13 May 2022

BSA SUBMISSION ON THE CYBERSECURITY CODE OF PRACTICE

Submitted Electronically to the Cybersecurity Agency of Singapore

BSA | The Software Alliance (**BSA**)[1] welcomes the opportunity to contribute towards the Cyber Security Agency of Singapore (**CSA**)'s proposed enhancements to the Cybersecurity Code of Practice (**CCoP**).

BSA is the leading advocate for the global software industry before governments and in the international marketplace. BSA's members are among the world's most innovative companies, creating software solutions that help businesses of all sizes in every part of the economy to modernise and grow. Many of BSA's member companies have made significant investments in Singapore, and we are proud that many Singaporean organisations and consumers continue to rely on our members' products and services to support Singapore's economy.

BSA recognises that the protection of critical information infrastructure (**CII**) is an important priority for governments all around the world and we fully support the Government of Singapore's efforts to update the CCoP to ensure the resiliency and improve the security environment of Singapore's CIIs.

BSA also appreciates the inclusive and wide-ranging industry engagement undertaken by the CSA to consult on the CCoP. BSA's submission is centred around 4 key recommendations that aim to improve security, build resilience, and encourage technological innovation while reducing unnecessary and counter-productive obligations.

Summary of BSA's Recommendations

- Ensure that the criteria for risk assessments are clear and well-defined, and aligned with internationally recognised standards.
- Remove the consultation (and implied approval) requirement and adopt modern approaches to security evaluation and monitoring.
- Avoid unintended localisation consequences.

[1] BSA's members include: Adobe, Alteryx, Altium, Amazon Web Services, Atlassian, Autodesk, Aveva, Bentley Systems, Box, Cisco, CNC/Mastercam, Dassault, DocuSign, Dropbox, IBM, Informatica, Intel, MathWorks, Microsoft, Nikon, Okta, Oracle, PTC, Rockwell, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc.

300 Beach Road
#30-06 The Concourse
Singapore 199555

P: +65 6292 2072
F: +65 6292 6369
W: bsa.org

Regional Representative Office
UEN: S97RF0005K

- Avoid defining requirements at the level of technical implementation which will develop faster than regulations can keep pace.

Recommendation 1: Ensure the criteria for risk assessments are transparent, clear and well-defined and aligned with internationally recognised standards

BSA understands that CSA intends to work closely with CIIOs, CSPs, and the sectoral regulators to develop risk assessment criteria relevant to the specific sector and industry. While in principle BSA is supportive of such an approach, it is important for CSA and the sectoral regulators to align risk assessment criteria with internationally recognised standards. For cloud services, these could include the International Organization for Standardization and the International Electrotechnical Commission 27001, 27017, 27018, etc.[2] Internationally recognised standards are typically developed in open, transparent, consensus-based processes which leverage global security expertise from governments, industry, and academia, and are widely adopted in the international marketplace.

Policies that are based on internationally recognised standards enable international interoperability, allow governments and businesses to better communicate at the technical level, have a track record of being developed and updated more efficiently than laws, increase competitiveness, incentivise innovation, and account for how technology is evolving. Ultimately, internationally recognised standards result in services that are more effective, efficient, and innovative, while also being less expensive. In contrast, regional, national, or local standards fragment this landscape and increase the costs to customers (including government customers) and decrease both the ability to provide innovative solutions and the number of cloud service providers competing for business.

More importantly, the integration of and alignment with internationally recognised standards in risk assessment, as well as transparency of these criteria, would provide greater clarity and certainty for both CSPs and CIIOs. This can then facilitate a more effective implementation across the different CII sectors.

Additionally, rather than conducting an audit of their vendors, CIIOs should leverage the vendor's existing, standards-based reports in their review of the vendor's cybersecurity posture. This will ensure consistent risk assessment results across vendors, reduce unnecessary costs, overheads, and complexities. It would also avoid potential confidentiality conflicts that could arise should CIIOs undertake, on their own or through a third-party firm, an audit of the vendor's internal operations or infrastructure.

BSA recommends amending Section 3.8.3 (c) as follows:

3.8.3 (c) Rights of the CIIO to ~~commission audit of vendor's cybersecurity posture; or~~ obtain a copy of the vendor's cybersecurity audit report.

Recommendation 2: Remove the consultation requirement and adopt modern approaches to security evaluation and monitoring

BSA notes that the requirement in Section 3.7.2 for the CIIO to consult with and impliedly obtain CSA's approval prior to moving to the cloud is to allow CSA to review CIIOs' due diligence when conducting their own risk assessment. However, a "consultation" approach should not be necessary given CSA's intention to work closely with the industry and sectoral regulators to develop the risk

[2] https://www.iso.org/standard/43757.html

assessment criteria. As CSA's policy intent is to ensure that CIIOs factor in national security interests when considering a move to the cloud, it is more important to ensure that there is sufficient discussion on the risks involved and that CSA provides adequate guidance on the risk assessment criteria.

