

VERISIGN, INC.'S RESPONSE TO REPORT FROM THE ICANN  
SECURITY AND STABILITY COMMITTEE RE "*REDIRECTION IN  
THE COM AND NET DOMAINS*"

August 5, 2004

The following is the response of VeriSign, Inc. (“VeriSign”) to the report submitted to the ICANN Board of Directors by ICANN’s Security and Stability Advisory Committee (“SSAC”) entitled “*Redirection in the COM and NET Domains*” (the “Report”), dated July 9, 2004. The Report sets forth SSAC’s findings and recommendations regarding VeriSign’s implementation, between September 15, 2003 and October 3, 2003, of “Site Finder,” a wildcard response to user queries that included mistyped domain names or domain names that, for technical purposes, were not present in the .com or .net zones.

## **I. EXECUTIVE SUMMARY**

SSAC is an advisory committee to ICANN whose only chartered purpose is to advise “the ICANN community and Board on matters relating to the security and integrity of the Internet’s *naming and address allocation systems*.”<sup>1</sup> With respect to Site Finder specifically, SSAC was instructed by ICANN to gather and assess quantitative evidence to support the conclusion in SSAC’s preliminary report,<sup>2</sup> issued on September 22, 2003, that Site Finder weakened the stability of the Internet.<sup>3</sup>

The Report contains *no evidence* that the introduction of Site Finder destabilized the naming (“Domain Name System” or “DNS”) and address allocation system or the Internet. Rather, the Report acknowledges that Site Finder “did not have network-shattering effects”<sup>4</sup> and that “RFC 1034 allows for flexibility in the way that DNS can respond to queries for uninstantiated names,”<sup>5</sup> including through use of a wildcard that synthesizes a response to user queries for non-existent domain names. The report further notes that “the wildcard mechanism had been a part of the DNS protocol since the specifications were originally written.”<sup>6</sup> These findings echo those reached by the Internet Architecture Board (“IAB”), which concluded that Site Finder is “a legitimate

---

<sup>1</sup> Report at p. ii (citing Security Committee Charter at 1) (emphasis added).

<sup>2</sup> ICANN Advisory Concerning VeriSign’s Deployment of DNS Wildcard Service, 19 Sept. 2003 (<http://www.icann.org/announcements/advisory-19sep03.htm>); Final Resolution regarding VeriSign Registry Site Finder Service from GNSO Secretariat, 25 Sept. 2003 (<http://gnso.icann.org/mailling-lists/archives/council/msg00136.html>).

<sup>3</sup> Message from Security and Stability Advisory Committee to ICANN Board 22 Sept. 2003 (<http://www.icann.org/correspondence/secsac-to-board-22sep03.htm>).

<sup>4</sup> Report at p. iv.

<sup>5</sup> *Id.* at p. 11.

<sup>6</sup> *Id.* at p. 12.

use of wildcard records that did not in any way violate the DNS specifications.”<sup>7</sup> These findings also are consistent with the findings of the Technical Review Panel (“TRP”) formed by VeriSign to assess Site Finder.<sup>8</sup>

Based not on evidence but on purported universally accepted technical principles, the Report recommends that wildcards should not be introduced by so-called “public” zones “whose contents are primarily delegations,” that existing RFCs be modified to “clarify” the proper use of wildcards, and that all changes in services offered by a registry should take place only after “a substantial period of notice, comment and consensus involving both the technical community and the larger user community.”<sup>9</sup>

SSAC’s purported “findings” and “recommendations” are inappropriate, unsubstantiated, and themselves contrary to longstanding written standards and specifications for the operation of the DNS and the Internet. None of SSAC’s findings conclude that Site Finder, or wildcards generally, pose a threat to the security and stability of the Internet’s naming and address allocation system. That is the limit of SSAC’s mandate. Accordingly, those “findings” and “recommendations” it does make exceed the scope of SSAC’s charter as a limited technical advisory committee – to evaluate security and stability threats to the Internet’s naming and address allocation systems – and are not derived from the supposed principles espoused by SSAC.

Such overreaching is an understandable by-product of the context in which the Report was created. SSAC began its analysis with the predetermined conclusion that Site Finder, and all other wildcards, should be prohibited. Indeed, a draft of SSAC’s September 22, 2003 report reveals that the “Opinions” and “Recommendations” were drafted before the committee had undertaken any reasoned evaluation of Site Finder. The September 19, 2003 draft of the report entitled *Recommendations Regarding Veri[S]ign’s Introduction of Wild Card Response to Unregistered Domains within .com and .net.*, circulated by Steven Crocker, contained fully formed conclusions and recommendations, yet nothing under the “Analysis” heading except a plea for Paul Vixie, among others, to

---

<sup>7</sup> IAB Commentary: Architectural Concerns on the Use of DNS Wildcards at p. 4 (<http://www.iab.org/documents/docs/2003-09-20-dns-wildcards.html>).

<sup>8</sup> See VeriSign Site Finder Technical Review Panel Summary, slide 8, presented by Scott Hollenbeck, VeriSign Director of Technology, at 15 Oct. 2003 SSAC meeting. One of SSAC’s third party committee members, Bruce Tonkin of Melbourne IT, also was a member of the TRP.

