12 Nov 2020

Department of Home Affairs

Submitted Electronically

CRITICAL TECHNOLOGY SUPPLY CHAIN PRINCIPLES — BSA COMMENTS

BSA | The Software Alliance (**BSA**) appreciates the opportunity to provide comments to the Australian Government on the Critical Technology Supply Chain Principles[1] consultation document prepared as part of the review into how to protect critical technologies and their supply chains.

BSA is the leading advocate for the global software industry before governments and in the international marketplace. BSA's members[2] are among the world's most innovative companies, creating software solutions that spark the economy. BSA member companies have made significant investments in Australia and we are proud that many Australian organisations and consumers continue to rely on their products and services to support Australia's economy.

Managing security risks to critical technology supply chains is an important priority for both governments and businesses globally. When malicious actors exploit supply chain vulnerabilities, they can cause unacceptable harm to privacy, security, and commerce. Forward-looking national supply chain risk management policies are key to enhancing the security, integrity, and vitality of the global digital economy. On the other hand, misguided policy interventions aimed at improving security can introduce unintended consequences by causing severe damage to the technologies and economic activities they seek to protect.

BSA and Supply Chain Risk Management

BSA has produced a set of principles as a guide to governments on best approaches for national supply chain security policies.[3] The principles note that effective government approaches to supply chain security take a risk management approach and promote mechanisms such as transparency and fairness which help create an environment of certainty and predictability without limiting tools for mitigating risk. They call for governments to recognize the global, interconnected nature of supply

[1] Critical Technology Supply Chain Principles: A call for views, https://www.homeaffairs.gov.au/reports-and-pubs/files/critical-technology-supply-chain-principles-discussion-paper.pdf

[2] BSA's members include: Adobe, Amazon Web Services, Atlassian, Autodesk, AVEVA, Bentley Systems, Box, Cadence, Cisco, CNC/Mastercam, DocuSign, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens Industry Software Inc., Sitecore, Slack, Splunk, Synopsys, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

[3] BSA Principles for Good Governance: Supply Chain Risk Management, https://www.bsa.org/files/policy-filings/07172019bsasupplychainprinciples.pdf

300 Beach Road
#25-08 The Concourse
Singapore 199555

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

Regional Representative Office
UEN: S97RF0005K

chains and the threats against them, identifying and disrupting malicious actors through policies and processes that are sustainable, reciprocal, and transparent.

BSA's *Framework for Secure Software*[4] provides an in-depth approach to addressing software security that highlights the importance of understanding and managing risk in the software supply chain. The Framework recognizes that security is a persistent requirement. While the security of software, and its related supply chain at any moment in time is important to consider, it is far less effective than a sustained, security-focused approach to lifecycle management.

In addition to these documents, BSA is a strong supporter of the Prague Proposals.[5] The principles identified in the Proposals are focused on the deployment of 5G communications infrastructure, but are broadly applicable to technology supply chains more generally and include important concepts including transparency, fairness, collaboration, and interoperability..

BSA members lead a number of private sector initiatives to tackle the challenge of securing critical technology supply chains. These include the Charter of Trust[6] initiative with Cisco, IBM and Siemens, and the Cybersecurity Tech Accord[7] involving 90 signatories including Atlassian, Cisco, DocuSign, Microsoft, Oracle, Salesforce, and Trend Micro.

Suggested critical technology supply chain principles

The discussion paper proposes 10 principles divided across three "agreed pillars". The overall structure appears to be a sound approach for organizations to take when addressing supply chain risk. As a set of voluntary principles, they will be a valuable contribution to the supply chain security conversation in Australia. A voluntary and flexible risk management approach based on generally accepted industry practices is a more effective and inclusive approach to supply chain security.

It is unclear how the Australian Government intends to apply these principles in the longer term. The concern is that a regulator, State or Federal government entity, either explicitly or de facto require compliance with these principles across a certain class of companies or sector. This would erode their usefulness to flexibly guide supply chain security discipline in Australia. They would also require significantly more focus and rigor, clear measures of success, and a framework for reporting compliance. The Government should be explicitly in stating that the Principles are not to be used in that fashion.

