI, uncovering critical areas of overlap, duplication, inconsistency and a lack of clarity in the regulatory framework. Next, in Part V, we make some recommendations for reform and further research. Part VI concludes.

Regulatory failure in critical infrastructure protection is a serious problem because functioning CI underpins economic, societal and national security and stability. Regulation designed to uplift the security of critical infrastructure may be at risk of failing to meet its objectives due to regulatory overlap. Regulatory overlap creates regulatory burdens on regulated sectors. It may lead to non-compliance or weak compliance, increased complexity, overburdening critical infrastructure industries and their supply chains, and causing inefficiencies for businesses that operate in multiple jurisdictions, at a state, national and international level. This paper sheds light on the complexity and makes recommendations for reform and further research.

Due to the volume and complexity of the regulation and regulatory agencies at issue, we have used many abbreviations in this article: these are explained in the text when they first appear, but also additionally in a separate glossary.[19]

---

10 Robert Baldwin, Martin Cave and Martin Lodge, *Understanding Regulation – Theory, Strategy and Practice* (Oxford University Press, 2nd ed, 2012) 2-3.

11 Arie Freiberg, *Regulation in Australia* (Federation Press, 2017) 42.

12 Julia Black, 'Critical Reflections on Regulation' (2002) 27 *Australian Journal of Legal Philosophy* 1, 26 ('Critical Reflections').

13 Baldwin, Cave and Lodge (n 10) 3.

14 Department of the Prime Minister and Cabinet, 'User Guide to the Australian Government Guide to Regulatory Impact Analysis', *Resources* (Web Page, 09 June 2023) 3 <https://oia.pmc.gov.au/resources/guidance-impact-analysis/user-guide-australian-government-guide-regulatory-impact>.

15 Baldwin, Cave and Lodge (n 10) 3.

16 David Levi-Faur, 'From "Big Government" to "Big Governance" ' in David Levi-Faur (ed), *The Oxford Handbook of Governance* (Oxford University Press, 2012) 6, 7.

17 Australian Bureau of Statistics, 'Governance', *4160.0.55.001 - Frameworks for Australian Social Statistics* (Web Page, 24 June 2015) <www.abs.gov.au/ausstats/abs@.nsf/Lookup/by%20Subject/4160.0.55.001~Jun%202015~Main%20Features~Governance~10012>.

18 Lachlan Robb, Trent Candy and Felicity Deane, 'Regulatory Overlap: A Systematic Quantitative Literature Review' [2022] *Regulation & Governance* 15.

19 The glossary is available via the Australian Cyber Law Map at https://austlii.community/wiki/CyberLaw/AustralianCyberLawMap.

II 'Regulation in Many Rooms': Regulatory Space and Regulatory Overlap

Regulation exists because governments identify a problem that requires an intervention to minimise, mitigate or eliminate some kind of harm.[20]

Cloud services occupy a position in the national and global economy that traverses multiple sectors, jurisdictions and regulatory frameworks. A study of its regulation is an opportunity to reflect on the underlying rationale for regulation that affects the cloud services sector. Governments regulate for many reasons, including to solve problems, influence behaviours, manage risks and reduce harms.[21] Regulatory issues that governments seek to influence, steer or direct can be social, economic, criminal or concern harm or an impact on the national interest.[22] Regulation has many guises and is operationalised through a variety of methods and tools. It can be responsive or reflexive, direct or indirect, command and control or co-regulatory, self-regulatory or community driven. Regulation can be formal, informal, legally enforceable, voluntary or customary.[23] Koop and Lodge note that the language and tools of regulation are so prevalent nowadays that its operation and effectiveness has come under scrutiny.[24] Scrutiny has included concerns about compliance and overburdening businesses with regulation.[25]

An aspect of regulation that has come under sustained scrutiny is the phenomenon of 'regulatory overlap.' Theoretical and empirical studies of regulatory overlap sit within a broad body of literature about regulation and governance that has been the subject of inquiry and analysis for centuries.[26] Our discussion of regulatory overlap and governance begins in modern times with the origins of the concept of 'regulatory space', which provides an entry point for the study of regulatory overlap in complex systems such as the cloud services sector. The cloud services sector emerged at a time when deep structural changes had already occurred in the organisation of the state and its institutions.[27] Since the beginnings of economic liberalism, privatisation and deregulation in the late 1980s and 1990s, many regulatory theorists posited that state-based regulation was 'decentring' or 'fragmenting'.[28] According to Julia Black, decentring regulation means that regulation is diffused through society. It points to the fact that governments are not the sole regulators, and that regulation is happening among various social actors, including large organisations, associations, technical committees and professions, at times without government involvement or approval, and 'in many rooms'.[29]

Traditional regulation, such as command and control regulation, envisages and encompasses a 'centred state', which is the 'counter point of decentred regulation'.[30] Decentred regulation invokes the concept of fragmentation in a regulatory context. In this setting, power is dispersed between actors, agencies, institutions and the state.[31] In the context of a fragmented and decentred regulatory state, many scholars have explored complexity by studying instances of regulatory overlap, fragmentation and duplication in what Freeman and Rossi call 'shared regulatory space'.[32] Shared regulatory space is an analytical construct that describes a situation where multiple agencies or institutions have overlapping jurisdictions and responsibilities.[33] Hancher and Moran note that in complex, interdependent processes and practices, the concept of regulatory space highlights not just the participants in regulation, but also the structural elements that help form and develop networks, leading to institutionalised connections.[34] By starting with the nature of these links, it allows for a systematic comparison of their characteristics across various industrial sectors and national contexts.[35]

---

20 House of Representatives Standing Committee on Economics, Parliament of Australia, *Better Competition, Better Prices Report on the Inquiry into Promoting Economic Dynamism, Competition and Business Formation* (Report, March 2024) 62.

21 Freiberg (n 11) 47-62.

22 John Braithwaite, 'Neoliberalism or Regulatory Capitalism' *Occasional Paper 5* (Australian National University Regulatory Institutions Network, 2005); Black, 'Critical Reflections' (n 12).

23 Baldwin, Cave and Lodge (n 10).

24 Cristel Koop and Martin Lodge, 'What Is Regulation? An Interdisciplinary Concept Analysis' (2017) 11(1) *Regulation & Governance* 95, 95-96.

25 See, eg, Justin Douglas and Amy Land Pejoska, *Regulation and Small Business* (Treasury Paper, March 2019) <https://treasury.gov.au/sites/default/files/2019-03/p2017-t213722-Roundup_Sml_bus_regulation-final.pdf>.

26 Baldwin, Cave and Lodge (n 10) 4.

27 For a historical perspective on the structural reforms to Australia and other states, see: Witold Henisz, Bennet Zelner and Mauro Guillen, 'The Worldwide Diffusion of Market-oriented Infrastructure Reform, 1977-1999' (2005) 70(6) *American Sociological Review* 871, 873-4; Chris Berg, *The Growth of Australia's Regulatory State: Ideology, Accountability and the Mega-Regulators* (Institute of Public Affairs, 2008) 4-8; Braithwaite (n 22).

28 Mark Leiser and Andrew Murray, 'The Role of Non-State Actors and Institutions in the Governance of New and Emerging Digital Technologies' in Roger Brownsword (ed), *The Oxford Handbook of Law, Regulation and Technology* (Oxford University Press, 2016) 674.

29 Julia Black, 'Decentring Regulation: Understanding the Role of Regulation and Self-Regulation in a "Post-Regulatory" World' (2001) 54 *Current Legal Problems* 103 ('Decentring Regulation').

30 Black, 'Critical Reflections' (n 12).

31 Ibid 6.

32 Freeman and Rossi (n 2).

33 Bronwen Morgan and Karen Yeung, *An Introduction to Law and Regulation: Text and Materials* (Cambridge University Press, 2007) 59-68.

34 Leigh Hancher and Michael Moran, 'Organizing Regulatory Space', in Robert Baldwin, Colin Scott, and Christopher Hood (eds), *A Reader on Regulation*, Oxford Readings in Socio-Legal Studies (Oxford University Press, 8 October 1998).

35 Ibid.

The cloud services sector is a highly regulated sector and at greater risk of regulatory overlap than other sectors of the economy due to its underpinning of much economic activity and its increasing ubiquity in Australian business operations in sectoral and cross-sectoral contexts.

The discussion that follows traces regulatory overlap in the cloud services sector and is informed by the theoretical foundation that the regulatory environment in which cloud services operate is fragmented and decentred. The regulatory spaces in which cloud services conduct business are influenced by a wide range of legal, economic and technological factors.

Regulatory overlap has been identified as: substantive and functional overlap, inter- and intra-governmental overlap, duplicative regulation, inconsistent obligations, multiple departments and regulators, 'gaps', uncertainty, and/or redundancy.[36] Regulatory overlap has also been usefully conceptualised into three categories: 'fragmentation', 'duplication', and 'true' overlap.[37] Fragmentation occurs when one or more entities are involved in the same area of regulation; duplication when one or more agencies are engaged in the same activities or services or are seeking to address the same concern; and true overlap when multiple agencies or programs have similar goals, or engage in similar activities, or have the same or similar objective.

In 2022, Robb, Candy, and Deane published the results of a systematic review examining 327 articles on regulatory overlap spanning 2010-21.[38] The authors identified the most prevalent harms arising from regulatory overlap as: uncertainty, departmental problems, inconsistency, increased costs, worse outcomes, regulatory undermining, poor business outcomes, regulatory gaming, time wastage, and international inconsistency.[39] However, this investigation (and others) concluded that regulatory overlap could also be beneficial in some instances.[40] For instance, Aagaard argued that overlap can provide useful positive redundancy and can operate effectively with the proper cooperation, coordination, and collaboration practices.[41] Freeman and Rossi describe regulatory overlap as 'shared regulatory space', arguing that it is more nuanced and capable of providing benefits and even protections against an agency's failure, if well-managed.[42] Furthermore, some scholars consider that regulatory overlap is inevitable: for example, in a federal structure, such as the US and Australia; or due to the way a particular system administers legal problems or fields and allocates regulatory responsibility.[43]

As part of their review, Robb, Candy, and Deane developed a helpful taxonomy ('the 2022 Taxonomy') for classifying regulatory overlap.[44] The 2022 Taxonomy allows for the classification and analysis of overlap through three tiers:

1. *Orientation*. Overlap is *vertical* (arises among various levels of government) or *horizontal* (arises among the same level of government, eg Federal agencies and departments).
2. *Cause*. Causes of overlap may be *action*-based (such as a piece of legislation delegating powers and authority) and/or *evolved* (eg discretion in the exercise of a regulatory power). An action cause occurs when 'a specific type of action created the overlap'[45] – eg a new piece of legislation, such as the *SOCI Act*. An evolved cause comes from 'a gradual process [where] system or policies shifted over time… that is, fluid subject matters, changes in customs or norms, or new technologies.'[46]
3. *Focus*. Whether the overlap pertains to laws or departments, suggesting a distinction between overlap in legal rules and in bureaucratic governance of specific issues or problems.

We adopted the 2022 Taxonomy to assist us in evaluating the results of our examination of the regulatory framework in the cloud services sector. It allowed us to observe emerging trends and provided a structured approach to identifying problems arising from regulatory overlap.

The cloud services sector provides a fertile case study in regulatory overlap. Our analysis in Part IV identifies broad instances of regulatory overlap in the cloud sector's regulatory environment that map to the 2022 Taxonomy. Also, as regulation applicable to cloud services appears in both sector-specific and cross-sectoral forms, we were able to observe *additional* dimensions that have allowed us to expand on the 2022

---

36 See Robb, Candy, and Deane (n 18).

37 Jeremy Straughter and Kathleen Carley, 'Toward a Network Theory of Regulatory Burden' (2021) 6(70) *Applied Network Science* 1, 2.

38 Robb, Candy, and Deane (n 18) 16.

39 See, eg, ibid 7-8; Todd S Aagaard, 'Regulatory Overlap, Overlapping Legal Fields, and Statutory Discontinuities' (2011) 29(3) *Virginia Environmental Law Journal* 237; Freeman and Rossi (n 2) 1137-8; Alejandro Camacho and Robert Glicksman, 'Functional Government in 3-D: A Framework for Evaluating Allocations of Government Authority' (2014) 51(1) *Harvard Journal on Legislation* 19, 71.

40 Robb, Candy, and Deane (n 18) 11.

41 Aagaard (n 39) 241.

42 Freeman and Rossi (n 2) 1137.

43 Aagaard (n 39); Freeman and Rossi (n 2) 1136. See also Robb, Candy, and Deane (n 18) 11.

44 Robb, Candy, and Deane (n 18) 15.

45 Ibid 18.

46 Ibid.

Taxonomy. For instance, while *orientation* in the 2022 Taxonomy is visualised along two axes, the vertical and horizontal, our research indicates that regulatory overlap in the cloud services sector has a *multi-dimensional* orientation, due to the impact of the source of regulation on both the vertical and horizontal axes.

In Australia, identifying conflicts between, and gaps arising from, federal-state (*vertical* orientation), or state-state/federal-federal (*horizontal*) institutions and rules is important. For instance, in the cloud sector, there may be multiple sources of regulation not only at federal and state levels but also from sector-specific and cross-sectoral sources, and these can be critical in identifying any regulatory overlap. In our discussion, we label these sources of regulation the *direction* of the regulation, which is as important as the distinct jurisdictional space it occupies. Identifying 'directional' overlap invites the use of a navigation metaphor, which provides an opportunity to engage with the multidirectional nature of regulation in the cloud sector. The compass with its broad orientation of north, south, east and west can accommodate nuanced navigation, such as north-east, north-west, south-east, south-west. Directional overlap comprises not only vertical (north-south, denoting hierarchical government) and horizontal overlap (east west, denoting same level government, eg state-state or federal), but also sectoral sources of regulation (eg north-east, north-west) and cross-sectoral sources of regulation (eg south-east, south-west).

Thinking about regulatory overlap through a 'compass' lens allowed us to 'point the needle' to explain more accurately the sources of regulatory overlap for the cloud services sector. As cloud services are used in multiple CI sectors, relevant regulation is multidirectional. For example, it originates from sectoral sources (eg energy-, water-, transport- or finance-specific regulation) and cross-sectoral regulation (eg foreign investment, corporations, critical infrastructure and cyber security), and this regulation emanates from both federal and state jurisdictions. Not only is the cloud services sector impacted by state-federal regulation and its combinations identified by Robb, Candy and Deane, the sector also experiences overlap in those dimensions from sectoral and cross-sectoral regulation (which may be state or federal or both). We added our further dimension to the 2022 taxonomy to identify and explain the sectoral and cross-sectoral regulation within the concept of regulatory overlap.

