BSA Comments on the Guidelines on the Roles Expected of Cyber Infrastructure Providers (draft)

December 23, 2025

［御意見］Comments

・該当箇所（どの部分についての意見か、該当箇所が分かるように明記してください。）
Relevant Section (Clearly indicate the section of the Guidelines to which the comments relate.)

・意見内容 Comment
The Business Software Alliance (BSA) (1) appreciates the opportunity to provide comments on the Guidelines on the Roles Expected of Cyber Infrastructure Providers (draft).

BSA is the global trade association of the enterprise software industry, representing companies that are leaders in cybersecurity, artificial intelligence (AI), cloud computing, quantum, and other breakthrough technologies. BSA members provide cutting-edge security tools, pioneering many of the software security best practices used throughout governments and industry today. Together with BSA members, BSA works closely with governments around the world on developing cybersecurity policies and based on these global experiences, we provide our comments below.

(1) BSA's members include: Adobe, Alteryx, Amadeus, Amazon Web Services, Asana, Atlassian, Autodesk, Avalara, Bentley Systems, Box, Cisco, Cloudflare, Cohere, Cohesity, Dassault Systemes, Databricks, Docusign, Dropbox, Elastic, EY, Graphisoft, HubSpot, IBM, Informatica, Kyndryl, MathWorks, Microsoft, Notion, Okta, OpenAI, Oracle, PagerDuty, Palo Alto Networks, PTC, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Trend Micro, TriNet, Veeam, Workday, Zendesk, and Zoom Communications Inc.

・理由（可能であれば、根拠となる出典等を添付又は併記してください。）
Reason（If possible, attach or include supporting references or sources.）
https://www.bsa.org/ (global site) / https://bsa.or.jp/ (Japanese site)

・該当箇所（どの部分についての意見か、該当箇所が分かるように明記してください。）
Relevant Section (Clearly indicate the section of the Guidelines to which the comments relate.)
Overall

・意見内容 Comments
We agree that organizations, including government agencies, should focus on improving their cybersecurity and resilience and that many of the recommendations contained in the

22F Shibuya Mark City West 1-12-1 Dogenzaka, Shibuyaku, Tokyo 150-0043
+81 3 4360 5474 **www.bsa.org**

draft document advance our shared goal. However, we see an opportunity to achieve this goal while reducing the risks of negatively impacting harmonization and consequently negatively impacting cybersecurity.

Harmonizing requirements across governments strengthens both government and private-sector cybersecurity in many ways, including by:

- Enabling governments to track and compare incidents and campaigns with precision.
- Allowing businesses, especially small and mid-sized firms, to redirect compliance costs into better security innovations.
- Refocusing governments from developing new, overlapping, duplicative, or contradictory requirements, to supporting cybersecurity operations
- Shifting the cybersecurity culture away from paperwork and toward secure design, effective risk management, and resilience. (2)

(2) BSA's "Resilience Through Recovery: Elevating Backup in Cybersecurity Preparedness" https://www.bsa.org/files/policy-filings/10212025bsaresilencecybersec.pdf

・理由（可能であれば、根拠となる出典等を添付又は併記してください。）
Reason（If possible, attach or include supporting references or sources.）
While clearly thoughtful and well intentioned, in general, the draft document's current approach of combining, adapting, and reinterpreting requirements from other documents will necessitate further interpretation by industry and create confusion, duplication, and complexity. A more effective path would be to require direct compliance with the US National Institute of Standards and Technology's Secure Software Development Framework, the BSA Framework for Secure Software, or similar documents, and then – if necessary for cybersecurity purposes

- The BSA Framework for Secure Software: https://www.bsa.org/files/reports/bsa_framework_secure_software_update_2020.pdf

-BSA's Cyber Policies for Cyber Purposes - How Choice Improves and Politics Degrades Cybersecurity": https://www.bsa.org/files/policy-filings/0418205bsacyberpolpur.pdf

