

Mike's Pretty-Good Project Next-Step Questionnaire

		Option A		Option B	
Demographics					
Your name		---			
Constituency		---			
Problem Statement					
What problem should the next group look at?	Focus on Fast Flux, a rapidly-emerging technique that hardens malicious networks, or focus on the broader issues of fraud and abuse, and explore ways that ICANN stakeholders can address these issues?	---	FF? 6 FA? 2	---	FF? 1 FA? 2
Scope					
What is the scope of the next project? Indicate what you think should be included (if anything)	Phase I -- Assess need				
	A definition of fast flux which: -- provides a precise definition for subsequent data and policy analysis?	---	Yes? 8 No? 0	---	Yes? 1 No? 1
Note - this section really only applies if you chose to look at Fast Flux, rather than the broader "fraud and abuse" problem. I couldn't figure out how to manage around that.	-- avoids the need to determine legality and intent?	---	Yes? 4 No? 3	---	Yes? 1 No? 0
	Algorithms that: -- detect fast flux based on the definition above?	---	Yes? 7 No? 1	---	Yes? 1 No? 1
	-- have safeguards to minimize false-positives?	---	Yes? 8 No? 0	---	Yes? 1 No? 1
	Partners who can provide: -- data for analysis?	---	Yes? 6 No? 2	---	Yes? 1 No? 1
	-- tools to analyze data?	---	Yes? 6 No? 2	---	Yes? 1 No? 1
	Data that quantifies: -- the quantity & trend of fast flux hosts and DNS servers?	---	Yes? 6 No? 2	---	Yes? 0 No? 1
	-- the proportion of fraud/abuse attacks that utilize fast flux networks?	---	Yes? 7 No? 1	---	Yes? 0 No? 1
	-- the difference fast flux makes in the length of time it takes to disrupt the attack?	---	Yes? 5 No? 2	---	Yes? 1 No? 0
	-- the financial impacts of fast flux, extrapolated from the proportions above?	---	Yes? 6 No? 2	---	Yes? 0 No? 1
	-- the quantifiable non-financial impacts of fast flux, extrapolated from the proportions above?	---	Yes? 6 No? 2	---	Yes? 0 No? 1
	Analyses that describe how reductions in fast flux would help stakeholders: -- increase revenue -- become more nimble -- improve quality -- reduce costs	---	Yes? 3 No? 3	---	Yes? 1 No? 1
	Analysis to determine the "cost of delay" associated with inaction?	---	Yes? 3 No? 3	---	Yes? 1 No? 1
	Should the project pause and take a check-point here, or continue on to subsequent phases?	---	Stop? 5 More? 3	---	Stop? 6 More? 3
	If the project should continue on to more phases, indicate which ones should be included;				
Note: "solutions" in this context could range from policy changes to software tools. They could be mandatory or optional. They would most likely be ratified by PDP processes along the way.	Phase II - Define solutions and requirements	---	Yes? 5 No? 0	---	Yes? 0 No? 1
	Phase III - Design, build and test solutions	---	Yes? 3 No? 2	---	Yes? 0 No? 1
	Phase IV - Deploy solutions	---	Yes? 3 No? 2	---	Yes? 0 No? 1
Stakeholders					
Which supporting organizations should participate in the project?	GNSO?	---	Yes? 8 No? 0	---	Yes? 1 No? 1
	CCNSO?	---	Yes? 7 No? 1	---	Yes? 1 No? 1
	ALAC?	---	Yes? 7 No? 1	---	Yes? 1 No? 1

	ASO?	---	Yes? 4	No? 3	---	Yes? 2	No? 0
	IETF?	---	Yes? 3	No? 4	---	Yes? 2	No? 0
	Should organizations outside ICANN participate? If so, list some examples		Law enforcement, APWG, MAAWG Governments (GAC), CCERT, FIRST, Artists Against 419.org StopBadware.org, Regulatory enforcement (eg FTC)				
Which organization should "champion" this project?	GNSO?	---	FF	FF	---		
			Yes? 3	No? 4			
			F&A	F&A			
			Yes? 0	No? 3			
			FF	FF			
			Yes? 4	No? 1	---		
			F&A	F&A			
Approach			Yes? 2	No? 1			
What approach should we take to planning the work?	Continue to use the GNSO PDP process?	---	Yes? 2	No? 6	---		
	Use a "project" approach that is less focused on pure policy-making?	---	Yes? 5	No? 3	---		
	If you favor the "project" approach, should we include a "ratify the results" PDP at the end of each phase to provide a connection back to the policy-making process?	---	Yes? 3	No? 1	---		
Readiness			Yes? 4	No? 3	---		
	Does this project need to happen?	---	Yes? 4	No? 3	---		
Should ICANN (primarily a policy-making body) be doing this project at all, or is there some other organization that is better-positioned to do this kind of work?	Should ICANN take the lead?	---	Yes? 4	No? 3	---		
	If your answer was "no", list some better-suited organizations that we could approach to develop this information for us.		Law enforcement, Gov't (GAC), SSAC, APWG, security vendors				
Resources							
What kind of resources and timing do you think this project would require?	Provide a list of the types of people who would need to be involved if the project is to succeed;		Law enforcement, Gov't (GAC), See existing WG roster. Need data from researchers & anti-crime organizations + analysis by same AND industry operators before any further policy work. Researchers Technical Implementers Policy developers Project management Dave Piscitello, APWG, MAAWG People in the anti-fraud community Consumer stakeholders Statisticians, data-management, data- analysis, risk-analysis, Internet protocol experts, project management, rights-protection				
	What's your best guess as to the elapsed time this project would take (in weeks)?		104, 16, 16-20, 52, 20, 12, 26				
	Do you think there are people available to undertake this project right now?	---	Yes? 3	No? 3	---		
	Has ICANN been successful in doing this kind of project before?	---	Yes? 2	No? 3	---		
	If your answer was "yes", please list some examples of such projects that the team can use as a model		UDRP policy development SSAC studies re WHOIS and spam. GNSO Domain Tasting 'ad hoc' group				