Public Interest Registry (PIR) appreciates this opportunity to provide comments on the Continuing Operations Instrument (COI) requirements. We also commend ICANN staff for soliciting the community's feedback on the issue, both at the panel debate in Dakar and through this public comment period.

We still believe that the Registries Stakeholder Group (RySG) alternative proposal – the Continuing Operations Fund (COF) – is a better approach to achieving ICANN's presumed goals of (a) guaranteeing the continuity of the five "critical registry functions" in the event of a new TLD business failure and (b) avoiding unnecessary barriers of entry in the new TLD application process:

- By escrowing a $50,000 fee per new gTLD upon execution of each Registry Agreement, ICANN will have available substantial resources to ensure continuity of the key registry functions. Should ICANN and the RySG determine that the existing COF balance is insufficient to meet actual demands, a special fee per domain year on each new TLD registration would be levied to raise additional resources. This approach is more reasonable than requiring significant resources upfront, i.e. at the time application under the existing COI, when it could be many months before any new gTLD is delegated and/or years before the potential need for the contingency arises.

- As was made clear in Dakar, applicants from many jurisdictions will face significant challenges finding a financial institution that meets ICANN's stringent requirements to be an acceptable issuer of a Letter of Credit. Likewise, many if not most applicants will be severely burdened if they need to set aside significant resources, i.e. a substantial percentage of back-end registry costs, because few service providers break down their costs along these lines and are counseling applicants to "estimate conservatively." Again, the COF proposal is more reasonable. Since the COF wouldn't take effect until the new gTLD contract is awarded, successful applicants would only have to secure such necessities as the need actually arises. This approach also should better position applicants to secure the required support on more favorable terms since they will be in late stages of securing a new TLD contract.

The COF approach also offers a more predictable way forward in the face of ongoing uncertainties. Nobody knows how many applications there will be, when the first new gTLDs will enter the root, or how long it may be before any of these ventures begin to show strains of business failure. Likewise, the community still doesn't have sufficient information to accurately estimate contingency costs. This lack of clarity means that many applicants could miscalculate cost estimates, perhaps to the detriment of their application's scoring. This level of uncertainty might even dissuade some from applying. Such disincentives are at cross-purposes with one of the key rationales of the new TLD program, i.e. fostering competition through new and innovative uses of the DNS.

Of course, the lack of information is understandable to a degree. Few back-end registry operators break down their costs to identify the five critical registry functions. Divorcing those line items from the broader costs of securely and stably operating a registry seems rather artificial. It's also questionable to expect those providers to publicly share such confidential information in a competitive marketplace. Even when pressed for "guesstimates," the range is so wide and full of caveats that a simple solution becomes even more desirable. We believe that the COF approach best meets this need.

PIR recognizes that other alternatives have been suggested. For example, a private insurance model is one possibility. Such an approach, however, will need to be carefully studied. Immediate questions that spring to mind are: What firm will do the actuarial work? What are their bona fides and credit rating? How well do they understand the peculiarities of the registration services market? Perhaps most importantly, would the coverage really extend to the specific services that ICANN expects to see covered? Insurance policies for cyber incidents such as a data breach are currently available, but too often do not adequately anticipate, and therefore cover, all of the true costs. Given these concerns, we come back to the RySG alternative proposal as the most satisfactory way forward.

Ultimately, ICANN and the community have precious little time to analyze and debate COI alternatives. While it's usually good to have options, further delay should not be one of those options. Adding any more uncertainty to the application process is definitely not in the public interest. We believe the COF approach offers ICANN a credible and easy to understand alternative to the existing COI model. We strongly encourage staff to revise the Guidebook's implementation procedures in line with the RySG alternative proposal.

Sincerely,

Paul Diaz
Director of Policy
Public Interest Registry