<sup>9</sup> Report at pp. vi, 25.

“*please dump stuff* into this section.”<sup>10</sup> Under these circumstances, SSAC’s adherence to its preliminary conclusion, notwithstanding the absence of any evidence of a security or stability threat to the DNS or the Internet, should come as no surprise.

Moreover, the Report appears primarily to have been composed and/or contributed to by persons who are opponents of Site Finder and/or competitors of VeriSign, a fact the Report fails to acknowledge. For example, Paul Vixie, a member of the committee who is cited three times as evidentiary support for the Committee’s conclusions, fails to disclose that he is the president of Internet Systems Corporation (“ISC”), which released the BIND software patch discussed in the Report as one of the technical responses to VeriSign’s wildcard implementation, and competes with VeriSign in other relevant respects, including the provision of DNS services and as a potential TLD registry operator. The Report also fails to identify that Suzanne Woolf, an employee of ISC, K.C. Claffy, an associate of Paul Vixie, and Mike StJohns as members of the committee who were added to the committee by SSAC’s committee chair, specifically for the purpose of rendering conclusions about Site Finder. Ms. Woolf and Ms. Claffy’s association with Mr. Vixie suggests they were added for the purpose of packing the committee with Site Finder opponents. Indeed, the unilateral addition of these new members by the committee chairman was a direct violation of ICANN’s Bylaws.<sup>11</sup> By contrast, both VeriSign members of the committee recused themselves from the Site Finder assessment due to their obvious conflict.<sup>12</sup> Other members of the committee with clear conflicts of interest likewise should have recused themselves. They did not.

As to the Report’s findings and recommendations, they would in effect restrain technical innovation and commercial practices on the Internet on the basis of vague and unwritten “codes of conduct” and self-styled “established practices” that, contrary to the Report, do not represent consistent Internet practices or conduct. For example, the Report condemns Site Finder as violating a “well-defined boundary between architectural layers.” Yet multiple technologies widely used on the Internet, such as network address

---

<sup>10</sup> September 19, 2003 draft of report entitled *Recommendations Regarding VeriSign’s Introduction of Wild Card Response to Unregistered Domains within .com and .net.*, circulated by Dr. Crocker, at p. 2 (capitalization in original) (emphasis added). A copy of this draft is attached as Exhibit A.

<sup>11</sup> Bylaws for Internet Corporation for Assigned Names and Numbers, Art. XI §§ 2(2)(b), 5 (<http://www.icann.org/general/bylaws.htm#XI>).

<sup>12</sup> The body of the Report fails to note that Mark Kosters and Ken Silva, VeriSign’s employees on the SSAC Committee, recused themselves from the drafting of the Report and the adoption of the findings and recommendations of the Committee in the Report.

translators and firewalls, to name but two examples, “violate” this purportedly immutable principle. Furthermore, Site Finder did not change the positioning of the DNS in the layering of network services. Indeed, SSAC itself recently *endorsed* the processing of internationalized domain names (“IDNs”) at the DNS level, a technical innovation that, based on the analysis in the Report, would “blur” the boundaries between architectural layers. SSAC’s own inability to articulate and to apply in a consistent manner the “principles” by which it purports to judge Site Finder undercuts its purported justification for constraining implementation of RFC-compliant wildcards on that basis.

In essence, SSAC uses a façade of technical orthodoxy to mask a rigid adherence to the status quo of the DNS, which is antithetical to the very nature of the Internet and inconsistent with the RFCs, which themselves recognize the importance of innovation to the Internet. The Internet was born out of a spirit of innovation and has rapidly evolved and grown since its inception. Such evolution and growth would have been impossible had improvements and modifications been subjected to an “appropriateness” review based solely on their consistency with the technical status quo, as contemplated in the Report. Yet that is precisely what SSAC has proposed. Contrary to the Report’s implication, a secure and stable Internet does not equate to an unchanging one. SSAC’s approach stifles the very innovation necessary to ensure a robust, secure and stable Internet.

Finally, in an effort to de-emphasize the lack of evidence to support its findings and recommendations, the Report cites a handful of alleged problems purportedly experienced by certain software applications while Site Finder was operational. None of these purported problems, however, affected the security and stability of the DNS or the Internet. Moreover, contrary to ICANN’s clear directive, SSAC has failed to quantify or independently to verify *any* of the purported problems described in the Report, raising serious doubts that they were real, serious, or widespread. Indeed, the Report acknowledges that the committee made no quantitative assessment of any data, stating “[w]e offer up no quantitative measures of the magnitude of this change [*i.e.*, Site Finder] and its potential differential impacts among different populations of users around the world . . . .”<sup>13</sup> Yet that was precisely what SSAC was supposed to do.

At base, the tenor of the Report suggests pre-judgment by SSAC, while the scope of the Report inappropriately exceeds SSAC’s supposed competence. Despite nine months of review, SSAC has failed to identify any evidence that Site Finder affected the security and stability of the Internet or the DNS.

---

<sup>13</sup> Report at p. 20.

