7 December 2017

SPRING Singapore
Attention: **Mrs Kay Chua**
Manager, Standards Division

INVITATION FOR PUBLIC COMMENTS ON DRAFT SINGAPORE STANDARD - GUIDELINES FOR CLOUD OUTAGE INCIDENT RESPONSE

BSA | The Software Alliance (**BSA**)[1] and the US-ASEAN Business Council (**US-ABC**)[2] greatly appreciate the opportunity to comment on the revised draft "*Guidelines for cloud outage incident response (COIR)*" standard (**Revised Draft Standard**).

We thank the Singapore Government for having addressed some of the concerns in our earlier comments of 13 July 2017 (attached for easy reference). In particular, we note that the Revised Draft Standard has:

- eliminated requirements/controls pertaining to data breach;
- removed the requirement for cloud service providers (**CSPs**) to disclose their service performance levels against specific tiers, instead allowing CSPs to choose to voluntarily disclose their current practice across 16 specified parameters; and
- included more guidance to cloud service customers (**CSCs**) on their responsibilities vis-à-vis CSPs and CSCs' own customers.

However, some of our more fundamental comments have not been addressed, and we continue to have serious concerns with the Singapore Government's proposal to adopt the Revised Draft Standard as a Singapore standard.

As currently drafted, the Revised Draft Standard still does not properly account for fundamental concepts of cloud computing architecture, business models and usage models. Accordingly, rather than assisting CSCs in their decisions regarding cloud computing services, the Revised Draft Standard is likely to generate confusion, undermining efforts to drive greater cloud adoption and innovation in Singapore's economy.

---

[1] BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, creating software solutions that spark the economy and improve modern life. With headquarters in Washington, DC, and operations in more than 60 countries, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy.

BSA's members include: Adobe, Amazon Web Services, ANSYS, Apple, Autodesk, AVEVA, Bentley Systems, CA Technologies, Cisco, CNC/Mastercam, DataStax, DocuSign, IBM, Intel, Microsoft, Oracle, salesforce.com, SAS Institute, Siemens PLM Software, Splunk, Symantec, The MathWorks, Trend Micro, Trimble Solutions Corporation, and Workday.

[2] For over 30 years, the US-ASEAN Business Council has been the premier advocacy organization for US corporations operating within the dynamic Association of Southeast Asian Nations (ASEAN). Worldwide, the Council's 150+ membership generates over $6 trillion in revenue and employ more than 13 million people. Members include the largest US companies conducting business in ASEAN, and range from newcomers to the region to companies that have been working in Southeast Asia for over 100 years. The Council has offices in: Washington, DC; New York, NY; Bangkok, Thailand; Hanoi, Vietnam; Jakarta, Indonesia; Kuala Lumpur, Malaysia; Manila, Philippines; and Singapore.

The development of a Singapore standard inconsistent with international standards and best practices emerging at international forums, which leading countries are participating in, will increase barriers to providing and accessing cutting-edge cloud computing services in Singapore. This will ultimately result in costs to the Singapore economy, and risks diminishing Singapore's leadership in establishing pro-innovation policies and promoting seamless, interoperable standards regimes regionally and globally.

We commend the Singapore Government's historical leadership in clarifying technical complexity, and its desire to educate and empower CSCs in their procurement of cloud computing services. In this instance, however, it would be premature to develop a national standard that could limit the adoption of new technologies, particularly where there remains significant opportunity to collaborate with CSPs and CSCs in exploring approaches that are better suited to the industry and that take into account the complexities of cloud computing services.

Accordingly, instead of proceeding further with the Revised Draft Standard, we urge the Singapore Government to partner with the industry in developing appropriate guidance for CSCs, and to leverage and demonstrate its thought leadership at active international standards development forums (including but not limited to ISO/IEC JTC 1/SC 27 for "*ISO/IEC DIS 19086-4: Information technology -- Cloud computing -- Service level agreement (SLA) framework -- Part 4: Security and privacy*").

CSPs are constantly improving service offerings and outage response procedures to address CSC expectations and feedback. Responsiveness to CSCs' needs and concern is key to CSPs competing for and retaining CSCs. Our member companies therefore remain eager to partner with the Singapore Government in finding optimal ways of addressing our concerns, while providing appropriate guidance to CSCs on cloud computing service procurement.

