BSA Comments on Common Standards for Cybersecurity Measures for Government Agencies and Related Agencies (FY 2021)

May 13, 2021

BSA | The Software Alliance (**BSA**)[1] welcomes this opportunity to provide our response to the draft Common Standards for Cybersecurity Measures for Government Agencies and Related Agencies (FY 2021) (**Common Standards**), published by the National Center of Incident Readiness and Strategy for Cybersecurity (**NISC**).

General Comments

As the leading advocate for the global software industry before governments and in the international marketplace, BSA applauds the Government of Japan's (**GOJ**) continued efforts to uniformly raise the level of cybersecurity across agencies. BSA members lead the world in offering cutting-edge technologies and services that support the digital transformation of governments and societies, including cloud computing, security solutions, data analytics, and artificial intelligence.

BSA works closely with governments around the world on the development of national cybersecurity policies and legislation. We have witnessed first-hand the potential for such policies and legislation to effectively deter and manage cybersecurity threats while protecting the privacy and civil liberties of citizens. Through this effort, BSA has developed the "International Cybersecurity Policy Framework",[2] which provides a recommended model for a comprehensive national cybersecurity policy. The Framework provides recommendation on key elements of a national cybersecurity policy such as alignment with internationally recognized standards, taking a risk-based, outcome focused, technology neutral approach, and developing adaptable policies to encourage innovation.

Addressing cybersecurity challenges requires innovative tools and practices to defend the integrity, confidentiality, and resilience of the connected ecosystem. It is important to be able to use the best available encryption technology when appropriate. We, therefore, encourage that the Government work closely with the private sector to develop security policies that benefit from the latest advancements in security approaches.

[1]BSA's members include: Adobe, Altium, Amazon Web Services, Atlassian, Autodesk, 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, and Workday.

[2] BSA International Cybersecurity Policy Framework at: https://bsacybersecurity.bsa.org/report-item/bsa-international-cybersecurity-policy-framework/

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

To support the purpose of the Common Standards, we provide specific comments below.

Observations and Recommendations

Chapter 1 General Provisions / 1.3 Definition of Terms
Chapter 6 Security Requirements for Information Systems / 6.1 Security Functions of Information Systems

BSA supports NISC's approach in the "Review of Unified Set of Common Standards for Information Security Measures for Government Agencies and Related Agencies (Draft)"[3] (**Review**), identifying appropriate key cybersecurity issues on which to focus. The revised Common Standards would further benefit by clearly defining the keywords mentioned in the Review such as "continuous access judgment / permission architecture", and "continuous system diagnosis / countermeasure", to ensure that the infrastructure of information security measures will be further enhanced. We therefore respectfully request that these keywords be added in the Section 1.3 - Definition of Terms and Chapter 6, Section 6.1. - Security Functions of Information Systems (for example by adding: 6.1.6 continuous access judgment / permission architecture, 6.1.7 continuous system diagnosis / countermeasure).

BSA also appreciates the additional explanation in the revised Common Standards on the use of various outsourced service providers, clarifying that cloud services are "external services", describing that "external service refers to a service that provides some or all of the functions of an information system to the public by a person outside Agencies etc. However, it is limited to the case in which the information of the Agency etc. is handled using the said functions." To ensure that government officials and relevant stakeholders share the same understanding, the document could further be improved by clarifying which cases will fall as external services "handling information'. It would also be helpful to clarify whether the "external service administrator" described as "a person who manages the external services designated by the person who has the authority to approve the application for use of the external services at the time of approval" refers to a public official or a business operator.

Chapter 4 Outsourcing / 4.2 Use of External Service

We are encouraged to see the Government providing additional description of the security of cloud services. To facilitate the Government of Japan's goal of achieving their publicly stated "cloud-by default principle (**Principle**)" in the public sector, we encourage directly reflecting the Principle in the Common Standards, to ensure that security requirements do not unnecessarily deter public sector entities from adopting innovative cloud computing solutions. It is important to ensure that this Principle is uniformly understood and applied across agencies.

We also welcome the revised Common Standards acknowledging internationally recognized standards and reflecting the shared responsibility security model in the Compliance Requirements. Effective cloud security policies assign appropriate requirements to providers and customers relative to their role in, and level of control over, the cloud environment. Policies that do not recognize this fundamental separation of security duties increase risk to government workloads by forcing the removal of vital security controls, reducing governments' ability to control the security of their cloud environments, and increasing the chance of missing important security signals. For example, two parties to a cloud service arrangement may assume that the security of a particular piece of infrastructure was the other's

[3] https://public-comment.e-gov.go.jp/servlet/PcmFileDownload?seqNo=0000218291

responsibility. This would create a blind spot that can become a major security vulnerability. We therefore encourage NISC to ensure this security model is understood across agencies.

Chapter 5 Lifecycle of Information Systems / 5.2.1 Planning and definition of requirements for information systems / (2) Formulation of security requirements for information systems (a)

As mentioned in our previous submission in 2018[4], BSA continues to be concerned with the guidance in the Common Standards in which Information system security officers are to formulate security requirements "after determining whether it is necessary to isolate the said system from the internet or from systems connected to the internet (including external service)". While recognizing that the decision should be made based on the "purpose of constructing the information system, task requirements for the targeted tasks etc., as well as classification of information handled by said system" and may not be intended to be the default choice, separating an information system from the Internet would significantly reduce the ability to access and utilize information held in such a system. This approach would also limit the government agency from benefiting from cutting edge security solution deployed by leading cloud computing service providers (**CSPs**).

Many cloud services enable world class data security by implementing internationally recognized functions such as encryption and strict access management systems. The massive investments in data security by global CSPs, including those of many BSA members, provide the most effective data security for sensitive personal information available and it is imperative that the Government of Japan ensure that its policies enable the use of these best-in-class secure solutions. We, therefore, recommend the Government of Japan delete references to isolating information systems from the Internet in 5.2.1 (2) (a) of the Common Standards and in the Guideline for Developing Measures Standards for the Central Government Agencies (2021 Edition) (page 173). This will help ensure that the Common Standards do not inadvertently imply to public officials that network separation is the most effective way of securing an information system.

Conclusion

BSA would like to thank NISC for granting the opportunity to provide these comments. We hope the above will be useful as NISC finalizes the Common Standards. Please let us know if you have any questions or would like to discuss these comments in more detail.

[4] https://www.bsa.org/files/policy-filings/06282018BSACommentsNISC2018CommonStands_en.pdf