kaspersky

Kaspersky Lab Singapore Pte. Ltd,
1 Harbourfront Place #09-05, Harbourfront Tower One,
Singapore 098633
Business Registration No. 201425483H

T +65 6870 2320
www.kaspersky.com.sg
www.securelist.com

Mr Andrew Hastie
Chairman
C/o: Committee Secretary
Parliamentary Joint Committee on Intelligence and Security
Parliament House

26 November 2020

Submission to the Parliamentary Joint Committee on Intelligence and Security

Review of the Operation of Part 14 of the Telecommunications Act 1997 – Telecommunications Sector Security Reforms

Dear Mr Hastie,

Kaspersky is grateful to the Parliamentary Joint Committee on Intelligence and Security (further, the 'Committee') for the opportunity to provide comments on the operation of Part 14 of the Telecommunications Act 1997, to the extent it was amended by the Telecommunications and Other Legislation Amendment Act 2017—Telecommunications Sector Security Reforms (further, the 'Act').

Our company remains supportive of the intention of the Parliament and Government of the Commonwealth of Australia to ensure the security and safety of its citizens. Below we provide our comments to Part 14, with a focus on (i) the security of critical and sensitive data; (ii) the adequacy of information-sharing arrangements between government and industry; and (iii) the sufficiency and effectiveness of the administrative guidelines in providing clarity to industry on how it can demonstrate compliance with the requirements set out in the Bill.

Security of critical and sensitive data

For the purposes of security, subsections 313 (1A), (1B) and (2A) of the Act ask carriers, carriage service providers and carriage service intermediaries to do their best to protect the telecommunications networks and facilities they own, operate or use from unauthorized interference or unauthorized access. While the Telecommunications Sector Security Reforms (TSSR) Administrative Guidelines provide examples of how these security obligations should be implemented, **the implementation process includes aspects that are not defined and which may therefore pose risks to ensuring the security of critical and sensitive data**. In particular, these aspects include:

1. **Decision-making and evaluation criteria in assessing the changes planned by the Communications Access Coordinator.** The Act does not provide clarity on particular evaluation criteria to be considered in assessing the changes submitted by the carrier or provider. This subjects the technical evaluation process to too much subjectivity of the administrative decision-maker, who may not be well-placed to make a sound judgment call, which ought to be based on specific knowledge and technical competence. Without the third party's technical expertise and balanced technical option on how planned changes might impact the obligations of carriers or providers, the security and integrity of their services might be greatly undermined.

kaspersky

Kaspersky Lab Singapore Pte. Ltd,
1 Harbourfront Place #09-05, Harbourfront Tower One,
Singapore 098633
Business Registration No. 201425483H

T +65 6870 2320
www.kaspersky.com.sg
www.securelist.com

2. **The mechanism to challenge/object to the decision of the Communications Access Coordinator**. If the decision of the Communications Access Coordinator raises concerns over a potential risk that the security and integrity of telecommunications services are undermined, the Act does not provide effective mechanisms for carriers or providers to challenge the decision or to call for a review of the decision by an overriding authority. A more balanced approach, given the burden which carriers and providers bear in order to comply with the Act, would be to provide a mechanism for them to call for a review of the Coordinator's decision should the need arise. Understandably, however, there may be frivolous objections which ought to be deterred. Frivolity issues can be circumvented by setting out clear criteria that must be met before such objections can be filed, complete with substantive evidence as proof.
3. **The authority to require carriers or providers to ensure transparency in their regulatory compliance**. Absent in the draft are provisions that would require carriers or providers to ensure transparency in their regulatory compliance and thus ensure the trust and confidence of their customers. If carriers or providers are not explicitly required to disclose their security and notification obligations with their customers, this would undermine customers' trust that the security of customer data is ensured as well.

