BSA Recommendations to NISC re: 2019 Implementing Plans for Japan's Cybersecurity Strategy

February 25, 2019

BSA | The Software Alliance (**BSA**)[1] welcomes this opportunity to provide input to the National Center for Incident Readiness and Strategy for Cybersecurity (**NISC**) on measures to implement the Government of Japan's Cybersecurity Strategy during 2019. BSA applauds NISC for its continuing leadership on cybersecurity both in Japan and in the region, its conscientious collaboration with industry stakeholders in the development of cybersecurity policies, and its intent to take concrete measures in 2019 to implement the Cybersecurity Strategy compiled in 2018.

Statement of BSA Interest

BSA's members are at the forefront of data-driven innovation, developing and offering essential software, security tools, communications devices, servers, and computers that drive the global information economy and improve our daily lives. Our members develop essential technologies, including industrial control systems and Internet of Things (IoT) devices, that will form the backbone of the digitally connected industry discussed in the Cybersecurity Strategy's vision of *Society 5.0*. They earn their users' confidence by providing security technologies to protect these users and technologies from cyber threats. BSA's members thus have a significant interest in the implementation of the Cybersecurity Strategy and are eager to collaborate with NISC in developing effective approaches to improving security across Japan's connected economy.

General Comments on 2019 Implementation of the Cybersecurity Strategy

The Cybersecurity Strategy offers a compelling vision for enhancing cybersecurity in Japan and globally. Its emphasis on multi-stakeholder collaboration presents the optimal pathway to the development of smart, practical, effective policies that can markedly advance security and bolster the digital economy at the same time. As NISC considers how to pursue implementation of the strategy in 2019, BSA recommends that implementation measures be grounded in six overarching principles, which are described in BSA's *International Cybersecurity Policy Framework:*[2]

1. *Policies Should Be Aligned with Internationally Recognized Technical Standards.* Internationally recognized technical standards provide widely vetted, consensus-based frameworks for defining and implementing effective approaches to cybersecurity and

[1] BSA (www.bsa.org) is the leading advocate for the global software industry before governments and in the international marketplace. BSA's members include: Adobe, Akamai, Amazon Web Services, Apple, Autodesk, AVEVA, Bentley Systems, Box, Cadence, Cisco, CNC/Mastercam, DataStax, DocuSign, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, Siemens PLM Software, Slack, Splunk, Symantec, Synopsys, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

[2] The BSA International Cybersecurity Framework is available on-line at: https://bsacybersecurity.bsa.org/wp-content/uploads/2018/04/BSA_cybersecurity-policy.pdf. More information is available at https://bsacybersecurity.bsa.org/

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

facilitate common approaches to common challenges, thus enabling collaboration and interoperability.

2. *Policies Should Be Risk-Based, Outcome-Focused, and Technology-Neutral.* Policies should reflect the diversity and constant evolution of the technological landscape, prioritizing approaches that address different levels of risk and enable owners and operators of networks and systems to defend their infrastructure with the technologies and approaches they deem best to meet the level of security desired.
3. *Policies Should Rely on Market-Driven Mechanisms Where Possible*. Policies that leverage market forces to drive cybersecurity are likely to be most successful in keeping pace with the changing security environment and in achieving the broadest effect.
4. *Policies Should Be Flexible and Adaptable to Encourage Innovation.* Policies must be flexible and adaptable to enable businesses to develop new approaches to new challenges and to deliver innovative products to the customers that depend on them.
5. *Policies Should Be Rooted in Public-Private Collaboration*. Cybersecurity is a shared responsibility across government and private stakeholders; only by working in close collaboration with the private sector can governments truly combat cybersecurity threats while sustaining the vitality of the digital economy.
6. *Policies Should Be Oriented to Protect Privacy.* No approach to cybersecurity should compromise the integrity of the data it seeks to defend against malicious cyber activity; cybersecurity policies should be carefully attuned to privacy considerations.

Beyond these overarching policies, BSA would like to provide input on a number of specific issues that we recommend as priorities for implementation in 2019.

Supply Chain Risk Management

One important area discussed in the 2018 Cybersecurity Strategy is the protection of the security and integrity of technology supply chains. In the time since the report's release, supply chain security issues have gained prominence amid allegations of state-sponsored interventions in supply chains, identification of significant vulnerabilities among broadly used components, and state actions to mitigate supply chain risks. Meanwhile industry has increasingly exerted leadership in securing supply chains by establishing global principles for supply chain integrity and organizing initiatives to enforce security at every level across global supply chains.

Security, integrity, and trust in global supply chains underpin the digital economy and are essential to sustaining the innovation and interconnection that are advancing Japan's vision of Society 5.0. For that reason, as Japan implements its Cybersecurity Strategy, BSA encourages Japan to prioritize a sophisticated approach to supply chain risk management that reduces supply chain threats, improves defenses against malicious activity, and enables the innovation and interoperability necessary for global digital commerce to thrive.