One of the strengths of the Principles is that they are broad and can be flexibly applied to different parts in the supply chain. However, any accompanying documentation for the principles would be strengthened by making it clearer which entities in the supply chain they are addressing. The current paper addresses technology manufacturers in some sections and in others refers to procurers of technology. The considerations are not necessarily the same. To enhance clarity and better implementation in Australia it will be important for future documentation supporting the Principles to address different parts of the supply chain separately.

Security-by-design

BSA agrees that security should be a core component of critical technologies and should be built-in from the outset. The suggested principles proposed under this pillar aim to design security into critical technologies from the ground up by understanding what needs to be protected, understanding the security risks in the specific supply chain, build security considerations into the contracting process, and raising awareness in the supply chain.

---

[4] BSA Framework for Secure Software, https://sso.agc.gov.sg/Bills-Supp/37-2020/Published/20201005?DocDate=20201005

[5] The Prague Proposals: The Chairman Statement on cyber security of communication networks in a globally digitalized world, https://www.vlada.cz/en/media-centrum/aktualne/prague-5g-security-conference-announced-series-of-recommendations-the-prague-proposals-173422/

[6] Charter of Trust, https://www.charteroftrust.com/

[7] Cybersecurity Tech Accord, https://cybertechaccord.org/

Principle #2, “Understand the security risks posed by your supply chain”, is an important consideration for supply chain security, but could go further. BSA recommends that the Australian Government apply more of the risk management cycle to this principle with the following edit:

> “Understand and prioritize the security risks posed by your supply chain, **and mitigate critical risks.**”

Understanding is important but consumers of technologies should take a flexible approach to treat risks identified as critical and reduce them to an acceptable level.

BSA recommends that security by design consider the entire lifecycle of the critical technology, and that at present, the principles suggest a point in time analysis. BSA members have pioneered security by design for software development, including accounting for software supply chain security. The best practices developed from this experience are detailed in the *Framework for Secure Software* and can be used by both organisations developing software and by procurers of business software to better understand what makes software secure through its entire lifecycle.

Security that is measured at a single point in time is a useful data point, but security is a persistent requirement and so should encompass mechanisms and processes to secure a procured product or service throughout its entire lifecycle. This includes having an effective vulnerability discovery and disclosure program, mechanisms in place for timely fixes for identified issues, and clear information of expected support lifetime.

The Australian Government could further strengthen the security by design pillar by recommending that procurers of technology consider security of the product or service, and its supply chain, throughout its entire lifecycle, as an essential procurement requirement.

Transparency

Transparency is an essential component of supply chain security that provides visibility, traceability, and security of components to a procured product or service. Again, BSA recommends that companies take a risk management approach to building transparency into their supply chains.

BSA strongly supports all three principles proposed by the Australian Government – know who your suppliers are, set and communicate minimum transparency requirements, and encourage suppliers to understand their supply chains.

However, BSA is of the view that the principles could adopt a stronger position on transparency. BSA recommends that companies should take a risk management approach to documenting and to the extent feasible, tracing to their original source all components directly acquired and incorporated into hardware or software they have procured. The extent to which components and subcomponents are traced should be determined by a risk management analysis of their criticality to the business or access to critical data.

Relevant information may include the provider’s own processes for controlling access to software components, product development and testing standards, their own supply chain risk management practices, software development environment, and vulnerability management processes.

BSA also recommends that companies be aware of what suppliers are incorporating into their products and services to prevent counterfeiting or tampering, and validate the integrity of software.

Autonomy and integrity

Of the three suggested pillars in the paper, this is the least well-defined and its relationship with the security of the technology supply chain is least clear.

The paper takes a position that technology sourced from outside of Australia is less secure. However, when considering supply chain security, merely containing technology sourced from offshore is not necessarily a risky proposition. Considering the integrated way modern technology is developed and manufactured, an in-depth analysis of any manufacturers’ supply chains would mean very few, if any technologies would not source at least some aspect of their product from outside of Australia. What is important however, is how the technology is sourced, the security managed throughout its entire lifecycle, and how the supplier understands and mitigates any risks.