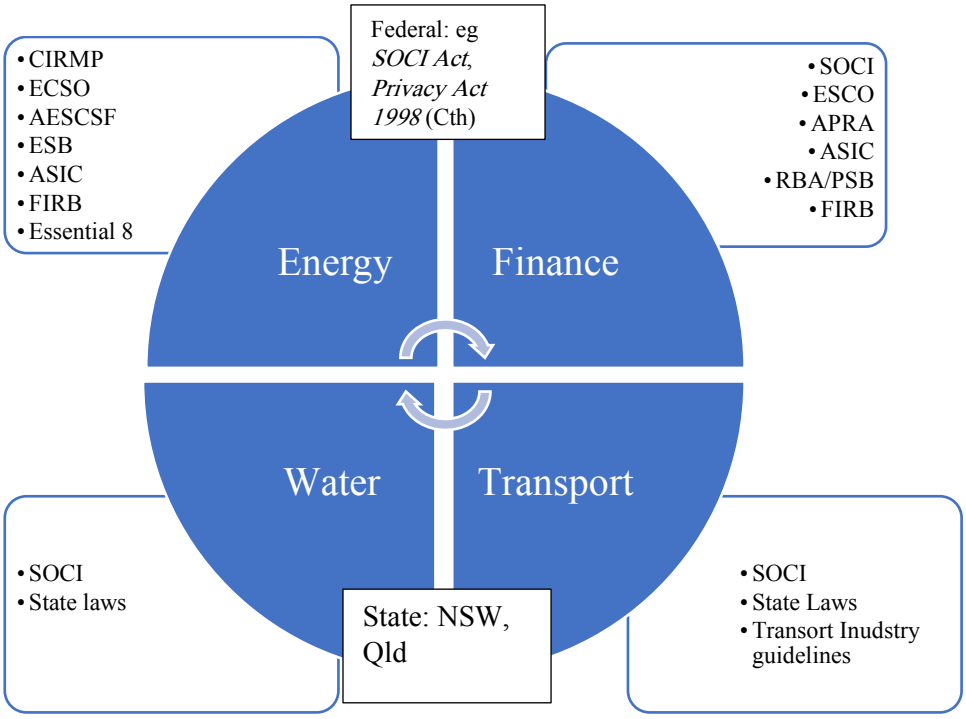
Based on the insights from the case study, we suggest the following additions to the 2022 Taxonomy, marked in *italics*:

Table 1: adaptation of the 2022 Taxonomy to include additional dimensions of regulatory overlap that we discerned from our empirical work on cloud regulation in Australia.

Taxonomy	Dimensions	Definition
Orientation	Vertical	Overlap exists due to actions between regulatory bodies on different levels of a governance hierarchy.
	Horizontal	Overlap occurs due to laws or governance on the same level of a governance hierarchy.
	Directional	*Overlap that occurs because of the source or 'direction" of regulation on the vertical and horizontal axes (eg, CI entities in the energy sector experience directional overlap from the AESCSF and other areas of regulation impacting the sector, in addition to cross-sectoral regulation).*
Cause	Action	Regulatory overlap is directly linked to an action of government (eg *SOCI Act*).
	Evolved	Regulatory overlap exists because of activities or issues that have evolved from substantive, delegated or discretionary authority, delegations, and functions (eg the Australian Energy Sector Cyber Security Framework ('AESCSF') is an example of discretionary sector-specific activity on cyber security).
Focus	Legal field/law	Classification of the regulatory overlap as having a legal focus.
	Departmental	Classification of regulatory overlap as having a governance focus, eg department or agency.
	Sector-Specific	*Classification of regulatory overlap as having sector-specific focus, eg energy regulation.*
	Cross-Sectoral	*Classification of overlap as having a cross-sectoral focus, eg corporations regulation.*

Based on the explanation above, Figure One depicts multidirectional regulation in the cloud services sector:

Figure 1: Orientation of CI Sectors. Vertical axis represents Federal-State government hierarchy, horizontal is State/State or Federal/Federal. The segments represent CI sectors and attempts to identify 'directional' overlap by listing different regulation that applies to the sector.



III Cloud Computing in Australia

Australia's cloud services sector is growing significantly.[47] While the shift to greater use of cloud services may deliver benefits, the experience from other countries indicates that the greater uptake will also introduce new risks and dependencies. David and Walden note that when multiple functions are performed by interconnected networks, services, systems and devices, instances of weakness increase and risks of malicious attack are heightened.[48] In response, the Australian Government has expanded the scope of the *SOCI Act* to apply to the 'data storage or data processing' industry, which includes cloud computing services and SaaS providers.[49] The newly imposed obligations on cloud services providers add to existing significant ad hoc regulation and guidance at state,[50] federal[51] and international levels.[52]

The *SOCI Act* adds to the existing security-related regulation of cloud providers, which include, inter alia, general obligations under the *Privacy Act 1988* (Cth) ('*Privacy Act*') to take reasonable steps to keep personal information secure,[53] obligations under Parts 14 and 15 of the *Telecommunications Act 1997* (Cth)

---

47 Tom Raynel, 'Australian Public Cloud Spending to Exceed AUD $23.3 Billion', *TelcoNews Australia* (Web Page, 20 May 2024) <https://telconews.com.au/story/australian-public-cloud-spending-to-exceed-aud-23-3-billion>: 'The largest segment of growth within this forecasted increase… is expected in infrastructure-as-a-service (IaaS), with a remarkable 24.5% rise. Following closely is platform-as-a-service (PaaS), which is predicted to grow by 22.4%. Software-as-a-service (SaaS) holds its position as the largest spending category, projected to reach nearly AUD $11 billion in 2024, up 18.3% from 2023'.

48 Johan David and Ian Walden, 'Cybersecurity, Cloud and Critical Infrastructure' in Christopher Millard (ed), *Cloud Computing Law* (Oxford University Press, 2nd ed, 2021) 382.

49 See, eg, *Security of Critical Infrastructure Act 2018* (Cth) ss 8D(b), 8E(3), 12F.

50 See, eg, NSW Government, *NSW Cyber Security Policy* (V5, January 2022) <www.digital.nsw.gov.au/sites/default/files/NSW-Cyber-Security-Policy-2021-2022.pdf> ('*NSWCSP*').

51 See, eg, Attorney-General's Department (Cth), *Protective Security Policy Framework (PSPF)*<www.protectivesecurity.gov.au>; Australian Signals Directorate (Cth), *Information Security Manual*, <www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism>. Australian Energy Market Operator, *Australian Energy Sector Cyber Security Framework and Resources* (19 April) <www.aemo.com.au/en/initiatives/major-programs/cyber-security/aescsf-framework-and-resources> ('AESCSF'); Australian Prudential Regulatory Authority, *Prudential Standard CPS 234 Information Security* (*APRA*, July 2019) <www.apra.gov.au/sites/default/files/cps_234_july_2019_for_public_release.pdf>.

52 See, eg, 'National Institute of Standards and Technology', *US Department of Commerce* (Web Page, 1 June 2023) <www.nist.gov>; ' International Organization for Standardization', *ISO* (Web Page, 28 April 2023) <www.iso.org/home.html>.

53 *Privacy Act 1998* (Cth) sch 1 s 11.

('*Telecommunications Act*') to provide assistance and access,[54] cyber security requirements (including compliance with international standards) imposed by government agencies and commercial businesses on third-party service providers, and guidance documents issued by various government agencies and regulators.[55]

A *Cloud Computing*

Cloud services are used widely across many sectors of the Australian economy, including for state and federal government agencies, and in newly designated CI industries, including communications (encompassing broadcasting and telecommunication), financial services, energy and transport.[56] What, then, is meant by the term 'cloud computing'? Hon, Millard and Singh discuss its various characteristics and uses in a recent UK work.[57] Their *simplest* definition is '[c]loud computing is a way of delivering computing resources as a utility service via a network, typically the internet, and generally scalable up or down according to user requirements.'[58]

In Australia, the Cyber Security Cooperative Research Centre ('CSCRC') adopted[59] the US's National Institute of Standards and Technology ('NIST') definition in a 2021 report outlining the operation of the cloud services sector: a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (eg, networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.[60]

The *SOCI Act* provides a general, descriptive definition. Rather than referring to cloud services, it uses the term 'data storage or processing provider', meaning an entity providing a 'data storage or processing service': that is, a service that enables end-users to store or back-up data; or a data processing service.[61] The services typically offered by cloud services providers to their individual, business and government customers are shown below and are usually referred to as layers in a 'stack':

---

54 Part 14 of the TA concerns national interest matters and applies to carriers, carriage service providers and carriage service intermediaries. Not all cloud services will be considered a relevant service provider for the purposes of the TA. Part 14 requires carriers, carriage service providers and carriage service intermediaries to 'do their best' to protect telecommunications networks and facilities from, inter alia, unauthorised interference or unauthorised access for the purpose of security. This includes a requirement on carriers and carriage service providers to maintain 'competent supervision' and 'effective control' over telecommunications networks and facilities owned or operated by the relevant entity. Part 15 of the TA concerns industry assistance to law enforcement and security agencies and access to communications. It covers *designated communications providers*. Some businesses in the cloud services sector are considered designated communications providers for the purposes of section 317C of Part 15. For examples of designated communications providers, see, Department of Home Affairs, *The Assistance and Access Act - An Interim Guide for: Security, Intelligence and Law Enforcement* (26 July 2019, documents released under the *Freedom of Information Act 1982* (Cth), FA 19/06/00892). If an entity is a designated communications provider for the purposes of Part 15, that entity must cooperate with law enforcement and national security agencies when those agencies request or require assistance to access communications and data held by those entities.

55 See, eg, Australian Cyber Security Centre (Cth), *Essential Eight* (Web page) <www.cyber.gov.au/acsc/view-all-content/essential-eight≥.

56 Deloitte Access Economics, *The economic value of cloud services in Australia* (Report, July 2019) <www2.deloitte.com/content/dam/Deloitte/au/Documents/Economics/deloitte-au-economics-value-cloud-services-australia-230719.pdf> 6.

57 W Kuan Hon, Christopher Millard, and Jatinder Singh, 'Cloud Technologies and Services' in Millard (ed), *Cloud Computing Law* (Oxford University Press, 2nd ed, 2021) ch 1.

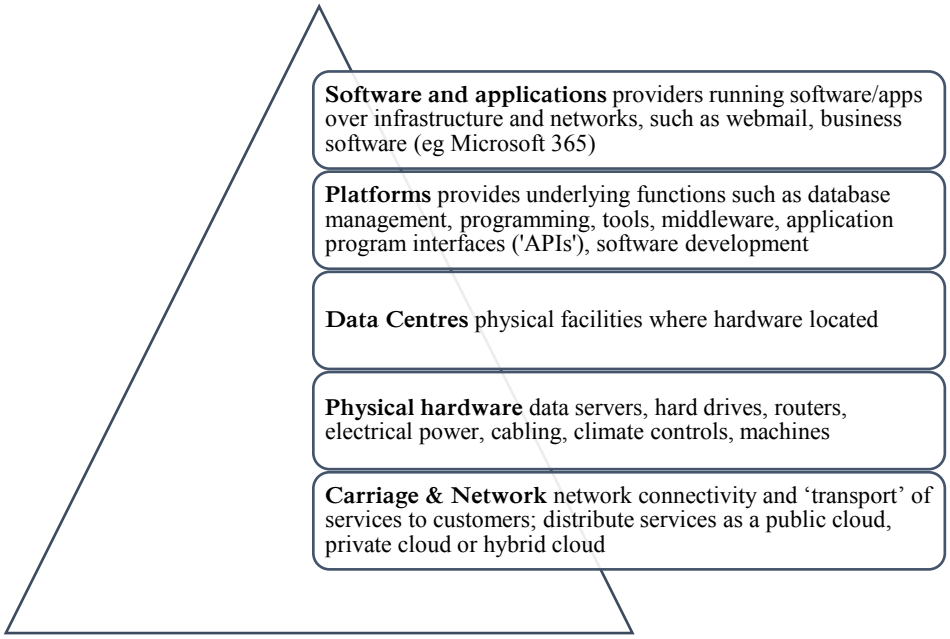
58 Ibid 4.

59 Cyber Security Cooperative Research Centre ('CSCRC') and SAP, *Cloud Control: What the Cloud is, What it does and How it can be Securely Adopted* (Report, 2 December 2021) 4 <https://cybersecuritycrc.org.au/sites/default/files/2021-12/CSCRC-Cloud-Control-Paper-2021.pdf>. The CSCRC provides research on the cyber ecosystem and cyber threats through collaborations between industry, government, and academia.

60 National Institute of Standards and Technology, 'Cloud Computing*', Computer Security Resource Center* (Web Page, 10 December 2021) <https://csrc.nist.gov/projects/cloud-computing>.

61 See *SOCI Act* (Cth) s 6.

Figure 2: Cloud Services Stack



The structure of the cloud services industry is traditionally expressed as encompassing three distinct, but at times overlapping, service models[62] namely:

1. Infrastructure as a Service ('IaaS');[63];
2. Platform as a Service ('PaaS');[64] and
3. Software as a Service (SaaS) (defined below).

However, the business and services models for an individual entity or corporate group do not necessarily fit within these categories. For example, some businesses, such as *hyperscalers* and *aggregators* (eg Google Cloud, AWS, Azure), provide their customers with multiple sets or all these service models in some cases. Other cloud services providers 'often depend… on complex, multilayered arrangements between various cloud providers'.[65] This variety and complexity in the business models of cloud service providers makes it challenging to keep track of the regulatory requirements that may apply to those services.

B *Software as a Service (SaaS)*

SaaS comprises the largest cloud services segment globally, with end-user expenditure predicted to reach US$247.2 billion in 2024, a growth of 20% from the previous year.[66] In Australia, the end-user cost is estimated to exceed $10.9 billion.[67] SaaS is a cloud services model that runs atop the cloud infrastructure provided at the lower levels of the 'cloud stack.' SaaS, also known as a 'software cloud,'[68] is commonly defined as an application hosted by a cloud vendor and delivered as a distributed service to users over the internet or a dedicated network.[69] It usually provides customers with:

> [t]he capability … to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (eg web-based email), or a

62 Cyber Security Cooperative Research Centre and SAP (n 59) 5.

63 Infrastructure as a Service ('IaaS') is defined as 'the capability … to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g, host firewalls).': Peter Mell and Tim Grance, *The NIST Definition of Cloud Computing* (NIST Special Publication 800-145, September 2011) 3.

