Dr. Rajendra Kumar,
Additional Secretary,
Ministry of Electronics and Information Technology (MeitY)

Cc: Dr. Sanjay Bahl, Director General, CERT-In

Monday, May 30, 2022

Dear Sir,

Subject: BSA concerns on the CERT-In Directions on Information Security Practices

Greetings! BSA | The Software Alliance (**BSA**)[1] wishes you and your family good health and safety.

On April 28, the Indian Computer Emergency Response Team (**CERT- In**) issued directions under sub-section (6) of section 70B of the Information Technology Act, 2000 (**IT Act**) relating to information security practices, procedure, prevention, response and reporting of cyber incidents for safe & trusted internet (**Directions**).[2] BSA supports the goals of the Notification to augment and strengthen cyber security in India.

On May 18, the CERT-In, along with the Ministry of Electronics and Information Technology (**MEITY**), issued a clarification and guidance document containing the government's responses to certain Frequently Asked Questions (**FAQs**) on the Directions.[3] BSA appreciates CERT-In and MEITY's efforts to clarify the Directions through these FAQs.

[1] BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry. Its members are among the world's most innovative companies, creating software solutions that help businesses of all sizes in every part of the economy to modernize and grow. With headquarters in Washington, DC, and operations in more than 30 countries, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy. Follow BSA at @BSAnews.

BSA's members include: Adobe, Alteryx, Altium, Amazon Web Services, Atlassian, Autodesk, Aveva, Bentley Systems, Box, Cisco, CNC/Mastercam, Dassault, DocuSign, Dropbox, IBM, Informatica, Intel, MathWorks, Microsoft, Nikon, Okta, Oracle, PTC, Rockwell, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc

[2] Directions under sub-section (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for safe & trusted internet, issued on 28 April, 2022, by the Indian Computer Emergency Response Team (CERT-In) https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf.

[3] Open, Safe & Trusted and Accountable Internet, Frequently Asked Questions (**FAQs**) on Cyber Security Directions of 28.04.2022 https://www.cert-in.org.in/PDF/FAQs_on_CyberSecurityDirections_May2022.pdf

The FAQs document is not legally binding.[4] The FAQs also state that it is an 'evolving document'. The fact that the document is not legally binding means neither BSA members nor any other organization can effectively rely on the FAQs to ensure compliance with the Directions. This could hurt their commercial operations, investments, and R&D activities.

Therefore, BSA recommends that the CERT-In and MEITY incorporate the intent driving the FAQs into the Directions. This would mean hardcoding the specific answers set out in the FAQs into the Directions, subject to certain changes discussed below. As the FAQs already contain much of the hard work of identifying and addresses areas which necessitate clarification, making those concepts binding would have a large return on investment. Additionally, the issues raised and considered in the Directions/FAQs – such as the meaning of the terms 'severe' and 'large-scale', along with determining risk and impact-based reporting timelines etc. – would benefit from a proper industry consultation. Given that cybersecurity is a shared responsibility among the private sector and the government, working in close collaboration with and by understanding the inputs of interested stakeholders will enable the CERT-In to effectively combat cybersecurity threats while sustaining the vitality of the digital economy. Further, making changes to the Directions, as opposed to capturing clarifications in the FAQs, would provide organizations with a reliable legal foundation for compliance. We also urge the CERT-In to pause the implementation of the Directions until it includes such clarifications directly in the Directions.

BSA notes that CERT-In has already invested the resources to consider and clarify numerous issues in the FAQ. While we appreciate the effort, as mentioned above, as CERT-In incorporates the FAQ into the Direction, it can provide greater clarity while still achieving its desired goals. So, while incorporating the clarifications into the Directions, we recommend that the CERT-In:

1. **Define the scope of 'severe' and 'large-scale' incidents:** We welcome the CERT-In's objective to adopt an impact and risk-based approach to determine which incidents are reportable under the 6-hour timeframe.[5] But the FAQs do not provide any principled guidance on what a 'severe incident' or 'large-scale incident' would mean (despite providing specific examples). Similarly, the definitions of 'data breach' and 'data leak' do not establish a threshold based on risk – meaning that all data breaches or leaks would have to be reported. For instance, a minor incident involving an email being sent inadvertently to incorrect recipient(s) within an organization, could be categorized as a 'data breach' internally, however, the ensuing risk is rather low, with possibly no impact on individuals or the organization. Further, the lack of guidance creates ambiguity for organizations seeking to identify 'severe' or 'large-scale' incidents. The approach set out in the FAQs does not align with the CERT-In's objective to mandate reporting of high-impact incidents. We urge the CERT-In to define a principled guidance to determine 'high-impact' or 'severe' incidents

[4] The FAQs note: "is not a legal document and in no way whatsoever replaces, amends, or alters any part of the IT Act, 2000 and/or the Information Technology (the Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 (hereinafter referred as CERT-In Rules, 2013)".
[5] Q30, FAQs.

clearly within the Directions. These guiding principles should also be applicable to data breaches and data leaks.