Furthermore, traditional compliance audit and approval processes can only measure security up to a specific point in time and do not adapt well to the scale and continuous evolution of cloud services. Indeed, an over-reliance on "consultation" or "approval" (even as implied) may induce a false sense of security without adding material value in terms of cybersecurity. It could also negate and impede the ability of CIIOs to gain access to global supply chains, advanced security technologies and practices, and innovative solutions.

New software-enabled approaches to monitoring, auditing and compliance that automate these functions should also be considered as an alternative to the out-of-date "consultation" approach to provide flexibility and real-time visibility of the cloud environment's security posture.

BSA recommends that the consultation requirement be removed in Section 3.7.2 and to amend Section 3.7.5 as follows:

3.7.2 The CIIO shall ~~consult~~ notify the Commissioner when planning to move the CII to the Cloud.

3.7.5 **When planning to move CII components to the cloud,** the CIIO shall conduct a cybersecurity risks assessment to ensure that the risks of the CII moving to the Cloud are adequately addressed. The completed cybersecurity risks assessment must be formally accepted by the CIIO and submitted to the Commissioner no later than 30 days after completion for review.

Recommendation 3: Avoid unintended localisation consequences

BSA notes that Section 3.7.3 requires CIIOs to ensure that their CII assets in the Cloud are governed under Singapore laws and regulations. We are concerned that the current drafting of Section 3.7.3 could be interpreted to require such CII assets to be physically located in Singapore for them to be governed under Singapore's law and regulations.

While we understand that CSA's policy objective is not to localise data, we are concerned that the language in Section 3.7.3 could run contrary to Singapore's cloud-first policy and the strong commitments that Singapore has signed on to in its free trade and digital trade agreements regarding cross border data transfers. Indeed, Singapore's advocacy on cloud adoption and the importance of cross border data transfers has facilitated Singapore's digital transformation and the continued growth of its digital economy.

To be clear, BSA supports the risk-based implementation of security controls in the cloud, and BSA members work with their customers – including government customers – to implement the security controls they require to ensure regulatory compliance in the jurisdictions which they operate in. If CSA's policy objective is to ensure CII assets in the Cloud are in compliance with Singapore laws and regulations, **BSA recommends amending Section 3.7.3 as follows**:

3.7.3 The CIIO shall ensure that CII assets in the Cloud are **in compliance with relevant** ~~governed under~~ Singapore laws and regulations.

Recommendation 4: Avoid defining requirements at the level of technical implementation which will develop faster than regulations can keep pace.

Requirements articulated at a functional, rather than technical level, promote adoption of outcome-based capabilities that keep pace with technological advances. BSA notes that the requirements in Section 10.1 for CIIOs to adopt Domain Name System Security Extension (DNSSEC) are aimed at limiting vectors of attack against vital DNS services. However, requirement 10.1.1.3 is defined at a level of technical implementation that can limit implementation of protective DNS capabilities that serve to reduce security threats. Furthermore, while "implementing capabilities to validate the integrity of DNS records" would likely be achieved by adopting DNSSEC for now, this may not hold true especially as the industry continues to evolve and cybersecurity is enhanced.

BSA recommends that requirement 10.1.1.3 be amended as follows:

10.1.1.3 The CIIO shall ~~enable DNSSEC on the DNS Resolvers~~ **implement capabilities** to validate the integrity of the DNS records.

Additionally, the technical-level requirement for diversity of cybersecurity products can be interpreted as necessitating vendor diversity (e.g. two layers of firewalls from different vendors or firewalls from one vendor, and intrusion protection from another) which might lead to a proliferation of standalone cybersecurity products. This can undermine efforts to adopt an integrated cybersecurity architecture that improves threat visibility, facilitates automation, and builds a foundation for zero-trust and instead have the unfortunate effect of increased management and operational complexity without yielding demonstrable improvements in cybersecurity efficacy.

BSA recommends that requirement 3.5.4 be amended as follows:

3.5.4 (a) ~~Defence-by-Diversity of cybersecurity products~~ **Defence-in-depth through integrated security architectures that promote visibility and control automation** to reduce the attack vector; and

Conclusion

Once again, we would like to thank CSA for the opportunity to contribute to the review and drafting of the CCoP. We hope that our concerns and recommendations will assist in the development of enduring solutions to address the security of CII in Singapore. Please do not hesitate to contact me if you have any questions regarding this submission or if I can be of further assistance.

Sincerely,

Eunice Lim

Eunice Lim

Senior Manager, Policy – APAC

BSA | The Software Alliance