## II. SSAC'S FAILURE OF PROCESS

SSAC's proceedings in this matter have failed to comport with basic principles of fairness, openness and transparency supposedly fundamental to ICANN and its committees. One week after VeriSign launched Site Finder, on September 22, 2003, SSAC submitted a Report to the ICANN Board of Directors entitled, *Recommendations Regarding VeriSign's Introduction of Wild Card Response to Uninstantiated Domains within COM and NET.*" This report had been circulated in draft form on September 19, 2003, just four days after VeriSign launched Site Finder. The report already included its prejudged conclusion Site Finder had impacted the stability of the Internet, even though the facts and analysis necessary to that conclusion were not yet known:

This is where we need to include the factual information to support the opinions and recommendations that follow. PAUL VIXE [sic] and SUZANNE, AMONG OTEHRS [sic], please dump stuff into this section.<sup>14</sup>

This comment demonstrates that SSAC reached its recommendation that Site Finder should be suspended *before* review or consideration of *any evidence* that would support that recommendation.<sup>15</sup> Indeed, SSAC was not interested in, and never followed up on, VeriSign's offer to provide relevant data before the report was published, including: (1) a description of the methods and technologies used by VeriSign to implement its wildcard initiative; (2) the extensive body of data that VeriSign had developed in the course of researching and testing its wildcard implementation; (3) the operational data VeriSign had collected since launching Site Finder; and (4) the feedback VeriSign had received from the Internet community since the launch.<sup>16</sup>

SSAC has failed to correct any of the original deficiencies in its process.<sup>17</sup> Although SSAC did hold meetings (at VeriSign's request) for the purpose of appearing to

---

<sup>14</sup> See note 10 above, Exh. A (19 Sept. 2003 draft of SSAC report).

<sup>15</sup> The final version of the report, issued on September 22, 2003, did not address this deficiency. It also did not include any facts or evidence concerning the purported effects of VeriSign's wildcard implementation. See note 3 above.

<sup>16</sup> SSAC did not follow-up on VeriSign's offer. Indeed, at one point, a SSAC member actually requested payment from VeriSign before she would analyze VeriSign's data.

<sup>17</sup> VeriSign first brought these issues regarding SSAC's process to ICANN's attention by letter dated 3 Oct. 2003, a copy of which is attached as Exhibit B. VeriSign then repeated its objections in a subsequent letter to ICANN dated 9 Oct. 2003, a copy of which is attached as Exhibit C.

gather evidence regarding Site Finder, including several presentations by VeriSign, the Report, with the sole exception of one undated anecdotal example, fails to include any information subsequent to the September 22, 2003 report, including any information that was disclosed at the October SSAC meetings. In short, SSAC appears to have found no factual information to “dump into” the Report. SSAC’s unexplained and lengthy delay in issuing the Report, coupled with the lack of discernible improvement in the factual and evidentiary underpinnings of the Report, erodes its credibility.

Moreover, during its investigation process, SSAC appears to have solicited only negative comments about Site Finder. Specifically, the Report relies on comments received in response to the request for comment by the At-Large Advisory Committee (“ALAC”), dated September 17, 2003.<sup>18</sup> The Report implies that ALAC’s request for comment was a neutral, fact-finding tool. Instead, the ALAC request for comment targeted those opposed to Site Finder by prefacing its request with a reprint of ALAC’s September 16, 2003 Statement to the ICANN Board that Site Finder raised “grave technical concerns.”<sup>19</sup>

Further, SSAC failed to conform to the procedures outlined by ICANN to govern its review of Site Finder. On October 6, 2003, Paul Twomey wrote to VeriSign “to explain the next steps in ICANN’s technical review and evaluation of [Site Finder], specifically as it involves ICANN’s Security and Stability Advisory Committee . . . .”<sup>20</sup> Through that letter, ICANN explained that SSAC would gather information to conduct a *technical analysis* of Site Finder in a fair and timely fashion that would include VeriSign’s participation and data. SSAC, however, ignored these instructions: The Report includes no quantifiable evidence regarding the alleged effects of Site Finder, and SSAC did not fairly consider VeriSign’s data in the process.

In addition, SSAC has not been open and transparent in the process leading to creation of the Report. Among other things, the primary “evidence” relied on by the Report concerning the purported effect of Site Finder on content filters, are off-line communications to Ms. Woolf and Dr. Crocker that have not been made public by the committee.<sup>21</sup> SSAC also has attempted to prevent SSAC members from disclosing

---

<sup>18</sup> Report at pp. 4 n. 37, 17 n. 48-51.

<sup>19</sup> *see also* VeriSign Site Finder Request for Comments, posted by ALAC on 17 Sept. 2003 (<http://alac.icann.org/redirect/request-comments-17sep03.htm>).

<sup>20</sup> Letter from Paul Twomey to VeriSign, 6 Oct. 2003.

<sup>21</sup> *See* Report at p.19 n. 57.

information regarding its deliberations about the Report,<sup>22</sup> and has failed to clearly indicate which committee members, beyond the Report's authors, support its findings and recommendations. Such secrecy is contrary to ICANN's charter and precludes effective and thorough rebuttal.