64 Ibid 2-3: Platform as a Service ('PaaS') can be defined as 'the capability … to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.'

65 Hon, Millard, and Singh (n 57) 4.

66 'Gartner Forecasts Worldwide Public Cloud End-User Spending to Surpass $675 Billion in 2024', *Gartner* (Press Release, 20 May 2024) <https://www.gartner.com/en/newsroom/press-releases/2024-05-20-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-surpass-675-billion-in-2024>.

67 Andrew Starc, 'Australia Public Cloud Spend to Hit $23.3B in 2024', *CRN: Connecting the Australian Channel* (Web Page, 20 May 2024) <https://www.crn.com.au/news/australian-public-cloud-spend-to-hit-233b-in-2024-gartner-608107>.

68 Sam Murugesan and Irena Bojanova (eds), *Encyclopedia of Cloud Computing* (Wiley - IEEE Press, 2016) 6.

69 Ibid.

> program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, except for limited user-specific application configuration settings.[70]

SaaS providers run their services over networks and use hardware such as a physical server for storage and processing. However, SaaS providers may subcontract some or all these services from one or multiple platform and cloud infrastructure providers. Maintenance, upgrades, patches, and other activities associated with the software are undertaken by the service provider, not the end-user.[71] In this scenario, the end-user has no control over the network, servers, operating systems, storage, or individual application capabilities beyond what is set up in their SaaS agreement. For example, a customer may have strict requirements for the servers' location[72] but no day-to-day operational control.[73] Examples of SaaS include webmail services, applications, accounting software, payroll management, and customer relations management software. Running concurrently with SaaS are a range of cloud support services that can be built into or enhance existing SaaS. This typically includes cloud support services such as data storage, analytics, security, identity and access management, monitoring, and desktop support.[74]

Therefore, the range of SaaS can be broad, from simple aggregation to complex enterprise resource planning and customer relationship management systems. The industry's major service providers in Australia are Atlassian, Microsoft, Google, Oracle, and Salesforce.[75] While issues of overlap are also likely to arise regarding IaaS and PaaS models, examining those contexts is beyond this article's scope.

C *Cyber Security Threat Environment*

The cloud services sector faces significant challenges relating to cyber security due to several factors, including the increased uptake of cloud services by businesses and governments. Emerging technologies like the Internet of Things and quantum computing add to an already complicated mix. Additionally, more immediate threats such as terrorism, cybercrime, and foreign interference are wide-ranging and vary in frequency and sophistication.[76] However, unique risks apply to SaaS and its architecture due to shared resources, multiple network and system links and a loss of 'hands-on control of systems, applications, data security, and other resources.'[77] Amongst the threats associated with SaaS are a loss of control or misuse of resources,[78] different delivery models, insecure interfaces, malicious actors, data scavenging,[79] service hijacking,[80] risk profiling, and identity theft.[81] Consequently, the role of SaaS in assuring cyber security for clients is increasing in prominence.[82] The evolving threat environment has driven perceptions of the need for better cyber security in the cloud services sector, given its expanding role in providing infrastructure, platforms, and services for the digital economy and government.[83]

Moreover, cloud supply chains operate in a complex system of interconnected and interdependent services, platforms, networks, and systems. If supply chains are compromised, the business entity may be unable to source essential goods and services for day-to-day operations. For instance, all cloud services providers – at any level of the stack – rely on energy supply to conduct business. Similarly, all cloud providers rely on communications infrastructure providers to provide carriage of data and communications, and the

---

70 Mell and Grance (n 63) 2.

71 Ibid.

72 For example, to comply with a European Commission 'adequacy decision' as to which countries outside the EU offer an adequate level of data protection. See *GDPR* (n 4).

73 Murugesan and Bojanova (n 68) 6.

74 Ibid 7.

75 For further discussion of consolidation in the online services sector, including an indication of the 50 most frequent interactions with third-party domains, see Cobbe, Norval and Singh (n 9) 76.

76 World Economic Forum, *The Global Risks Report 2022* (Report, 11 January 2022) 45-56 <www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf>; see also Cyber and Infrastructure Security Centre, *Risk Assessment Advisory for Critical Infrastructure: Data Storage and Processing Sector* (*Department of Home Affairs, Commonwealth of Australia*, 2023) <www.cisc.gov.au/critical-infrastructure-centre-subsite/Files/raa-data-storage-or-processing.pdf>.

77 Murugesan and Bojanova (n 68) 220.

78 See, eg, such as in the Optus data breach in 2022. See David Kolevski et al, 'Cloud computing data breaches in news media: Disclosure of personal and sensitive data' (2022) *IEEE International Symposium on Technology and Society* 1.

79 Data scavenging refers to the practice of '[t]he collection of information from recovered bits of data': Muhammad Imran Iftikhar, Abdul Azia Ghazi and Muhammad Irfan Khan, 'Security Problems Analysis Private Cloud Computing vs Public Cloud Computing in Giant Organisations' (2018) 179(10) *International Journal of Computer Applications* 12, 13.

80 This refers to the theft of user credentials which 'can be used to access and compromise cloud services': Muhammed Kazim and Shao Ying Zhu, 'A survey on top security threats in cloud computing' (2015) 6(3) *International Journal of Advanced Computer Science and Applications* 109, 110.

81 Miguel Ángel Díaz de León Guillén, Víctor Morales-Rocha and Luis Felipe Fernández Martínez, 'A Systematic Review of Security Threats and Countermeasures in SaaS' (2020) 28 *Journal of Computer Security* 635.

82 Mamoona Humayun et al, 'Software-as-a-Service Security Challenges and Best Practices: A Multivocal Literature Review' (2022) 12(8) *Applied Sciences* 3953, 2-7.

83 Ibid.

interconnection, interoperability, and continuity of those services. Other aspects of the supply chain may include freight for hardware delivery and other physical parts. The importance of supply chain resilience was recently demonstrated during the global supply chain disruptions associated with the COVID-19 pandemic[84] and the Ukraine-Russia conflict.

The structure of the cloud services sector, the length of supply chains and the multiplicity of threats and hazards work together to create a complex, multi-faceted operating environment for the sector. In the next section, we provide a map of the regulatory environment, including responsible government agencies and institutions, and an overview of the volume of applicable laws and regulations, policies, and other guidance instruments.

IV Map of the Regulatory Environment

A *Responsible Agencies and Institutions*

An examination of the regulatory framework governing cyber security and CI in relation to cloud services reveals multiple instances of multidirectional regulatory overlap. This section outlines the responsibilities of government agencies, regulators, and other institutions involved in cyber security regulation along horizontal, vertical, and directional orientations.[85] Governments and regulators collaborate and cooperate through various mechanisms, including inter-governmental committees,[86] industry advisory committees,[87] formal legislative processes,[88] and memoranda of understanding ('MoUs') for specific purposes.[89] The primary Commonwealth departments and associated regulators responsible for cyber security-related regulation are listed in Table 2.

*Table 2: Cyber security departments and regulators. *Sector-specific regulators for the energy and financial services sectors.*

Responsible department	Sub-agency/regulator
Department of Prime Minister and Cabinet	Whole of government national security and intelligence policy co-ordination, including cyber security
Department of Defence	Australian Signals Directorate ('ASD')
	Australian Cyber Security Centre ('ACSC')
Attorney-General's Department	Australian Federal Police ('AFP')
	Australian Security Intelligence Organisation ('ASIO')
	Office of the Australian Information Commissioner ('OAIC')
	Australian Criminal Intelligence Commission ('ACIC')
Department of Home Affairs	Cyber and Infrastructure Security Group[90] ('CISG')
	National Cyber Security Coordinator[91] ('NCSC')
	National Office of Cyber Security[92] ('NOCS')
	Cyber and Infrastructure Security Centre ('CISC')
Finance	Digital Transformation Agency ('DTA')
Foreign Affairs	Ambassador for Cyber Affairs and Technology

84 Tarek Sultan, '5 ways the COVID-19 pandemic has changed the supply chain', *World Economic Forum* (Blog post, 14 January 2022) <www.weforum.org/agenda/2022/01/5-ways-the-covid-19-pandemic-has-changed-the-supply-chain/>.

85 See, eg, the Energy Security Board ('ESB') and Australian Prudential Regulation Authority ('APRA') both administer sector-specific cyber security frameworks.

86 For example the 'National Cyber Security Committee ('NCSC') provides a platform for detailed engagement and collaboration between the Commonwealth and state and territory governments on cyber security issues' Australian Signals Directorate, *Annual Report 2019-2020* (Report, 12 October 2020) 25 <www.asd.gov.au/sites/default/files/2022-03/asd-annual-report-2019-20.pdf>.

87 See, eg, Department of Home Affairs, 'Expert Advisory Board appointed as Development of New Cyber Security Strategy begins' (*Media Release*, 8 December 2022) <https://minister.homeaffairs.gov.au/ClareONeil/Pages/expert-advisory-board-appointed-as-development.aspx>.

88 The Australian Signals Directorate ('ASD') is an authorised agency under s 5 *SOCI Act*. It can be directed to take specified action under the *SOCI Act*. See, eg, *SOCI Act* pt 3A – Responding to Serious Cyber Incidents.

89 See, eg, Australian Communications and Media Authority, 'Memorandum of Understanding for the Australian Cyber Security Centre and the ACMA' (Web Page, 11 November 2021) <www.acma.gov.au/publications/2021-10/plan/memorandum-understanding-australian-cyber-security-centre-and-acma>; Australian Energy Regulator, 'Agreements & MOUs' (Web Page) <www.aer.gov.au/about-us/agreements-mous>.

90 Michael Pezzullo, 'Home Affairs Cyber and Infrastructure Security Conference' (Media Release, 24 March 2023): <www.homeaffairs.gov.au/news-media/speeches/2023/24-march-home-affairs-cyber-and-infrastructure-security-conference>.

91 Clare O'Neil, 'Cyber Security Roundtable Press Conference' (Press Conference, 27 February 2023) <https://minister.homeaffairs.gov.au/ClareONeil/Pages/cyber-security-coordinator-27022022.aspx>; Department of Home Affairs, Cyber Coordinator <https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/cyber-coordinator>.

92 'Cyber Coordinator', *Department of Home Affairs* (Web Page) <https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/cyber-coordinator>.

	International Cyber and Critical Technology Engagement Strategy[93] (ICCTES)
	Cyber and Critical Tech Cooperation Program[94] ('CCTCP')
Treasury	Australian Competition and Consumer Commission
	*Australian Energy Regulator ('AER')
	*Energy Security Board ('ESB')
	*Australian Securities and Investment Commission ('ASIC')
	*Australian Prudential Regulatory Authority ('APRA')
	Foreign Investment Review Board ('FIRB')

At least on a governance level, the Australian federal government collaborates with the states and territories on matters of national significance under the *Australian Government Crisis Management Framework* ('AGCMF').[95] The AGCMF outlines the government's approach to crisis management and incorporates inter-jurisdictional and inter-governmental arrangements. Where there is a cyber security element, the *Cyber Incident Management Arrangements* will operate.[96] In addition, the Joint Cyber Security Centres ('JCSC') coordinate dependencies between the Australian, state and territory levels of government on cyber security, from incident response to cross-jurisdictional coordination in the event of a national cyber incident.[97]

The states and territories also have government departments and independent regulators who conduct similar or identical functions to the Commonwealth Government. For instance, in NSW there is the NSW Department of Customer Service, which is responsible for Cyber Security NSW; and in Queensland there is the Queensland Government Cyber Security Unit.

B *Applicable Laws, Regulations and Policies*

The breadth of regulation surrounding cyber security in Australia is complex. Our research indicates that this complexity results in multidirectional regulatory overlap. This overlap occurs in inter-governmental and intra-governmental settings, national and international standards, and in private and public sector contractual arrangements. Intensifying the multi-dimensional nature of regulatory overlap in this environment, contractual obligations remain significant in delivering cloud services in Australia. Consequently, the ACSC recommends that cloud services customers set cyber security expectations in contracts and other binding contractual arrangements, including MoUs.[98]Accordingly, regulatory provisions and guidance that do not directly apply to the cloud services provider may nevertheless be imposed as a contractual obligation.[99] Contractual terms may conflict with statutory and other regulations, policies and guidance in areas such as incident response provisions.[100] In this section, we first discuss regulation that applies broadly across the economy and then provide examples of how it applies in two particular sectors: energy and financial services. We briefly discuss the rationale behind the regulation that applies to cloud services.

---

93 'Cyber Security – Our Partners, Foreign Affairs', *Department of Home Affairs* (Web Page) <https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/our-partners>.

94 Cyber Affairs and Critical Technology, *Department of Foreign Affairs* (Web Page) <https://www.internationalcybertech.gov.au/>.

95 Department of Prime Minister and Cabinet, *Australian Government Crisis Management Framework* (Version 3.3, September 2023, Australian Government); includes the addition of the Cyber Incident Annex.

96 Australian Cyber Security Centre, 'Cyber Incident Management Arrangements for Australian Governments', *Australian Signals Directorate* (Web Page, 18 September 2023) <www.cyber.gov.au/resources-business-and-government/governance-and-user-education/governance/cyber-incident-management-arrangements-australian-governments>.

97 The JCSCs are part of the ACSC's partnership program. For more information, see Australian Cyber Security Centre, 'Australian Signals Directorate's Cyber Security Partnership Program', *Australian Signals Directorate* (Web Page) <https://www.cyber.gov.au/partnershipprogram>.

98 See generally, Australian Cyber Security Centre, 'Cloud Security Considerations', *Australian Signals Directorate* (Web Page, 6 October 2021) <https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/cloud-security-guidance/cloud-computing-security-considerations>; Australian Cyber Security Centre, 'Cyber Supply Chain Risk Management', *Australian Signals Directorate* (Web Page, 22 May 2023) <www.cyber.gov.au/acsc/view-all-content/publications/cyber-supply-chain-risk-management>.

99 See, eg, para 13.1.1, of the Digital Transformation Agency, 'Digital Sourcing Contract Templates' (*Australian Government, BuyICT*, 10 August 2023) <https://www.buyict.gov.au/sp?id=resources_and_policies&kb=KB0010684&kb_parent=KB0010686> and <https://www.buyict.gov.au/sys_attachment.do?sys_id=6c0e5eb1dbe8f11008439517f39619c1>.

