Consultation on the Independent Review of the Security of Critical Infrastructure Act 2018

SAP Australia Response

Version: [<1.0>]
Date: 2025-12-22
Owner: [redacted]

Table of contents

This document is SAP Australia's response as the Responsible Entity for a Critical Infrastructure Asset to the *Consultation on the Independent Review of the Security of Critical Infrastructure Act 2018*.

Summary

SAP understands that the intended objective of the regulation of Australian-based data storage or processing services (DSoP) as critical infrastructure seeks to provide confidence in the adoption of cloud computing by providing a common foundational base line for security with the provider held to the same obligations as the consumer. SAP's experience of implementing the SOCI Act's obligations has contributed to good security uplift and suggests the Act is achieving this intended objective. Nevertheless, there are challenges with s12F of the Act, the Meaning of a critical DSoP asset, that suggest the threshold for regulatory capture of DSoP services is often not known or is poorly understood. Many consumers of those services don't fully understand the regulatory interplay between risk management of their own asset or essential services and the DSoP sector. This has probably resulted in a sub-optimal capture of DSoP services as critical infrastructure. It has also resulted in unnecessary regulatory impost on the DSoP critical sector based on attempts by customers to contractually obligate the sector to requirements that it is already accountable to Government for under the Act. These issues are explored in more detail herein.

Response to questions of industry

SAP's response herein is limited to its status as a responsible entity for a critical DSoP asset.

Is the SOCI Act achieving its intended objectives?

Security uplift of cloud computing in support of critical infrastructure protection

SAP understands the intent of the DSoP sector as a critical sector was to provide confidence in the adoption of cloud computing to enable industry and government to achieve efficiencies and economies of scale. Conceptually, confidence comes from consumers and providers of cloud services that store or process business critical data to be regulated to a common and foundational level of security, which may be factored into management of risk. In this context, SAP proactively registered its services that would reasonably be anticipated to store or process business critical data, and actively set about implementation of obligations, which as a global multinational has involved engagement, participation and compliance of its global enterprise. In that process, the obligations in the Act have contributed to an ongoing program of security uplift, notably in the rigour of security risk management. Therefore, it can be said, regarding SAP as a single impacted cloud services provider, the Act has achieved an intended objective.

However, SAP has the organisational size and scale, and experience of regulation of cloud computing as critical infrastructure in Germany, to have a dedicated critical infrastructure

protection function that has been able to engage with the legislation and implement its obligations. Not all cloud services providers would have benefited from experience or having such a function. Therefore, based on the issues raised below, there may be limitations on whether this intended objective behind the capture of cloud computing as critical infrastructure has been achieved more broadly.

Government Business Critical Data

Section 12F(1) essentially captures cloud computing as critical infrastructure if it involves the storage or processing of business critical data of federal and state or territory government entities. If the intended objective was to ensure that DSoP providers to government are captured as critical infrastructure when they involve sensitive government information then the objective had very little chance to be achieved based on the definition of business critical data, which is (SOCI Act, s5):

(a) personal information (within the meaning of the Privacy Act 1988) that relates to at least 20,000 individuals; or
(b) information relating to any research and development in relation to a critical infrastructure asset; or
(c) information relating to any systems needed to operate a critical infrastructure asset; or
(d) information needed to operate a critical infrastructure asset; or
(e) information relating to risk management and business continuity (however described).

The flaw in the application of the definition to s12F(1), is that (b) to (e) relate specifically to critical infrastructure assets. Therefore, this would only apply to government entities that are responsible entities for critical infrastructure assets, e.g., state government agencies running significant public transport networks. Outside of such government entities, only element (a) of the definition would apply to all government entities. This raises the question whether s12F(1) is necessary at all, based on two key considerations:

1. If a government entity is the Responsible Entity of a critical infrastructure asset they will be adequately covered by s12F(2).
2. In the case of federal government entities (and by adoption state and territory government entities) there is established processes for cloud assessment and authorisation (https://www.cyber.gov.au/business-government/protecting-devices-systems/cloud-computing/cloud-assessment-and-authorisation) that considers the security of the cloud service within the operating context of the government entity to enable a risk-based decision to authorise its operation. This risk-based decision would factor in the applicability and scale of personal information stored or processed by the service.

Two lesser considerations as to the need for s12F(1) are:

1. The data centre and infrastructure layers for cloud computing are captured for federal government entities (and by adoption state and territory) by the Hosting Certification Framework (https://www.hostingcertification.gov.au/).

2. The new Systems of Government Significance (SoGS) policy in the Australian Government Protective Security Policy Framework could be harnessed to place heightened security requirements on DSoP providers through the cloud assessment and authorisation process referred above. This consideration also offers an alternative approach to the identification of critical DSoP services in support of government entities based on the services relevance to the secure operation of a SoGS.

However, if the intended objective of s12F(1) is to capture cloud service providers across the infrastructure, platform and software-as-a-service stack that store or process sensitive government information as critical infrastructure, then the business critical data definition could be simply extended to include government information classified as OFFICIAL: Sensitive or higher, or, depending on the intent, the bottom threshold could be increased to the PROTECTED classification level.

Assuming the intended objective of s12F(1) has always been to only capture element (a) of the definition for government entities, there remains a flaw in the application of the requirement. Unlike entities covered by s12F(2), government entities are not required to inform their DSoP provider that business critical data is associated with the service and it is incumbent on the provider knowing "...that the asset is used as described ...". SAP suggests there would be greater potential to achieve the intended objective if government entities were obligated to inform their provider.