Notwithstanding the Report's self-congratulatory "acknowledgements," the process by which conclusions contained in the SSAC Report were reached was also not unbiased or inclusive. Opponents and competitors of VeriSign dominated, at all stages, the process followed by SSAC, and SSAC members with stated biases participated in the deliberation and drafting of the SSAC Report.<sup>23</sup> For example, the Report relies heavily on the opinion of Paul Vixie, an outspoken critic and competitor of VeriSign, on the issue of Internet stability following the implementation of VeriSign's wildcard.<sup>24</sup> Yet the Report fails to include a conflict of interest statement for Mr. Vixie, even though he is the president of ISC, which released the BIND software patch discussed in the Report as one of the technical responses to VeriSign's wildcard implementation. Ironically, Mr. Vixie's BIND patch was a primary source of the "incoherence" described in the Report.

In response to VeriSign's concerns regarding the composition of SSAC, Mr. Twomey, in an October 6 letter, explained that "it is important to note that the membership of SSAC was established prior to" the launch of the Site Finder service. His statement sought to offer the assurance that only properly nominated and pre-existing SSAC members would be participating in the committee's technical review of Site Finder. However, that was not the case. SSAC's chairman, Steven Crocker, added at least three individuals to the committee, in violation of ICANN Bylaws,<sup>25</sup> including Suzanne Woolf, K.C. Claffy and Mike St. John. The addition of these individuals for the sole purpose of participating in SSAC's review of Site Finder is not disclosed in the Report. Nor did SSAC add additional members to SSAC to counterbalance the Site Finder opponents added by Steven Crocker. The inclusion of persons with conflicts of interest in the drafting of the Report effectively compromised the legitimacy of SSAC's process and its ultimate findings and recommendations.

---

<sup>22</sup> See June 22, 2004 email from Steve Crocker to Ken Silva re "SSAC Ground Rules."

<sup>23</sup> As explained in note 12, above, the Report inappropriately implies that VeriSign employees Ken Silva and Mark Kosters participated in the drafting of the Report and endorse its findings. Instead, although not mentioned in the body of the Report, Messrs. Kosters and Silva rightly recused themselves from the exercise.

<sup>24</sup> Report at pp. 14 n. 38, 20 n. 60, *see* below at pp. 17-18.

<sup>25</sup> ICANN Bylaws provide that members of SSAC may be appointed only by the ICANN Board. *See* note 11, above. A review of the ICANN Board minutes reveals that no such Board action occurred.



Finally, the overall tone of the Report suggests prejudice and is inconsistent with a dispassionate, technical assessment of Site Finder. The Report gratuitously uses emotional and evocative language that clearly shows the committee's bias against VeriSign and Site Finder and its desire to foment hysteria regarding Site Finder. SSAC's decision to include hostile information from press reports characterizing Site Finder as a "potentially highly lucrative business venture" that could generate "tens of millions of dollars of revenue" further calls into question the objectivity and motives of the Committee.<sup>26</sup> Clearly, such statements are not relevant to a neutral "technical analysis" of Site Finder.

### **III. VERISIGN'S SITE FINDER SERVICE**

#### *User Response to Site Finder*

The Report purports to assess the "impact" of Site Finder on the Internet. The Report, however, fails to acknowledge the significant value provided by Site Finder to an important Internet constituency – users browsing the Internet. This constituency, which generated 69% of the traffic to Site Finder,<sup>27</sup> overwhelmingly supported Site Finder.

VeriSign referred users to the Site Finder website through the use of a wildcard address (A) record entry in the .com and .net zones. In doing so, VeriSign processed queries for nonexistent domain names in full compliance with provisions of the DNS protocol that address wildcards and with all applicable RFCs and specifications.<sup>28</sup> As stated above, SSAC and the IAB have both acknowledged that Site Finder complied with all applicable RFCs.<sup>29</sup>

VeriSign's Site Finder service improved the user web browsing experience when the user submitted a query for a non-existent second-level domain name in the .com and .net top level domains. Before this service was implemented, when a user entered a URL containing a nonexistent domain name (*e.g.*, unregistered or not present in the zone)

---

<sup>26</sup> Report at p. 3.

<sup>27</sup> Hollenbeck, note 8, above, VeriSign Site Finder Technical Review Panel Summary, slide 7; Usability Market Research, slide 4, presented by Ben Turner, VeriSign Vice President of Naming Services at 15 Oct. 2003 SSAC meeting.

<sup>28</sup> See IAB Commentary, note 7, above.

<sup>29</sup> See above at notes 7, 8. As explained, below at pp. 12-13. VeriSign's independent Technical Review Panel also reached this same conclusion.

ending in .com or .net, his or her web browser returned an error message that contained no useful information. With Site Finder, in the same situation, users received a user-friendly help screen that included, not only a clear message that what was entered could not be found, but also such information as (i) alternative web addresses the user may have been seeking; (ii) a search engine; and (iii) links to popular categories of websites the user could search.