100 See, eg, Digital Transformation Agency, 'Cloud Sourcing Contract Template' (*Australian Government,* Template, December 2020) s 13.1.1.1 (j)

1 *Cross-sector regulation*

(a) Critical infrastructure regulation and cloud services

In 2018, the *SOCI Act* was introduced and later significantly amended in 2021[101] and 2022[102] ('the 2021/22 amendments') to include the primary Federal obligations on designated critical infrastructure industries responsible for declared CI assets. The government's underlying rationale for the 'whole-of-economy' approach to critical infrastructure regulation was to uplift the extant regulatory framework, considered to be inadequate to mitigate and manage the increasingly complex threats, hazards and harms experienced by critical infrastructure sectors and assets globally.[103] The mix of regulatory instruments, obligations and tools found in the *SOCI Act* reflects its hybrid approach to critical infrastructure regulation.[104] The tools of the *SOCI Act* include registration of CI assets, reporting of cyber incidents, risk management, information gathering and incident response. The regulatory powers of enforcement in the Act reflect a graduated approach to enforcement and are governed by the *Regulatory Powers (Standard Provisions) Act 2014* (Cth).[105]

In this context of uplifting critical infrastructure regulation to include both sectors and assets, CI assets are assets considered 'essential to the functioning of the economy, society, or national security' of Australia.[106] The *SOCI Act* established a register of CI assets and instituted rulemaking, declaration, and prescription powers by the Minister for Home Affairs. Since 2016, successive governments have strengthened the regulatory regime surrounding CI assets and all transactions involving them. Notably, the 2021/22 amendments expanded the coverage of the *SOCI Act* beyond its original application (to the electricity, gas, water, and maritime port sectors) to apply to additional regulated industry sectors, including data storage or processing ('DSoP'), communications, financial services, and energy, as well as many other sectors. The extension of the *SOCI Act* to apply to the DSoP sector (covering many cloud services) provides an obvious example of 'action overlap' from the 2022 Taxonomy.

The *SOCI Act* contains extensive statutory obligations relating to CI assets.[107] Operators of CI assets must report to the government's Register of Critical Infrastructure Assets on ownership and control, as well as other operational information, such as location and responsible entity.[108] Additional obligations under the 2021/22 amendments included:

- obligations on the operator to:
  - notify cyber incidents impacting CI assets to the ASD;[109]
  - notify their DSoP providers they are managing 'business critical data';[110] and
  - establish, maintain, and comply with a written risk management program; [111] and
- the ability of the government to:
  - in the case of some cyber-attacks, require the responsible entity to provide information, take or refrain from taking action, and/or authorise the ASD to intervene to defend the asset;[112] and
  - declare certain CI assets as 'Systems of National Significance' ('SoNS'), subjecting the responsible entity to enhanced cyber security obligations, such as incidence response plans, cyber security exercises, and government access to system information and undertake cyber security exercises[113]

DSoP is unique among CI sectors as the only sector designated critical due to its status as part of other sectors' supply chains. For example, a cloud services provider may combine hardware and/or SaaS from different suppliers. The cloud services provider may be a hyperscaler, for example, Microsoft Azure, and thus offer

---

101 *Security Legislation Amendment (Critical Infrastructure) Act 2021* (Cth); *Security of Critical Infrastructure (Definitions) Rules (LIN 21/039) 2021* (Cth).

102 *Security Legislation Amendment (Critical Infrastructure Protection) Act 2022* (Cth); Security of Critical Infrastructure (Application) Rules (LIN 22/026) 2022.

103 Department of Home Affairs, *Regulation Impact Statement* (OBPR Reference Number 25902, 2020) 5-6.

104 For a discussion of hybrid regulatory approaches, see Michiel Heldeweg, 'Hybrid regulation as a Legal Design Challenge' in *Derde NILG jaarcongres 2011: voorbij de tweedeling tussen publiekrecht en privaatrecht?* (Eleven International Publishing, 2013) 107-39.

105 *Security of Critical Infrastructure Act 2018* (Cth) s 4 – simplified outline of the Act.

106 Gilbert + Tobin, 'A Guide to Critical Infrastructure Assets in Australia' (Web Page, 2022) <www.gtlaw.com.au/knowledge/guide-critical-infrastructure-assets-australia>. The definition of 'CI assets' in s 9 of *Security of Critical Infrastructure Act 2018* (Cth) does not define this term generally, but by reference to industry assets.

107 The asset definitions are set out in *SOCI Act* s 12F and the *Security of Critical Infrastructure (Definitions) Rules (LIN 21/039) 2021* (Cth) ('CIRMP Rules').

108 *SOCI Act* pt 2 Register of Critical Infrastructure Assets and 12L (definition of 'responsible entity').

109 Ibid pt 2B.

110 Ibid s 12F.

111 Ibid pt 2A.

112 Ibid pt 2B.

113 Ibid pts 6A, 2C.

different hardware and software services to varying layers of the 'stack.' As a result of this complexity, it falls to the cloud providers to secure their supply contracts, which also form a secure component of another sector's supply chain. Therefore, SaaS providers may attract direct statutory obligations under the *SOCI Act*, and/or contractual obligations imposed by other CI asset operators. A further example of regulatory overlap involves the *Foreign Acquisitions and Takeovers Act 1975* (Cth), recently amended by the *Foreign Investment Reform (Protecting Australia's National Security) Act 2020* (Cth) to include important *SOCI Act* definitions. Any foreign investment in a responsible entity under the *SOCI Act* or direct interest in a CI asset is now subject to notification to the Foreign Investment and Review Board ('FIRB'), which can undertake its own motion review of transactions if it has national security concerns.[114] Finally, any changes in ownership and control, including personnel, may impact a SaaS provider's eligibility to provide government services.[115]

In addition, several other Commonwealth legislative frameworks demonstrating multi-dimensional regulatory overlap may apply to one or more cloud services providers operating at various levels of the stack, including private clouds.[116] The following list is not exhaustive[117] but highlights the most significant instances where regulatory overlap occurs.

(b) Data protection

Cross-sectoral overlap occurs around data and data protection. The stated rationale for regulation in Australia's key data protection legislation is 'to promote the protection of the privacy of individuals.'[118] SaaS providers that are Australian Privacy Principles ('APP') entities are directly obliged under the *Privacy Act* to keep 'personal information' secure from misuse, interference and loss, as well as from unauthorised access, modification, or disclosure (the 'Security Principle').[119] APP entities include private sector organisations with an annual turnover in excess of AUD 3 million, as well as all Commonwealth contractors, which brings many SaaS providers within the scope of privacy laws. The *Privacy Act* also imposes obligations to report certain data breaches to the Office of the Australian Information Commissioner ('OAIC') and those subject to the breach. In response to recent high-profile cyber-attacks,[120] legislative reforms have increased the maximum pecuniary penalties for serious or repeated breaches of the Security Principle (and other obligations).[121] Further proposed changes contemplate a widening of privacy protections affecting the obligations of cloud providers.[122] Furthermore, under EU data protection regulation, cloud providers dealing with the data of EU citizens (even if situated outside the EU) must 'implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk'.[123]

(c) Directors' duties

Directors' duties have a long history in business administration and company law. The rationale for the regulation of company directors in Australia is to provide incentives for the managers of companies to run those enterprises in a way that maximises value for shareholders.[124] Section 180 of the *Corporations Act 2001*

---

114 For more details, see Foreign Investment Review Board, 'Guidance Note 8 - National Security Test' (Guide, 17 December 2020) <https://firb.gov.au/sites/firb.gov.au/files/guidance-notes/G08-Nationalsecurity.pdf>.

115 See, eg, PSPF – Policy 6 and ISM for requirements and risks regarding foreign ownership and control of a responsible entity, and foreign personnel, and how it may impact the authority to operate or gain access to the market.

116 See, eg, Rebecca Iglesias, Rob Nicholls and Anisha Travis, 'Private Clouds with No Silver Lining: Legal Risk in Private Cloud Services' (2012) 85(1) *Digiworld Economic Journal* 125.

117 There are other areas that may impact cyber security eg consumer guarantees under the Australian Consumer Law, *Competition and Consumer Act 2012* (Cth) sch 2 Part 3-2 Div 1. See David Lindsay, Genevieve Wilkinson and Evana Wright, 'Responding to the Challenges of Consumer Internet of Things Devices: The Case for Reforming the Australian Consumer Guarantees' (2022) 29 *Competition and Consumer Law Journal* 226 pt V. Also, there are Commonwealth, state, and territory offences for crimes committed by either a cloud customer or by the cloud provider, including computer intrusions, unauthorised data modification, denial of service attacks, creation and distribution of malicious software, dishonestly obtaining or dealing in personal or financial information. Note that while the state and territory legislation covers similar ground to the Commonwealth, drafting differs in each jurisdiction. See *Criminal Code Act 1995* (Cth) sch 1 pts 10.6-10.8; *Crimes Act 1958* (Vic) ss 247A–I; *Crimes Act 1900* (NSW) pt 6 ss 308–308I; *Summary Offences Act 1953* (SA) s 44; *Criminal Code 2002* (ACT) ss 412–21; *Criminal Code Compilation Act 1913* (WA) s 440A; *Criminal Code 1899* (Qld) s 408E; *Criminal Code Act 1924* (Tas) sch 1, ss 257A-F.

118 *Privacy Act 1988* (Cth) s 2A.

119 For example, *Privacy Act 1988* (Cth) sch 1 APP 11.1.

120 Such as the Optus, Medibank and MyDeal cyber-attacks: Attorney-General Mark Dreyfus, 'Second Reading Speech, Privacy Legislation Amendment (Enforcement and Other Measures Bill 2022' (Speech, House Hansard), 26 October 2022) <https://parlinfo.aph.gov.au/parlInfo/genpdf/chamber/hansardr/26227/0016/hansard_frag.pdf;fileType=application%2Fpdf>.

121 *Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022* (Cth).

122 Attorney-General's Department, *Privacy Act Review Report 2022* (Report, 16 February 2023) 23-46, 52-92 <www.ag.gov.au/rights-and-protections/publications/privacy-act-review-report> particularly proposal groups 4 (changes to the definition of personal information) 6, 7, 8 and 9 (amendments to exemptions).

123 *GDPR* (n 4) art 32.

124 Commonwealth of Australia, 'Directors' Duties and Corporate Governance: Facilitating innovation and protecting investors' (*Corporate Law Economic Reform Program Proposals for Reform: Paper No 3*, 1997) <https://treasury.gov.au/sites/default/files/2019-03/full-13.pdf>.

(Cth) ('*Corporations Act*') imposes a duty of care and diligence on *all* company directors. Scholars consider this duty to extend to ensuring the corporation has reasonable cyber security protections for customer data.[125] Listed companies are also subject to the Australian Securities Exchange ('ASX') Corporate Governance Principles and Recommendations, which require the board of directors or a committee of the board to review its risk management framework annually and satisfy itself that it 'deals adequately' with risks, including cyber security, privacy, and data breaches, or provide a public explanation as to why they have not complied with this recommendation.[126] ASIC, a cross-sectoral regulator, has been active in litigating,[127] researching and educating directors about their duties and responsibilities around cyber security risks and cyber resilience, including outlining best practice and issuing guidance notes.[128]

(d) Telecommunications assistance, interception and access

Telecommunications services are regulated in Australia under the *Telecommunications Act*, a legislative regime introduced to facilitate competition, consumer protection and access in the telecommunications market.[129] Rapid technological change and market liberalisation created the conditions for transforming the industry's regulation from a sole monopoly provider to a competitive, multi-service provider market.[130] Cloud services providers deliver their services using telecommunications networks and services. They may operate in the telecommunications sector and have telecommunications clients. In addition, some carriers offer cloud storage and other cloud services.[131] In addition to rules applying to carriers, carriage service providers, and content service providers generally, the telecommunications sector security reforms, including access and assistance requirements, imposed security-related obligations on telecommunications service providers that could potentially apply to certain cloud services providers.[132]

Whether a cloud services provider is captured by one or more of the service provider definitions in the *Telecommunications Act* will depend on the products and services it offers. For example, cloud services providers offering data storage will most likely not be considered a carriage service provider for the purposes of the *Telecommunications Act* but may be considered a designated communications provider under the *Telecommunications Act* pt 15. Part 15 concerns industry assistance obligations for the purpose of safeguarding national security, protecting Australia's foreign relations and economic well-being, and assisting with law enforcement.[133] Some businesses in the cloud services sector are considered designated communications providers for the purposes of pt 15 s 317C. The Department of Home Affairs has explicitly listed cloud services, including SaaS providers, as designated communications providers in its guidance materials.[134]

Telecommunications assistance, interception and access has a long legislative history. The rationale for regulating interception of telecommunications was initially to protect the privacy of communications.[135] However, the *Telecommunications Act* now operates as a lawful access and assistance regime for law enforcement and security agencies to obtain access to communications and data.[136] Under the *Telecommunications (Interception and Access) Act 1979* (Cth), law enforcement and security agencies can request reasonable assistance, including decryption and technical assistance, to access data within the cloud or the metadata associated with access to the cloud. These obligations may be incompatible with service provider

---

125 James Duffy, 'How Should Directors Tackle Cyber Risks?' (2018) 46(2) *Australian Business Law Review* 134; Kayleen Manwaring and Pamela Hanrahan, 'BEARing Responsibility for Cyber Security in Australian Financial Institutions: The Rising Tide of Directors' Personal Liability' (2019) 30 *Journal of Banking and Finance Law and Practice* 20.

126 ASX Corporate Governance Council, 'Corporate Governance Principles and Recommendations' (4th ed, February 2019) Recommendation 7.2.

127 Australian Securities and Investment Commission, 'Court finds RI Advice failed to adequately manage cybersecurity risks' (5 May 2022, *Media Release* 22-104MR).

128 See Cyber Resilience, *Australian Securities and Investment Commission* (Web Page) <https://asic.gov.au/regulatory-resources/corporate-governance/cyber-resilience/>.

129 Holly Raiche, 'The Policy Context' in Alasdair Grant (ed) *Australian Telecommunications Regulation* (UNSW Press, 3rd ed, 1997) 1, 1-2.

130 Ibid 1.

131 Australian Communications and Media Authority, 'Communications and Media in Australia - Trends and developments in telecommunications 2020–21' (Report, December 2021) 24 <www.acma.gov.au/sites/default/files/2021-12/Trends%20and%20developments%20in%20telecommunications%202020-21_0.pdf>.

132 See *Telecommunications and Other Legislation Amendment Act 2017* (Cth) and *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth); see also, *Telecommunications Act 1997* (Cth) s 127; Department of Communications, *Cloud Computing Regulator Stock Take* (Report Version No 1, May 2014) 28 <www.infrastructure.gov.au/sites/default/files/Cloud_Computing_Regulatory_Stock_Take_-_May_2014.pdf>.

133 *Telecommunications Act 1997* (Cth) pt 15, s 317A.