・該当箇所（どの部分についての意見か、該当箇所が分かるように明記してください。）
Relevant Section (Clearly indicate the section of the Guidelines to which the comments relate).
Page 66 of English version,5. Reference Information S(2)-1.3 Risk assessment of software components5.4. Examples of measures implemented to meet requirements / / (2) Life cycle management and assurance of transparency / S(2)-1.1Arrangement of software components

・意見内容 Comment

The meaning of the requirement to adopt third-party software component that meet the "in-house requirements" is unclear. Mandating the exact same requirements may be nearly impossible in third parties because of the strength of the security requirements software developers apply to their own code. Developers should be rewarded for continuously strengthening their own security, whereas this requirement brings that approach into question. Notably, the Cyber Resilience Act in the European Union mandates that developers conduct due diligence to verify the conformity of third-party components, which is a more effective approach.

・理由（可能であれば、根拠となる出典等を添付又は併記してください。）
-BSA Response to the Cybersecurity and Infrastructure Security Agency's Request for Comment on 2025 Minimum Elements of a Software Bill of Materials: https://www.bsa.org/policy-filings/us-bsa-response-to-the-cybersecurity-and-infrastructure-security-agencys-request-for-comment-on-2025-minimum-elements-of-a-software-bill-of-materials

The above was in response to the following request for comment: https://www.federalregister.gov/documents/2025/08/22/2025-16147/request-for-comment-on-2025-minimum-elements-for-a-software-bill-of-materials

・該当箇所（どの部分についての意見か、該当箇所が分かるように明記してください。）
Relevant Section (Clearly indicate the section of the Guidelines to which the comments relate.)
Page 67 of English version / 5. Reference Information/ 5.4. Examples of measures implemented to meet requirement / / (2) Life cycle management and assurance of transparency /S(2)-1.3 Risk assessment of software components

・意見内容 Comment
The requirement to "acquire and analyze provenance information for respective software components and assess risks result from components" is, unfortunately, premature given the current status of software bills of materials (SBOMs). For example, important work is ongoing at the US Cybersecurity and Infrastructure Security Agency – in conjunction with experts from academia, industry, and other governments – to define a set of minimum elements for an SBOM. This requirement may create unrealistic expectations and confuse customers who are not as deeply involved with the development and deployment of SBOMs as experts at METI.

・理由（可能であれば、根拠となる出典等を添付又は併記してください。）
Reason (If possible, attach or include supporting references or sources.)

-BSA Response to the Cybersecurity and Infrastructure Security Agency's Request for Comment on 2025 Minimum Elements of a Software Bill of Materials:

https://www.bsa.org/policy-filings/us-bsa-response-to-the-cybersecurity-and-infrastructure-security-agencys-request-for-comment-on-2025-minimum-elements-of-a-software-bill-of-materials The above was in response to the following request: https://www.federalregister.gov/documents/2025/08/22/2025-16147/request-for-comment-on-2025-minimum-elements-for-a-software-bill-of-materials
・該当箇所（どの部分についての意見か、該当箇所が分かるように明記してください。） Relevant Section（Clearly indicate the section of the Guidelines to which the comments relate.） Page 70 of English version 5. Reference information / 5.4. Examples of measures implemented to meet requirements / S(2)-2.3 Sharing of release provenance data ・意見内容 Comment The requirement to “collect, protect, maintain, and share provenance data for all components of respective releases” is, unfortunately, premature given the current status of software bills of materials (SBOMs). For example, important work is ongoing at the US Cybersecurity and Infrastructure Security Agency – in conjunction with experts from academia, industry, and other governments – to define a set of minimum elements for an SBOM. Further, the document should distinguish between providing SBOMs to a customer when requested and proactively sharing for multiple reasons including revealing information like configurations and integration strategies which may qualify as trade secrets or information like dependencies which may increase security risks. ・理由（可能であれば、根拠となる出典等を添付又は併記してください。） Reason (If possible, attach or include supporting references or sources.) -BSA Response to the Cybersecurity and Infrastructure Security Agency’s Request for Comment on 2025 Minimum Elements of a Software Bill of Materials: https://www.bsa.org/policy-filings/us-bsa-response-to-the-cybersecurity-and-infrastructure-security-agencys-request-for-comment-on-2025-minimum-elements-of-a-software-bill-of-materials The above was in response to the following request: https://www.federalregister.gov/documents/2025/08/22/2025-16147/request-for-comment-on-2025-minimum-elements-for-a-software-bill-of-materials
・該当箇所（どの部分についての意見か、該当箇所が分かるように明記してください。） Relevant Section (Clearly indicate the section of the Guidelines to which the comments relate.） P77 of English version/ . Reference Information /5.4. Examples of measures implemented to meet requirements /(3) Prompt responses to remaining vulnerabilities / S(3)-2.3 Security recommendations