Survey results, which VeriSign provided to SSAC prior to the issuance of its Report, indicated that 84% of Internet users who tried Site Finder preferred the service to receiving an error message and a majority of respondents said that Site Finder *improved the Internet*.<sup>30</sup> Internet users also took advantage of the innovative features Site Finder offered. Feedback indicated that 80% of those surveyed used Site Finder's web suggestions and 84% used the popular category web links.<sup>31</sup> A majority of Site Finder users surveyed also found the service to be useful, convenient, and easy to operate.<sup>32</sup> As one Site Finder user noted:

As a heavy but non-technical computer user it has been extremely frustrating for me to encounter 404 errors. Naturally, they happen at the busiest times. Many of us have become dependent on computers and expect all functions to work at a highly consistent level. Alternative suggestions instead of a project-stopping 404 is a welcome and functional improvement to my use of the Web and related searches. It is difficult for me to see a downside to this user friendly enhancement.<sup>33</sup>

This positive response from Internet web users is particularly significant given that the majority of the traffic received by Site Finder came from Internet users attempting to locate websites (the HTTP protocol).

The Report attempts to dismiss VeriSign's evidence of positive user response to Site Finder by suggesting that VeriSign refused to provide information regarding the overall methodology and release of the survey instrument to the committee. This is incorrect. During its October 15, 2003 presentations to SSAC, VeriSign provided the sample sizes (1,027, 1,000 and 300), the method of sampling (random), the general geographic distribution of survey participants, and informed SSAC that the survey was

---

<sup>30</sup> Turner, note 27, above, Usability Market Research, slides 3-4.

<sup>31</sup> *Id.* at slide 4.

<sup>32</sup> *Id.* at slide 5.

<sup>33</sup> *Id.* at slide 7.

conducted on-line. VeriSign also provided the dates that the surveys were distributed, along with the names of the survey firms that administered the surveys.<sup>34</sup> The Report acknowledges VeriSign's "copious" evidence but, nonetheless, dismisses it without any citation to contrary survey evidence that Internet users were displeased by Site Finder. A fair and impartial assessment of the "impact" of Site Finder should have taken into consideration the favorable response of the constituency most exposed to and affected by it.

Finally, the Report asserts that, notwithstanding consumer acceptance of Site Finder, the service had two adverse effects on end-users: "substitution for existing services and removal of choice."<sup>35</sup> More particularly, the Report asserts that Site Finder displaced similar services offered by MSN and AOL.<sup>36</sup> However, assessment of the alleged impact of Site Finder on "consumer choice" is outside the scope of SSAC's competence and ICANN's mandate that SSAC assess the *technical* impact of Site Finder. Moreover, the Report's assertion is demonstrably untrue. In the very next section of the Report, SSAC acknowledges that "patches were released by ISPs and by vendors of DNS resolver software" that transformed the Site Finder response back to the "no such domain" error code.<sup>37</sup> Thus, contrary to the Report's assertion, existing services were not displaced and consumer choice remained.<sup>38</sup>

#### *VeriSign's extensive testing and research of Site Finder*

The Report mentions, but fails to provide any details regarding, VeriSign's pre-launch testing and research of Site Finder, despite the fact that VeriSign gave presentations to SSAC that described in detail its testing and research process.

---

<sup>34</sup> *Id.* at slide 2. SSAC's dismissal of VeriSign's survey on the grounds that its methodology was unverified is inconsistent with SSAC's unquestioning acceptance of unverified emails criticizing Site Finder. SSAC's inconsistent consideration of data again suggests bias and prejudgment on the part of SSAC and its members.

<sup>35</sup> Report at p. 17.

<sup>36</sup> *Id.*

<sup>37</sup> *Id.* at pp. 18, 19.

<sup>38</sup> *Id.* at p. 19. The Report attempts to avoid this contradiction by asserting that these responses to Site Finder "introduce[d] the network or resolver operator into the decision process, further removing users from exercising choice." *Id.* Yet, prior to the introduction of Site Finder, the "consumer choice" for address directory services was the result of application or network operator modification of VeriSign's "no such domain" error response. SSAC's "consumer choice" argument collapses under the weight of its own contradictions.

Prior to deployment of Site Finder, VeriSign undertook extensive research regarding the needs of Internet users. In connection with that research, users, responding to a free-form question regarding the “current pains” they experience with the Internet, identified the need for new ways to find URLs they were looking for or to provide a form of spell correction on the World Wide Web.

To understand those responses better, VeriSign conducted additional market research in 2002 and 2003 to test the need for and desirability of an alternative to a typical error page response to a mistyped or mistaken web address. An overwhelming majority of the Internet users interviewed indicated that they would prefer the ability to initiate a web search and to receive links to related or relevant web sites.<sup>39</sup>

To meet this un-filled end-user need, VeriSign began research and testing to determine if a solution could be created that improved the web browsing experience for Internet users, that was standards compliant and scalable, and that would maintain the stability and security of the DNS and the Internet.<sup>40</sup> To that end, VeriSign reviewed existing wildcard solutions. For example, VeriSign had been operating a wildcard A record in its .cc and .tv ccTLD registries for several years, without criticism or comment from ICANN or SSAC. Additionally, in connection with internationalized domain names (“IDN”), VeriSign implemented synthesized records – an innovation endorsed by SSAC.<sup>41</sup>