Specifically, BSA suggests that Japan's approach supply chain security should be crafted according to the following principles:

- ***Discretion.*** Enhancing supply chain security means, in part, developing a more secure global cybersecurity ecosystem that recognizes norms for responsible behavior and prioritizes collective defense against malicious threats. Japan can send an important message by committing that it will not undertake systemic interventions in global supply chains.
- ***Interoperability.*** In formulating its supply chain risk management policies, Japan should embrace internationally recognized, industry driven standards for security throughout the digital supply chain. Building policies around such standards ensures that technology

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

providers can develop, maintain, and secure innovative products across global boundaries and help to facilitate transnational operational collaboration against significant cyber threats.

- ***Collaboration.*** Government supply chain risk management efforts will be most effective when undertaken in collaboration with key non-governmental stakeholders, including industry. As industry increasingly provides leadership on addressing supply chain concerns, the Government of Japan should embrace creative opportunities for public-private partnerships aimed at securing supply chains and developing best practices for supply chain risk management. Likewise, collaboration should be sought on a government-to-government basis with key partners through the expansion of supply chain threat information-sharing and operational cooperation against supply chain threats.
- ***Transparency.*** Opaque supply chain risk management processes, such as the debarment of certain foreign vendors from acquisition processes without notification, create confusion and can prompt protectionist interventions by other governments, undermining the economic competitiveness of global businesses. Absent exceptional circumstances, supply chain risk management processes should be transparent to the public, with specific actions notified to impacted stakeholders. In addition, the transparency principle should oblige the governments to provide for disclosure of identified supply chain vulnerabilities to suppliers in accordance with vulnerability disclosure methodologies described in ISO/IEC 29147.
- ***Fairness.*** Similarly, supply chain risk management processes should establish fair mechanisms for resolving disputes, including opportunities for impacted stakeholders to appeal or protest decisions, provide defense against any alleged offenses, and remediate past concerns. Fair dispute resolution mechanisms, like transparency, create an environment of certainty and predictability without limiting tools for mitigating risk.
- ***Innovation.*** Securing 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. By investing in the research and development of new technological approaches to fostering supply chain integrity, Japan can ensure that it remains at the forefront of effective supply chain risk management practices and technologies. Promising areas of research include the use of blockchain-based technologies, development of processes to vet third-party components for security issues, and application of artificial intelligence for the analysis of supply chain data and anomaly detection, among others.
- ***Enforcement.*** While state actors may present the most sophisticated measures against threats, supply chains are also under constant pressure from non-state actors engaging in malicious cybersecurity activity, counterfeiting, and related activities. A key element of Japan's supply chain risk management strategy must be to continue aggressive law enforcement against malicious actors within its jurisdiction.

These principles are applicable not only to Japan's Cybersecurity Strategy but also to broader global supply chain security efforts. Therefore, BSA encourages Japan to adopt these principles both within its own policies and through its role as a global leader. Japan has opportunities to advance these principles, for example, through its leadership in hosting the 2019 G-20 Summit, through bilateral and multilateral trade agreements, at the United Nations, and through other multilateral fora. BSA is eager to partner with the Government of Japan in pursuing these opportunities in the coming year.

Internet of Things

A second key focus of the Cybersecurity Strategy is securing the Internet of Things (IoT). IoT devices are reshaping the landscape of both individual consumer and industrial technologies, bringing tremendous potential to unlock improved productivity, better quality of life, more

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

responsive governance, and dramatic technological breakthroughs. However, these devices also bring new risks, and BSA is eager to work in partnership with the Government of Japan to address IoT security risks.

BSA supports the establishment of security baselines for IoT devices that provide guidance on essential security capabilities, best practices for secure design and lifecycle maintenance, and related capabilities. In fact, BSA is already providing input to efforts to develop such baselines, including the US National Institute for Standards and Technology (NIST) as it seeks to publish recommended IoT security baselines and to the European Union Network and Information Security Administration (ENISA) as it seeks to develop a certification scheme for IoT devices. As these efforts suggest, one vital necessity for efforts to develop IoT security baselines is that they remain aligned with similar efforts around the world. Interoperability plays a foundational role in facilitating global commerce and cybersecurity, and contradictory guidance or mandates in the IoT space would negatively impact both digital trade and the security of these devices. Secondly, it is important that IoT security baselines are risk-based and flexible, accounting for the tremendous diversity among IoT devices with regard to function, capability, and risk.

BSA is eager to partner with the Government of Japan in pursuing security baselines for IoT devices according to these priorities.

