Tabular Mapping of Stakeholders' Responses to the TRAI Privacy Consultation Paper: Part X of XII- Safety and Security of Telecommunications Infrastructure and Digital Ecosystem

The following table was prepared after an analysis of all fifty-three (53) responses to question eight (8) of the Consultation Paper: *"What are the measures that should be considered in order to strengthen and preserve the safety and security of telecommunications infrastructure and the digital ecosystem as a whole?"*

The table identifies the stances of the stakeholders and their response to the question. It also states the suggestions made by them to TRAI in view of the question posed. As mentioned earlier, the responses of the stakeholders have been categorized in a manner that corresponds with some of the issues raised in Part 4 the White Paper, namely, regulation and enforcement of provisions.

Sl. No	Stakeholder	Recommendations of the stakeholders on the regulation and implementation of uniform security measures	Issues raised			
			Raising of encryption	User oriented process	Better training to workforce and technology improvements	Sharing of information in the industry and publishing of attacks and security breaches
1.	IAMAI	Data encryption freedom based on the user(s) requirement, hence not resulting in blanket encryption of data and prescribing a lower limit for encryption for basic protection and in favor of self-regulatory mechanisms.	Against the current 40 bit encryption standard that is in contradiction with the encryption standards set by RBI and SEBI.	Privacy of data to be of key importance and hence more control of data to the users and consent of collection.	Better on job training to handle critical data related tasks i.e. collection, monitoring, recording and improvements to technology to augment the above tasks.	—
2.	ACTO	—	In favor of regulations based on 84A of the IT Act resulting in raising of	—	Practices aimed at Improvements to the	—

			the current archaic 40bit telecom encryption standard.		workforce and better training to employees.	
3.	ASSOCHAM	Proposed a collaborative effort between the private and the public sector facilitating innovation in cybersecurity and compliance including by encouraging research and self-regulatory and certifications schemes.	Amendment to the archaic 40-bit encryption standards.	—	—	—
4.	COAI	Existing security measures pertaining to telcos should extend to internet eco-system stakeholders and there should be a uniform framework between OTT communication providers and TSPs.	—	—	—	—
5.	GSMA	Uniform security measures to apply to TSP and Internet Eco-system stakeholders and acknowledgement of protocols to protect mobile networks.	—	—	—	Proactive approach to attacks - ensure mechanisms are in place to keep the whole ecosystem aware of threats.
6.	ISPAI	Formation of stringent rules pertaining to sending data outside of country and uniform framework governing digital eco-system stakeholders and TSP.	—	—	—	—
7.	NLUD	—	—	—	—	—

8.	Span	Need for promulgation of a Data Protection Law.	—	The law is to be cognizant about the extent to which individuals are able to exercise control over their personal data. Industry's use of such data in the digital world during process of collection and portability for any kind of data processing / analysis has to ensure that user's privacy is not compromised.	—	—
9.	TRA	—	—	—	—	—
10.	NASSCOM-DSCI	Industry and government work in tandem to create a security framework that is dynamic and robust.	—	—	—	Threat and risk assessment to be published.
11.	ACT	—	Strong Encryption policies without putting in backdoors for the government to exploit in name of security as that is a violation to the right of privacy and end to end encryption policies.	—	—	—

12.	Zeotap	—	—	Education of both the stakeholders and customers pertaining to personal data security and user-oriented process of data collection and monitoring involving consent to erasure if exceeding the use of data.	—	—
13.	Takshashila	No further measures required to current telcos infrastructure.	—	—	—	—
14.	ISACA	Application of Dynamic, organic and iterative public policies to regulate data.	—	Improvements to the workforce and training of employees and improvements to the technology used by them.	—	—
15.	IBM	Focus on risk-based cybersecurity and adding cybersecurity to the legal framework of companies.	Application of cryptography to data encryption and amendments to the archaic 40-bit encryption protocols resulting in dichotomy of encryption standards of SEBI and RBI. Policies imposing legal mandates on technology providers to be avoided as companies	—	—	—