VeriSign also reviewed available data in connection with other gTLD and ccTLD registries known to operate wildcards, including .bz, .cn, .cx, .io, .mp, .museum, .nu, .ph, .pw, .td, .tk, .tw, .va, and .ws. In so doing, VeriSign noted that no objection had been raised by SSAC, the IAB, or by any other ICANN committee or constituency, in response

---

<sup>39</sup> Specifically, in December 2002 testing, 67% of the 955 Internet users interviewed rated the ability to initiate a search as “highly useful.” Additionally, 65% of those interviewed rated links to related/relevant sites as “highly useful.” Testing conducted in January 2003 revealed that 70% of those interviewed showed a high preference for search capabilities and 68% had a high preference for links to related sites. VeriSign Site Finder Pre-Launch Activities, slide 4, presented by Anthony Renzette, VeriSign Director of Product Development, at 15 Oct. 2003 SSAC Meeting.

<sup>40</sup> *Id.* at slide 5.

<sup>41</sup> See SSAC’s *Comments on VGRS* at p. 2, a copy of which is attached as Exhibit D (stating, with respect to VeriSign’s support for international domain names, that SSAC “can’t really see a technical basis for objecting to what VeriSign is doing”).

to those wildcard deployments in top-level domains.<sup>42</sup> VeriSign also developed and published guidelines for the deployment of wildcards and discussed this concept.<sup>43</sup>

Furthermore, VeriSign conducted extensive testing prior to introduction of Site Finder. That testing included third party testing to evaluate the effect of a DNS A record wildcard on protocols and applications.<sup>44</sup> VeriSign also performed live tests to determine the types, volumes, and sources of DNS traffic.<sup>45</sup> In addition, through an external survey and review process, VeriSign worked with a wide range of companies to test and refine the Site Finder service. VeriSign contacted over 600 companies and notified them of the upcoming Site Finder launch, briefed 55 companies on Site Finder (pursuant to non-disclosure agreements), and tested Site Finder with 35 companies. The companies participating in testing represented a wide cross-section of industries, including health care, telecommunications, finance, transportation, and software. This testing involved a subset of protocols (including HTTP, HTTPS, SSH, FTP, SMTP, DNS, VPN and custom applications) and key applications, some of which were intentionally mis-configured with

---

<sup>42</sup> VeriSign brought the implementation of a wildcard by .biz to SSAC's attention on May 19, 2003, and solicited the committee's comments regarding the service. SSAC never followed-up or took any action with respect to .biz. On the contrary, SSAC members recognized that wildcards are RFC-compliant and that the committee did not have standing to review the .biz wildcard. For example, on May 21, 2003, Jaap Akkerhuis agreed with Johan Ihren's statement that: "I think wildcards are a bad mistake that should be avoided (religious pov) but as others have commented *it is not up to us or anyone else but the zone owner to decide the contents of the zone so long as these contents adhere to relevant RFCs*" (emphasis added). Mr. Akkerhuis then explained: "A wildcard as in the normal DNS is within the protocol. If people do that, there is not a lot you can do. And, to make things worse, for .museum it is a requirement according to the contract they have with ICANN." On May 19, 2003, Paul Vixie wrote: "speaking for dnssac, [I] don't think we have standing. [D]ns is a distributed, reliable, autonomous, hierarchical database system. The key word for this purpose is "autonomous". Delegating something to somebody and then telling them what they can and cannot put into it is false (and I might add, offensively so.)" And that same day, David Conrad wrote: "As long as no RFCs are violated, I don't see a problem with it per se." These email messages are attached as Exhibit E. The inconsistency in approach by SSAC significantly undermines the credibility and objectivity of its purported conclusions with respect to VeriSign's implementation of a wildcard.

<sup>43</sup> Domain Name System Wild cards in Top-Level Domain Zones, Scott Hollenbeck and Matt Larson, VeriSign Naming and Directory Services, 9 Sept. 2003. (<http://www.verisign.com/resources/gd/sitefinder/bestpractices.pdf>).

<sup>44</sup> Renzette, note 39, above, VeriSign Site Finder Pre-Launch Activities, slides 6, 8.

<sup>45</sup> *Id.* at slide 7.

non-existent domain names.<sup>46</sup> The testing companies reported no issues to VeriSign resulting from the Site Finder service.<sup>47</sup>

Finally, after launching Site Finder, VeriSign assembled a technical review panel (the “TRP”) of industry experts<sup>48</sup> to gather and evaluate technical data concerning Site Finder from interested parties in the Internet community. Specifically, the TRP: (1) quantified the likelihood of an issue arising for Internet users and any resulting consequences, (2) determined what enhancements could be made to improve Site Finder, and (3) reported the observed implementation issues to VeriSign, along with any supporting data. In so doing, the TRP looked at Site Finder from three perspectives: reported issues, protocol analysis, and use case analysis. It also considered possible issues identified by the IAB, as well as those reported by NANOG, Slashdot, online press and others.