2. **Revise the reporting timeline to no later than 72 hours after discovery:** We agree that timely reporting to the CERT-In of significant or severe cybersecurity incidents is critical for facilitating better-coordinated, and more effective response of individuals and organizations affected by an attack. The time period for reporting should help achieve these objectives and align with operational realities. But the 6-hour reporting period will not help meet these objectives. Based on our experience and research, the initial 24-72 hours after a potential incident is discovered involves uncertainty and fast-paced investigative, containment, and remediation work. This is a critical period, since there is a consistent need to react in unexpected ways to new information as it is discovered. An organization's understanding and evidence as to the cause and scope of an incident are often vague and fluid. Affected systems and victims are unknown. So, it is essential that information systems personnel maintain consistent, focused attention on investigation, containment, and remediation without pressure to guess or otherwise devote scarce resources to activities that detracts from these primary pursuits. An obligation to provide an initial incident report before 72 hours has elapsed after confirmation of an incident – elevating speed and speculation over clarity and certainty – carries significant risk both for the reporting entity and the CERT-In who will be receiving the report. Such reports will likely not be of the requisite quality. As FAQ Q30 acknowledges, organizations likely will have little to no useful information to share after an initial 6-hour period beyond "something happened". The CERT-In also stands to be flooded with incomplete information that will not present actionable data or, even worse, will include inaccurate data that distracts it's attention and resources in the midst of critical incident response. Accordingly, we urge the CERT-In to revise the Directions to require entities to provide an initial report of significant or severe cyber incidents as soon as practicable or within 72 hours of the confirmation of an incident, whichever is faster. A 72-hour period allows a reporting organization to identify information to aid in incident investigation and response, including the deployment of defensive measures, and will ensure that the information provided is grounded in fact, rather than initial speculation. Moreover, a 72-hour period is commonly used in other jurisdictions and would allow businesses to develop consistent processes across different countries and regions. We also urge to CERT-In to clarify that the reporting timeframe commences once the incident and its severity are confirmed by the organization.

3. **Provide greater flexibility on log-keeping requirements:** We commend the CERT-In for clarifying that organisations can store logs abroad as long as organizations can produce them for CERT-In within a reasonable timeframe.[6] The FAQs also provide an indicative – not exhaustive – list of logs to be stored, that is provided to give a 'flavor' of the logs to be maintained.[7] While this offers organizations a certain amount of flexibility, it does not fully address concerns on the impact of localized log-keeping requirements on global cybersecurity

[6] Q35, FAQs.
[7] Q37, FAQs.

operations. It does not also properly address the issue of excessive log-keeping. The Directions should reflect CERT-In's focus (Q35 in FAQs) on 'obligation to produce logs in a reasonable time' as opposed to mandating local storage or imposing a broad log-keeping requirement that do not contribute to a more secure environment. Moreover, in a Cloud environment, customers control what event logs are generated by their workloads in the cloud, therefore, customers should be the point of contact to provide event logs. The CSP collects logs for limited purposes including operational maintenance, security of the cloud and for billing purposes. These are mostly related to customers, as opposed to any security incidents.

4. **Delay the implementation of requirement to collect user information:** Gathering more information is unlikely to deter cybercrimes. The linkage between collecting additional data, and effective cyber security incident responses, is also unclear. Notably, current on boarding practices for cloud service providers involve collecting payment and contact details and an OTP based confirmation, and this should be considered as sufficient. Phone numbers and credit cards already have a KYC process associated with them and further validation will be duplicatve. Regardless, we request a consultation to understand the objectives for any additional validation steps as it will require significant time, effort and investments to develop onboarding processes. Also, the mandate to maintain user information for 5 years or longer can place undue burden on organizations. Such information could include personal data of individuals and organizations are bound by both privacy as well as confidentiality obligations to customers not to disclose this information or retain it for longer than it is necessary. Also, organizations may face operational challenges with the nature of information mentioned in the provision. For instance, with people working remotely, many users have dynamic IP addresses that change regularly, and it could be challenging to identify and record all "IPs allotted to / being used by the members". For these reasons, we request that the CERT-In to delay the implementation of this provision, until it can gather and understand the concerns of relevant stakeholders.

5. **Clarify that reporting obligations apply to end-user businesses, not to third-party service providers:** Reporting obligations under the Directions apply to all organisations, including the organisation that has been affected by the incident, and third-party service providers supporting the affected entity. The FAQs reinforce this view. [8] This can be problematic, since third party service providers are not in a position to know if an incident is severe or large-scale and therefore cannot make a risk-based determination. Only the affected, end-user facing entity will have knowledge of the impact, and it will be able to share incident information of the appropriate quality with the CERT-In. Any other approach can create confusion in the event of an incident involving a third-party service provider. This can result in over-disclosure of cyber incidents, disrupting the marketplace, creating unnecessary noise that would confuse companies and the CERT-In alike. This ambiguity would exacerbate the consequences of the incident — and without reason. Instead, the CERT-In should support existing cooperative and agreed-upon approach through which third-party service providers

[8] Q13,22, FAQs.

report cyber incidents to their customers. Changing these established practices would greatly increase complexity and uncertainty without improving either market fairness or cybersecurity.

While the FAQs help in clarifying the CERT-In’s intention, organizations cannot rely on a non-legally binding document. We urge the CERT-In to incorporate the clarifications discussed above in the Directions and to pause the implementation of the Directions until it includes such clarifications directly in the Directions.

Ultimately, this effort to incorporate the clarifications into the Directions, and further consideration of the issues noted above, would be most fruitful if done in consultation with industry who are committed to improving cybersecurity. Such a dialogue or consultation will result in CERT-In achieving our shared goal of a more secure future, while simultaneously supporting the growth of the Indian economy.

Sincerely,

BSA | The Software Alliance