August 18, 2026

BSA COMMENTS ON THE DRAFT GUIDELINES CONCERNING NOTIFICATION OF SPECIFIED CRITICAL COMPUTERS AND REPORTING OF SPECIFIED CYBERSECURITY INCIDENTS

The Business Software Alliance (**BSA**)[1] appreciates the continued efforts of the Government of Japan to strengthen cyber defense and response capability of Specified Essential Infrastructure Service Providers (SEISPs) and appreciates the publication of the Draft Guidelines[2] to provide greater clarity regarding notification and reporting obligations under the Act on Enhancing Cyber Response Capability.[3]

BSA is the leading advocate for the global enterprise software industry, and our members are enterprise software companies that lead in cybersecurity solutions, AI, cloud storage services, quantum computing, 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.

Recommendations

To support effective implementation, BSA recommends further clarification regarding the allocation of responsibilities between SEISPs and technology suppliers, as well as additional refinements to incident reporting requirements to ensure they remain risk-based, proportionate, and aligned with international best practices.

---

[1] The Business Software Alliance (www.bsa.org) is the global trade association of the enterprise software industry, representing companies that are leaders in artificial intelligence, cybersecurity, cloud computing, quantum, and other breakthrough technologies. We work in over 20 markets in the US, Europe, and Asia, advocating for policies that build trust in technology so that every industry sector and the public can benefit from innovation.

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

[2] https://public-comment.e-gov.go.jp/pcm/download?seqNo=0000317900

[3] https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo_torikumi/pdf/houritsu.pdf

Clarify That Statutory Notification and Reporting Obligations Apply to SEISPs

The Guidelines should expressly clarify that the statutory obligations to notify Specified Critical Computers and report Specified Cybersecurity Incidents are imposed on the designated SEISPs, including where cloud services are identified as Specified Critical Computers.

The Guidelines appropriately recognize that a SEISP may rely on information obtained from external parties, including cloud service providers, network service providers, or , contractors responsible for system operation and monitoring. However, it would be helpful to state explicitly that compliance obligations remain with the SEISP and are not transferred to technology providers by virtue of their products or services being within scope of the regime.

Cloud service providers and other technology suppliers routinely support customers' compliance and security activities through contractual arrangements and operational cooperation. However, the statutory framework should not create uncertainty regarding responsibility for notification or reporting. Clear delineation of responsibilities between regulated infrastructure operators and their technology or service providers will improve compliance outcomes, reduce confusion during incidents, and avoid duplicative reporting obligations.

We recommend including the following texts in Guidelines to provide clarity: *"Where a cloud service, managed service, or other third-party service is identified as a Specified Critical Computer, the obligation to submit notifications and reports pursuant to Articles2, 4 and 5 remains with the relevant SEISP. Technology or service providers may support compliance activities through contractual arrangements, but are not independently subject to such obligations solely by virtue of providing the technology or service."*

Clarify the Scope of Reportable "Traces" of Specified Cybersecurity Incidents

BSA welcomes the Government's efforts to support early awareness of cyber threats affecting SEISPs. However, additional clarification would be valuable regarding reporting obligations associated with "traces of Specified Cybersecurity Incidents" and "events that may become causes of Specified Cybersecurity Incidents."

The current draft appears to require reporting not only of confirmed cyber incidents, including ransomware, unauthorized access, and DDoS attacks, but also certain attack attempts, malware delivery events, credential theft activity, and circumstances in which traces suggest that such events may have occurred related to specified critical facilities. It is critical to recognize that these attempts or events often represent unconfirmed, failed, or automatically mitigated activity rather than actual security breaches.

In today's threat environment, modern security operations centers can process millions of "events" daily — including blocked connection attempts, failed authentications, and neutralized malware — a volume that is only set to accelerate with the advancement of AI-driven cyber threats. These events are importantly differentiated from a confirmed cyber security "incident"

Because modern security monitoring systems generate a large volume of alerts, indicators, and potential detections, additional clarification is needed regarding what level of analysis or confidence or validation is required before reporting obligations arise.

Routine scanning activity, unsuccessful intrusion attempts, automatically blocked connections, benign anomalies, duplicate detections, and false positives may all generate artifacts or traces within security monitoring systems. However, such observations do not necessarily indicate that malware was executed, unauthorized access occurred, or that business operations were affected.

To ensure meaningful reporting and avoid excessive reporting volumes, BSA recommends clarifying that reportable traces should be linked to a reasonable assessment that an actual cyber incident has occurred or is reasonably likely to have occurred.

This would be consistent with risk-based incident reporting approaches adopted in other jurisdictions, which focus reporting on incidents that have been validated through reasonable investigation and are relevant to cybersecurity risk management, to avoid generating low-value reports that overwhelm authorities and reduce the overall value of reported information.

While Section 5-5 presents examples of recognizing the occurrence of a cybersecurity incidents including confirming through forensic investigations or threat hunting, BSA recommends clarifying that: *"traces of a Specified Cybersecurity Incident should be reportable where the SEISP has conducted a reasonable assessment and determined that the traces provides a credible basis to conclude that a Specified Cybersecurity Incident, or an event likely to cause a Specified Cybersecurity Incident, has occurred*."

BSA further recommends providing practical examples illustrating the distinction between:

- reportable trace of a likely cyber incident; and
- non-reportable routine, unsuccessful, or automatically mitigated activity.

A formal definition of "trace" (e.g., "a recognized technical evidence of an underlying covered incident") with an objective recognition threshold would be helpful.

Promote Proportionality and International Alignment in Incident Reporting

The Draft Guidelines establish detailed classifications of systems, reportable events, and reporting obligations. While BSA appreciates the objective of enhancing cyber situational awareness, we

encourage continued efforts to simplify reporting requirements and align them with established international cybersecurity reporting frameworks where appropriate.

Greater consistency with international practices would 1) reduce compliance complexity 2) support more efficient incident response 3) improve reporting quality by allowing organizations to focus resources on material cybersecurity events; and 4) facilitate more effective cyber risk management across globally integrated systems.

BSA therefore encourages adoption of a risk-based approach that focuses on incidents with meaningful operational, confidentiality, integrity, or availability impacts, while avoiding reporting obligations for low-risk or speculative events that do not materially affect cybersecurity outcomes.

The Government should consider providing guidance that reporting obligations are intended to support the identification and mitigation of material cybersecurity risks and should be implemented in a manner consistent with internationally recognized incident reporting practices and the principle of proportionality.

Conclusion

BSA supports the objectives of the Draft Guidelines and respectfully recommends further clarification regarding 1) the allocation of responsibilities between SEISPs and technology providers 2) the treatment of evidence or traces of cybersecurity incidents; and 3) the proportional, risk-based implementation of incident reporting obligations consistent with international practice. These clarifications would strengthen the effectiveness of the framework while reducing uncertainty for regulated entities and their technology partners. We look forward to working with the Government to enhance Japan's cyber response capabilities.

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