BSA Comments on the Draft of IoT/5G Security Comprehensive Measures 2020

June 25, 2020

BSA | The Software Alliance (**BSA**)[1] appreciates the opportunity to submit the following opinions to the Ministry of Internal Affairs and Communications (**MIC**) on the **"Draft IoT/5G Security Comprehensive Measures 2020"** (**draft Measures**).

General Comments

BSA is the leading advocate for the global software industry in the international marketplace. 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 products and services that will build on the foundation of 5G network infrastructure and services to bring about new innovation. As global leaders in the development of data-driven products and services, and in advancing cybersecurity, BSA has developed a Cybersecurity Agenda[2] that urges governments around the world to embrace software solutions to address priority cybersecurity challenges, seeking to expand and make interoperable efforts to strengthen cybersecurity through robust public-private collaboration and broad-based international cooperation. Specifically, we strongly support a partnership between government and industry to:

- Promote a secure software ecosystem by leveraging industry standards, developing novel tools to understand critical security information, and strengthening security research and vulnerability disclosure.
- Advocate collaborative approaches to strengthen supply chain security by supporting interoperable, risk-based supply chain security policies, strengthening the security of 5G and software supply chains, and prioritizing cybersecurity in government acquisition.
- Pursue international consensus for cybersecurity action by supporting international standards development as well as working to align international security laws and promote agreement on global norms.
- Develop a 21st century cybersecurity workforce by increasing access to computer science as well as science, technology, engineering, and mathematics (**STEM**) education, opening new paths to cybersecurity careers, and empowering workers with technology.
- Advance cybersecurity by embracing digital transformation, advancing innovative cloud security solutions, leveraging the potential of emerging technologies, and forging innovative partnerships to combat emerging risks.

The draft Measures align closely with these priorities. We commend MIC for recognizing the importance of workforce and human resource development, investment in research and

[1] BSA's members include: Adobe, Amazon Web Services, Atlassian, Autodesk, AVEVA, Bentley Systems, Box, Cadence, Cisco, CNC/Mastercam, 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.

[2] "Securing Tomorrow: BSA's Cybersecurity Priorities and Software's Essential Role" https://bsacybersecurity.bsa.org/wp-content/uploads/2020/02/02032020BSACybersecurityAgenda.pdf

22F Shibuya Mark City West
1-12-1 Dogenzaka Shibuyaku,
Tokyo 150-0043

P +81 3 4360 5473
F +81 3 4360 5301
W bsa.org

Japan Representative Office

development (**R&D**), public-private cooperation, international cooperation and standardization, and advancing security-by-design.

Furthermore, we also would like to take this opportunity to express our deepest appreciation for the hard work undertaken by the Government of Japan during this current global pandemic. BSA members have been supporting governments around the world, launching an array of initiatives to provide relief and support.[3] Enterprise software companies are providing advice and often free resources to educators and businesses, directing supercomputing and analytics tools for urgent medical research, donating emergency funds, and embracing collaborations as we work to together to rise to the challenge.

As part of this initiative, BSA recently developed its Response & Recovery Agenda[4] (**R&R Agenda**), providing recommendations for governments to build a resilient and accessible remote economy. The R&R Agenda calls on governments to promote strong cybersecurity practices, support robust incident response capacity, and, in recovering from the pandemic, advance universal, affordable, secure high-speed Internet access, including 5G networks, and promote responsible migration to advanced cloud services.

We see that these views are aligned with MIC's draft Measures, and below, we would like to add specific comments to support the Government of Japan to further enhance security to recover from COVID-19, strengthen the resilience of the Japanese economy, and prepare for the Tokyo Olympics and Paralympics Games in 2021.