			don't have decryption keys to decrypt the data encrypted.			
16.	Make My Trip	—	—	—	—	—
17.	Accessnow	Against laws pertaining to auditing of data as that would result in more parties having access to data resulting in further monetization. Framework instilled should be framed in a way that doesn't get affected by the ever-evolving technology, so that framework does not have to be amended every few years.	—	—	—	Government should provide information on their own experience with cybersecurity and data security breaches so as to provide information to the industry on how they can improve on the breaches.
18.	USISPF	Uniform security measures applied to all players whether telcos or internet OTT communication providers.	—	—	—	—
19.	ITI	Security must be risk based and the regulations pertaining to risk-based security must be dynamic and robust to avoid narrow solutions to problems Formulation of policies restricting borderless internet should be avoided as imposing restrictions on the internet causes economic growth hampering as businesses need	Policies imposing legal mandates on technology providers to be avoided as companies don't have decryption keys to decrypt the data encrypted.	—	—	—

		to get in touch with foreign players as well.				
20.	Sigfox	Data security laws should be dynamic as they should address the risk at its source creating a risk-based security system taking cue from NIST and working in tandem with CERT.	—	—	—	—
21.	Exotel	—	—	—	—	—
22.	KOAN	Policies mandating certain regulations must be mindful of the consequences it will have on the framework of the industry as to not be negative and cause more harm than good.	—	—	—	Sharing and publishing of information pertaining to cybersecurity must be active on threads through formal and informal means like WhatsApp groups or company newsletters.
23.	IFF	Laws pertaining to criminal action against any one who reports breaches in security must be done away it. Presently anyone reporting a breach is entitled to receiving a legal notice.	—	Mandatory linkage of Aadhar for telecom must be done away with in the interest of privacy and security of the users.	Research on security and training to employees must be given more importance and bug bounty programs must be encouraged with appropriate rewards for finding breaches in security.	—
24.	Mozilla	Strong security standards, including obligations to use encryption, role-based access control, and	—	—	—	Publishing of vulnerabilities must be encouraged and guidance on how to

		multifactor authentication is critical to ensuring the safety and security of telecommunications infrastructure and the digital ecosystem as a whole. The process of reporting vulnerabilities should be codified in law where possible to ensure that the policy decisions are made in part by legislative bodies, understood by the public, and not subject to revision behind closed doors.				prevent the same. Public reporting by a civilian agency can be formed tasked with the above mentioned actions. Recommended that TRAI work in concert with the data protection authority and other relevant regulatory bodies to regularly publish guidance on how best to secure infrastructure and users.
25.	IDC	—	—	Increased transparency on the use of data and providing a notice to disclose consent of the user and providing the user with control over access, privacy and portability in case they shift from providers. Further they must be alerted of a breach and should be given a notification on profiling of data.	—	—
26.	Citibank	All data controllers and telecom service providers to be controlled under a centralized	—	—	—	—

		authority. Provide a strong legal framework for the telecommunications sector by amending the Indian Telegraph Act and integrating it with other statutes such as the IT Act 2000 etc. would ensure safety of telecom infrastructure.				
27.	iSPIRT	Proposal of strong security standards based on the highest standard.	__	__	Invitation to bug bounty programs providing adequate rewards.	Publishing of vulnerabilities as well breaches or threats to security.
28.	ITC	__	__	__	__	__
29.	CIS	__	Raising of the current encryption standard of 40bit.	Reporting of breach by users and giving them a notification of the same. Provide educational material on security breach to consumers to help them be more vigilant to threats.	__	__
30.	USIBC	Establish a robust and a uniform encryption requirement.	Amendment to the 40bit encryption protocol by raising it to a global standard. Policies imposing legal mandates on technology providers to be avoided as companies don't have decryption keys to	__	__	__

			decrypt the data encrypted.			
31.	Disney India	Gaps in the current framework to be resolved by transparent provisions to better facilitate the customers.	—	—	—	—
32.	BSA	Proposed a framework by learning from the experience of the US based NIST framework and a risk-based security framework that adheres to global standards and is dynamic.	—	—	—	—
33.	SFLC	Use of FOSS that is not auditable by anyone but is auditable by a proprietary software that is closed and not auditable.	—	—	—	—
34.	EBG	—	Policies imposing legal mandates on technology providers to be avoided as companies don't have decryption keys to decrypt the data encrypted. Encryption standards to be harmonized and uniform to stakeholders.	—	—	—
35.	AT&T	Risk based security framework to be adopted by the stakeholders and Industry and government work in tandem to	Policies imposing legal mandates on technology providers to be avoided as companies don't have decryption keys to	—	—	—

