November 21, 2025

COMMENTS ON THE BASIC POLICY FOR THE PREVENTION OF DAMAGE FROM SPECIFIED UNAUTHORIZED ACTS AGAINST CRITICAL COMPUTERS (DRAFT)

The Business Software Alliance (**BSA**) [1] appreciates the opportunity to comment on the "Basic Policy for the Prevention of Damage from Specified Unauthorized Acts Against Critical Computers (Draft)" (**draft Policy**)[2] , which sets basic matters to ensure measures are effectively implemented under the Act on the Prevention of Damage from Unauthorized Acts Against Critical Computers[3] (**the Act**). BSA fully supports the ongoing effort of the Government of Japan to develop a system to enhance Japan's response capabilities against increasing cyberattacks threatening the lives of citizens and economic activities.

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. Based on these global experiences, we provide our comments below to support the Government's objective to prevent damage and to ensure continuity of essential infrastructure services[4], designated under the Economic Security Promotion Act. [5]

Our recommendations aim to provide the government of Japan and local Japanese businesses access to the best and most secure cloud services so that they may better serve Japanese citizens and customers. We encourage developing implementation policies to ensure alignment with other

---

[1] The Business Software Alliance (www.bsa.org) works 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, 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.

[2] https://public-comment.e-gov.go.jp/pcm/download?seqNo=0000301883

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

[4] Summary of System for Ensuring Stable Provision of Specified Essential Infrastructure Services under the Economic Security Promotion Act: https://www.cao.go.jp/keizai_anzen_hosho/suishinhou/infra/doc/infra_setsumeikai_eng.pdf

[5] https://www.japaneselawtranslation.go.jp/en/laws/view/4716

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

international practices, consistency with existing and emerging business practices and technological considerations. We also encourage minimization of unintended impacts that might deter, rather than promote, the adoption of best-in-class secure software-enabled technologies by designated business operators using critical computers specified under the Act ("Special Essential Infrastructure Service Providers" (**SEISPs**)).

To achieve the stated objectives in the daft Policy, we encourage the Government of Japan to **provide adequate public consultation on the detailed policy proposal before implementation, and frequent review of the policies** once implemented to ensure the legislation and implementing rules are fit for purpose and not interfering with other important goals such as digital transformation and cloud adoption by SEISPs.

Our recommendations, described below, address the following subjects:

- ***Notification of "Specified Critical Computers"***
- ***Incident Reporting***
- ***Vulnerability Disclosure and Strengthening Vulnerability Response***

Notification of Specified Critical Computers

Among the variety of measures to promote greater public-private collaboration to enhance the resilience of SEISPs in Japan, the draft Policy provides an explanation of the new obligation introduced for SEISPs to notify the designated critical computers being used ("Specified Critical Computers"), which cover not only critical equipment/devices, but also information systems including cloud computing services. We understand that the scope of Specified Critical Computers will be elaborated in the Cabinet Ordinance and Ministerial Ordinance to be issued next year. As we stated in our earlier recommendations[6], we encourage the Government to take a risk-based approach in the designation of such computers, focusing attention on the specific systems which are necessary for the continuous delivery of the essential services provided by SEISPs, in line with the Act, and not include other non-essential systems used by the SEISPs.

As the draft Policy states at Chapter 4, Section 2 (1), considering the volume of equipment/devices being used by SEISPs, the notification is expected to be substantial with the process anticipated to be heavily time-consuming. To make the policy implementable, it will be important to minimize the burden on SEISPs adopting advanced computing systems and government agencies managing notifications. In this respect, we recommend narrowing the scope of cloud computing services to those that support critical functions covering only the tenant of SEISPs.

The policy should be reasonably designed for effective implementation by relevant stakeholders, and in this sense, we support the approach proposed in the draft Policy to exclude devices or products specially designed for individual businesses and to take into consideration the burden of notification requirements on changes made to critical computers, such as equipment renewal.

In line with the Act and the draft Policy, it is important to ensure that various measures continue to be carried out by SEISPs directly, and not by cloud service providers.

[6] https://www.bsa.org/files/policy-filings/en04112025recccyberdef.pdf

We also encourage the Government to avoid requiring the disclosure of excessively detailed information during the notification process. It is particularly important that the notification does not require SEISPs to collect information such as trade secrets or systems security-related information that would be difficult for the suppliers to share with SEISPs.