134 See, Department of Home Affairs, *The Assistance and Access Act - An interim guide for: Security, Intelligence and Law Enforcement* (26 July 2019, documents released under the *Freedom of Information Act 1982* (Cth), FA 19/06/00892).

135 *Telecommunications Interception Act 1960* (Cth).

136 See Dennis Richardson AC, *Comprehensive Review of the Legal Framework of the National Intelligence Community: Volume I* (Australian Government Report, December 2019); Anthony Blunn, *Review of the Regulation of Access to Communications* (Australian Government Report, August 2005).

efforts to secure the cloud with strong encryption systems designed to protect against interception and access.[137] Cloud services providers, depending on their status under the *Telecommunications Act*, may be the subject of warrants and authorisations for access to information directly, in addition to other warrant regimes, such as search warrants of premises owned and operated by cloud services providers.[138]

2 *Sector-specific regulation examples*

Regulation of economic sectors in the Australian economy is underpinned by economy-wide competition policy reforms that have been ongoing since the deregulation and privatisation of government utilities from the 1970s onwards.[139] Industries that were deregulated during this time include financial services, telecommunications, transport, and energy.[140] Many critical infrastructure sectors have continued to be reformed to improve competition and consumer protection. Cyber security regulation is a recent addition to the regulatory landscape on account of the evolving threat landscape, and interconnectedness of critical infrastructure sectors as technology has advanced. Cloud services providers operate across different sectors of the economy. As a result, it is possible for a single SaaS provider to supply its services to multiple regulated sectors governed by separate legislation and regulatory frameworks. Cloud services providers delivering their services in Australia will encounter several sector-specific frameworks (in addition to the *SOCI Act*) potentially requiring direct compliance or obligations passed on through service agreements. The following sections consider developments in the regulated sectors of relevance to the cloud services sector.

(a) Energy (electricity)

The energy sector is one of the key sector-specific sources of multidirectional regulatory overlap. The Commonwealth-level cyber security framework for the electricity sector is the Australian Energy Sector Cyber Security Framework ('AESCSF'), providing an example of evolved overlap, because the framework derives from regulatory action in response to changing circumstances.[141] The AESCSF was developed in response to the Finkel National Electricity Review recommendation 2.10 in 2018 by the Australian Energy Market Operator ('AEMO') with energy industry stakeholders, prior to the *SOCI Act* reforms.[142] This framework provides a structure for assessing cyber security 'maturity' across the Australian energy sector, including gas, electricity grids, and markets. Maturity in a cyber security context means an organisation's ability to respond to and defend itself against a cyber-attack orchestrated by malicious actors. Maturity levels operate to describe what level of protection an organisation should aim to achieve and the practices it needs in place to achieve cyber security. Cloud services intersect with maturity frameworks such as the AESCSF through their customers and their own energy needs. This means that cloud service providers supplying goods and services to the Australian energy sector will have multiple cyber security compliance obligations to fulfil either contractually or under statute or both. Due to regulatory overlap, the compliance obligations may not be the same or consistent. For example, multinational cloud service providers may have standardised their cyber security systems and processes according to European rather than US standards. Additionally, AESCSF obligations may arise in a service contract between the cloud services provider and a member of the energy sector.

The AESCSF is based on the US Department of Energy's *Cybersecurity Capability Maturity Model* and is recognised as an equivalent cyber security framework under the *SOCI Act*.[143] The AESCSF is in line with Australian regulations and guidance, such as the Australian Privacy Principles and the Australian Government Information Security Manual ('ISM'),[144] the ACSC Essential 8 Strategies to Mitigate Cyber Security Incidents, the APPs, and the Notifiable Data Breaches ('NDB') scheme. While sector-specific rules, such as those related

---

137 For a discussion of the issues and possible solutions, Carnegie Endowment for International Peace, *Moving the Encryption Policy Conversation Forward* (Working Group Report, 10 September 2019) <https://carnegieendowment.org/2019/09/10/moving-%20encryption-%20policy-%20conversation-forward-pub-79573>.

138 For example, the Commonwealth search warrant provision is found in s 3E of the *Crimes Act 1914* (Cth). However, specific search warrants exist in many other legislative frameworks, including the *Customs Act 1901* (Cth) and the *ASIC Act 2001* (Cth), in addition to State and Territory laws.

139 Justin Douglas, 'Deregulation in Australia', *Economic Round-up 2014* (Treasury Paper, 2014) 56 <https://treasury.gov.au/sites/default/files/2019-03/04_Douglas.pdf>.

140 Laura Berger-Thomson, John Breusch and Louise Lilley, *Australia's Experience with Economic Reform* (Treasury Working Paper, October 2018) 5.

141 Ibid.

142 Australian Energy Market Operator, 'Australian Energy Sector Cyber Security Framework' (Web Page) <https://aemo.com.au/en/initiatives/major-programs/cyber-security>.

143 For example, the AESCSF references: US Department of Energy's Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2); National Institute of Standards and Technology Cyber Security Framework (NIST CSF) and Global best-practice control standards (eg ISO/IEC 27001, NIST SP 800-53, COBIT).

144 Australian Cyber Security Centre, 'Information Security Manual' (2 March 2023) <www.cyber.gov.au/sites/default/files/2023-03/Information%20Security%20Manual%20-%20%28March%202023%29.pdf>.

to metering under national electricity law, may not directly apply to cloud services providers, certain obligations could still be passed on to them through their service contracts.

The above example highlights the complexity of a cloud service providers operating environment. It is an environment where multiple national and international regulatory frameworks are operating. The burden falls on the cloud services provider to meet its statutory and contractual obligations as best it can. In practice, compliance is a business practice that is supported with policies, systems and processes to ensure that the company adheres to the relevant standards, rules and laws with which it must comply.

Energy Sector Case Study

The energy sector is subject to multidirectional regulation. From the perspective of cloud services providers, this creates challenges for managing their businesses across multiple sectors. For example, SaaS providers may be required to comply with the Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023 ('CIRMP Rules'). The CIRMP Rules state a minimum sector requirement for responsible entities for CI assets in the energy sector is compliance with Security Profile 1 of the AESCSF.[145] Security Profile 1 is the lowest level of maturity under the AESCF. The AESCSF contains multiple Security Profiles and corresponding Maturity Indicator Levels, which are used together as measures of an energy sector participant's cyber security capability, its practices and level of development.[146] The challenge for cloud providers is managing the potential gap between what the law requires of it and what its clients expect – especially if the client is a 'high criticality participant' under the AESCSF[147] and is aiming to achieve Security Profile that is higher than the profile specified in the CIRMP. A high criticality participant is an entity that has been assessed by the Australian Energy Market Operator under the AESCSF Electricity Criticality Assessment Tool. Examples of high criticality participants include electricity generators, transmission network service providers, distribution network operators and market operators. Criticality is assessed using a scale model and includes factors such as the goods or services a participant provides, the regions it covers.[148] Adding to the complexity, the energy sector connects to the financial markets and services sector through the market mechanisms for energy trading. This presents another layer of compliance with a different cyber security framework, APRA's CPS 234. Additionally, Australian and international standards operate within each sector. Finally, sector participant licence conditions may introduce additional security obligations.[149]

(b) Financial services

The financial services sector provides another example of sector-specific regulatory overlap for the cloud services sector. Australian financial services licensees ('AFSLs') attract obligations under ss 912A(1)(a) and (h) of the *Corporations Act* to do all things necessary to ensure that financial services are provided efficiently and fairly and to have 'adequate risk management systems.' In 2022, the Federal Court found for the first time that an AFSL had breached its licence by having inadequate cyber security risk management in place.[150] Resulting orders included appointing an external cyber security expert to report to ASIC on further measures and implementation outcomes.[151]

---

145 *CIRMP Rules* s 8(4)(b).

146 Australian Energy Market Operator, 'Australian Energy Sector Cyber Security Framework Overview' (Framework, 2022) 7 <https://aemo.com.au/-/media/files/initiatives/cyber-security/aescsf/aescsf-framework-overview.pdf?la=en>.

147 Ibid 9 [1.5].

148 See Australian Energy Market Operator, Australian Energy Sector Cyber Security Framework Electricity Criticality Assessment Tool (Guideline, 2023 AESCSF Program) 4-5 <https://aemo.com.au/-/media/files/initiatives/cyber-security/aescsf/2023/aescsf-electricity-criticality-assessment-tool-ecat.pdf?la=en>.

149 For example, see CI licence conditions in Distributors Licence from Minister for Industry, Resources and Energy to Ausgrid Operator Partnership (*IPART*, 25 June 2015) 8 <www.ipart.nsw.gov.au/sites/default/files/documents/ausgrid-distributors-license-consolidated-licence-conditions-december-2017.pdf>. For example, Part 10.1(a) imposes data security conditions, such that data on operational technology and ICT infrastructure may only be held in, or accessed from, within Australia.

150 *Australian Securities and Investments Commission v RI Advice Group Pty Ltd* [2022] FCA 496 ('*ASIC v RI Advice Group*'). Rofe J's judgment, while relevant in showing potential judicial attitudes, is limited in direct effect as: the orders were made by consent; solely based on an agreed statement of facts ('SAFA') between the Australian Securities and Investments Commission ('ASIC') and an AFSL; and the relevant sections only apply to ASFL entities. The SAFA indicated the AFSL had failed to implement adequate cyber security and cyber resilience risk management controls. The SAFA indicated that between June 2014 and May 2020, nine cyber security incidents occurred at the practices of authorised representatives of RI Advice Group, the holder of an Australian authorised financial services licence. The incidents included fraudulent emails being sent to clients, the creation of fake home pages, and various types of unauthorised use of client personal information taken from a practice's server. Some of the poor risk management practices attracting the Federal Court's ire included systems without up-to-date anti-virus software, no filtering of emails, no backups and poor password practices. The judge held that the SAFA provided a proper basis for making declarations the AFSL had breached its obligations under ss 912A(1)(a) and (h) of the *Corporations Act 2001* (Cth).

151 Ibid [86] (Rofe J), orders were by consent.

A further example of multidirectional regulatory overlap is the Australian Prudential Regulatory Authority's ('APRA') Prudential Standard CPS 234 – Information Security ('CPS 234').[152] Under this standard, regulated entities (such as banks) are subject to security obligations in APRA's mandatory CPS 234.[153] and the associated Prudential Practice Guide CPG 234 – Information Security ('CPG 234').[154] Under CPS 234, the Board of an APRA-regulated entity is responsible for the information security of the entity. However, the CPG notes it is increasingly common for third parties to rely on other service providers to deliver an end-to-end service. APRA's expectation is that an APRA-regulated entity would take reasonable steps to satisfy itself and that the third party has sufficient information security capability to manage additional threats and vulnerabilities resulting from such arrangements. However, there may also be instances of directional overlap for the cloud services provider operating, who is also operating in the energy sector and/or another critical infrastructure sector subject to information security standards or contractual requirements.

Cloud providers often contract as third-party service providers to APRA-regulated entities, who impose contractual obligations on the third party to meet the entity's compliance obligations. Obligations under CPS 234 will then be passed on to cloud providers, such as maintenance of information security capability, evaluation, assessment, criticality of information assets, controls, secure software development and acquisition, response to security incidents, information and data life cycles, automation and audits of all systems and controls in place.

In addition to CPS 234, cloud entities must be familiar with Prudential Standard CPS 231 relating to outsourcing[155] and CPG 235 relating to managing data risk.[156] If the cloud provider is not an APRA regulated entity, these obligations may flow through to providers under their service agreements. For example, under CPS 234 for Information Security, where a related party or third party manages information assets, the APRA-regulated entity must assess its information security capability, commensurate with the potential consequences of an information security incident affecting those assets.

In July 2023, APRA released the final version of its new cross-industry Prudential Standard 230 Operational Risk Management. This standard (commencing from 1 July 2025) specifies new minimum standards for managing operational risk and replaces Prudential Standard SPS 231 concerning outsourcing arrangements and Prudential Standard CPS 232 concerning management of business continuity.[157] This new standard has implications for supply chain management and contractual obligations relating to cloud services providers. For example, an APRA-regulated entity may have a 'material arrangement'[158] with a SaaS provider to perform a 'critical operation'[159] for the regulated entity, such as providing core technology services. But this arrangement may be a third, or fourth, party arrangement in some cases. Any outage that the SaaS provider experiences may interrupt the regulated entity's operations to the extent that it causes a 'material adverse impact' on the entity's customers or its role in the financial system. APRA explains that:

> Draft CPS 230 would require a regulated entity's service provider management policy to set out its approach to managing risks with fourth parties. APRA expects that entities would also seek to be aware of, and manage, the risks associated with any further downstream service providers, to maintain a thorough understanding of the supply chain and potential issues that could affect the entity's ability to maintain critical operations.[160]

---

152 APRA's references to 'CPS' and 'CPG' refer to 'Cross-Industry Practice Standard' and 'Cross-Industry Practice Guide' respectively. Note that the abbreviations are most often used in the title of the APRA documents.

153 Australian Prudential Regulatory Authority, 'Prudential Standard CPS 234 Information Security' (July 2019) <www.apra.gov.au/sites/default/files/cps_234_july_2019_for_public_release.pdf>.

154 Australian Prudential Regulatory Authority, 'Prudential Practice Guide CPG 234 Information Security' (June 2019) <www.apra.gov.au/sites/default/files/cpg_234_information_security_june_2019_0.pdf>.

155 CPS 231 'requires that all outsourcing arrangements involving material business activities entered into by an APRA-regulated institution … be subject to appropriate due diligence, approval and ongoing monitoring. All risks arising from outsourcing material business activities must be appropriately managed to ensure that the APRA-regulated institution… is able to meet its financial and service obligations to its depositors and/or policyholders': Australian Prudential Regulatory Authority, 'Prudential Standard CPS 231 Outsourcing' (*APRA*, July 2017) <https://www.apra.gov.au/sites/default/files/Prudential-Standard-CPS-231-Outsourcing-%28July-2017%29.pdf>.

156 CPG 235 'provides guidance on data risk management where weaknesses continue to be identified… [it] aims to provide guidance to senior management, risk management, business and technical specialists… [and] also provides examples to illustrate a range of controls that could be deployed to address a stated principle': Australian Prudential Regulatory Authority, 'Prudential Practice Guide CPG 235 – Managing Data Risk' (September 2013) <https://www.apra.gov.au/sites/default/files/Prudential-Practice-Guide-CPG-235-Managing-Data-Risk_1.pdf> 6, paras 1, 4, 9.