After an extensive quantitative technical review, the TRP concluded that: (1) No security or stability problems had been identified; and (2) Site Finder caused no material irresolvable problems for the Internet.<sup>49</sup> These conclusions were based on a detailed analysis of the top ten most used protocols and the likelihood and impact of the possible issues identified by IAB and others.<sup>50</sup>

The SSAC Report relegates these technical findings to a footnote. Rather than evaluate them based upon evidence, SSAC dismisses them without analysis, stating that the summary of TRP’s conclusions “does not reflect our reading of the Technical Review Committee’s specific findings.”<sup>51</sup> Consistent with the rest of the Report, however, SSAC

---

<sup>46</sup> *Id.* at slide 9.

<sup>47</sup> *Id.*

<sup>48</sup> Hollenbeck, note 8, above, VeriSign Site Finder Technical Review Panel Summary, slide 4. The TRP included, among others, Bruce Tonkin (chair), CTO of Melbourne IT, Ken Schneider, CTO and VP of Operations for Brightmail, George Sherman, CTO office of Morgan Stanley, and Keith Teare, Chairman, President, and CEO of Santa Cruz Networks. Four VeriSign engineers also sat on the TRP. Their role, however, was limited to listening to and answering questions from the industry experts.

<sup>49</sup> *Id.* at slide 8.

<sup>50</sup> *Id.* at slides 7, 10. Specifically, the HTTP, SMTP, DNS, IRC, epmap, pop3, microsoft-ds, netbios-ns, netbios-ssn, and ftp protocols were analyzed. These protocols were the most common protocols based on the number of connection attempts to the Site Finder server. *Id.* at slide 7.

<sup>51</sup> Report at pp. 7-8 n. 25.

fails to explain how its “reading” of the available information differs from the TRP’s reading of it. Further, SSAC does not define the “specific findings” of the TRP to which it refers. These vague and conclusory references are irresponsible and disingenuous.

Without including specific information about Site Finder’s development, testing, and post-launch evaluation, all of which was presented and made available to SSAC by VeriSign, the Report fails to describe accurately the service or its genesis and purported “impact.”

#### **IV. SSAC’S FINDINGS AND RECOMMENDATIONS**

The Executive Summary appearing at the outset of the SSAC Report contains eight “findings,” and four “recommendations” purportedly based on those findings. The structure of the Report suggests that the evidentiary support for these findings and recommendations is set forth later, in the body of the Report. That evidence, however, is never set forth. Rather, the Report relies on self-reflexive citations back to its own earlier opinion statements to support its findings and recommendations, none of which was based on any evidence in the first place.

Instead of a quantitative assessment of Site Finder’s alleged “impact” on the Internet, the primary focus of the Report is on Site Finder’s alleged non-conformance with vague “Internet engineering principles” and its effect on a narrow range of applications that are not themselves a part of the Internet’s infrastructure, but which interact with that infrastructure in some way. Given SSAC’s narrow purpose to assess security and stability threats to the Internet’s *naming and address allocation systems*, the appropriateness of SSAC’s exposition on Internet engineering principles and assessment of the effect of a standards compliant wildcard implementation on non-compliant applications that are not part of the Internet’s infrastructure, is questionable. Moreover, as set forth below, SSAC’s “fundamental engineering principles,” to the extent they exist, either are not universally accepted or applied, or have no relevance to wildcards.

Furthermore, SSAC’s recommendations, despite the Report’s statement to the contrary, do not flow from its purported findings and are fundamentally flawed:

- Recommendation (1): SSAC recommends that “[s]ynthesized responses should not be introduced into top-level domains (TLDs) or zones that serve the public, whose contents are primarily delegations and glue, and where delegations cross organizational boundaries over which the operator may have little control or influence.”<sup>52</sup>

---

<sup>52</sup> *Id.* at pp. iv, 24.

This recommendation is unwarranted and inappropriate given SSAC's failure to find that Site Finder affected the security or stability of the DNS or the Internet, and SSAC's acknowledgment that wildcards *are* RFC-compliant. Further, the Report contains no explanation or justification for several artificial qualifications placed on this recommendation, namely that wildcards should only be prohibited in (a) what the committee calls "public" zones, (b) whose contents are "primarily delegations and glue," and (c) "whose delegations cross organizational boundaries." These qualifications are irrelevant to wildcard implementation from a technical standpoint.<sup>53</sup> SSAC's recommendation appears to be nothing more than a naked gerrymandering intended to

---

<sup>53</sup> The Report fails to define what it means by a "public" zone. However, it appears that SSAC means to distinguish between TLDs that are limited to specific entities (such as museums for .museum) and TLDs that are not so limited. This distinction, as well as the "delegations and glue" and "cross organizational boundary" distinctions, however, have no impact on the technical manner in which a wildcard would operate within a zone. At the protocol level, a DNS wildcard does not provide semantic distinctions between "public" zones, "private" zones, or any other type of zone. The expected DNS protocol response (and the underlying implications of that response for applications that use the DNS) is exactly the same.

