

May 5, 2022

Respected Dr. Sanjay Bahl ji,

Greetings from ITI. The Information Technology Industry Council (ITI) is the premier global advocate for technology, representing the world's most innovative companies.¹ Founded in 1916, ITI is an international trade association with a team of professionals on four continents. We promote public policies and industry standards that advance competition and innovation worldwide. Cybersecurity and cybersecurity technology are critical to ITI members, and our members have extensive experience working with governments around the world as both producers and users of cybersecurity products and services. Consequently, ITI has been a leading voice in advocating effective approaches to cybersecurity policy globally.

We write to you regarding the recent directions issued from Cert-In relating to *Information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet* issued on 28 April 2022 (the Directive). While we appreciate that with this Directive Cert-In is seeking to improve cybersecurity, we fear that as drafted and without significant revisions the Directive may negatively impact Indian and global enterprises and actually undermine cybersecurity in India. In particular, we have concerns with several of the incident reporting obligations, including the mandatory reporting of cyber incidents within 6 hours of noticing, the requirement to enable logs of all ICT systems and maintain them securely within Indian jurisdiction for a rolling period of 180 days, the overbroad definition of reportable incidents, and the requirement that companies connect to the servers of Indian government entities. If left unaddressed, these provisions may have severe consequences for enterprises and their global customers without solving the genuine security concerns. We further elaborate on this non-exhaustive set of concerning provisions below.

- **6-hour reporting timeline (part ii).** We recognize that incident notification is a priority for India and other governments around the world and have developed *Global Incident Reporting Policy Principles* to help guide the development of incident reporting regimes globally that will help governments gain visibility into incidents and aid in incident response activities.² We encourage Cert-In to take into account our recommendation to **establish feasible incident reporting timelines of at least 72 hours, commensurate with incident severity levels in alignment with global best practices.** Doing so will ensure that companies are able to focus on responding appropriately to an incident and that any information provided to the government is contextualized.
- **Logging requirements (part iv).** To enable logs of all covered entities' ICT systems, maintain logs of entities' ICT systems "securely for a rolling period of 180 days" within

¹ Visit www.itic.org to learn more.

² Available here: <https://www.itic.org/documents/cybersecurity/ITIGlobalPolicyPrinciples-SecurityIncidentReporting.pdf>

India, and make them available to the Indian government upon request is not a best practice. It would make such repositories of logged information a target for global threat actors, in addition to requiring significant resources (both human and technical) to implement.

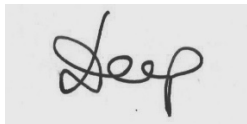
- **Incident definition (Annexure I).** The current definition of reportable incident to include activities such as probing and scanning is far too broad given probes and scans are everyday occurrences. It would not be useful for companies or Cert-In to spend time gathering, transmitting, receiving, and storing such a large volume of insignificant information that arguably will not be followed up on.
- **Connection to NTP servers (part i).** The requirement that “all service providers, intermediaries, data centres, body corporate and Government organisations shall connect to the NTP servers [of Indian labs and other entities] for synchronisation of all their ICT systems clocks” is very concerning because it could negatively affect companies’ security operations as well as the functionality of their systems, networks, and applications, amongst other reasons.

With the above in mind, we request that Cert-In:

- Delay the period of implementation of the stated Directive (currently 60 days post April 28, 2022) to allow time to address the concerns raised;
- Revise the Directive to address the concerning provisions with regard to incident reporting obligations, including related to the reporting timeline, scope of covered incidents and logging data localization requirements; and
- Launch a wider stakeholder consultation to ensure that the Directive can be effectively implemented in a revised format, including that Cert-In open a detailed technical consultation for public reply.

We look forward your response and having a dialogue with the Department on these issues at the earliest opportunity. Please find our coordinates below for further engagement on the Directive.

Sincerely,



Kumar Deep
Country Manager, India
ITI
kdeep@itic.org
9811736847



Courtney Lang
Senior Director of Policy
ITI
clang@itic.org