Specific Comments Regarding the Measures

I - (2) Major Policy Issues in the Revision - ①Promoting Security Measures in Response to COVID 19 - 1) Responding to Increased Use of Telework / Ⅲ - (5) Institutionalization and Promotion of Trust Services

We are encouraged that MIC is actively promoting telework and staggered work hours, recognizing the necessity for further digitization of documents and business operations to prevent situations requiring employees to come to the office to process paper documents such as managing invoices, affixing seals, and printing. In this sense, the current discussion at MIC to promote trust services, including time stamps, remote signatures, e-seals, and the establishment of a public framework that certifies these services, will be critical. We encourage the Government of Japan to modernize the Act on Electronic Signatures and Certification Business (Act), as it was enacted in 2000 when cloud services were not yet widely adopted. The Government of Japan should ensure that requirements for compliance with the relevant standards appropriately enable the use of today's technology so that private companies may fully leverage digital-signatures and electronic time stamps to validate documents. During the state of emergency declaration in response to COVID-19, workers were required to go to offices simply because the law does not recognize remote-signature or time stamps as official legal means for authentication.

Based on the draft Measures, the discussion regarding a national certification system and standards as well as positioning of trust services in existing law are expected to be concluded within two years. We encourage the government to accelerate driving this initiative and actively involve the private sector in this process. For these services to be adopted widely in society the government must ensure that the services are easily accessible and usable for everyone from any device, and the government itself across all Ministries must widely adopt these services. We also encourage the government to introduce various use cases to facilitate implementation and continue to actively promote adoption of cloud services that function as the key foundation for all remote-based activities.

---

[3] To learn more, see https://www.bsa.org/covid19.

[4] BSA Response and Recovery Agenda https://www.bsa.org/policy-filings/bsa-response-recovery-agenda

Ⅲ - (3) Security Measures for Cloud Services

The draft Measures indicate the government's plan to promote cloud adoption across ministries through the introduction of the Information system Security Management and Assessment Program（**ISMAP**), which recognizes the "shared responsibility model", the common recognition that responsibilities for the management of the cloud environment, including security, are shared between service providers and service users and procurers. The draft Measures also highlight the importance of improving the literacy of not only service providers but also service users and procurers. As cloud services become more integral to IoT and 5G networks and the many applications and services they support, cloud environments will become more complex and dynamic. Vendors offer a range of security services that customers embed within their cloud environments, such as embedded identity management or threat monitoring services. Roles and responsibilities may also differ across different types of cloud services, such as Infrastructure-as-a-Service or Software-as-a-Service.

Therefore, when developing comprehensive security policies, MIC must enable careful distinction of roles and responsibilities within such diverse environments and should stress the need of raising security awareness under the shared responsibility model.

III - (7) Security Measures of Information and Communications Sector as Critical Infrastructure

We also welcome MIC's ongoing review on updating the Guidelines for Information Security Policies in Local Governments (**Guidelines**), responding to requests from local governments to improve usability by enabling greater alignment of recent developments in government policies, including the cloud-by-default principle and the enactment of the Digital Procedure Bill, as well as promoting more teleworking in local governments. BSA continues to encourage MIC to revise the guidelines to focus on CSPs handling data securely appropriately and in accordance with the governing law, rather than the location of data centers, to ensure that CSPs can utilize regional and global infrastructure to store and process data. We also urge MIC to eliminate the recommendation on physical network separation from the Internet, or at least to narrow the scope of the recommendation, to enable local governments to fully leverage cloud services to provide enhanced digital government services to residents.

We also strongly recommend granting local governments the autonomy to select the best IT solutions and information security approaches based on commercially negotiated cloud services agreements to fit their needs, coupled with active information-sharing on the adoption of best practices. Providing flexible guidance that enables mobility, choice of services, and autonomy allows local governments to make the best choices on systems needed to effectively support citizens.

Ⅲ - (1) IoT Security Measures / IV – (3) Promotion of International Collaboration - ③Promotion of International Standardization

Upon developing IoT security policies, BSA recommends MIC be informed by, and to the extent possible, aligned with other similar efforts underway around the world. As more governments rightly focus on this pressing issue, the risk of fragmentation among policies increases, which would be problematic as IoT solutions are inherently interconnected and interdependent. As government approaches to IoT security take shape, security will suffer if multinational technology companies are deterred from developing and deploying the best security solutions by national and international policy landscapes that are disjointed, incoherent, and conflicting. Such an outcome will suppress innovation and competitiveness, interoperable approaches to IoT security are critical for Japan and the global economy.

