

June 27, 2022

To:

Shri Sanjay Behl
Director General
Indian Computer Emergency Response Team (CERT-in)
Ministry of Electronics and Information Technology
Government of India

CC:

Shri Alkesh Kumar Sharma
Secretary
Ministry of Electronics and Information Technology
Government of India

Subject: Request to defer the implementation of the Directions issued on April 28, 2022 by CERT-In and initiate an open process of public consultation.

Sir,

We write to you as a group of cybersecurity experts and technologists committed to maintaining an open, trustworthy, and secure internet for all. We are deeply concerned by the Directions issued by CERT-In on April 28, 2022, and urge you to please defer their implementation, and initiate a process of in-depth public consultation aimed at modifying the Directions with inputs from all stakeholders and experts.

The Directions, as they stand, will have the unintended consequence of weakening cyber security, and its crucial component, online privacy. We are cognisant of the need for a framework to govern cyber incident reporting, but the reporting timelines and excessive data retention mandates prescribed in the Directions, will have negative implications in practice and impede effectiveness, while endangering online privacy and security.

We appreciate that a [consultation](#) was held on June 10, 2022, with invited stakeholders. However, we do not believe this to be sufficient, and the public, including the complete range of stakeholders and experts, must be given an opportunity to submit feedback. We therefore respectfully urge MeitY and CERT-In to conduct open and in-depth consultations, and invite inputs from the public at large, in order to devise a holistic framework, and to defer the implementation of the Directions until such consultation is concluded and suitable amendments are made. It is crucial that CERT-In and MeitY ensure that the regulations advance systemic and user-centric approaches to cybersecurity, focusing

on effective cyber incident response — which is also the specific, limited rulemaking power given to CERT-In by the Indian Parliament in this section of the Information Technology Act.

We remain available and anticipate opportunities to engage with you on this issue, and assist in the development of a framework that truly strengthens cybersecurity that empowers users in India.

Signatories:

Adam Shostack, Author, Threat Modeling: Designing for Security

Adebunmi Adeola Akinbo, CEO, DNS Africa Media and Communications

Dr. Brian Haberman, Johns Hopkins University & Internet Society Board of Trustees

Charles Mok, Member of Board of Trustees, Internet Society

Christian Dawson, Executive Director, VPN Trust Initiative

Georgia Bullen, Executive Director, Simply Secure

Gytis Malinauskas, Head of Legal, Surfshark

Jorge Pinto, Cybersecurity Professional, Portugal

Joseph Lorenzo Hall, Distinguished Technologist, Internet Society

Jyoti Panday, Internet Governance Project, Georgia Institute of Technology

Kailash Nadh, CTO, Zerodha

Prof. Kapil Goyal, Academic Member, Global Encryption Coalition

Karen O'Donoghue, Director, Internet Trust and Technology, Internet Society

Keith Robert Fernández, ISOC president Peru Chapter

L. Jean Camp, Professor at the School of Informatics and Computing at Indiana University

Mallory Knodel, Chief Technology Officer, Centre for Democracy & Technology

Moses Owiny, Centre for Multilateral Affairs (CfMA), Uganda

Prasanth Sugathan, Legal Director, SFLC.in

Prateek Waghre, Internet Freedom Foundation

Raman Jit Singh Chima, Senior International Counsel & Global Cybersecurity Lead, Access Now

Dr. Stephen Farrell, School of Computer Science and Statistics, Trinity College Dublin, Ireland

Tarah Wheeler, International Security Fellow, New America