Principle #8 – Consider the potential influence of foreign governments on suppliers and whether they operate with appropriate levels of autonomy

BSA is generally supportive of this principle as a way to understand risk in the supply chain. However, it is important that this principle is applied with discrimination. Analysis of the potential influence of foreign governments should be supported by concrete intelligence or evidence of foreign governments' intent or behavior in connection with a particular supplier or class of suppliers. A supplier should not be deemed to be a risk simply because it has operations in a country of concern.

This principle could be further strengthened by explicitly stating that companies should take a risk management approach to dealing with the risk of government interference in the supply chain and consequently mitigate any risks that are unacceptably high.

Principle #9 – Consider if suppliers operate ethically, with integrity, and consistently with their human rights responsibilities

It is not immediately clear how the government proposes companies manage supply chain risk through this principle. As responsible entities, all companies should as a course of normal business only deal with suppliers that operate with the highest of ethical business practices, use ethically sourced products, seek low environmental impact inputs, and act with respect to human rights. However, the relationship with supply chain security seems spurious and could confuse the security focused process for some companies.

From a supply chain security perspective, BSA sees it as crucial that companies should be confident of the integrity of the product and its components is sound with respect to its sourced intellectual property, without counterfeit components, and free from tampering. Companies should also be cautious of fake claims of certification or certifications of dubious value that are not underpinned by widely used international standards.

BSA also notes the risks that can be introduced to the supply chain raised by the Australian Treasury regarding court order penalties imposed on company directors or practices such as phoenixing, bribery or corruption.[8] With respect to these concerns, the Australian Government could consider adding a recommendation for suppliers to 'operate legally' as part of Principle #9 and a consideration of whether the supplier will be able to support the product through the entire time it is in use by the company. Alternatively, the Government could suggest some analysis of the history of operations or the origin of the company as part of the risk assessment process.

Principle #10 – Build trusted, strategic relationships with suppliers

BSA supports the idea of companies maintaining good relationships with their suppliers of technology. However, it is also not explicitly clear how this principle contributes to the security of the supply chain. BSA recommends that companies take a risk management approach to building relationships with its suppliers and looks to build strategic partnerships with suppliers of critical technologies that are essential to the operation of their businesses.

What is missing?

The discussion paper asks respondents what may be missing from the proposed supply chain security policy. BSA suggests that the Australian government could also consider the following factors:

- Companies should consider the security of the product in transit from the supplier to the company, and via any intermediaries or agents, using mitigation strategies such as strong encryption and robust authentication of product integrity.

- The Government should support this effort by investing in the research and development of new technological approaches to fostering supply chain integrity.

[8] Black economy – increasing the integrity of government procurement, https://treasury.gov.au/sites/default/files/2019-03/c2018-t343354_01-Procurement_Connected_Policy_GL-1.pdf

- Government supply chain risk management efforts will be most effective when undertaken in collaboration with industry through private public partnerships aimed at sharing supply chain security information and jointly developing best practices.

- Companies may need help developing the skills to conduct supply chain risk management. The Government should consider a national training program to assist companies develop their risk management analysis workforces.

- The principles only deal with the first stage of the risk management process. Companies need to understand what their target state should look like, how to treat risks and that supply chain security is an ongoing process.

- Companies may need guidance on how to remediate supply chain security incidents.

- The Government could consider coordinating a supply chain vulnerability disclosure program on behalf of Australian companies.

The paper seems to presuppose that the greatest threat to supply chain security comes from other governments. Supply chains are also under constant pressure from non-state actors engaging in malicious cybersecurity activity, counterfeiting, product diversion, and related activities. A key element of a government's supply chain risk management strategy must be to pursue aggressive law enforcement against malicious actors within its jurisdiction, and work with governments more widely.

Conclusion

Security global supply chains will be an ongoing challenge — one in which security techniques must adapt to an ever-changing environment of new technologies and new threats. BSA commends the Australian Government for this contribution to technology supply chain security in Australia.

BSA thanks the Australian Government for having the opportunity to comment on the Bill and we look forward to continuing to collaborate with the government on supply chain risk management policies. If you require any clarification or further information in respect of this submission, please contact the undersigned at brianf@bsa.org or +65 8328 0140.

Yours faithfully,

Brian Fletcher

Director, Policy – APAC

BSA | The Software Alliance