

September 28, 2006

**Network  
Solutions**

Chairman F. Duane Ackerman  
National Security Telecommunications Advisory Committee  
245 Murray Lane, S.W.  
Mailstop 8510  
Washington, D.C. 20528

W.G. Champion Mitchell  
Chairman & CEO  
13861 Sunrise Valley Dr.  
Herndon, Virginia 20171  
Phone: 703.668.5200  
Fax: 703.668.5888  
cmitchell@networksolutions.com

Dear Chairman Ackerman:

I am writing to request that the National Security Telecommunications Advisory Committee review the proposed .com registry renewal agreement between the Internet Corporation for Assigned Names and Numbers (ICANN) and VeriSign, Inc., now pending before the U.S. Department of Commerce for review and approval or disapproval. NSTAC provides expert advice to the President on issues related to national security and emergency preparedness communications policy. NSTAC should examine the profound security and stability concerns that the proposed .com registry renewal agreement poses for the Internet.

As a pioneer of domain name registration services, Network Solutions takes the security of the Internet very seriously. Indeed, it is beyond dispute that the security and stability of the Domain Name System (DNS), which forms the backbone of the Internet, is critically important to both the national security and economy of the United States. In the United States, .com accounts for more than 75% of registered domain names, and the economic consequences of any disruption in the security of this registry is underscored by the more than \$650 billion—5% of U.S. GDP—attributable to the Internet.

Unfortunately, the proposed .com agreement with VeriSign will undermine critical security goals. The proposed agreement awards VeriSign a virtually unregulated and perpetual monopoly over the operation of the .com Top Level Domain (TLD) registry, but is virtually silent on the issue of Internet security. It does not include sufficient contractual requirements for addressing fundamental security requirements, provide for ICANN oversight of VeriSign's security policies, or promote competition as a means of enhancing security. While the absence of each of these mechanisms is independently problematic, the total absence of any meaningful security measures will make it impossible to ensure the significant investment of resources and robust security reporting, management, and planning necessary to maintain successful defenses of the DNS.

*First*, the proposed .com agreement includes only minimal contractual requirements designed to mitigate security risk. At a minimum, the proposed agreement should include: (1) requirements for specific security reporting from VeriSign; (2) provisions requiring VeriSign to provide detailed security plans and regular testing of DNS defenses; (3) auditing provisions permitting ICANN to independently assess VeriSign's capabilities regarding potential and ongoing DNS security breaches; (4) oversight of VeriSign's DNS operations that permits ICANN to conduct risk analysis of the operations; and (5) provisions permitting ICANN to conduct regular security reviews.

Instead, the proposed agreement includes only one provision related to security, requiring VeriSign to “engage in discussion” with ICANN twice annually “on trends impacting the Security and/or Stability of the Registry, the DNS, or the Internet.” The proposed agreement contains no provisions for translating such “discussions” into meaningful security requirements. Without specific enforceable security requirements, including mandatory auditing and reporting requirements, VeriSign will be free to implement security measures as it sees fit and as its bottom line permits. By relying on nothing more than VeriSign’s goodwill to deploy and maintain adequate security of the DNS, ICANN and its stakeholders are left with a DNS security model accountable only to VeriSign’s shareholders. In other words, not only will this agreement not improve .com security, it does not even require VeriSign to maintain the status quo.

*Second*, the proposed agreement permits VeriSign to increase fees without justification up to 7% in four of the six years of the contract. (In the other two years, VeriSign would be required to justify any increase based on costs incurred in addressing security issues.) While VeriSign has attempted to justify the price increases authorized by the proposed .com registry renewal agreement on the ground that they are necessary to promote security and stability, the agreement *does not require* VeriSign to provide a justification for these price increases. In other words, VeriSign would have no requirement of investing the increased funds—estimated at \$1.3 billion—on the security and stability of the DNS. Indeed, recent securities analyst reports have noted that almost all of the additional cumulative revenue that VeriSign would gain over six years under the proposed .com agreement would go directly to its bottom line, not to security. Requiring justification for a price increase in all years of the contract would ensure that the additional revenue is actually used to develop a more secure DNS, as opposed to padding VeriSign’s profit margin.

*Third*, even in the absence of explicit contractual requirements regarding security, effective ICANN oversight could go some distance toward protecting the security and stability of the DNS. By providing for presumptive perpetual renewal, however, the proposed .com agreement effectively eliminates ICANN oversight of VeriSign’s performance in the areas of security and stability. Under the proposed agreement, ICANN has virtually no discretion to deny renewal even if VeriSign fails to implement the most basic and essential security and stability measures.