		create a security framework that is dynamic and robust.	decrypt the data encrypted. Amendment to the 40bit encryption protocol by raising it to a global standard and resolving the dichotomy of the regulations imposed by the RBI and SBI of 128bit compared to the GOI standard.			
36.	BIF	Make organisations have accountability through self regulation instead of strict compliance. That way organisations will tackle threats over trying to achieve compliance.	Amendment to the 40bit encryption protocol by raising it to a global standard and resolving the dichotomy of the regulations imposed by the RBI and SBI of 128bit compared to the GOI standard.	Grievance redressal practices rather than monitoring in customer service programs. Further policies should be about preventing misuse of data rather than focus on the control of it.	—	—
37.	Sangeet	—	—	—	Advanced threat detection programs and measures to be implemented.	—
38.	Redmorph	Telcos tend to have strong data security and privacy norms they work with outsourced service providers like call centers, collection agencies etc. who are susceptible to data leaks. TRAI needs to have a min policy framework set for data privacy.	—	—	—	—

		Care needs to be taken that personal information cannot be shared with marketing organizations without proper compliance.				
39.	Baijayant Panda	__	__	__	__	__
40.	Apurv Jain	__	__	__	__	__
41.	RJIL	Sensitive Data should be localized and cybersecurity should be incorporated as part of the framework. Framework instilled should be framed in a way that doesn't get affected by the ever-evolving technology, so that framework does not have to be amended every few years and the regulations imposed must not overbear on other laws or regulations already in play.	__	Data privacy should be of the utmost importance and hence the users must be made aware of the same when data is collected and consent should be priority.	__	__
42.	Airtel	Uniform security measures to apply to TSP and Internet Eco-system stakeholders. Data must be stored in a secure manner. Industry and government work in tandem to create a security framework that is dynamic and robust.	__	__	__	__

43.	Idea	Telecoms being classified as CII; the regulations must be dynamic to not hinder its importance. Uniform security measures to apply to TSP and Internet Eco-system stakeholders pertaining to security and privacy. Directives must be announced by the public authority ensuring availability of services. For the digital ecosystem there is need of application data storage monitoring mechanism and the application owner should be bound by governmental data security norms.	—	—	—	—
44.	MTNL	Auditing of Telecom infrastructure for reliability, availability and confidentiality.	—	—	—	—
45.	RCOM	—	Amendment to the 40bit encryption protocol by raising it to a global standard and resolving the dichotomy of the regulations imposed by the RBI and SBI of 128bit compared to the GOI.	Technologies like Network Function Visualization (NFV) virtual mobile networks become vulnerable to multiple security threats and these threats must be addressed.	—	—

			Internationally proven encryption algorithms, such as a) DES 56 bits, (b) 3DES 128 bits and (c) AES 256 bits are adopted in India in consonance with the IT Act, 2000. Uniform application of the same across all players.			
46.	TTL	Existing measures in play sufficient and support for future measures.	—	—	—	—
47.	BSNL	Auditing of service providers to provide information on their data handling situation. Uniform regulation measures across all stakeholders.	—	Grievance redressal of data misuse and applying time limits on how long data can be stored before erasure.	Development of advanced telecom hardware to increase the security of data handling.	Reporting of security breaches and publishing of the same.
48.	Telenor	Industry players and the Government must work in tandem to undertake initiatives regarding ecosystem monitoring. There must be exchange of information to trace threats and put in place adequate safeguards. A national legislation under an independent privacy regulator would be beneficial.	—	—	—	Sharing of information on breaches and threats to security.

49.	Vodafone	Existing measures sufficient.	—	—	—	Sharing of information on breaches and threats to security.
50.	FCSO	Impose heavy penalties.	—	—	—	—
51.	CUTS	—	—	—	—	—
52.	CGS	—	—	—	Timely updating of data security and adhering to globally accepted security standards by using advanced technology.	—
53.	CPO	Develop a more detailed plan for CIIs by incorporating globally tested security standards. Mandating foreign companies to set up servers to monitor the digital ecosystem for protection from security breach.	—	—	Create awareness among employees and give them better training to handle data security breach.	—