We look forward to continued engagement with the Singapore Government on this important issue.

Yours faithfully,

BSA | The Software Alliance and **the US-ASEAN Business Council**

Attachment: *BSA-USABC Comments of 13 July 2017 on Guidelines for Cloud Outage Incident Response*

INVITATION FOR PUBLIC COMMENTS ON DRAFT SINGAPORE STANDARD

Title of Standard: Guidelines for cloud outage incident response (COIR)

Reference No.: _____

Date of Submission (DD/MM/YYYY): 13/07/2017

SUBMITTED BY

Full Name : * Sunita Kapoor

Contact Number: * 65 6339 8885

Email Address: * skapoor@usasean.org

Name of Company: On behalf of US-ASEAN Business Council and BSA | The Software Alliance (BSA)

Designation: Senior Manager, Singapore, US-ASEAN Business Council

Address of Company: US-ASEAN Business Council, 100 Beach Road, Shaw Towers, Singapore 189702; BSA | The Software Alliance (BSA), 300 Beach Road, #25-08 The Concourse, Singapore 199555

Note: Items marked with an * are compulsory.

COMMENTS / RECOMMENDED CHANGES

1. General Comments

BSA | The Software Alliance (BSA)1 and the US-ASEAN Business Council2 (USABC) wish to express our concerns regarding the proposal to convert the Cloud Outage Incident Response (COIR) Guidelines (Guidelines) into a Singapore Standard (Standard). In the past, we and our member companies have raised concerns about specific elements within the Guidelines, as well as our concern about converting the Guidelines into a Singapore Standard. As currently drafted, we do not believe the Standard aligns with fundamental concepts of cloud computing architecture, business models and usage models. As such, rather than assisting consumers in decisions regarding cloud computing services, the Standard is likely to confuse them, undermining efforts to drive greater cloud adoption and innovation in Singapore's economy.

We commend the serious commitment of the Government of Singapore to position Singapore as a global leader and regional hub for the advanced technologies and services, including cloud computing, that will drive the 21st Century economy. Instead of adopting a national standard that could limit the adoption of new technologies, we urge the Government of Singapore instead to engage in relevant discussions with industry stakeholders and among international standards development organizations.

Publicly available cloud computing services are now well established across the world and are providing easy to use enterprise-level services for a very wide range of business and government users. Many of these services leverage the latest technology developments at such a low cost that even very small organizations can compete with much larger players – not only in the local market, but also across the world. By encouraging the use of cloud computing services, countries such as Singapore may see significant benefits in productivity and export earnings. While we urge the Government of Singapore to reconsider its plans to develop a Singapore Standard based on the COIR Guidelines, if it is the Government's determination to proceed, we urge the Standard be amended in the following general ways:

Clause / Figure / Table	Page No.	Paragraph	Recommended Changes & Reasons (Note: Exact wording of recommended changes should be given.)
Clause 0/Introduction 0.2 Motivation	6	"These guidelines are built on recognised Singapore and International Standards on cloud computing, IT security, business continuity management, and IT disaster recovery."	The Standard should align with accepted international standards. Guidelines to assist in the adoption and use of cloud services are welcomed by the industry. However, we believe that the COIR Guidelines in their current form do not reflect the state of the cloud computing industry or the intended use of cloud computing. Furthermore, the Guidelines do not reflect emerging international standards on the subject. There is active work in the International Standards Organization (ISO) on service level agreements (SLAs) and the National Institute of Standards and Technology (NIST) has a work program on cloud standards. The development of a Singapore Standard that is, or will become, out of alignment with emerging international standards and industry best practices will increase costs and reduce the availability of cutting edge cloud computing services in Singapore. Moreover, cloud services are often provided on a global basis to customers who are equally global in nature. To impose Singapore specific requirements not only results in difficulties for cloud service providers (CSPs) that must conform with different service level requirements in different parts of the world, it also imposes different service levels within the customers' global operations despite a customer's desire to have a unique and consistent platform worldwide. For these reasons, establishing a Singapore-specific standard outside of global standards efforts is likely to impede Singapore's effort to attract investment as a cloud services hub.
Clause 4.1/Table 1	8-9	Multi-tiered COIR framework	There should be no requirement or expectation that a CSP's disclosure or communication would be made against the pre-defined "tiers" of Table 1. Most CSPs, especially hyper-scale, multi-tenant public cloud service providers offer a single tier of service, with commitments and obligations to the CSCs specified in the negotiated commercial agreements.
Clause 4.2/Criteria #1/Criteria #3/Table 2	11-15	**Criteria #1:** Availability % **Criteria #3:** Notification of planned maintenance to CSCs	Eliminate the prescriptive requirements (e.g. % Availability; Time to Notification; etc.) in Table 2. ▪ Many appear arbitrary and without reference to current and emerging technologies and business practices. ▪ For example, the requirement to provide notification of scheduled maintenance 6 months in advance is incongruous in a setting characterized by rapidly evolving technologies and threats. Such a requirement would not be practical and would in fact undermine the security that cloud service customers (CSCs) rightfully expect and demand if CSPs felt compelled to delay system improvements to