・意見内容 Comment
The requirement to “report to authorities as specified” is unclear and may conflict with other leading approaches. Effective coordinated vulnerability disclosure minimizes risk to technology users by establishing processes that increase the likelihood that information about vulnerabilities becomes public simultaneously with patches or other remediations that enable users to protect themselves and should be managed pursuant to existing internationally recognized standards like ISO/IEC 29147 and 30111 directly, rather than to, for example, the CRA.

・理由（可能であれば、根拠となる出典等を添付又は併記してください。）
Reason（If possible, attach or include supporting references or sources.）
-The BSA Framework for Secure Software Ver. 1.1:
https://www.bsa.org/files/reports/bsa_framework_secure_software_update_2020.pdf

-ISO/IEC 29147:2018/ Information technology — Security techniques — Vulnerability disclosure: https://www.iso.org/standard/72311.html

-ISO/IEC 30111:2019 / Information technology — Security techniques — Vulnerability handling processes: https://www.iso.org/standard/69725.html

・該当箇所（どの部分についての意見か、該当箇所が分かるように明記してください。）
Relevant Section (Clearly indicate the section of the Guidelines to which the comments relate.）
Page 83 of English version / 5. Reference Information/ 5.4. Examples of measures implemented to meet requirements / (4) Arrangement of human resources, processes, and technologies / S(4)-2.3 Sharing of cost recognition and budgeting

・意見内容 Comment
The requirement to “Secure necessary budgets to ensure security based on policy” should acknowledge, explicitly, that this activity should be risk-based.

・理由（可能であれば、根拠となる出典等を添付又は併記してください。）
Reason（If possible, attach or include supporting references or sources.）
-Cybersecurity Management Guidelines for Japanese Enterprise Executives Ver. 3.0:
https://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v3.0_en.pdf

-The BSA Framework for Secure Software Ver. 1.1:
https://www.bsa.org/files/reports/bsa_framework_secure_software_update_2020.pdf

-NIST SP 800-218 - Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities
https://csrc.nist.gov/pubs/sp/800/218/final

・該当箇所（どの部分についての意見か、該当箇所が分かるように明記してください。）

Relevant Section（Clearly indicate the section of the Guidelines to which the comments relate.）
P70-72 of English version / 5.4. Examples of measures implemented to meet requirements/ (2) Life cycle management and assurance of transparency / /S(2)-3 Establishment of security requirements among stakeholders

・意見内容 Comment
Some of the itemized requirements, descriptions and example measure within S(2)-3 vary from cross mapped NIST Secure Software Development Framework (SSDF) objectives PO 1.3 and PW4.4 in ways that cause confusion for how they might be implemented. We recommend more directly adopting language for this section from the objectives and tasks in the SSDF to promote greater alignment and understanding. If there is desire to require something beyond what is in the SSDF, it would be helpful to explicitly identify where the guidance is choosing to expand beyond the SSDF.

・理由（可能であれば、根拠となる出典等を添付又は併記してください。）
Reason（If possible, attach or include supporting references or sources.）

-NIST SP 800-218 - Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities
https://csrc.nist.gov/pubs/sp/800/218/final