To: DNSSEC@ntia.doc.gov
From: rmohan@afilias.info
Re: Docket Number: 0810021307–81308–01 - Deployment of Security Technology Within the Internet Domain Name System
Date: November 24, 2008

Dear Assistant Secretary Baker,

Afilias welcomes the opportunity to provide comments to the Department of Commerce (DoC) with respect to the potential deployment of DNSSEC at the Internet root zone level. Afilias has been an active participant in the DNS and Internet security arena since its inception and has addressed DNS and Internet security issues both as a TLD registry operator and as an active participant in the Internet Corporation for Assigned Names and Numbers (ICANN). Afilias is the registry operator for the .info TLD under contract with ICANN and also provides “backend” registry services for numerous TLDs including, .ORG, .mobi, .asia, .aero as well as a number of country code TLDs. Afilias provides registry services to approximately 14 million domain names and is working currently on the implementation of DNSSEC in the .ORG zone which is operated by Public Interest Registry (PIR).

The DoC’s Notice of Inquiry is timely since Dan Kaminsky revealed, in mid-2008, a particular DNS cache poisoning exploit that threatens core DNS functionality. While overall DNS security has been an ongoing concern for the Internet community, the nature of the exploit identified by Kaminsky, with its attendant threats to the stability and security of the DNS, warrant immediate and thoughtful focus.

Afilias supports the implementation of DNSSEC at the Internet root zone level. Establishing an anchor of trust at the root is a logical first step toward full, end-to-end DNSSEC implementation and would itself be a signal to the community that DNSSEC can provide valuable security for DNS operators and Internet users alike. However, DNSSEC should not be viewed as a panacea and the Internet community should engage in a dialogue to ensure that operators and users alike understand the limits of security provided by DNSSEC.

Education concerning security best practices at the network, business applications and end user level is paramount. In fact, broader collaboration among all players may be the most valuable result of DNSSEC implementation. Indeed, the response of DNS operators, after Kiminsky publicized the cache poisoning exploit, demonstrated the fact that there is broad coordination and collaboration among DNS and Internet operators to address security threats as they arise. Even recognizing that the “fix” itself was not full proof, end-to-end DNSSEC implementation – anchored by DNSSEC at the root zone -- can strengthen this coordination and potentially extend it to include Internet end users.

DNSSEC implementation at the root zone level and beyond should be undertaken recognizing that the nature and sophistication of security threats continuously evolve. Even if DNSSEC were implemented end-to-end today, undoubtedly bad actors would attempt to exploit the system and bad actors who have access to significant computing resources would continue to pose a threat to even the most sophisticated security measures. To address the concerns raised by cache poisoning and related exploits it is important to note that cryptography is a deterrent not a silver bullet solution. This fact, however, should not inhibit the community from implementing DNSSEC nor should the search for perfect security be the enemy of the good.

The implementation of DNSSEC should be analyzed through a cost/benefit lens. At present, there are no security tools that are more effective than DNSSEC to defeat the specific exploit in question. However, complete end-to-end implementation of DNSSEC – which is required to derive the maximum benefit of the protocol – is by no means a certainty and will require a significant level of coordination between and among registries, registrars, ISPs, operators of subdomains or enterprise networks and governments. While the opt-in nature of DNSSEC can be viewed as a virtue, one of the factors inhibiting the deployment of DNSSEC to date has been the lack of an incentive or the absence of a business model to motivate operators to take on the cost of DNSSEC implementation and operational maintenance. In the absence of such incentives or forcing functions, end-to-end DNSSEC implementation may remain out of reach. If that is the end state, then the DoC and the Internet community should evaluate the prospect of security in the context of partial DNSSEC deployment.

DoC should consider that the effectiveness of full DNSSEC deployment will be impacted by the existing operational, technical and process approaches in place today across the spectrum of operators on the Internet. Specific factors that will impact the potential efficacy of DNSSEC include, but are not limited to, the relative strength of deployed encryption, key rollover policies and practices and the use of algorithms. One cannot assume uniform approaches to these critical elements of DNSSEC implementation and, as in any system, the chain will only be as strong as its weakest link.

Afilias notes the various “DNSSEC proposed process flow” models put forward for consideration but comments here on selected aspects of certain models rather than recommending one model over another. Clearly, certain proposals implicate both policy and procedural issues concerning management of the root zone that fall within the purview of the DoC’s IANA contract and may lie beyond the scope of this inquiry.

Consolidation of the root zone signing and editing functions is recommended due to security concerns about transfer of the zone file from one entity to another prior to signing.   While this recommendation may be sound from a security standpoint, it nevertheless reflects a fundamental process shift from the existing root zone change model which raises operational concerns that need to be addressed. The current split between the IANA function and root operation requires not only a collaborative exercise in managing changes to the root but also provides a form a checks and balances in the sense that more than one entity – each having shared but also unique responsibilities – participates in the process. DoC should carefully consider the implications of a model that consolidates all aspects of the process in one entity, regardless of who that entity might be.[1]

Afilias concurs with the proposal of separating the Zone Signing Key and Key Signing Key functions and with the "M of N" concept in general. The M of N concept is sensible to the extent that it entrusts a number of operators to share the Key Signing Key responsibility. While VeriSign's proposal that existing root server operators constitute the trusted group is logically sound, this trusted group need not be limited to the existing root server operators. Other trusted operators should be considered as participants in this model should DoC and the community recommend the M of N approach. While the attempt to identify a group that has no "political interests" has inherent appeal, the reality of such an approach may be difficult in practice. However, selection of operators to participate in that group should focus on a "trusted operator" model to be judged, in large degree, by the operator's track record.

Afilias believes that testing of DNSSEC at the root zone level prior to live implementation is appropriate and notes that both ICANN and VeriSign highlight the benefits of testing in their respective proposals. Testing that includes as broad a community of participants as possible in an end-to-end environment is desirable. End-to-end testing will require numerous participants and, assuming that players from all levels are prepared to participate, a minimum time fame in the range of 12 to 18 months.

With regard to estimated costs, DoC should consider that full adoption of DNSSEC could increase the overhead of existing DNS services through the resulting increase in packet size after deployment. The increase in packet size may vary depending on the type of signatures deployed but would, in any event, result in increased network traffic/bandwidth overhead for the management of both "normal" traffic and "attack" traffic. Other costs include CPU overhead on both caching and authoritative nameservers as well as substantial costs associated with the administration of key management zone signing activities. These and other additional costs could be examined as part of an end-to-end test bed implementation since they will impact the ultimate adoption of DNSSEC by all players.

Afilias looks forward to working with the DoC, root server operators, ICANN and the Internet community to enhance the security of the DNS and to improve collaboration among all stakeholders to ensure that the Internet continues to provide a secure, global platform for communication, information sharing and innovation.

[1] In their "Root Server Management Transition Completion Agreement," ICANN and VeriSign agreed to present a "joint approach" to the DoC concerning, *inter alia*, the transition of root editing, signing and publication functions. The process flow proposals do not reflect a joint approach -- the absence of which warrants consideration by the DoC.