In this respect, we recommend MIC ground IoT security policies on internationally recognized standards. In addition to facilitating interoperability, such standards enable consistent security outcomes based on the consensus of industry, government, and academic experts. Though they should not substitute for consensus-based international standards, industry best practices can also be useful in guiding IoT device and component manufacturers. In addition, MIC should expand security considerations beyond a focus on measures for IoT devices to include harnessing the network and carrier infrastructure to safeguard such devices (e.g. secure onboarding, access policy, threat monitoring, domain name service layer security).

BSA has been engaging in industry consensus-building efforts, developing widely accepted security guidance. For example, the BSA Framework for Secure Software[5] draws on best practices from leading enterprise software companies for assessing and encouraging security across the software life cycle, including the software that powers IoT solutions and 5G. We encourage MIC to reference these materials when considering security approaches. We also would like to highlight that the C2 Consensus[6] on IoT Security Capabilities brings together a group of 20 major cybersecurity and technology organizations to provide guidance to IoT device manufacturers on important security capabilities that IoT devices need to meet the market's security expectations and make policies interoperable around the world.

Also, with respect to the security-by-design approach indicated in the draft Measures, we want to add that long-term security requires a life cycle management approach for maintaining software, hardware, and firmware components and measures addressing vulnerabilities post-deployment.

III- (2) 5G Security Measures - ①Establishment of Vulnerability Verification Methods and Development of System / ②Building a Framework for Information-Sharing on 5G Vulnerability and Threat

Vulnerabilities are often identified by independent security experts and others in research communities and reported to vendors. Security professionals have developed guidance and standards on coordinated vulnerability disclosure (**CVD**) programs[7] to address this critical need; all such programs should be aligned with the internationally recognized ISO/IEC 29147[8] and 30111[9] standards.

To improve security outcomes throughout the IoT life cycle, policymakers should incentivize businesses to voluntarily establish CVD processes that (1) align with internationally recognized standards, particularly ISO/IEC 29147 and 30111; (2) avoid counterproductive requirements, such as artificial mitigation timelines; and (3) reflect a holistic approach to vulnerability management throughout the life cycle of the IoT solution.

The draft Measures highlight a concern about the vulnerability of hardware caused by maliciously inserted chips. Suppliers are increasingly developing capabilities to validate vendor supply chain security to detect and mitigate infrastructure and service tampering. Anti-tamper technologies such as trust anchors and software image signing can provide assurance of the authenticity and integrity of hardware and software components. We recommend working with industry to expand adoption of such measures to address risks cited in the Measures.

---

[5] BSA Framework for Secure Software: https://www.bsa.org/reports/bsa-framework-for-secure-software

[6] https://securingdigitaleconomy.org/wp-content/uploads/2019/09/CSDE_IoT-C2-Consensus-Report_FINAL.pdf

[7] For more on software vulnerability disclosure, see the BSA Guiding Principles for Coordinated Vulnerability Disclosure, https://www.bsa.org/files/policy-filings/2019globalbsacoordinatedvulnerabilitydisclosure.pdf. On hardware vulnerability disclosure, see Center for Cybersecurity Policy and Law, "Improving Hardware Component Vulnerability Disclosure," https://centerforcybersecuritypolicy.org/improving-hardware-component-vulnerability-disclosure.

[8] https://www.iso.org/obp/ui/#iso:std:iso-iec:29147:ed-2:v1:en

[9] https://www.iso.org/standard/69725.html

Ⅲ - (2) 5G Security Measures

As the foundation of 5G networks, innovative software-powered tools and techniques will fundamentally reshape how 5G networks operate — and how they can be secured. The government should incentivize the adoption of software-enabled solutions to address security challenges. Specifically, investing in technologies to virtualize network functions, using new software innovations to enhance cybersecurity, and prioritizing security in 5G research and development will all maximize the impact of security efforts related to 5G networks, which are approaches MIC recognizes in the draft Measures.