			comply with the Standard. ▪ Instead, the Standard should focus on clear and transparent communication of the CSPs commitments and obligations to the CSC, according to commercial agreements.
Clause 4.2/Criteria #8/Table 2/; Clause 6.1.2; Clause 6.2.1-Table 5 Clause 6.2.4	14;22-28	Clause 4.2: Notification by CSP to CSC as a result of incident detected by CSP Clause 6.1.2: Conduct assessment and analysis Table 5: Data Breach and Notification Clause 6.2.4: Manage data breach/lost implications	Eliminate data breach requirements. Data breach requirements are already established in Singapore law – merging outage incident response with data breach response in the Standard would complicate matters.
Clause 5.1.1.1	16	Cloud deployment models	The Standard should clearly indicate the shared responsibilities of the CSPs and CSCs across different cloud service models. In the end, as the CSC is the entity with the direct relationships both to its customers and the data the CSC provides to the CSP, the risks related to data remain those of the CSC.
Clause 1.2; Clause 7	7;29	Clause 1.2: Target Audience (CSCs, CSPs, and Regulators) Clause 7: COIR Self Disclosure	Cloud services provide advantages over on-premises and other information management architectures because they are flexible, extensible and scalable. Permitting CSCs to make decisions about service obligations at an individual contract level is a contributing factor in cloud computing's value to customers. Many of the requirements included in the Standard do not recognize the role of CSPs and CSCs in various cloud models. For example, in many cloud models, the CSP has no insight into the nature, content, sensitivity, or status of encryption of the CSC's data at the time of incident. Consequently, the CSP would have no insight into the legal or regulatory obligations of the CSC with respect to an outage incident or data breach. In addition, the Standard does not acknowledge that connectivity to a CSP's service is often influenced by factors, such as network access, which are wholly out of the control of the CSP.

Conclusion

Taken together, we feel these concerns argue against issuing a COIR Standard in the first place.

CSPs are constantly improving their outage response procedures in light of CSC expectations and feedback – as well as constantly evolving technology capabilities. Responsiveness to CSC needs and concerns is one way CSPs will compete for business. Our members are available to describe in detail the different ways they provide transparent and tailorable information to their users.

We and our member companies are eager to meet with relevant officials to discuss in more depth the nature of our concerns and how CSPs are already implementing plans and procedures to effectively deal with this important issue.

About BSA

BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, creating software solutions that spark the economy and improve modern life. With headquarters in Washington, DC, and operations in more than 60 countries, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy. BSA's members include: Adobe, Amazon Web Services, ANSYS, Apple, Autodesk, AVEVA, Bentley Systems, CA Technologies, Cisco, CNC/Mastercam, DataStax, DocuSign, IBM, Intel, Microsoft, Oracle, salesforce.com, SAS Institute, Siemens PLM Software, Splunk, Symantec, The MathWorks, Trend Micro, Trimble Solutions Corporation, and Workday.

About US-ASEAN Business Council

For over 30 years, the US-ASEAN Business Council has been the premier advocacy organization for US corporations operating within the dynamic Association of Southeast Asian Nations (ASEAN). Worldwide, the Council's 150+ membership generates over $6 trillion in revenue and employ more than 13 million people. Members include the largest US companies conducting business in ASEAN, and range from newcomers to the region to companies that have been working in Southeast Asia for over 100 years. The Council has offices in: Washington, DC; New York, NY; Bangkok, Thailand; Hanoi, Vietnam; Jakarta, Indonesia; Kuala Lumpur, Malaysia; Manila, Philippines; and Singapore.