BSA Comments on the Fifth Report (Draft) from IP Network Facilities Subcommittee

August 3, 2021

BSA | The Software Alliance (**BSA**)[1] appreciates the opportunity to submit the following comments to the Ministry of Internal Affairs and Communications (**MIC)** on the "Fifth Report from the IP Network Facilities Subcommittee (Draft)" (**Draft Report**).

General Comments

BSA is the leading advocate for the global software industry in the international marketplace and our members are at the forefront of software-enabled innovation that is fueling global economic growth, including cloud computing, the Internet of Things (**IoT**), artificial intelligence (**AI**), and other innovative products and services.

BSA appreciates MIC's efforts to improve the security and reliability of communication services and networks by reviewing the current system for reporting and verifying communication accidents. In order to support MIC's goal, we provide the below observations and recommendations.

Observations and Recommendations

IV / Chapter 2 / 2. 2. Review of Reporting System for Communication Accidents 2.2.2 Approach to Reporting System for Communication Services and Networks Provided to the Critical Infrastructure Sector

Section 2.2.2 of the Draft Report explains the quantitative and qualitative changes in risks as well as the expansion of risks to multi-stakeholders, which calls for the need to

[1] BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry. Its 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 modernize and grow. With headquarters in Washington, DC, and operations in more than 30 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. Follow BSA at @BSAnews.

BSA's members include: Adobe, Altium, Amazon Web Services, Atlassian, Autesk, Aveva, Bentley Systems, Box, Cisco, CNC/Mastercam, Dassault, DocuSign, IBM, Informatica, Intel, MathWorks, Microsoft, Nikon, Okta, Oracle, PTC, Rockwell, Salesforce, ServiceNow, Siemens Industry Software Inc., Slack, Splunk, Synopsys, Trend Micro, Trimble Solutions Corporation, Twilio, Workday, and Zoom.

review the scope of serious accidents, incidents, etc., and targets for prompt reporting. With this view, the Draft Report provides a detailed examination of the number of affected users while also indicating the need for qualitative elements to be added to better prioritize reporting. While we fully acknowledge MIC's intention to clarify the standards for communication accidents, we recommend MIC focus on the qualitative elements to ensure that accidents with the most societal impact are given priority for reporting and analysis/assessment. If the reporting rules rely on the number of affected users alone, they may result in capturing or prioritizing widely used, but non-essential communications, such as entertainment related communications, while a service that is essential to emergency responders in which its extended outage may result in serious consequences, including the loss of lives, is overlooked. We encourage MIC to consider these factors in the review process.

2.2.2 / (4) Approach to Establishing a Reporting System for Communication Accidents in the Case of Communication Service Network Accident Amongst the Critical Infrastructure Service Failures Caused by Communication Accidents of Cloud Services as Communication Service

The Draft Report also explains that cloud services are increasingly intertwined with critical infrastructure (**CI**) and may be subject to the reporting system. It is important, however, that the "shared responsibly model" of cloud services is acknowledged, with cloud service providers (**CSPs**) and their customers taking on different responsibilities in cloud operations for the establishment and maintenance of security controls to manage risk. Understanding this model will help clarify which entity is responsible for the aspects of the environment over which they have control and are accountable. In order to ensure the reporting system effectively mitigates risk, we recommend MIC focus on developing a system in which CI operators using cloud services retain the primarily obligation to report cloud service outages affecting their operations and to analyze/assess the impact of such outages on their operations, rather than misplacing this obligation on CSPs that often do not have direct visibility into the applications and data running on their infrastructure and platforms that are under the direct control of the CI operators. CSPs, therefore, are not in position to confirm which customers use their services to deliver telecommunication services to their own customers.

Further, as the Draft Report rightfully acknowledges, cloud service users can select and use functions and services by themselves, using a single or multiple data centers, or even multiple regions, and these users — not their CSPs — are best positioned to understand how their choice of cloud services will change their IT environment as well as identify laws and regulations applicable for their specific use.

Also, depending on their relationship with their CI operator, the specific contractual arrangements between the parties, and the nature of the accident in question, a CSP may not be able to effectively report such outages or accidents directly to MIC.

A CSP may not be aware of specific outages in the first place and would have much less capability to analyze/assess the impact of the outage or accident on their customers. CI operators may require the CSPs to provide relevant information related to accidents or

outages pursuant to contractual arrangements with their CSPs. Requiring CSPs to directly report information regarding accidents to MIC could conflict with contractual arrangements between the CSP and the CI customer, where the CSP may be prohibited from sharing detailed information with third parties.

Ensuring that any reporting system recognizes the primary role of CI operators in assessing and reporting accidents and outages to MIC will contribute to MIC's timely awareness of the actual impact of accidents and outages on relevant CI and would clarify the relevant responsibilities of CSPs and their customers. CSPs providing infrastructure services to CI operators support their customers accident reporting obligations by offering cloud-based services such as service availability dashboards or service analysis reports and similar capabilities. These tools assist their CI operator customers to report appropriate and correct information to their own customers and MIC, pursuant to Telecommunication Business Act. As indicated in the Draft Report, it is important for CSPs and CI operators as cloud service users to collaborate and have interactive communication to understand the impact of cloud service failure on cloud service users and to take actions based on such understanding.

As MIC continues to work on improving the current reporting/verification system, including considering whether to expand the scope to include CSPs, we encourage MIC to collaborate with and solicit views from a wide range of stakeholders to ensure that the envisioned system is effective and implementable. There are large differences between different kinds of cloud services (e.g., IaaS, PaaS, and SaaS) and the impact on CI customers and society at large arising from accidents will depend on the type of cloud service involved and many other factors. As CI operators shift more workloads to the cloud, MIC should purposefully engage with CSPs before considering developing new requirements that would affect them. This will help MIC avoid imposing unnecessary requirements on CSPs while promoting safe and reliable communication services and networks for CI. We therefore recommend MIC to fully consult with variety of stakeholders to consider the best approach.

To promote such efforts, BSA and our members welcome the opportunity to collaborate with MIC and relevant stakeholders to raise awareness among cloud service users, including through educational sessions, and to identify or develop information sharing best practices under the shared responsible model. We also encourage MIC to continue to acknowledge the value of internationally recognized industry standards for reporting mechanisms.

Conclusion

BSA hopes the above comments will be useful as you finalize the Draft Report and continue to examine the direction to update the reporting/verification system. We look forward to working with MIC to improve the system to better respond to and prepare for the changing risk environment. Please let us know if you have any questions or would like to discuss these comments in more detail.