157 'APRA consults on new prudential standard to strengthen operational resilience', *Australian Prudential Regulatory Authority* (Media Release, 28 July 2022,).

158 'Material arrangements' under CPS 230 are 'those on which the entity relies to undertake a critical operation or that expose it to material operational risk': Australian Prudential Regulatory Authority, 'Prudential Standard CPS 230 – Operational Risk Management' (July 2025) CPS 230 – 10, para 49 <https://www.apra.gov.au/sites/default/files/2023-07/Prudential%20Standard%20CPS%20230%20Operational%20Risk%20Management%20-%20clean.pdf>.

159 'Critical operations are processes undertaken by an APRA-regulated entity or its service provider which, if disrupted beyond tolerance levels, would have a material adverse impact on its depositors, policyholders, beneficiaries or other customers, or its role in the financial system': ibid, CPS 230 – 8, para 35.

160 'Strengthening Operational Risk management – Discussion Paper', *Australian Prudential Regulatory Authority* (July 2022) 26.

Cloud services providers operating in the financial markets and services sector may be subject to provisions of the *Corporations Act*, for example, the risk management provisions applicable to some financial services firms;[161] the *Banking Act 1959* (Cth)[162] and related regulations. If the cloud provider provides services to an APRA-regulated entity, obligations under multiple laws may be translated into contractual obligations on the cloud services provider under their service agreement. Additionally, there may be private arrangements that are passed on through service agreements; for example, many merchant contracts require compliance with the Payment Card Industry Data Security Standard.[163] For cloud service providers, the sectoral and cross-sectoral layers of regulation add to the complexity of their business's operating environment. The risk of regulatory overlap and duplication is high, especially if those service providers also supply goods and services to other CI sectors. Additional research is required (beyond the scope of this paper) which maps applicable legislation, standards and guidance materials for *each* CI sector to determine where overlap and duplication occurs and identifies similarities and differences between regulatory mechanisms.

(c) The impact of the Consumer Data Right on the financial services and energy sectors

Further *action* overlap will occur because new information security obligations apply to the banking and energy sectors via the Consumer Data Right ('CDR') under pt IVD of the *Competition and Consumer Act 2010* (Cth) ('CDR CCA') and the accompanying *Competition and Consumer (Consumer Data Right) Rules 2020*[164] ('CDR Rules'). The CDR currently allows consumers to require banking institutions and energy retailers to share their data with an 'accredited data recipient' ('ADR') (such as a comparison website) to enable consumers to get better services and reduce costs. Privacy Safeguard 12.1 in the CDR CCA ('PS12.1') requires ADRs to take steps set out in CDR Rules sch 2 (implementing minimum security controls such as multi-factor authentication, encryption, firewalls, security patching, anti-virus software, content filtering, application whitelisting and security training) to protect CDR data from misuse, interference, loss, unauthorised access, modification and disclosure, and to destroy or de-identify data that is no longer necessary.[165] Additional security obligations are also set out in supplementary guidelines.[166]

C *Obligations on SaaS Providers Providing Services to Government*

This section discusses the multidimensional regulatory overlap occurring when SaaS providers provide services to government, outlining examples of vertical, horizontal, and directional overlap.

Data protection and disclosure obligations under state legislation applying to NSW government agencies are often included as contractual terms in SaaS agreements, such as *Privacy and Personal Information Protection Act 1998* (NSW) ('PPIPA'), *Government Information (Public Access) Act 2009* (NSW) and the *Health Records and Information Privacy Act 2002* (NSW) ('HRIPA'). For example, PPIPA and HRIPA impose obligations to keep personal information[167] and health information secure,[168] as well as obligations to notify the Privacy Commissioner and affected individuals of data breaches.[169] The *Information Privacy Act 2009* (Qld) also contains a privacy principle imposing data storage and security obligations, which also applies to healthcare agencies.[170]

As a matter of federal and state government policy, public sector agencies are subject to significant security requirements. Unsurprisingly, government policy expects agencies to ensure their contractors, including cloud services providers, comply with these requirements when providing services to government. The key documents setting out obligations on cloud providers providing government are:

---

161 *Corporations Act 2001* (Cth) s 912A(1)(h).

162 Eg *Banking Act 1959* (Cth) s 11AF.

163 PCI Security Standards Council, *Document Library* (Web Page) <www.pcisecuritystandards.org/document_library/>; Jessica Anderson, 'What Is the PCI DSS?', *E-Commerce* (Article, 29 September 2023) <https://legalvision.com.au/what-is-the-pci-dss/>.

164 In particular, *Competition and Consumer (Consumer Data Right) Rules 2020* (Cth) R7.11, para 5.12(1)(a), sch 2.

165 *Competition and Consumer Act 2010* (Cth) s 56EO(1).

166 Eg an 'assurance report' from a third-party independent auditor must be provided as evidence of actions taken under Sch 2 of the CDR Rules (depending on the level of accreditation required and what type of certification is held): Australian Government, *Supplementary accreditation guidelines: information security* (Version 5, Dec 2022) <https://www.cdr.gov.au/sites/default/files/2022-12/CDR-Supplementary-accreditation-guidelines-information-security-version-5-December-2022.pdf>.

167 *Privacy and Personal Information Protection Act 1998* (NSW) s 12 ('*PPIPA*').

168 *Health Records and Information Privacy Act 2002* (NSW) sch 1 HPP 5.

169 *PPIPA* (n 166) Part 6A.

170 *Information Privacy Act 2009* (Qld) sch 3 s 4 'IPP 4 – Storage and security of personal information'.

Table 3: Obligations of Commonwealth agencies

Commonwealth

Australian Government Information Security Manual ('ISM')	ASD	Creates standards for protecting information and data based on classification and contains guidelines for managing and reporting cyber incidents and outsourcing arrangements with third parties, such as cloud providers.
Protective Security Policy Framework ('PSPF')	DHA	Sets out requirements for government entities to classify and handle official information, and the controls/process they must implement to guard against information compromise, mitigate cyber threats, and safeguard systems.
Secure Cloud Strategy	DHA	Sets out principles for cloud implementation in government agencies, including cloud security, certification of service providers and accountability. The strategy references the ISM and PSPF as the mandatory guidance and obligations for government entities to meet when using cloud services for government data. Further, the cloud strategy recommends that the ISM's security controls are addressed in cloud service risk assessments undertaken by government entities.
Hosting Certification Framework ('HCF')	DHA	The HCF sets out the principles outlined in the Whole of Government Hosting Strategy ('Hosting Strategy') and supports the secure management of government systems and data. The Framework assists agencies in mitigating supply chain and data centre ownership risks and enables them to identify and source hosting and related services under DHA's Secure Cloud Strategy. It expressly applies to 'data service providers' and 'cloud services providers,' but not SaaS or managed service providers 'until the next iteration of the policy is defined.'[171]
Cloud Security Guidance particularly 'The Anatomy of a Cloud Assessment and Authorisation' and Cloud Security Assessment Report Template.	ASD	Cloud providers should be assessed for their suitability to provide services. This publication provides guidance to Infosec Registered Assessors Program ('IRAP') assessors, cloud consumers' cyber security practitioners, cloud architects and business representatives on how to assess a cloud services provider and its cloud services, and the cloud consumer's own self-developed systems hosted in the cloud.

[171] Digital Transformation Agency, 'Safeguarding Australian Government Data', *Hosting Certification Framework* (Web Page) <www.hostingcertification.gov.au/>.

Table 4: Obligations of NSW and Qld agencies

State

New South Wales	NSW Cyber Security Policy (v5, updated Jan 2022)	Outlines mandatory requirements for all NSW government departments and public service agencies to manage cyber security risks to their information and systems. It expressly contemplates the imposition of contractual terms on 'third party information and communications technology ('ICT') providers' (which would include cloud services providers) mandating compliance with this policy, and in such cases, it requires (amongst other things) terms requiring the provider to have an incident notification process and to follow 'reasonable direction' from the government agency arising out of incident investigations. [172]
	NSW Government Cloud Policy[173]	The NSW Government Cloud Policy provides guidance and direction to NSW government agencies in using public and private cloud services. It applies to all NSW government departments and public service agencies. NSW government agencies must use the policy to assess available cloud services and determine that the services are secure, meeting the NSW Cyber Security Policy and Data Classification Policy requirements. The policy contains provisions for procurement and securing cloud services.
Queensland	Information Security Policy[174]	Applies to all Queensland government departments (as defined by the *Public Service Act 2008* (Qld)). Accountable officers and statutory bodies under the Financial and Performance Management Standard 2019 must consider the policy when making decisions about internal controls, financial information management systems, and risk management.
	Information Security Classification Framework[175]	Applies to Queensland Government agencies and instructs them on how to classify information assets. It provides the minimum requirements for information security and aligns with the PSPF. The framework applies the ISM's security classifications to Queensland government agency information assets up to the level of 'protected', which is for high confidentiality information. National security information handled by Queensland government entities must be managed under the PSPF and ISM.[176]
	ICT as-a-service Security Assurance Guideline[177]	Designed to assist agencies in developing an assessment process for using ICT as-a-service (including cloud). Outlines key security considerations, questions, risks, and quality assurance guidance. Under the guideline, service providers will be assessed against several standards and regulations.[178]

National and international standards, such as the ISO 31000:2018 (a risk management framework that has also been adopted by Standards Australia[179]) [180] can be a significant additional source of multi-dimensional overlapping regulation and are often referred to in government regulatory and guidance instruments. For

[172] *NSWCSP* (n 50) 14.

[173] NSW Government, *NSW Government Cloud Policy* (Policy Version No 1.1, 7 October 2020) <www.digital.nsw.gov.au/sites/default/files/NSW%20Government%20Cloud%20Policy%20v1.1.pdf>.

[174] Queensland Government, *Information Security Policy (IS18:2018)* (Policy Version No 8.1.2, June 2019) <www.qgcio.qld.gov.au/documents/information-security-policy>.

[175] Queensland Government, *Information Security Classification Framework QGISCF* (Framework Version No 5.0.0, February 2020) <www.qgcio.qld.gov.au/documents/information-security-classification-framework-qgiscf>.

[176] Ibid.

[177] Queensland Government, *ICT-as-a-Service Security Assurance Guideline* (Guidelines, June 2016) 11 <www.qgcio.qld.gov.au/documents/ict-as-a-service-security-assurance-guideline>.

[178] For example ISO/IEC 27001:2013 (Information technology – Security techniques - Information security management systems – Requirements); ISO/IEC 27002 (Information technology – Security techniques – Code of practice for information security management); CCM 3.01 (Cloud Controls Matrix – Cloud Security Alliance); SSAE16 SOC-1 Type II SSAE16 SOC-2 Type II (Statement on Standards for Attestation Engagements No 16, Reporting on Controls at a Service Organization); ISO/IEC 38500 (ICT Governance); COBIT5 (Framework for IT Governance and Management); IT Audit and Assurance Program for Cloud Computing Cloud Computing Assurance Program – Information Systems Audit and Control Association; Cloud Computing Information Assurance Framework (ENISA); Cloud Computing Risk Assessment (ENISA); AS/NZS ISO 31000:2009 (Risk Management – Principles and Guidelines); NIST SP 800 and 1800 series (Computer Security and Cyber Security Practice Guides).

[179] Standards Australia is Australia's peak standards organisation and is the Australian representative of the International Organization for Standardization ('ISO'). See <www.standards.org.au/>.

[180] Standards Australia, 'AS ISO 31000:2018', *Standards Catalogue* (Webpage) <www.standards.org.au/standards-catalogue/sa-snz/publicsafety/ob-007/as--iso--31000-colon-2018>.

example, the ISM references at least 20 standards and compliance with these standards can be made mandatory through government procurement policy or by contract.

D *Areas of Concern for SaaS Providers*

In this section, we examine two areas of concern for SaaS providers, where multi-dimensional regulatory overlap may cause compliance difficulties and extra costs:

1. Incident response and reporting (ie what is required to be done when there is a cyber-attack and/or breach of security obligations, such as unauthorised disclosure of data); and
2. Risk management processes (a requirement for the cloud services provider and members of its supply chain, such as an IaaS provider).

1 *Incident response and reporting*

The ACSC defines a cyber incident as 'an unwanted or unexpected cyber security event, or a series of such events, that have a significant probability of compromising business operations.'[181] SaaS providers need to develop their own cyber incident response and management plan and, in some instances, consider their customers' plans and other overarching arrangements, such as the *Cyber Incident Management Arrangements for Australian Governments* ('CIMA').[182] While CIMA 'provides Australian governments with guidance on how they will collaborate in response to, and reduce the harm associated with, national cyber incidents', it does not override existing incident response management arrangements of different levels of government unless circumstances demand it.[183]

Appendix 1 contains a summary comparison of incident response and reporting obligations under different instruments. Appendix 1 indicates inconsistency between the instruments, notably in report timing and the type of information required. As cloud providers provide services across all government and private sectors, they must implement systems for all these different obligations. Obligations vary depending on who and what is under attack, clients in different sectors, what kind of information or services the client provides, and whether they are designated a SoNS under the *SOCI Act*. Cloud customers can also impose additional timelines and requirements on cloud providers under contract.[184]

Cloud services providers must conform to multiple frameworks requiring an incident response, which can lead to overlap and duplication of the response management processes. This can cause compliance issues when there are multiple clients across sectors and jurisdictions, as the complexity of staying on top of duplicated or inconsistent reporting obligations can dilute the focus on dealing with substantive security issues. This issue was brought to the forefront in recent data breaches and outages, as multiple regulatory frameworks were activated to manage the cross-sectoral and deep supply chain-related impacts.[185]

2 *Risk management for cloud services providers and the supply chain*

Risk management frameworks provide processes and structures for integrating information security and risk management into systems and operations. They form a key part of the *SOCI Act*. The Security of Critical Infrastructure (critical infrastructure risk management program) Rules (LIN 23/006) 2023 ('CIRMP Rules') issued under the *SOCI Act* require that responsible entities for CI assets have a CI risk management program, which (amongst other requirements):

- Identifies all cyber and information security hazards where there is a material risk they might impact the availability, reliability, integrity, or confidentiality of a CI asset; and

---

181 Australian Cyber Security Centre, 'Cyber Incident Response Plan Guidance', 2 <www.cyber.gov.au/sites/default/files/2023-03/ACSC%20Cyber%20Incident%20Response%20Plan%20Guidance_A4.pdf>. For example, if a cyber attacker blocks customer access to the services hosted by an SaaS provider and demands a ransom to restore access, this would be seen as a cyber incident, as it would shut down not only the SaaS' operations but also part or all of those of its customers who rely on the hosted services.