Critical Infrastructure Business Critical Data

Section 12F(2) captures cloud computing as critical infrastructure if it involves the storage or processing of business critical data associated with a critical infrastructure asset. This, with s12F(1) noted above makes the critical DSoP sector unique compared to other sectors in that its asset threshold for being critical infrastructure is by being in the supply chain of other critical infrastructure or government entities. Other sectors have a highly tangible threshold, for example a critical public transport asset is a public transport network that "... is capable of handling at least 5 million passenger journeys per month...".

For a DSoP provider to understand it has an obligation to register its service as a critical infrastructure asset, it either:

1. knows that the service involves business critical data of a government entity (s12F(1)), and this is likely from its own assessment as the government entity is not required to inform it
2. knows that the service involves business critical data associated with a critical infrastructure asset, and this is either from its own assessment, or by being informed by a responsible entity for a critical infrastructure asset based on the responsible entity's obligation to inform in s12F(3).

Thus, the identification of a DSoP service that meets the threshold for registration as a critical infrastructure asset is highly dependent on the exercise of the obligation on responsible entities for critical infrastructure asset in s12F(3). This is problematic as s12F is the Meaning of a critical DSoP asset, which raises the question whether responsible entities for other asset types would think to

read the meaning of an asset type not immediately relevant to its own regulatory capture. SAP's practical experience of this is that many responsible entities have not been aware of the requirement. This issue has been discussed with the Department of Home Affairs on several occasions and to its credit it made considerable communications efforts to point out the obligation to all critical sectors. However, SAP suggests that the obligation needs to be captured in a more general section of the Act to ensure greater awareness of the obligation, which would likely lead to increased regulatory capture of DSoP services and support the intended objective of regulating such services when they support essential service delivery across the critical sectors.

With regard to s12F(3), SAP has experienced being informed by formal correspondence and by reference to the SOCI Act within contracts. However, there is frequently insufficient identification of what DSoP service is assessed as storing or processing business critical data. Such clarification is important as across the sector not all services are tenanted in Australia and those that are not may not be registered as a critical infrastructure asset (SOCI Act s9(2A) refers). Having greater clarity will ensure consumers understand what services may or may not be registered, enabling them to consider the regulatory status of a given service as part of critical infrastructure risk management obligations. When being informed of s12F(3) relevance, if deficient of detail, SAP proactively seeks to clarify what specific services have been assessed as storing or processing business critical data, and if they are not already registered but are tenanted in Australia, to commence the process of adding them to the Register of Critical Infrastructure Assets. As there is no obligation in the Act currently on providers to inform the consumer whether the service in question is, will be, or could be registered as a critical infrastructure asset, SAP suggests such a requirement should be incorporated. This will ensure the consumer can appropriately factor into its critical infrastructure risk management program the SOCI Act status of the service identified through s12F(3) implementation.

Regarding critical infrastructure business critical data generally, SAP suggests that a CISC resource page that offers guidance on s12F(3), including the need for specificity and potential case studies would be beneficial for all parties.

Is the SOCI Act functioning as intended?

Confused implementation

A DSoP provider becomes a responsible entity for a critical infrastructure asset on the basis of its services being associated with business critical data relating to a critical infrastructure asset. Thus, both the provider and consumer are accountable to the Government for their regulatory compliance. SAP's experience is that this supply chain risk mitigation inherent in the Act is often misunderstood and consumers may seek to push their requirements for the secure management of their critical infrastructure asset on to the provider. For example, providers frequently experience attempts by consumers to insist on a contractual cyber security incident reporting requirement that falls inside timeframes for both parties' own obligations to Government, e.g. demanding the provider report incidents to the consumer within 12 hours of first awareness of the incident (the

critical cyber security incident threshold), and often without an acknowledgement of the severity of an incident that warrants, under the Act, the 12-hour timeframe. If providers agree to the contractual requirement, it amplifies the burden of SOCI Act compliance and misses the fundamental principle that the provider is accountable for its critical infrastructure asset, e.g., a particular DSoP service, and the consumer for its asset, e.g., a critical banking, electricity, gas, or public transport asset. While the service may store or process business critical data, the loss of availability of that service may not impact the availability of the said banking, electricity, gas, or public transport assets. In the case that it did, both the provider and consumer may be obligated to report, subject to the source and severity of the impact.

Complexity

The *Confused Implementation* and *Critical Infrastructure Business Critical Data* issues above emphasise the complexity of the Act. SAP's view is there is excessive cross referencing, which requires people intending to implement the Act effectively to have a solid understanding of all sections of the Act, which many do not. SAP suggests there could be a section where obligations relevant to all sectors is listed, and then sector-by-sector directions would be easier to consume.

Is the SOCI Act having any unintended consequences?

Effort to avoid or remove regulatory duplication during co-design with industry since 2021, in SAP's opinion, has been admirable with substantial industry consultation involved. Nevertheless, SAP contends that excessive regulatory impost can arise associated with the issue of *Confused implementation* raised above, i.e., SOCI Act-related obligations being passed on to entities that already have their own SOCI Act obligations. This consequence on the critical DSoP sector could be lessened through changes to the Act or effective use of CISC resource pages, which could be leveraged to ensure clarity of requirements and reduction of confusion.

www.sap.com.