INTERNET
FREEDOM
FOUNDATION

Members of the NCSS 2020 Task Force Secretariat:

We take great pleasure in making this submission on India's Cyber Security Policy for 2020. It is our firm belief that a secure and safe India proceeds from the safety of our digital infrastructure -- more importantly every Indian who today is using technology.

The Internet Freedom Foundation is an Indian member supported non-profit organisation that ensures technology respects fundamental rights, born out of the SaveTheInternet.in movement for net neutrality. We work across a wide spectrum of issues, with expertise in free speech, electronic surveillance, data protection, net neutrality and innovation; we aim to champion privacy protections, digital security, and individual freedoms in the digital age. We are providing a brief submission here, tailored to meet the character limit indicated by the task force for this consultation, in order to provide initial comments which we seek to supplement with a broader paper.

As part of its framing of the planned 2020 National Cybersecurity Strategy, we recommend at the outset that the Task Force adopt the approach that rights of Indians - particularly with respect to privacy, data, and the open web more generally - are taken as complementary to a holistic cybersecurity approach. Digital civil liberties and digital security should not be taken as competing with each other, when they in fact are complimentary. Below we illustrate some initial tangible ways to achieve this.

- *Recommendation 1: Independent vulnerability testers and cyber security specialists are strategic national assets*

  India's innovative and expanding community of security researchers is a net asset, for cybersecurity in both the public and private sectors. There should be a clear policy and standard operating procedure devised for departments to be notified by security researchers without the threat of civil or criminal prosecution. Such individuals should rather be offered rewards and recognition for upholding and securing our national interest; bug bounty programmes and responsible vulnerability disclosure mechanisms need to be adopted by the government and its agencies.

- *Recommendation 2: Encryption protects India by protecting Indians*

  The use of encryption has far too often come under political attack by some parts of the security ecosystem. Many of these concerns, though perhaps coming from potentially legitimate interests, far too often fail to under technical architectures of modern ICT devices and communications, and also do not honestly characterise the many elements of personal data that are often outside of encrypted channels.

  In fact, failure to encourage and expand the usage of encryption technologies puts individual users at risk. Here millions of Indians who today conduct their lives through digital tools are also entry point vulnerabilities unless their devices are secured through encryption. Hence, promoting encryption should feature as one of the primary focus areas of the Cyber Security Policy. We caution the Task Force from considering surveillance interests as always coinciding with national cybersecurity goals, which need to focus on allowing departments, firms, and individuals to effectively protect their data and securing the networks they use. More often than not, radically expansive surveillance measures do not advance any meaningful state capacity to prevent breaches of cyber security and increase costs and resource deployment without advancing the security interests of individuals and government institutions.

- *Recommendation 3: Encourage a strong data breach reporting mechanism in the Data Protection Act*

  Data breach reporting under a data protection legal framework is immensely useful for enhancing cybersecurity. To ensure a robust, coordinated institutional ecosystem on this is creating, we recommend that the Task Force provide strong support to strengthening the proposed data breach provision in the Data Protection Bill before Parliament, and also plan to institutionally engage the Data Protection Authority in any national cybersecurity coordination mechanism that may be further strengthened within the government.

- *Recommendation 4: Malware use makes all of insecure*

  We further recommend that the use of malware should be clearly prohibited. The collection of, “Zero-day” hacks or the proliferation in the use of technical exploits to hack into the devices and digital services of Indians makes the nation insecure. It promotes a race to the bottom where such tools can be used by private individuals and leads to further development of backdoors. These can and often are then used by malicious actors against private individuals, public officials and state institutions. Hence, the use of malware which is already recognised as a criminal offence under the Information Technology Act should be strongly discouraged within the Cyber Security Policy.

- *Recommendation 5: The open web is the secure web*

  Today, there are both economic forces and regulatory suggestions that threaten the decentralised framework of the internet. This undermines not only the stability of the public core but has a negative impact on cyber security in real and tangible ways. For instance, the consolidation of the underlying telecom networks which serve the internet and digital communications limits the diversity of network architectures. This inhibits choice and centralises the vector of attack which would ordinarily be spread over and distributed in different segments. Hence, for instance the fewer number of telecom and internet infrastructure providers would not only inhibit user choice but increase the risk of a single point of failure. Similar concerns arise from several regulatory suggestions which seek to create databases of sensitive personal information and then centralise them, or even proposals to create data exchange networks around, “community data”.

We also strongly recommend that the Task Force publish the draft text of its proposed National Cyber Security Strategy after this first round of inputs. National cybersecurity consultations globally have resulted in more effective strategies - including their adoption and stakeholder trust - when stakeholders have been engaged in the detail of the policy and the ecosystem it creates.

We remain committed to providing solution oriented inputs for securing our cyber infrastructure by securing everyday Indians.

Faithfully,

Apar Gupta,
Executive Director
Internet Freedom Foundation