The proposed .com registry agreement eliminates competition by creating a virtual perpetual monopoly over the control of the .com TLD. The elimination of competition runs counter to the domestic and worldwide regulatory trend over the last several decades, which recognizes that competition in the private sector bolsters investments in new technology and infrastructure. To this end, government agencies that rely on secure networks routinely award competitively bid contracts, with limited terms, for the operation of core components of data and communications systems. Similar competitive measures are critical to preserving the current level of security and stability in the DNS and encouraging continued innovation.

Without any of these checks in place to ensure continued investment and innovation in DNS security, the U.S. government will soon be faced with a highly vulnerable system in which security upgrades may be disregarded, without consequence, in favor of the bottom line. Moreover, because the proposed .com agreement will likely be used as a model for the renewals of other TLDs, including .biz, .info, and .org, these security concerns will likely multiply.

Tellingly, industries in which there is much less potential impact from a single point failure, such as banking and brokerage, are much more closely regulated, even with regard to cyber-security, than VeriSign would be under the proposed agreement. The failure of any single registry operator, particularly the operator responsible for .com, could cause catastrophic results.

The significant security shortcomings of the proposed .com registry agreement are evident when the agreement is contrasted with the contract governing the operation of the .us country code TLD. The United States has avoided monopoly terms, granting NeuStar, Inc., administration of the .us TLD under an agreement that provides for a fixed term of four years with two optional one-year extensions, "termination for the government's convenience," and a requirement that any fee increases be cost-justified. Moreover, the .us agreement specifically requires NeuStar to meet security and stability objectives and includes broad review and audit provisions and significant disclosure requirements, which increase transparency and accountability for security measures. The Department of Commerce has also designated an entity to continuously monitor and oversee NeuStar's performance and adherence to these contract terms. In its proposal to the Department of Commerce, NeuStar provided a complete security plan and technical specifications describing in significant detail how NeuStar's security and defenses are designed, provisioned, updated, and operated. The NeuStar agreement is thus demonstrably preferable to the proposed .com renewal agreement, in the very areas of most concern to you and NSTAC.

Network Solutions does not question VeriSign's ability to manage the .com registry. But the absence of express security requirements or even a requirement to justify price increases, the lack of adequate oversight, and the lack of competition places the continued security of these operations exclusively in the hands of VeriSign, rather than those designated to perform the oversight function. There is no guarantee that VeriSign will continue to provide a secure registry by its own goodwill, particularly because any change of control of VeriSign will have no effect on the virtually perpetual monopoly this proposed agreement awards.

Review of the national security implications raised by this proposed agreement is fully consistent with the functions laid out in the Executive Order that authorized the creation of NSTAC, including that it "provide technical information and advice in the identification and solution of problems which the Committee considers will affect national security telecommunications capability." President's National Security Telecommunications Advisory Committee, Exec. Order No. 12382 (1982), *as amended by* Exec. Order No. 13286 (2003). Evolving network security concerns have been a priority of the industry and the government expertise that NSTAC has brought to bear in areas such as Next Generation Networks. The security issues raised by this proposed agreement are so critical to these domestic policy and national security objectives as to compel further and immediate review by NSTAC.

In light of the above, Network Solutions requests that NSTAC formally consider the security concerns raised by the proposed .com registry renewal agreement. Network Solutions also asks that NSTAC alert the Department of Commerce and interested Members of Congress of its intent (a number of members of Congress have expressed similar concerns with the proposed .com renewal agreement; a few of their letters are attached for your review), in order to ensure that the Committee may review the proposed agreement and provide its own views before the Department issues any final decision. In addition, because of the nature of NSTAC's public-private partnership, Network Solutions requests that individuals associated with VeriSign, including Stratton Sclavos and Michael Aisenberg, be recused from consideration of these issues as they are interested parties.

I welcome the opportunity to discuss the security implications of the proposed .com registry agreement with the Committee.

Sincerely,



W. G. Champion Mitchell  
Chairman & CEO

Enclosures

cc: James F. Albaugh  
Lawrence T. Babbio, Jr.  
Gregory Q. Brown  
Ken Dahlberg  
Gary D. Forsee  
Van B. Honeycutt  
Arthur E. Johnson  
Clayton M. Jones  
Scott G. Kriens  
Craig O. McCaw  
Walter B. McCormick, Jr.  
Craig T. Mundie  
Richard C. Notebaert  
Donald J. Obert  
Stratton Sclavos  
Stanley Sigman  
Randall Stephenson  
William H. Swanson  
Lawrence Weinbach