OCSC
Oceania Cyber Security Centre

Critical Technology Supply Chain Principles – Public Submission

November 2020

1. Do you think there is a need for Government to address the security of critical technology supply chains?

Legacy physical systems lack security both at hardware and software levels making them vulnerable to high risks. Malicious threats cannot be easily prevented by just adding boundary security controls as potential vulnerabilities can stem from the lack of upgrading operating systems, inability to patch applications, poor software development practices, inclusion of vulnerable components or even deliberate inclusion of backdoors.

Governments need to play an important role in addressing the security of supply chain systems for critical processes such as critical technology and food security. However, it is not clear what the Government considers to be critical technology. It will be important to develop a clear definition with criteria and examples for determining what is considered critical technology. This definition should involve widespread consultation, though care must be taken to avoid an all-encompassing definition which loses focus on protecting what is important. An unnecessarily strict regulation of supply chains stifles innovation and limits the ability of organisations to compete on a global scale.

Further, any regulation of the supply chain of such technology must come with sufficient support to enable entities affected to respond effectively. Governments need to provide threat information related to supply chains and services for validating or verifying the security of components for critical technology.

2. How do you think the suggested Principles will help address the need for trusted critical technology supply chains? Does anything else need to be adjusted or included?

In order to build trust in the supply chain we would recommend adding the principle of openness, where participants in the supply chain are encouraged to make all relevant information (source code, designs etc) available for peer-review and independent testing.

This process will not only build trust but will result in more secure critical technology. Closed systems could masquerade as secure systems, but their lack of openness could result in creating a gateway for cyber harm to the whole sector. For example, previously unknown vulnerabilities and hidden backdoors have been exploited by various nation-state actors. These examples show that openness is necessary regardless of the origin of the products.

Another important aspect is the reliance on open source components. While open source software provides a lot of convenience for quick product development, the quality control and security evaluation for software components may become compromised. Security reviews and vulnerability scanning will improve the quality of open source components, resulting in a more secure outcome for all.

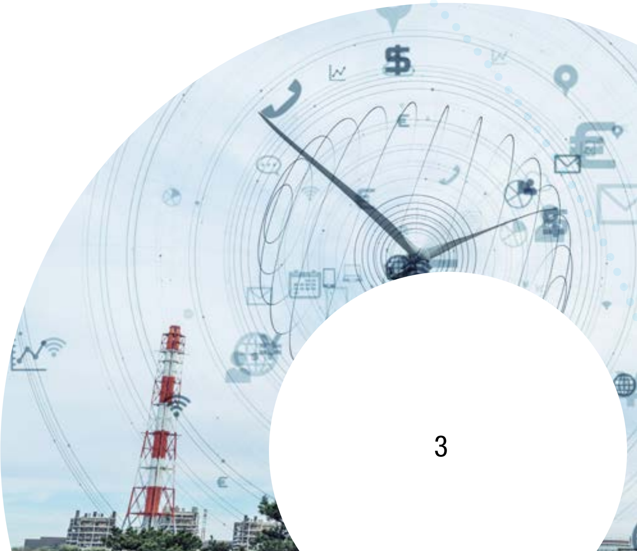
8. What could Government do to increase the uptake of the suggested Principles? What else do you think Government could consider to help make the supply chains of critical technologies more trusted and resilient?

In addition to adding the principle of openness, more needs to be done to ensure reliable processes are in place to assure the integrity of security updates and their timely deployment. It may be opportune for Government to work with other governments in developing international cyber rules of engagement, making these actions a crime that can be governed and prosecuted if unauthorised access to critical technologies occur in another country.

9. Is there anything else Government should consider when finalising the proposed Principles?

Ongoing support for critical technology will be important, so the supply chain to support and maintain such technology in the short, medium and long-term is assured. The relevance for a system-level view of support and maintenance is even stronger if critical technology relies on the availability of components accessed via the Internet, such as cloud services. If a device requires server access to properly function, security of these servers and their long-term availability needs to be ensured. With complex cloud interdependencies, the critical technology supply chain is truly global. Widespread consultation and exploration of these issues and how they impact critical technology must be considered.

Another important issue around supply chain is that sometimes supply chain security questions are mixed with political relations between countries. Technical guidelines should be just that and should not be used as a vehicle to support a political agenda. They should ensure that components are evaluated and vulnerabilities and backdoors in products can be detected, rather than only relying on trust to vendors. Established security testing can be enhanced with more recent research on detecting vulnerabilities via fuzzing and AI-supported approaches. These should be promoted and the development supported.



[1] www.reuters.com/article/us-usa-security-congress-insight/spy-agency-ducks-questions-about-back-doors-in-tech-products-idUSKBN27D1CS

Co-authors in alphabetical order:
Dr. James Boorman, Head of Research and Capacity, Oceania Cyber Security Centre
Professor. Iqbal Gondal, Federation University
A/Prof. Carsten Rudolph, Monash University

OCSC
Oceania Cyber Security Centre

Door 34, Goods Shed,
Village Street, Docklands VIC 3008

Email: info@ocsc.com.au

ocsc.com.au