Username	Question received on chat	Reply received on chat
Harish Chowdhary	May i ask do we have any domain name system measurements framework to provide data points and indicators to flag a domain as malicious	
2640 479 1155	Hello Mr.Singhal, is KYC of whois information mandatory? If so, will NIXI conduct it or the Registrar needs to do it?	
avinash kaur	As Geographical Indications" are integral compent o Intellectual Property Rights NIXI may also add " Geopgraphical Indications" in its definition clause 4(m)	
Harish Chowdhary	<question>did we consider latest intermediary guidelines 2021 while creating these guidelines	@harish & Priya Do the intermediary guidelines notify Registrars as intermediaries explicitly? That is quite a slippery slope except in cases where Registrars are also hosting providers and also deviating from the global consensus on the infrastructure stack
Priya & Rima S.S. Rana & Co.	Section VI- Clause C- add Counsels alongside Authorized representative	
Priya & Rima S.S. Rana & Co.	Section VI- Clause D- may add Who may be the victim of the abuse in the first line	
Priya & Rima S.S. Rana & Co.	Section X- Clause A- Validate may be added before the word -Verify. This is in consonance with ICANN agreement with DNRs	
Priya & Rima S.S. Rana & Co.	Section X- a policy is being proposed to incentives the DNRs for handling abuse situations however it does not provide for making the DNRs liable for their inaction or non-cooperation in handling abuse situations. The Delhi High Court has recently asked Meity Dot to action in this regard.	
Swapneel Patnekar	Can we rename this as Domain name anti-abuse policy? The reason being, DNS anti-abuse will comprise of many things - For example to name a few, Open resolver abuse for Distributed of Denial of Service(DDoS) or Man-in-the-middle attacks in the context of DNS hijacking etc?	from Ajith Francis to everyone: 6:19 PM@Swapneel, i think your point on domain name abuse vs. DNS abuse makes sense. DNS abuse is often used as a short had - Though by DNS hijacking do you mean cache poisoning? On your second point, i'm not sure DNS operators have the technically ability to act solely at the sub-domain level.
Swapneel Patnekar	A suggestion - We also need to add the word "sub-domain" abuse as well in addition to domain names whereever in the document. For example - a domain shadowing attack will result in the attacker adding a sub-domain under a legitimate domain name which points to the attacker's infrastructure which hosts malicious content etc.	
2640 479 1155	Implementing AI to stop registration of trade mark domain names will cause a lot of false positives. As, some names are trademarks in different verticals.	

Ajith Francis	@swapnil: are these the sub-domains of the legit user's domain or cyber-squatted typo that it's pointing to?	from Swapneel Patnekar to everyone: 6:34 PM @Ajith - The sub-domains added by the attacker which have shown in the presentation, they were all legitimate domain names.
Ajith Francis	@swapnil: Wow, okay, next question because i'm quite intrigued. Was the main domain ever compromised? How else is the sub-domain being registered	from Swapneel Patnekar to everyone: 6:37 PM @Ajith - The compromise is via a brute force attack on the domain name control panel. Once attacker gains access to the control panel, they add a DNS record (sub-domain) which is pointing to an IP address controlled by the attacker.
Deepak Singhal	@ajith and @swapneel - correct me if i am wrong. Isn't sub-domain a merely a web-page hosted on the registered domain name? Can't the very URL be taken down without actually taking down the actual domain name	from Swapneel Patnekar to everyone: 6:39 PMIn the cases of domain shadowing attacks we haven seen so far, the main domain is unaffected. The reason - the attacker is using a stealth method to remain under the radar. from Ajith Francis to everyone: 6:42 PM@Deepank: DNS Operators i.e. Registrys and in most cases Registrars can only take a whole domain out of circulation from the root server and not specific urls. So probably it needs to happen either at the ISP level (need to check technically if they have targetted interventions) or through the Registrant itselffrom Vinay Murarka to everyone: 6:44 PMThe subdomain hack in general happen on dns level, so need to check with isp / dns provider for the same