Promoting Cloud Computing for Enhanced Security

The Cybersecurity Strategy recognizes the importance of promoting cloud computing to enhance the efficiency and security of agency operations. In this regard, we urge NISC to take the opportunity to revisit some of the guidance it has put out in the past relating to cloud computing, to ensure that the Government of Japan's messaging is consistent and not open to misinterpretation by agencies and other stakeholders. Specifically, we remain concerned that sections (e.g. Section 4.1.4) in the Common Standards for Information Security Measures for Government Agencies (FY 2018)[3] continue to imply that cloud computing and related services have enhanced risks. Such statements may create the misleading impression that risks of cloud computing are greater than on-premise IT system. It is also important to take into consideration the varying cloud service models such as private cloud, public cloud, and hybrid cloud, and as with on premises systems, the specific risks must be assessed based on the context for which they will be used.

We also remain concerned about the suggestion in the same document that physical network separation is a solution when instead, in many cases, physical network separation may increase risks by interfering with the benefits of real-time security updates (see Sections 5.2.1-(2)a).[4]

In a related matter, we commend the government of Japan, specifically the Ministry of Economy, Trade and Industry (**METI**) and the Ministry of Internal Affairs and Communications (**MIC**) on their effort to increase cloud adoption across the government and improve procedures for security assessment of cloud services. We were also encouraged to see the "Basic Policy on Use of Cloud Services in Government Information Systems" compiled by the Liaison Conference of CIOs,[5] which promotes a 'Cloud-by-Default Principle', and we hope the current

[3] NISC Common Standards for Information Security Measures for Government Agencies (FY 2018) at https://www.nisc.go.jp/active/general/pdf/kijyun30.pdf

[4] See BSA Comments on the NISC Common Standards for Information Security Measures for Government Agencies (FY 2018) – June 28, 2018 at https://www.bsa.org/~/media/Files/Policy/Data/06282018BSACommentsNISC2018CommonStands_en.pdf. Japanese translation at https://www.bsa.org/~/media/Files/Policy/Data/06282018BSACommentsNISC2018CommonStands_jp.pdf.

[5] Basic Policy on Use of Cloud Services in Government Information Systems at

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

efforts undertaken by METI and MIC will conform with and maximize the use of this policy. As METI and MIC consider developing a security assessment mechanism for cloud services used by the public sector, we wish to reiterate the importance of designing such a system so that it is globally interoperable with other public sector cloud security assessment and certification schemes and tailored to internationally-recognized standards. It should also ensure that risk-based approaches and multi-layered defense systems apply uniformly across government agencies. In this way, Japan's proposed cloud security assessment mechanism will promote the adoption of secure and effective cloud computing services by public sector entities and others who may follow the assessments in the future.

International Capacity-Building

BSA strongly supports Japan's commitment to international cybersecurity capacity building as expressed in the Cybersecurity Strategy. Cybersecurity is a transnational challenge that demands international cooperative solutions; cyberspace can only be secured to the extent that nations can work together to strengthen the entire Internet ecosystem. Targeted support to help less sophisticated nations develop stronger cyber defense and cyber governance capacities is essential in this regard, and BSA welcomes Japan's leadership. BSA encourages the Government of Japan to sustain and expand its support for international capacity-building, with a particular focus in the Southeast Asia region, where a number of nations are currently at the early stages of developing or implementing new cybersecurity laws.

In addition, Japan can help strengthen the global digital ecosystem by participating in multi-national operational collaboration to confront specific cybersecurity threats, supporting the establishment of international cybersecurity norms or confidence building measures, participating in international cybersecurity standards development, and participating in multilateral governance mechanisms. In particular, Japan is well-positioned to advance international norms and confidence-building measures through its leadership in hosting this year's G-20.

Workforce 5.0

The Cybersecurity Strategy rightly recognizes that human resource development is a necessary foundation to pursuing the broader policy goals outlined in the strategy and developing a robust cybersecurity workforce should be a priority for implementation in 2019. Japan's vision of a Society 5.0 must be built upon a Workforce 5.0 — a workforce that can support technological innovation across economic sectors and meet the rapidly rising demand for cybersecurity professionals able to secure the benefits of a connected economy.

Building a cybersecurity workforce to meet current and future needs begins with educating a broader generation of future practitioners. It is especially important to incentivize more female students to pursue computer science, including cybersecurity education, to address tremendous imbalances in the current workforce. BSA's members have invested significant resources in programs that support alternative pathways to cybersecurity capabilities and promote greater participation by women and others that remain under represented in the software workforce; government investment in these efforts could expand their scope and effectiveness considerably.

Conclusion

Once again, BSA applauds NISC for its cybersecurity leadership, and we grateful for its collaborative, multi-stakeholder outreach. BSA and our members hope our input will be useful as you consider implementation of the Cybersecurity Strategy in 2019, and we welcome the

---

https://cio.go.jp/sites/default/files/uploads/documents/cloud_%20policy.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

opportunity to work with NISC as these efforts take shape. Please let us know if you have any questions or would like to discuss these comments in more detail.

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