Incident Reporting

The draft Policy at Chapter 4, Section 2 (2) also presents the approach to the new obligation for SEISPs to report Specified Security Incidents that may affect the Specificed Critical Computers. BSA has laid out how governments can build a cyber incident reporting ecosystem that meets their needs while not unduly encumbering businesses's ability to respond to and recover from a cyber incident in BSA's 10 Principles for Cyber Incident Reporting Harmonization Around the Globe.[7] We welcome the approach in the draft Policy to reduce the burden of the affected stakeholders through standardization of reporting formats and unifying reporting channels through the public-private partnership platform. We encourage continuing to explore ways to design incident reporting requirements to maximize benefits while minimizing additonal workloads for both SEISPs and the Goverment. Any obligations imposed on SEISPs will likely impact, directly or indirectly, companies providing critical IT services, including BSA members.

We wecome the direction in the draft Policy to align cyber incident notification and reporting requirements domestically across agencies and internationally with emerging international trends. Given the cross-sectoral and cross-border nature of many large-scale cybersecurity incidents, the more the Government of Japan's system aligns with those of other major jurisdictions the more seamlessly business, both domestic and multinational, will be able to respond effectively and expeditiously. The objective should be to quickly identify and mitigate significant incidents to minimize harm, not to impose unique compliance obligations on businesses in Japan.

Specifically, we recommend the Government work closely with industry partners and other relevant stakeholders, including BSA member companies, to establish a risk-based threshold for determining whether a cybersecurity incident is "reportable". Reportable cyber incidents should be narrowly defined so that they include only actual cyber incidents resulting in harm that are significant and compromise a business's ability to deliver critical functions, and not suspected activities or those that only risk, jeopardize, or otherwise make a cyber incident more likely. In this respect, we support the approach in the draft Policy which recognizes that equipment such as firewalls – that serve as gateways of connection points to the Internet – blocks a large volume of attack-type communications during normal times and requiring reporting on such incidents uniformly would impose an excessive burden on SEISPs.

It is also important that the commencement of any reporting obligations and associated timelines should be when an SEISPs knows (i.e., has made a determination) that they are subject to a reporable incident. We support the direction in the draft Policy to target only incidents clearly detected after intrusion. The obligation should not be based on suspicion or belief that a SEISP has suffered an incident. This point is particularly important as the Government moves to defining in the future "the event that could cause Specified Security Incident, stipulated in Article 5 of the Act . The recent

[7] https://www.bsa.org/files/policy-filings/02182025bsacyberincidreporting.pdf

document summarizing the issues for further discussion[8] indicates the consideration on requiring reporting to be made "when traces of specific incidents are recognized." We encourage narrowing the scope of what will be considered as 'traces' to make incident reporting scheme practical and effective.

The draft Policy also notes that the reporting deadlines "shall be set based on examples from countries with similar reporting procedures and considering the need for effective public-private response." We appreciate the Government referencing various international benchmarks. Often times, it takes time for businesses to understand the nature of an incident even once they have determined they are subject to a reportable incident. While in many cases, a company may provide a simple notification more quickly, imposing a standard of no less than 72 hours from when the SEISP reasonably belives it is the victim of a reportable incident, like that of the US Cyber Incident Reporting for Critical Infrastructure Act (**CIRCIA**), will allow SEISPs the time to 1) focus on understanding and responding to the incident and 2) provide a helpful report to the Government. It is counterproductive to force companies to shift limited resources away from responding to an incident to compliance obligations. Businesses are aligned with ensuring that governmental stakeholders recieive the most updated information possible. As such, we strongly encourage providing adequate time for providing a preliminary report.

With regards to the content of reports on Specified Security Incidents, the draft Policy states that it shall be sufficient to include information known at the time of reporting, including uncertain details, as a preliminary report. As the Government works to further define the information required for prelminiary reports, we encourage limiting such information to that which an SEISP knows about 1) the malicious actor, including its tactics, techniques, and procedures; 2) the vulnerability, including how it was exploited, if known; and 3) the impacted information and information systems. Given that incident report information SEISPs collect may be shared with a wide range of actors in related organizations, including employees of SEISPs, ministries overseeing the industry and the Cabinet Office should not require reports to include trade secret or sensitive proprietary information.

Further, as stated in Chapter 5, Section 5 of the draft Policy, appropriate measures should be taken on information related to incidents prior to public disclosure, as if the information were to leak, information could be misued, undermining public trust in the government's acquisition of information under the Act. We support the approach in the draft Policy to take organizational security management measures such as: identifying information handlers and providing training; implementing physical security management measures such as locking storage facilities; and ensuring technical security management measures such as access control for electronic files.