In this view, we specifically recommend government policies to emphasize the need for open standards and open-source-driven architecture. Radio Access Network (**RAN**) technology offers one important example of the way that software can be leveraged to address security challenges. The RAN market is currently dominated by a handful of vendors, some of whom have been associated with supply chain security concerns. Virtualizing the RAN — through approaches such as Virtualized Radio Access Network (**V-RAN**) and Open RAN technologies — can unlock competition and advance security at the network's edge.

Likewise, software-based technologies such as Software-Defined Networking, Network Slicing, and Network Function Virtualization bring new opportunities to mitigate cyber risks. Policymakers should develop guidance, invest in R&D, and pilot promising approaches to apply these technologies to new security techniques to segregate suspicious traffic, protect sensitive information, authenticate users, and address other key security needs. By adopting approaches such as deploying Zero Trust architectures (where there is explicit authentication between all assets in all areas), ensuring integrity (through the deployment of trustworthy products that continuously monitor and mitigate against tampering), enabling full visibility (to allow anomalous behaviors and communications to be detected), implementing segmentation (to partition asset groups appropriately to limit the impact of any compromise), and deploying effective threat protection (to provide defensive security controls and continuous monitoring with machine learning capabilities), a secure 5G environment can be built and rolled out.

As 5G becomes increasingly deployed across numerous sectors, there is a risk of incoherent and overlapping governance. 5G will be a critical technology in the communications sector (where 5G will provide ultra-reliable and low latency communications), the transportation sector (where 5G will enable broader adoption of intelligent traffic management), the health care sector (where 5G will support life-critical medical devices and remote operations), the manufacturing sector (where 5G will enable smart manufacturing through remote and assistive robotics), and others. Whereas previous generations of communications networks could be regulated strictly as telecommunications services, 5G depends on core infrastructure — such as cloud services — that simultaneously serves multiple functions and clients, making it a poor fit for traditional telecommunications-specific regulations. Successful governance will require a unified approach across sectors and agencies. Such governance mechanisms must be flexible and build risk-based approaches that tailor compliance requirements to each 5G network's specific uses and threats. Therefore, we encourage MIC to establish effective mechanisms to drive coordination with other agencies for coherence.

I - (2) Major Policy Issues in the Revision – ④Acceleration of Industry-Academic-Government Cooperation for Improvement of Cybersecurity Self-sufficiency in Japan / IV - (1) Promotion of Research and Development - ①Establishment of an Integrated Cybersecurity Intellectual Infrastructure

Cybersecurity threats are by nature global and not bound by national borders. Useful threat intelligence on cyber-attacks require the widest visibility possible for effective analysis and research.

This visibility can come from a range of sources, including customer install bases, published vulnerabilities, threat sharing networks, in addition to the options mentioned in the draft Measures such as open-source intelligence (OSINT) (at IV(1)①) and sector-specific information sharing and analysis centers (ISAC) (at III(1)③ and at IV(3)②). The ability to source threat information globally for meaningful analysis does not depend on the physical location where threat research is conducted. Domestic vendors in Japan, as with overseas operators, can undertake such research and derive actionable threat intelligence by drawing on threat information from worldwide sources, not just Japanese sources. Threat information sharing arrangements between domestic and foreign vendors can be an effective means to gather useful threat data to develop such domestic capabilities and avoid a "data loss spiral" described in the draft Measures. Many of BSA's members facilitate such intelligence sharing arrangements. We encourage MIC to strengthening information sharing and training for engineers in global scale, and avoid the risk of Japan-unique cybersecurity model being disjointed from the rest of the world, which could hinder Japan's interest to lead cybersecurity internationally.

Conclusion

BSA hopes the above comments will be useful as you finalize the draft Measures. We support MIC's international leadership on cybersecurity matters in support of Data Free Flow with Trust. In the future, we encourage the Government of Japan to provide a longer period for responding to calls for public input on draft policy proposals 60 days, instead of only 19 days, would better provide sufficient time to review and analyze the draft documents and for interested stakeholders to properly coordinate our positions and recommendations and to provide thoughtful and constructive input into the policy development process. Also, we want to note that BSA is currently developing principles on IoT and 5G security to support governments around the world in developing security policies. Please let us know if you have any questions or would like to discuss these comments in more detail.