To: Senate Judiciary Committee
From: Kathryn Kleiman, Esq., Director of Policy for the Public Interest Registry
Date: November 15, 2010
Re: How S.3804 Breaks the Internet: Unintended Consequences for Domain Name Security and the Newly-Implemented Security Standard of DNSSEC.

History: The Internet has a history of openness, and a long commitment to addressing security concerns and challenges. Over the years, we have seen *spoofing attacks*, in which an attacker can fool the DNS system into routing to the wrong website, and "man in the middle attacks" with similar results: sending an Internet user to a website that looks like the bank, e-commerce site, or organization he/she seeks -- but is not. The result is loss of personal data, financial data, money, time, and ultimately, confidence in the Internet.

So the Technical Community, together with Registries and Registrars, responded. At considerable cost of time and resources, we developed a new level of security: Domain Name System Security Extensions (DNSSEC). DNSSEC is a set of DNS extensions which provide 3 basic functions: Data Origin Authentication, Data Integrity, and Authenticated Denial of Existence. DNSSEC works on a chain of trust: passing an "electronic key" to Internet users to verify the address of the website they seek. It allows Internet users to reach the Internet sites they intend; it strengthens confidence in the Internet.

But Senate Bill 3804 breaks DNSSEC at this early pivotal time in its roll-out. It requires a blocking that damages and degrades DNSSEC security efforts.
In brief, S.3804:

- **Interrupts the DNSSEC "chain of trust"**
- **Requires domain name servers to prevent resolution of domain names**
- **Returns data that the Internet browser cannot decipher (browser technology) and that the Internet user (person) will not understand.**
- **Confounds the very security and trust systems that are being installed to build confidence and clarity into the Internet system.**

The negative long-term effects of this bill are clear to the leaders of the Internet technical and security community. The Bill will:

- Completely undermine efforts to ensure that people trust their local name servers when looking up their banks, e-commerce sites and search engines – and instead create greater security and stability risks for Internet users and the DNS (Dan Kaminsky, Computer Security Guru, and Finder of the Kaminsky Bug).

- Encourage people to "opt out" of the local domain name system: specifically, to change their resolving name servers to ones located outside their ISP and outside the US – which is easy and fast to accomplish (Dan Kaminsky).
- Undermine the strong cooperative arrangements with law enforcement, legislative and judicial authorities around the globe that we are working to build (Steve Crocker, Chairman of ICANN's Security and Stability Advisory Group).
- Undermine the stability and integrity of the network by creating confusion for the Internet user. If a website is not accessible due to blocking or filtering by an ISP at a court order, is it because the network is broken, someone typed in the wrong name, or something else? There's no easy way to tell, and the result is uncertainty and loss of confidence in the overall system. (Steve Crocker).
- Create a situation which it is difficult or impossible to correct. Even if a site cures itself or is subsequently determined not to be or have been a rogue site, it will be impossibly hard to remove the blockage from all of the ISPs. As Ray Donovan, former Secretary of Labor, said after being acquitted of larceny and fraud charges, "Which office do I go to get my reputation back?" (Steve Crocker)

Overall, S.3804 will encourage Internet users to opt-out of their DNS filters and shared DNS servers. This, in turn, will disrupt the dynamic balancing and load distribution of the Internet, and bypass the security systems we have installed. Thus, Internet systems will not work as efficiently or robustly today – or tomorrow, where there will be far more content to distribute.

PIR's Policy Staff together with international Internet technical experts are available to discuss the deep security and stability concerns voiced in this memo. ***We urge you to strongly reconsider passage of this bill by the Senate Judiciary Committee this week, and offer our support to draft a bill without the technical and security problems of S.3804.***