ICANN SSR-TY 2016
Letter of Motivation – Alexa Raad

This letter is to express my interest in becoming a member of the second Security Stability and Resilience Review Team (SSR2). I am submitting on behalf of the ccNSO and as their sponsored candidate.

The issue of security and stability has been a great passion of mine and evident in my track record within the DNS and ICANN community in the past 16 years. Below are highlights of relevant experience that I hope will help distinguish my candidacy:

- As CEO of PIR (2007 to 2010) I spearheaded the adoption of DNSSEC in .org. Although PIR was not strictly the first to implement (the industry owes a debt of gratitude to others such as .se) as a legacy gTLD of reasonable size, its adoption of DNSSEC helped pave the way for mandating DNSSEC as a requirement for all new gTLDs. I also led the adoption of an anti-abuse policy at PIR in 2008. Anti-abuse policies and procedures are now a regulatory requirement for new gTLDs.
- I also founded and set up an inter and intra industry collaborative group, called RISG (Registry Infrastructure Security Group) which was comprised of registries, registrars, and other players in the cyber security space such as Symantec and McAfee to help identify best practices and find ways to share critical data to minimize security threats such as phishing and malware.
- I am also the sole author of a patent in Internet security called "System and method for predictive modeling in a network security service".
- Most recently, as CEO of Architelos, I helped define a methodology for assessing the level of abuse in various TLDs, and shared the data and analysis as part of a free online report called the "NameSentry Report". Although some others such as McAfee had from time to time published reports on the relative safety of some TLDs, up to that time there had been no report with a published and consistent methodology that measured all TLDs (legacy gTLDs, ccTLDs as well as new gTLDs) across the internet.

A key feature in each of the above experiences has been my desire to make a positive contribution in the area of internet security, which outweighed commercial interests and or perceived risks. My motivation to volunteer for the team is very therefore still much aligned with the above experiences.

The landscape has changed much from 2010, however many of the same issues remain, this time with a starker contrast:

- increased severity and intensity of DDOS attacks while expectations of stability and resiliency are heightened;
- a sharper tug of war between voices of security and those of privacy;

- security threats which transcend not only national borders and laws, but also corporate and national security distinctions;
- bad actors and criminal elements which are increasingly more organized, well funded and nefarious;
- battle for governance of the internet pitting governments against a multi-stakeholder model.

This calls for an SSR2 team that is constituted of members with practical experience who can calibrate their recommendations and responses to be actionable and practical.
A thoughtful balance of technical, policy, analysis and business skills is key in continuing the good work of the SSR1.

I would welcome the opportunity volunteer my time and skills for something I have been and continue to be passionate about: operating a safe, secure, and resilient internet (governed by a collaborative and multi-stakeholder model) for future generations.