Adequacy of information-sharing arrangements between government and industry

Subsection 315A provides that the Minister may issue a direction not to use or supply, or to cease using or supplying a carriage service if: (i) a person who is a carrier or provider uses or supplies, or proposes to use or supply, for their own benefit, one or more carriage services; and (ii) the Minister, after consulting with the Prime Minister, considers the proposed use or supply would be prejudicial to security. The Act highlights that the direction is to be given after an *adverse security assessment* as defined by section 25 of the Australian Security Intelligence Organization Act 1979. However, after consulting with the 1979 Act, it remains unclear what (1) an adverse security assessment would include; and (2) whether there are effective mechanisms for carriers or providers to challenge the outcome of an assessment in order to avoid risks to the security and integrity of their services.

Furthermore, subsection 315H (1) provides a possibility for a person to obtain information or a document under section 31314A, 314B, 314C, 314D, 315C or 315H (1) and disclose the information, or provide the document (or a copy of it) to another person. However, it is not clear who this person would be or whether the Act includes the necessary safeguards to ensure that the information would be treated in a secure way.

Therefore, these aspects need to be clarified to ensure the adequacy as well as transparency and accountability of information-sharing arrangements as prescribed by the Act.

Adequacy and effectiveness of the administrative guidelines

Administrative guidelines are essential for industry to ensure effective implementation and regulatory compliance, and the TSSR Administrative Guidelines are very helpful in this regard. However, there are several aspects that are currently defined neither in the Guidelines nor the Act:

1. While the Guidelines say that the most effective way for carriers and providers to comply with their Security Obligation would be to 'do their best' and 'adopt a risk-based approach to protecting networks and facilities', **the Guidelines do not provide a list of necessary organizational and technical measures to be taken by companies**. We believe a more prescriptive set of measures

kaspersky

Kaspersky Lab Singapore Pte. Ltd,
1 Harbourfront Place #09-05, Harbourfront Tower One,
Singapore 098633
Business Registration No. 201425483H

T +65 6870 2320
www.kaspersky.com.sg
www.securelist.com

taking reference from existing standards and industry best practices would be a helpful tool for carriers and providers.

2. The TSSR Administrative Guidelines mention the necessity to ensure 'effective control' and, in particular, addressing issues of data sovereignty has been listed as an example of how carriers and providers can demonstrate this. However, **it is unclear what actions would be deemed sufficient to 'address issues of data sovereignty' or what 'issues of data sovereignty' would imply in particular.** In light of global discussions on data regulation and data sovereignty, clarifying the position of the Australian government in this regard would be helpful.
3. In clarifying what triggers the Notification Obligation, the TSSR Administrative Guidelines list 'new access technologies', **but do not provide clarity on how this should be interpreted by carriers and providers**. Given the rapidly developing technologies and their introduction in the operations of carriers and providers worldwide for delivering innovative solutions, we believe this should be clarified to make sure that the Act does not make parts of the Notification Obligation redundant and thereby stifle innovation and economic development.

   Additionally, we would like to ask for further clarification on how 'entering into arrangements to have telecommunications information accessed by persons outside Australia' should be interpreted as well in this regard. In case of businesses that have both organizational and technical personnel outside Australia, they need to ensure the free flow of internal business information for the efficiency, integrity and security of their services. The lack of clarity on this risks making parts of the Notification Obligation redundant and undermining the operations of international businesses.

Conclusion

We remain strong advocates of cooperation between the government and industry to ensure the security and safety of Australian citizens. We also believe that transparency and accountability need to be provided in the decision-making process from government and industry to ensure user trust and confidence in technology products and services produced and/or sold in Australia. Therefore, we are grateful to the Committee for the opportunity to review part 14 and share our feedback. Should clarifications be required in regard to this submission, we remain available for further discussions, and firmly believe that further consultations with industry on enhancing the effectiveness of part 14 would be beneficial.

We hope that our feedback as above will be useful for the Committee's consideration. For more information, or to discuss the contents of this submission, please contact our Head of Public Affairs, APAC, [redacted] Thank you.

About Kaspersky

Kaspersky is a global cybersecurity company founded in 1997. Kaspersky's deep threat intelligence and security expertise is constantly transforming into innovative security solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. The company's comprehensive security portfolio includes leading endpoint protection and a number of specialized security solutions and services to fight sophisticated and evolving digital threats. Over 400 million users are protected by Kaspersky technologies and we help 270,000 corporate clients protect what matters to them most. Learn more at www.kaspersky.com.