182 Cyber Incident Management Arrangements for Australian Governments (n 96).

183 Ibid 1.

184 Cloud Sourcing Contract Template (n 100) s 13.1.1.1(j).

185 On 6 July 2022, the Minister for Communication made security information obligations for carriers and eligible carriage service providers, requiring carriers and service providers to undertake asset registration and cyber incident reporting. The licence conditions were introduced to avoid duplication, as the *Telecommunications Act 1997* (Cth) contains an existing, well-established sectoral framework. The new conditions import the provisions from *SOCI Act*. See generally, 'Security information obligations for carriers and eligible carriage service providers', *Department of Infrastructure, Transport, Regional Development, Communications and the Arts* (Web Page, 25 February 2022) <www.infrastructure.gov.au/have-your-say/security-information-obligations-carriers-and-eligible-carriage-service-providers>. In October 2022, APRA announced that it was working with 'the Federal Government, peer regulators and other relevant bodies to facilitate closer coordination and a controlled process of data sharing between Optus and APRA-regulated entities.' See Australian Prudential Regulator, 'Optus Data Breach: update for APRA-regulated entities following Federal Government's planned changes to the Telecommunications Regulations 2021' (Media Release, 6 October 2022).

- Minimises and mitigates the material risk and impact of those hazards.

Under s 8 CIRMP Rules, entities must establish a process to comply with one of five identified frameworks[186] or an equivalent.

However, risk management frameworks exist in many locations besides the CIRMP Rules, including Australian and international standards.[187] A key issue is the lack of a consistent whole-of-government risk management standards framework. While our research indicated the most common standard referenced is ISO-31000, there were many others, including US and European standards, with which multinational cloud services providers may be expected to comply. This will make it difficult for cloud services providers, especially smaller entities, to know which standard or instrument should be applied, and it raises the issue of whether they can be accessed and applied simultaneously. For example, international standards, such as ISO 31000 and BSI Germany Standard 200-3, contain different definitions of risk,[188] which, in practice, may impact compliance systems and processes, potentially creating gaps in how entities define and engage with risk.

Moreover, the number of frameworks and practices referenced in the various guidance materials adds to the complexity of creating a risk management plan. This will advantage larger cloud services providers with more resources. However, smaller entities may not be able to understand and realistically operationalise all the instruments they are expected to contain in their risk management plan and systems. Additionally, multiple frameworks will lead to more significant costs, as cloud services providers must employ a skilled workforce to meet the risk management obligations. Small and medium enterprises ('SMEs') will likely face considerable challenges in finding qualified personnel who meet these requirements (including 'national sovereignty' requirements).[189] These functions *may* be carried out by legal representatives or specialist compliance teams, but these can be costly, especially for SMEs.

Through the Office of Supply Chain Resilience ('OSCR') housed within the Department of Industry, Science and Resources, the Australian Government has developed a Supply Chain Resilience Framework to assist government agencies in identifying and assessing risk and disruption to critical supply chains.[190] The OSCR applies the framework in the context of its monitoring role and engages with representatives from various industries such as healthcare, food production, chemicals, and construction to create a good understanding of Australia's supply chain risks.[191]

However, additional complexity is revealed when considering the delivery of many cloud services, which rely on a complex supply chain. It is common for one cloud services provider to combine multiple components of the cloud from different suppliers and deploy its services across multiple industries. For example, a cloud services provider may combine hardware and/or SaaS from different suppliers. The cloud provider may be a hyperscaler, like Microsoft Azure, and thus offer different hardware and software services at different layers of the 'stack.' As a result of this complexity, expectations fall on cloud providers to secure their own supply chains and form a secure component of another sector's supply chain.

There is no international standard for supply chain management and resilience, although there exist bilateral arrangements for international supply chain resilience.[192] Some sectors, such as defence, have specific

---

186 Australian Standard AS ISO/IEC 27001:2015 (Information Security Management Systems); Essential Eight Maturity Model published by the Australian Signals Directorate; Framework for Improving Critical Infrastructure Cybersecurity published by the National Institute of Standards and Technology of the United States of America; Cybersecurity Capability Maturity Model published by the Department of Energy of the United States of America; the 2020-21 AESCSF Framework Core published by Australian Energy Market Operator Limited.

187 See, eg, National Institute of Standards and Technology US Department of Commerce, 'NIST Special Publication 800 series General Information (2018) NIST Special Publication (SP) 800 series AS/NZS ISO 31000:2018' 3 <www.nist.gov/itl/publications-0/nist-special-publication-800-series-general-information>.

188 European Union Agency for Cybersecurity, *Risk Management Standards: Analysis of standardisation requirements in support of cybersecurity policy* (ENISA Report, March 2022) 13-14 <https://www.enisa.europa.eu/sites/default/files/publications/O.7.2-T2-Risk_Management_standards.pdf>.

189 For example, many defence contracts require personnel with a security clearance that is only available to Australian citizens: see Department of Home Affairs, *Australian Government Protective Security Policy Framework* (Annual Release, 2024) <https://www.protectivesecurity.gov.au/system/files/2025-01/pspf-release-2024.pdf>. See also the licence conditions described in n 189 for an example from the energy sector that would apply to cloud services providers contracting with the relevant entity.

190 'Office of Supply Chain Resilience', *Department of Industry, Science and Resources* (Web Page) <www.industry.gov.au/trade/office-supply-chain-resilience>.

191 The OSCR's stated (and very broad) remit is 'to advise the Australian government on supply chain risks and potential actions to improve resilience'. It does not name the cloud services sector specifically as part of the 'targeted [industry] sectors' it engages with. Note, however, that the widespread use of cloud services in Australian government agencies would certainly fall under any general definition of supply chain risk, as any disruption to the major cloud services provider services due, for example, to a cyber attack, would certainly disrupt the provision of services by both government agencies and industry.

192 For example, the Australia-UK Joint Supply Chain Resilience Initiative, which aims to foster supply chain resilience between Australia and the UK through risk management, sharing expertise and supporting cooperative international efforts. See 'Australia-UK Joint Supply Chain Resilience Initiative', *Department of Industry, Science and Resources* (Web Page, 19 September 2022) < https://www.industry.gov.au/publications/australia-uk-joint-supply-chain-resilience-initiative-introduction-module>.

requirements,[193] but overall, the approach to supply chain resilience is inconsistent. The *SOCI Act* improves this with the CIRMP Rules by requiring CI entities to manage their supply chain. Sectoral standards, such as APRA's Prudential Standard CPS 230, also address supply chain risk (and cloud services), including third- and fourth-party risks.[194]

The ACSC provides high-level guidance[195] on supply chain management in a cyber security context, referencing several domestic and international frameworks, standards and guidance, including the NISTIR 8276[196] and PSPF – Policy 6 .[197] The DHA hosting strategy requires a risk-based assessment of supply chain integrity and is linked to assessment and authorisation.[198] The international standard concerning risk management, ISO-3100, is also a key standard referenced in several guidance materials.

V Re-arranging the Room

A *The Great Unifiers: Coordination, cooperation and collaboration*

The cloud services sector is a complex industry. Our research reveals the multi-dimensional nature of cloud regulation in Australia. We identified broad vertical and horizontal overlap instances, such as that arising at the nexus of state and federal hard and soft law instruments or crossovers between sector-specific and cross-sectoral regulation and guidance. However, the orientation of regulatory overlap involves more dimensions than simply vertical or horizontal. The *direction* of the regulation can also lead to overlap, that is, the *object* of the regulation (ie which distinct legal field, jurisdiction, or sector) and those *responsible* for exercising discretion or enforcement (through authority, functions, and delegations). Additionally, the *focus* of the regulatory overlap should not be confined to legal fields or government agencies but also acknowledge the effect of *sector-specific* and *cross-sectoral* regulatory instruments.

Much of the regulatory overlap literature attempts to propose various solutions to detrimental effects arising from overlap. However, our review of the scholarship revealed a common thread: *coordination*, *cooperation,* and *collaboration* are essential components for managing overlap.[199] Freeman and Rossi argue that 'greater inter-agency coordination will be desirable where it helps to maximise the purported strengths of shared regulatory space by preserving "functional" aspects of overlap and fragmentation, while minimising its dysfunctions in terms of compromised efficiency, effectiveness and accountability.'[200] Freeman and Rossi s also suggest various coordination tools to 'help maximise the benefits and minimise the costs of shared regulatory space'.[201] Effective tools in building agency coordination include: informal coordination, interagency coordination, MOUs between agencies, coordination policies, and consultation.[202] As discussed, Australia's relevant agencies and institutions already use some of these. Aagaard identified several factors that favour effective coordination,[203] the most relevant of which to the cloud sector are:

> (1) agencies that report to the same government, or with similar perspectives and goals, are less likely to come into conflict;
> (2) a clear order of priority among agencies, with a quick trigger for other agencies to act if the primary agency does not; and
> (3) statutory coordination mechanisms and extensive direct communications.

---

193 See, eg, Department of Defence, *Defence Security Principles Framework* (Framework, 31 July 2020) 3-4 <www.defence.gov.au/sites/default/files/2020-12/DSPF-OFFICIAL.pdf>.

194 'Strengthening Operational Risk management – Discussion Paper', *Australian Prudential Regulatory Authority* (July 2022, Australian Government) 11.

195 Australian Cyber Security Centre, 'Cyber Supply Chain Risk Management', *Australian Signals Directorate* (Web page, 22 May 2023) <https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/outsourcing-and-procurement/cyber-supply-chains/cyber-supply-chain-risk-management>.

196 National Institute of Standards and Technology, *NISTR 8276 Key Practices in Cyber Supply Chain Risk Management: Observations from Industry* (Feb 2021) <https://doi.org/10.6028/NIST.IR.8276>.

197 Policy 6 relates to Third Party Risk Management.

198 Digital Transformation Agency, *Hosting Certification Framework* (Framework, Version No. 2, March 2021) 19;
see, eg, Table 7 - Certified Strategic Supply Chain Risk Controls ('Contractor must submit the Risk Management Plan to the DTA and the Agency on the Contract Start Date or at such other time as reasonably required by the DTA or the Agency. The Risk Management Plan should, as a minimum, comply with risk management standards AS/NZS ISO 31000:2018 and AS/NZS ISO 28001:2007') <www.hostingcertification.gov.au/sites/default/files/2021-11/Hosting%20Certification%20Framework%20-%20March%202021.v2.pdf>.

199 See, eg, ibid; Aagaard (n 39); Freeman and Rossi (n 2); Jody Freeman, 'Collaborative Governance in the Administrative State' (1997) 45 *UCLA Law Review* 1; Camacho and Glicksman (n 39); Jeremy Straughter and Kathleen Carley, 'Towards a Network Theory of Regulatory Burden' (2021) 6 *Applied Network Science* 70.

200 Freeman and Rossi (n 2) 1137.

201 Ibid 1155.

202 Ibid 1155-81.

203 Aagaard (n 39) 300-2.

The regulatory tools deployed by different levels of government and its agents are indicative of the complexity faced by a cross-sectoral industry like cloud services. We have demonstrated that legislative instruments, standards, accreditation, guidelines, and codes are part of a highly variable regulatory environment. In situations, such as under the *SOCI Act's* CIRMP, CI industries provide technical expertise through the Trusted Information Sharing Network ('TISN'),[204] but governments provide legislative obligations. This constitutes a co-regulatory or hybrid system. These are examples that apply a co-regulatory approach and can be considered collaborative because government engages the technical expertise of industry but also formulates its policy and legislative obligations and outcomes.

Much has been discussed about the downsides of regulatory overlap. Adverse effects include increased public and private sector costs through repetitive practices, inconsistent application of standards or application of differing standards, obfuscation of policy objectives, lack of a clear and effective regulatory framework, and consequent regulatory failure.[205] The identification of broad instances of regulatory overlap in this discussion indicates that the regulatory regime governing cyber security and critical infrastructure as it relates to the cloud services sector is at risk of developing some or all of these problems. Indeed, these problems may be exacerbated by subject matter regulators who lack expertise and understanding of the broader context in which they operate. Considering the multiple regulators responsible for cyber security policy, this significantly increases the risk of adverse effects on cloud services providers and the government. The following section outlines our recommendations for mitigating the adverse effects of regulatory overlap and leveraging its benefits.

B *Recommendations*

Multiple regulators and government agencies often operate independently in uncoordinated and ad hoc ways across the cloud regulatory environment. While it may be appropriate for a sector regulator to produce a cyber security framework for its industry stakeholders, cloud services providers working within and across multiple economic sectors will be impacted by this decision, resulting in increased regulatory burden for those service providers. For example, the financial markets and services sector and the energy (electricity) sector have areas of regulatory cross-over, which may translate into complex compliance requirements for multinational cloud businesses that provide services to both sectors in Australia and in other jurisdictions. There may be opportunities for cloud service providers to leverage areas of regulatory cross-over by satisfying a higher standard of compliance, eg, adopting AESCSF maturity levels which exceed CPS 234 or CIRMP requirements.

Past and present governments have justified *centralising* reforms in CI regulation as ways to correct flaws in the fragmented and *ad hoc* approach to cyber security evident in Australia. For example, subsequent federal governments centralised policy and regulation within the Department of Home Affairs ('DHA'), and centralised cyber security substantive and functional roles through the creation of CISG within DHA and the appointment of a Cyber Security Coordinator[206] More functions have been delegated to the ASD and the ACSC to leverage their specialist capability.[207] The Minister for Cyber Security announced additional moves to further harmonise the regulation of CI following the most recent Optus Outage.[208] The Minister announced reforms to the telecommunications sector security arrangements to bring the sector into the SOCI regime.[209] Other recent changes included shifting the administration of the Protective Security Policy Framework, the Information Security Manual, [210] the Hosting Certification Framework ('HCF') [211] and the Secure Cloud Strategy ('SCS') to the Department of Home Affairs.[212] These centralising moves may help bring into play the first of Aagaard's factors supporting coordination.

---

[204] The TISN is administered by the DHA and is an information sharing and collaboration network between all levels of government and industry members of the CI community: <https://www.cisc.gov.au/how-we-support-industry/partnership-and-collaboration/trusted-information-sharing-network>.

[205] Robb, Candy and Deane (n 18).

[206] See Table 2 for the translation of acronyms.

[207] O'Neil (n 91).

[208] Ronald Mizen, Jenny Wiggins and Mark Ludlow, 'Telco boards hit with strict cybersecurity rules', *Australian Financial Review* (online, 13 November 2023).

[209] Richard Chirgwin, 'Telcos to be added to SOCI regime', *IT News* (online, 13 November 2023) <https://www.itnews.com.au/news/telcos-to-be-added-to-soci-regime-602277>.

