Internet And Mobile Association Of India

COMMENTS /FEEDBACK ON NATIONAL INFORMATION SECURITY POLICY

Introduction:

On behalf of our members we would like to commend the Government of India for approaching the issue of cyber security on the basis of international best practices and cooperation with the private sector. We sincerely hope that further developments in policy measures related to NISP would be done in consultation with open public consultations and would also take into view the private sector initiatives in this space. Finally, NISP should also be based on two-way flow of information and dara sharing – private to government as well as government to private.

In this submission we are also assuming that issues such as Encryption and Escrow are not directly a part of this paper.

Here is our detailed feedback.

General Observations:

1. NISP requires being very flexible, responsive to ever-changing cyberspace and should have longer shelf life. It should therefore be kept opne for wider interpretation and be able to cut out dogmatism.
2. As a nation we need to much more actively involved in Internet governance rather, than control. This has been a weak area. As we are not active in Internet Governance bodies, this takes away our strategic depth and effective handling of issues with complete in-depth understanding. Thus a guidance in NISP, where as nation we need to be pro-active in Internet governance bodies may be necessary.
3. There is need to clearly state that NIB from time to time will declare as to what activities or actions in Indian Cyberspace would amount to aggression on India and if such parameters are crossed then we may retaliate diplomatically or mount counter offensive in Cyberspace against state as well as non-state actors.
4. Though there has been repeated mention of R&D but specific involvement and integration of 'Academia' in furthering the national cause of Cyber Security education may be necessary. This may include development of curricula, capacity building and hub of new ideas. Student exchange programme with other countries and publication of research papers at various universities level may be in the interest of our country. This may find mention in the NISP.
5. Our pro-active participation in developing standards (national as well as international) requires specific and clear mention. The STQC may be given similar charter as NIST of the US at least in the field of Cyber Security.

6. Though the "role and responsibilities" of private persons and bodies have been mentioned but same is kept hazy for government department. There is lack of clarity in charter. It may please be noted that overlaps especially in respect of surveillance of critical Information Infrastructure of enemy /probable enemy state can be jeopardised by the weakest link in the chain, and if there is any lack of coordination a major operation may collapse. Therefore tasking of surveillance and cyber –intelligence outside the country must be positively controlled by NIB and should be stated so unambiguously.
7. National policy on joining / creating international treaties / fora for joint cyber crime operation must be spelt out in NISP.

8. NISP must state the nodal point of interaction in case of any cooperation with foreign entity for Cyber Crime investigation.
9. Please read through draft ISO 27037 on International standardisation for capacity building for "First Responder" for gathering Cyber Evidences which can be admissible in courts of other countries. It will be necessary to align our procedures and practices so as to accept the Cyber evidences gathered in accordance with ISO 27037 in third nation. (This should be a MUST clause in NISP).
10. National policy must include the mechanism and methods for farming rules for Cyber crime in a transparent and consultative manner.
11. NISP is silent on privacy issue. The links with various existing laws in place should be drawn out explicitly.
12. There is no mention of abuse / misuse of power from information gathered for national security purposes by government officials/agencies. NISP must make clear and make an unambiguous policy statement as to how such cases should be treated. This will help preventing Human Rights violations as well as corruption.
13. Though TRAI planning to look into governance issues of Cloud Computing. This facet may require appropriate mention in the NISP after a due consultative process by stakeholders.
14. After introducing appropriate amendments, it may be prudent to go for last and final public inputs on such amendments prior to submitting it to CCS for clearance and publication.

Specific Observations:

1.2 Security of Cyber Space: Security measures proposed to be mandated under this policy should have direct relation to the electronic information / transaction proposed to be secured. Further all such security measures should be reasonable and commercially viable proposition.

1.4 Securing Cyber Space: Key Policy Considerations: While regulating cyber space, cyber space itself should be classified basis the nature of network access and information thereof. Accordingly security measures should be mandated for each classification.

2.2 International Cooperation: So far as private sector is concerned, it role in co-operation should be limited to providing specific information for investigative reasons. Business Information / secrets should not be covered within the ambit of this policy.

2.4 Priorities of Action: Since this call for creating conducive legal environment in support of safe and secure cyber space, there is already an existing set of laws in the form of Information Technology Act and rules there under. If at all, the same law may be amended and new set of law need not be enacted for regulating the cyber space. This shall avoid confusion and multiplicity of laws.

3.3 Securities and Best Practices: This mandates best security practices for critical sectors. The definition of critical sectors should be limited to such sectors which may affect national security or may lead to loss of life. Pure business ventures should not be covered under this definition / policy.

3.3 (c) Data Security and Privacy: A separate privacy and data security framework may not be required under this policy since the same is mandated under various rules framed under Information Technology Act.