In line with this approach, the Government should also protect information obtained in the above cyber incident reports from laws and policies that provide the public access to information and share only the anonymized analysis gathered from the cyber incident reports with other cybersecurity stakeholders to reduce barriers to businesses sharing information, reduce the likelihood of further harms to business victims, and improve the cybersecurity of other businesses.

[8] https://www.nisc.go.jp/pdf/council/cyber_anzen_hosyo/cyber_anzen_hosyo-03shiryo03.pdf

Vulnerability Disclosure and Strengthening Vulnerability Response

Chapter 4, Section 3 (1) of the draft Policy explains that the Cabinet Office will collect various information including notification and vulnerabilities of Specified Critical Computers and Specified Security Incidents to organize them through databases, etc. for cross-checking and analysis of various information that can be effectively used for preventive measures against cyberattacks and for strategic decision-making by organizations protecting critical computers, including private businesses. It also states that administrative agencies that receive such information ("Comprehensive Organized Analysis Information") from the Cabinet Office will effectively utilize that information by processing and sharing with relevant agencies and parties as necessary to encourage recipients of such information to take concrete action for countermeasures. If the information is not already publicly known, we recommend placing safeguards and delays on disseminating this information within government as sharing can create additional opportunities for exploitation, without meaningful positive impacts to cybersecurity.

Regarding the "necessary measures" stated in Chapter 5, Section 2 (6) of the Draft Policy that suppliers of critical computers must take upon receiving requests from competent ministries, we strongly recommend ensuring such requests are proportionate and focused on confirmed vulnerabilities, aligned with structured disclosure practices.

Further, Chapter 5, Section 2 (4) describes that pre-disclosure vulnerability information identified by the Government will be shared with SEISPs that are members of the Council that are subject to confidentiality obligations and security management measures. However, it is unclear what kind of pre-disclosure vulnerability information is being considered and from which entities the Government is planning to obtain such information. Providing greater clarity on the scope and process will be helpful to better understand how the proposed mechanism is intended to operate.

Additionally, Chapter 5, Section 2 (5) of the draft Policy states that due to cyberattacks being increasingly carried out using communication devices of general users -– for example, through malware infection – the Government may provide information to raise awareness after applying necessary processing to threat information, not only to users of critical computers but also to individuals using computers that may be used for specific unauthorized acts. While we support the intent of this measure, we also recommend the Government avoid premature disclosure of vulnerabilities to the public especially if a patch for the vulnerability is not yet available.

While vulnerabilities in software and hardware are inevitable, they are often identified by independent security researchers. It is therefore essential that vendors of such computing systems maintain procedures for processing third-party reports of identified vulnerabilities. In this regard, the information security community has developed a set of protocols known as "coordinated vulnerability disclosure" (**CVD**) to help vendors work with third-party stakeholders to mitigate potential risks to the public.[9] All CVD requirements should be aligned with existing internationally recognized standards ISO/IEC 29147 and 30111.The guiding principle of CVD is that security is best served when vulnerabilities are reported directly to vendors that can fix them and when public disclosures are delayed until the vendor has had an opportunity to develop, test, and deploy a patch to mitigate the underlying vulnerability. To operationalize this underlying principle, software vendors maintain CVD

[9] Guiding Principles for Coordinated Vulnerability Disclosure at https://www.bsa.org/files/policy-filings/2019globalbsacoordinatedvulnerabilitydisclosure.pdf

programs to respond to third-party vulnerability reports in a manner that minimizes the risk of malicious actors leveraging unpatched vulnerabilities to hack into systems.

As such, we urge the Government of Japan to ensure that identified vulnerabilities, especially those related to critical computing systems used by SEISPs NOT be disclosed publicly until the identified vulnerabilities are verified and successfully remediated.

We also encourage computing system vendors to publish vulnerability disclosure policies that facilitate the vendor receiving reports of newly discovered vulnerabilities, whether that information is discovered by security researchers, customers, or governments. Competent ministers would also benefit from vulnerability disclosure policies because it provides a way for them to contact the manufacturer and share vulnerability information, especially if the manufacturers are located outside of Japan. To help manufacturers remediate newly discovered vulnerabilities as fast as possible, the draft Policy should encourage stakeholders to report new vulnerabilities confidentially and directly to vendors.

Conclusion

We thank the Government of Japan for considering our comments. BSA looks forward to working with the Government to support its goal of enhancing cyber response capabilities. In addition to submitting comments, we would appreciate continued opportunity to discuss the Basic Policy to better understand the specific mechanisms to implement active cyber defense.