[210] Commonwealth of Australia, *Administrative Arrangements Order* (Legislative Instrument, 13 October 2022) Part 10,<https://www.legislation.gov.au/C2022Q00008/latest/text>.

[211] The Hosting Certification Framework for cloud services outlines the cloud services procurement requirements, creating an additional set of de facto security certification obligations for cloud services providers dependent on government work.

[212] Department of Home Affairs, 'Safeguarding Australian Government Data', *Hosting Certification Framework* (Web Page) <https://www.hostingcertification.gov.au/> which outlines the transfer of responsibility for the HCF and SCS from the Digital Transformation Agency to DHA in 2023, removing one of the more serious cases of fragmentation in cyber security policy.

Notably, a centralised approach was supported by several participants at various stages of the reform process.[213] The AER noted it would ensure regulatory consistency and outcomes by minimising duplication and delivering efficiencies, building expertise and experience, providing certainty to the industry, and creating a deeper understanding of cyber threats and interdependencies between sectors.[214] However, sector-specific expertise must be embedded within the regulators so that sector-specific expertise can inform the *SOCI Act* framework, such as a dedicated regulatory unit advising on sector-specific consequences. For instance, the AER noted that the CISC must consider sector-specific regulatory determinations.[215] In other words, the CISC must seek sector-specific feedback and have personnel who are competent to understand and translate sector specific feedback into regulatory action and outcomes.[216]

Enhanced coordination between government and agencies at intra- and inter-governmental levels is highly likely to benefit the cloud sector. Government and regulators have options available to them, including formalising broader, more coordinated regulatory activity by clarifying or cooperating around the respective legislative remits of industry sector-specific and cross-sectoral regulators.[217] Encouraging and formalising coordinated regulatory and jurisdictional overlap and more 'joined-up' governance mechanisms for industry regulators may provide more clarity for industry participants.[218] A complementary approach may be to delegate or share some functions under the *SOCI Act*, such as the risk management program and other matters, with sector regulators.[219]

Cloud services providers (particularly SMEs) face financial and expertise barriers to consistent and cost-effective cyber security compliance. This may result in weaker cyber security protections and a less competitive cloud services sector. To mitigate the detrimental effects on the sector arising out of regulatory overlap, we recommend the following:

1. *Create a forum for collaboration and coordination between cyber regulators ('Cyber-Reg').* Examples already operating include DP-REG or the Council of Australian Financial Regulators. This will allow collaboration between regulatory authorities operating across CI sectors and within sector-specific frameworks. It has the potential to encourage the sharing of expertise and capability, and enable the identification of potential gaps, cross-over and information asymmetries;
2. *Every sector-specific and cross-sectoral regulator should have a cyber security regulatory unit that provides expert advice and guidance on regulatory matters, identifies sector impacts, and coordinates with CISC*. This will provide dedicated *expertise* within sector-specific and cross-sectoral regulators to enhance knowledge of sector-specific cyber security problems and solutions,[220] and the link with CISC has the potential to strengthen cooperation across regulators. These units will also support senior managers who engage at the Cyber-Reg level;
3. *Standards Australia, in partnership with cyber regulators, should review standards relevant to cyber security in the cloud services sector to identify the concerns of users and any blockers to the adoption of international standards in Australia*;

---

213 See, eg, Email from Australian Energy Regulator to Department of Home Affairs, 14 May 2021, 1 <www.aer.gov.au/system/files/AER%20submission%20-%20DHA%20Critical%20Infrastructure%20Asset%20Definition%20Rules%20paper.pdf>.

214 Ibid.

215 Email from Australian Energy Regulator to Department of Home Affairs, 27 November 2020, 4 <www.aer.gov.au/system/files/AER%20-%20Submission%20to%20Department%20of%20Home%20Affair%E2%80%99s%20Exposure%20Draft%20Bill%20-%20Protecting%20critical%20infrastructure%20and%20systems%20of%20national%20significance%20-%2027%20November%202020.pdf>.

216 The Cyber and Infrastructure Security Centre ('CISC') supports the sector groups of the Trusted Information Sharing Network with secretariat and subject matter experts. See Cyber and Infrastructure Security Centre, 'TISN Sector Groups', *Department of Home Affairs* (Web Page, 2 August 2024) <https://www.cisc.gov.au/how-we-support-industry/partnership-and-collaboration/tisn-sector-groups>.

217 For example, the AER and ASIC have a memorandum of understanding for co-operation to assist them in discharging their respective functions and maximizing the effectiveness of their powers in relation to the regulation of the gas and electricity markets (by AER) and (gas and electricity) derivatives traded on the financial markets (and regulated by ASIC). See the 'Memorandum of Understanding Between the Australian Securities and Investment Commission and the Australian Energy Regulator' signed 23 December 2021 <www.aer.gov.au/system/files/Memorandum-of-Understanding-ASIC-AER-20211223.pdf>.

218 There are already examples of this in operation at the federal level: DP-Reg (a formal collaborative arrangement between the ACCC, the ACMA, the e-Safety Commissioner and the OAIC entered into in March 2022) , Council of Australian Financial Regulators (a formal coordinating body for APRA, ASIC, the Reserve Bank of Australia and The Department of Treasury, which together comprise Australia's main financial regulatory agencies), and various memoranda of understanding between regulators for coordination and collaboration.

219 An example of a shared regulatory structure is found in the *Telecommunications (Interception and Access) Act 1979* (Cth) ('*TIA Act*') where the Communications Access Coordinator and the ACMA work together on a range of matters, including interception capability, data retention plans and delivery capability. See, eg, *TIA Act* ss 187G, 187KA, 188, 193, 195, 198, 209, 210, 211.

220 Along similar lines, on 17 February 2023, the US Federal Trade Commission ('FTC') launched an 'Office of Technology' which is designed to 'boost the FTC's expertise to help the agency to achieve its mission': US Federal Trade Commission, 'FTC Launches New Office of Technology to Bolster Agency's Work' (Media Release, 17 February 2023) <www.ftc.gov/news-events/news/press-releases/2023/02/ftc-launches-new-office-technology-bolster-agencys-work>.

4. *Standards Australia and cyber regulators should review supply chain risk management processes with the aim of providing clarity and interoperability*;
5. *'Equivalence' principles for cyber security standards informing legislation or guidance should be created*. This approach has already been adopted in the *SOCI Act* to some extent,[221] but could be expanded into other areas. ASIC's *Regulatory Guide RG 54,*[222] which outlines 'Equivalence' principles for determining the sufficiency of an alternative regulatory framework could be used as a guide. For example, permitting a wider range of standards and frameworks to enable cloud service providers to standardise their cyber security practices across sectors and jurisdictions, while still being able to adjust for sector-specific requirements, such as protective security or sovereign capability; and
6. *The introduction of targeted guidelines and well-defined agency responsibilities (with a descending hierarchy of responsibility) for cyber-attack incident management and coordination*, congruent with Aagaard's second factor above, and reflected in the recent Cyber Security Strategy discussion paper[223] and operationalised in the new 2023-30 Cyber Security Strategy.[224]

Centralisation and coordination activities and initiatives have been slowly evolving in the governance structure of cyber security and CI in Australia over the last decade. The latest iteration of Australia's strategic approach to cyber security, the 2023-30 Australian Cyber Security Strategy, will set the tone for the next seven years, including a renewed emphasis on enhancing *whole-of-nation* coordination and cooperation, significantly between industry and governments in national and international contexts. For example, the strategy recommends the creation of a Cyber Incident Review Board, which models international and national boards of review, to review responses to major cyber incidents.[225] The success of these measures is yet untested and unknown.

VI Conclusion

As discussed, some of the key challenges arising from regulatory overlap faced by SaaS providers in complying with Australia's regulatory framework for managing cyber security and CI include:

1. *Complexity*: The regulatory framework's complexity (including its multilayered structure) increases compliance costs (particularly for smaller businesses) and the likelihood of liability from deficient or second-rate responses to incidents.
2. *Regulatory gaps*: These arise from the convergence of regulated sectors and are particularly evident in risk management and supply chain issues, such as differing definitions of risk in standards.[226]
3. *Lack of regulatory and legal certainty*: due to the multiplicity of sectoral, cross-sectoral and international frameworks within which cloud service providers must operate.
4. *Lack of flexibility*: due to its profoundly diverse customer base, the SaaS industry requires flexibility to operate efficiently. Costs arising from instituting various processes to achieve the same result (eg incident reporting) will be passed on to the Australian public and private sector.

In this article, we have outlined key areas of regulatory overlap in a complex regulatory landscape, which may result in increased costs, variable compliance, and decreased confidence in providing cyber security services by cloud services providers. While the literature indicates that some regulatory overlap is inevitable, particularly under Australia's federal structure, some of its detrimental effects can be mitigated with careful attention paid to developing better coordination, collaboration and cooperation between regulators, improved communication and collaboration between agencies and industry, and greater clarity between regulators and regulated entities.

The federal government's approach to cyber security, including the recently released 2023-30 Australian Cyber Security Strategy, provides an opportunity to improve in these areas. For example, the creation of a dedicated National Office of Cyber Security within the DHA in May 2023 and the appointment of a Cyber

---

221 *SOCI Act* s 30ANA goes some way to creating equivalence. See also the CIRMP Rules.

222 ASIC, *Regulatory Guide 54: Principles for Cross-Border Financial Regulation* (Regulatory Guide, June 2012) <https://asic.gov.au/regulatory-resources/find-a-document/regulatory-guides/rg-54-principles-for-cross-border-financial-regulation/>.

223 Andrew Penn, Mel Hupfield and Rachael Falk, *2023-2030 Australian Cyber Security Strategy* (Department of Home Affairs Discussion Paper 2023) <www.homeaffairs.gov.au/reports-and-pubs/files/2023-2030_australian_cyber_security_strategy_discussion_paper.pdf>.

224 See Department of Home Affairs, *2023-2030 Australian Cyber Security Strategy* (22 November 2023, Australian Government) <https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy/2023-2030-australian-cyber-security-strategy>.

225 Ibid.

226 European Union Agency for Cybersecurity, *Risk Management Standards: Analysis of standardisation requirements in support of cybersecurity policy* (ENISA Report, March 2022) 13-14 <https://www.enisa.europa.eu/sites/default/files/publications/O.7.2-T2-Risk_Management_standards.pdf>.

Security Coordinator may provide a greater level of operational coherence for industry and government participants, in much the same way as the Communications Access Coordinator provides clarity to industry and agencies on access to communications.[227] Establishing a Cyber Incident Review Board creates room for industry and government collaboration on ways to improve responses to major cyber incidents, drawing on existing sectoral review boards as working examples. These initiatives should be seen as simply the beginning. They may prove insufficient to deal comprehensively from both a legislative and governance perspective with the inherent complexities of regulatory overlap in the cloud services sector, including dealing with the complex and largely opaque third- and fourth-party level supply chains in which SaaS providers operate, and the extensive sectoral and cross-sectoral regulatory landscape in which the industry conducts business. Our recommendations aim to enhance cooperation, collaboration, and coordination between various levels of government and between government and industry. This is essential in protecting the cloud services sector and, in turn, the data of Australian citizens, businesses and the government stored and processed by this critical sector.

Acknowledgements

The work has been supported by the Cyber Security Research Centre Limited (CSRC) whose activities are partially funded by the Australian Government's Cooperative Research Centres Programme. In 2018, the CSCRC was awarded $50 million in Commonwealth funding over seven years. This funding is supplemented by contributions from industry, university, and government agency participants. Some parts of this article were drawn from work conducted for an industry research report funded by the CSCRC (Susanne Lloyd-Jones et al 2022, *Complex Regimes: Mapping Australia's Cyber Security Regulatory Landscape for Cloud Services* <http://dx.doi.org/10.26190/unsworks/28540>) and we acknowledge all contributors to that report. Additional funding was received from the UNSW Allens Hub for Technology, Law & Innovation. However, all opinions, errors and omissions expressed in this article belong to the authors of this article. Note that this article does not include a discussion of the amendments passed to the *SOCI Act*, *Telecommunications Act* and the *Privacy Act* on 29 November 2024. Two major changes introduced by these amendments included moving security and notification obligations from Part 14 of the *Telecommunications* Act into the *SOCI Act*, and the introduction of a statutory tort for serious invasions of privacy under the *Privacy Act*.

[227] '[The] Communications Access Coordinator liaises between security and law enforcement agencies and the telecommunications industry, and is committed to supporting industry in understanding its interception capability obligations': See Attorney-General's Department, 'Telecommunications interception and surveillance', *Crime* (Web Page) <https://www.ag.gov.au/crime/telecommunications-interception-and-surveillance>; *TIA Act 1979* ss 6K(1)-(3).

APPENDIX 1 – INCIDENT RESPONSE: Comparison of Incident Response Obligations

SOCI Act	**ACSC Cyber Incident Response Plan Guidance and Template**	**PSPF: Security Governance for contracted goods and service providers**	**APRA CPS 234**	**ISM – guidelines for cyber security incidents**	**NSW Cyber Security Policy**	**Qld Information Security Policy – Information Security incident reporting standard**
Requirement to report relevant incidents to the ACSC within 12 hours and 72 hours (as applicable) by no later than 8 July 2022 and take appropriate action to address the incident. Section 30BC - notification of critical cyber security incidents must be made within 12 hours after the entity becomes aware. If the report was given orally, a written report must be made within 84 hours after the oral report was given. Section 30BD - for other cyber security events, the entity has 72 hours to file a report, and a further 48 hours to file a written report if the initial report was oral.	Guidance materials and templates for establishing a response plan. While some timeframes are suggested for post-incident debriefs in the Guidance, there are no timeframes set for incident response times in either document.	Requirements set out in policy – C.3.2 Security Incidents, includes reporting incidents not immediately relevant to the contract.	Section 35 – notification as soon as possible and no later than 72 hours of becoming aware of an information security incident and 10 days of becoming aware of a weakness.	Reporting cyber security incidents, including unplanned outages, to an organisation's Chief Information Security Officer ('CISO'), or one of their delegates, as soon as possible after they occur or are discovered provides senior management with the opportunity to assess the impact on their organisation and to take remediation actions if necessary. Note, an organisation should be cognizant of any legislative obligations regarding reporting cyber security incidents to authorities, customers, or the public.	Current cyber incident response plan that integrates with the agency incident management process and the NSW Government Cyber Incident Response Plan.	Business Impact Level ('BIL') reporting system – immediate and quarterly reporting depending on incident type and impact. Reporting to the Queensland Government Information Security Virtual Response Team ('QGISVRT').