Before the
Department of Commerce
National Telecommunications and Information Administration
Washington, D.C. 20230

In the Matter of	)	
	)	
Assessment of the Transition of the	)	Docket No. 090420688–9689–01
Technical Coordination and	)	
Management of the Internet's Domain	)	
Name and Addressing System	)	

Notice of Inquiry

COMMENTS OF YAANA TECHNOLOGIES, LLC

Anthony M. Rutkowski
SVP, Regulatory Affairs and Standards
Yaana Technologies, LLC
44441 Blueridge Meadows Dr
Ashburn VA 20147-2895
tel: +1 703.999.8270
mailto:tony@yaanatech.com

Raj Puri
CEO
Yaana Technologies, LLC
500 Yosemite Drive, Suite 120
Milpitas, CA 95035
tel: +1 408.854.8030
mailto:raj@yaanatech.com

Filed: 8 June 2009

1. Yaana Technologies (Yaana) is a Silicon Valley based company focused globally on providing unique and high-value Managed Services to enterprises and communications service providers that include cybersecurity and forensic compliance capabilities for broadband service providers.

2. In its 24 April *Notice of Inquiry*, the Department seeks comment on a number of issues related to the Department's Memorandum of Understanding with the Internet Corporation for Assigned Names and Numbers (ICANN). In this context, Yaana in submitting these comments seeks a more diversified, open, and innovating environment in which Yaana can enter the Identity Management and cybersecurity markets presently controlled by ICANN under the MoU.

I.
The Notice does not sufficiently treat the array of critical Name and Address services and issues of which the Domain Name System is only one.

3. The recent release by the President's *Cyberspace Policy Review* was a watershed event that is a game-changer in the context of this proceeding. This significance is captured at the outset of the report:

> Cyberspace touches practically everything and everyone. It provides a platform for innovation and prosperity and the means to improve general welfare around the globe. But with the broad reach of a loose and lightly regulated digital infrastructure, great risks threaten nations, private enterprises, and individual rights. The government has a responsibility to address these strategic vulnerabilities to ensure that the United States and its citizens, together with the larger community of nations, can realize the full potential of the information technology revolution.[1]

Going forward, proceedings such as this one need to be examined in a new light that embraces cybersecurity and related identity management capabilities essential for dealing with the grave, rapidly growing vulnerabilities of and attacks on the national broadband network infrastructure. The MoU at issue here was crafted more than ten years ago in a

[1] Executive Office of the President, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, (29 May 2009) at i.

very different world where IP networks and services being treated here were not part of the nation's critical infrastructure, nor were they subject to the major vulnerabilities and attacks discovered and manifested exponentially over the past decade. As the *Cyberspace Policy Review* makes clear, we are no longer in an environment where cybersecurity and infrastructure protection can be simply left to the private sector.

4. The Dept of Commerce MoU involves at its essence a contract to provide Identity Management services specified by a set protocols developed by the U.S. government at a cost in excess of $5 billion for legacy R&D network collaboration. The awardee – which for the past ten years has been ICANN – has an exclusive right to provide these IANA services and to earn significant revenue by assessing various kinds of charges associated with their implementation and use.

5. Although DNS name resolution services tend to be the focus of the NOI, DNS services in fact are only one of scores of IANA IdM services under the MoU. Other services of significant interest include IP addresses, Enterprise Numbers, and other namespaces that have been instantiated on the DNS platform, including E.164 numbers.

II.
The four principles articulated by the White Paper (i.e., stability; competition; private, bottom–up coordination; and representation) are no longer sufficient.

6. The need for and character of these four principles has changed dramatically over the past decade. Cybersecurity trust and resilience are now far more significant than a "stability" principle – which was vaguely defined at best. The principle of competition, ironically, never applied to the awardee ICANN itself, but only to some designated dominant providers. The principle of private, bottom-up coordination patently no longer applies in the current environment focusing on these Identity Management services as essential for critical infrastructure protection, mitigating vulnerabilities, and ensuring cybersecurity. The principle of "representation" applied to a conceptualization of the MoU contract as a quasi-regulatory services rather than a secretariat services contract. The regulatory/governance conceptualization unfortunately led to significant

politicization of the contract that dramatically drove up costs in attempts to create and support a global regulatory body construct.

III.
Industry leadership and bottom–up policy making alone are no longer sufficient as the most appropriate model to increase competition and facilitate international participation in the coordination and management of the DNS

7. As noted above, the IANA Identity Management services provided under the MoU no longer fit into an "industry leadership and bottom-up policy making" model. What is being dealt with are an array of Identity Management services essential to the national infrastructure and related cybersecurity. Fundamental changes in the model, provisioning, and oversight are clearly appropriate.

IV.
A new model is necessary to provide for competition, and provide for national and global cybersecurity and resilience

8. The entire array of IANA Identity Management services and their trusted, real-time provisioning to enhance cybersecurity and resilience need to be considered. This involves a lot more than just DNS. Increasingly, all providers of broadband services and products are being identified by the DOD assigned OID numbers now being assigned worldwide by IANA at a rate of more than 200 per week. Almost of all of IANA's scores of assigned number databases still exist as flat text files as they did in the 1970s – rather than being structured to be provided by contemporary real-time query-response platforms. Little identity proofing is done for any of the identity management systems for which ICANN is responsible and trust levels are often minimal. Even the WHOIS directory system underpinning DNS still relies on an archaic 30 year old format and protocol devoid of any security.

9. The structuring of the MoU as a continuation of an exclusive government oversight of all IANA R&D network Identity Management services – including new ones continuously developed by new IETF standards - seems especially inappropriate today.

There is no reason why these services cannot be separated and provided by multiple parties such as Yaana who can be incented to innovate and provide substantially more trusted and resilient facilities to meet contemporary national and global cybersecurity needs.

V.
The current model has not, and inherently cannot, meet the needs sought in the original agreement or the ICANN asserted responsibilities. Further steps toward compliance under that model are not necessary.

10. In light of the President's *Cybersecurity Policy Review*, an interagency initiative should be undertaken to completely reexamine the premises of the original agreement and restructure it to meet contemporary cybersecurity Identity Management needs and objectives. Further steps toward compliance under the old agreement seem without purpose.

VII.
The risk to the stability and security of the IANA Identity Management Services including DNS has significantly increased. A transition of the technical coordination and management to ICANN would exacerbate that risk.

11. Given the enhanced importance of the IANA Identity Management Services, including DNS, to achieve trust and resilient infrastructure, and the ongoing implementation of the *Cybersecurity Policy Review*, any transition to ICANN seems completely inappropriate and would place the nation's cyber infrastructure at serious risk.

VIII.
Interim arrangements for continued security and stability of the IANA Identity Management Services including Internet DNS should be established during the Cybersecurity Policy Review followup

12. The only essential component of the existing MoU from the standpoint of security and stability are the continued provisioning of the Identity Management services including DNS. This can be effected through existing contractual relationships pending a new construct flowing from the Cybersecurity Policy Review.

XI.
A DNS Project Report relating to ICANN's policies and procedures is unnecessary

13. It is not apparent that any project report would be useful or appropriate.