SSAC's reference to TLDs whose contents are "primarily delegations and glue" also has no application in the context of a wildcard discussion. The .com and .net registries historically have been operated in a fashion that virtually all inquiries to its name servers are responded to with referrals to name servers with authoritative information for second level domains. This was done primarily to permit flexibility on the part of the operators of hosts to change data without requiring the hosts constantly to submit new data to the relevant TLD registry. Address information, called "glue," accompanied the response to provide the recipient of the referral with the necessary address information to contact the appropriate name servers. However, there is nothing in the RFCs or in any specification that requires any TLD registry operator to follow that pattern. In fact, other registries (for example, the .name registry) contain significant numbers of records directly correlating authoritative (i.e. non-delegation) data with secondary domain labels. There is no "expectation" that a response will always be a delegation.

From the standpoint of a resolver program, the only difference between receiving a delegation response and receiving the data sought is that the resolver must do less work in the latter situation than if it had received a direct response. Instead of having to query another name server, the resolver is finished once it receives the actual resource record set associated with the secondary domain label. Any resolver's job is to secure an actual data sought, if it exists within the resolver's scope of query, not just to find a referral to another name server. Once the resolver finds the data, it forwards it without comment to the application that requested it. A resolver simply does not "care" which name server it receives a response from.



affect only certain registry operators, such as VeriSign, while leaving other registries free to implement wildcards.<sup>54</sup>

- Recommendation (2): SSAC recommends that “[e]xisting use of synthesized responses should be phased out in TLDs or zones that serve the public, whose contents are primarily delegations and glue, and where delegations cross organizational boundaries.”<sup>55</sup> This recommendation contains the same baseless and unprincipled qualifications as Recommendation (1) with the same intended effect of exempting some, but not all, registry operators. As SSAC is aware, wildcards are a well-established feature of the DNS landscape, as demonstrated by the fact that the following top-level domains had supported wildcard functionality in their zones prior to VeriSign’s introduction of Site Finder: .bz, .cn, .cx, .io, .mp, .museum, .nu, .ph, .pw, .td, .tk, .tw, .va and .ws. Indeed, ICANN’s agreement with the registry operator for the .museum TLD specifically permits the implementation of a wildcard.<sup>56</sup> SSAC cites no valid reasons why wildcards in the .com and .net zone should be phased out, while they continue to be operated by these other TLDs.

- Recommendation (3): SSAC states “[T]here exist shortcomings in the specification of DNS wildcards and their usage” and recommends that the defining RFCs be “examined and modified.”<sup>57</sup> This recommendation falls far outside the scope of SSAC’s supposed competence and its function to assess security and stability issues concerning the DNS. SSAC is not a standards-setting organization with responsibility for review and modification of the RFCs.

- Recommendation (4): SSAC recommends that “[c]hanges in registry services should take place only after a substantial period of notice, comment and consensus involving both the technical community and the larger user community.”<sup>58</sup>

---

<sup>54</sup> A preliminary draft of the Report did not include these purported qualifications on SSAC’s recommendation. A copy of this preliminary draft is attached as Exhibit F. However, after the draft was circulated for comment, the operator of the .name TLD registry objected to SSAC’s preliminary recommendation, and called upon the committee to limit its recommendation to VeriSign and Site Finder. A copy of .name’s objection is attached as Exhibit G. SSAC’s qualifications on its recommendation thus appear to be a thinly disguised attempt to make SSAC’s recommendation appear neutral but, in reality, apply only to VeriSign.

<sup>55</sup> Report at pp. vi, 25.

<sup>56</sup> TLD Sponsorship Agreement: Attachment 13 (.museum) at p. 5.

<sup>57</sup> Report at pp. vi, 25.

<sup>58</sup> *Id.*

This recommendation too falls outside the scope of the committee’s supposed competence. Further, this recommendation is vague and fails to provide any guidance regarding the process contemplated by SSAC, or the scope of the services that would be subject to the recommendation. SSAC’s proposed review for all “technical” innovations is antithetical to a robust Internet.

V. **SITE FINDER DID NOT AFFECT THE STABILITY OR SECURITY OF THE INTERNET**

The Report neither identifies any event of instability or any lack of security of the DNS system or the Internet’s infrastructure, nor does it enumerate any specific effects that could fairly be characterized as threats to security or stability. On the contrary, it is clear from the Report that Site Finder did not and cannot have that effect.

The methodology used by VeriSign in the development and deployment of Site Finder ensured that, contrary to the suggestion of the SSAC Report, the core registry function continued to operate during the period of deployment with the same level of security, stability, and technical reliability as it has always demonstrated. DNS inquiries of VeriSign’s authoritative servers continued to produce responses as always, returning referrals for second-level domain names registered in the .com and .net top-level domains. Those responses were produced as rapidly as they were prior to introduction of Site Finder; there were no time-outs or other error conditions. Further, there were no security breaches. The integrity of VeriSign’s master files and authoritative servers – prior to, during, and after Site Finder – remained secure.<sup>59</sup>

The SSAC Report fails to acknowledge that the Site Finder service operated without affecting the availability or stability of the DNS or the Internet infrastructure. During its deployment, and over the last six years as a whole, VeriSign has maintained 100% availability and response. VeriSign is resolving in excess of 100,000 DNS queries

---

<sup>59</sup> The Report attempts to avoid these undisputed facts by engaging in a linguistic shell game with the term “stability.” The Report appears to use the word “stability” in two different ways, without distinguishing between them. “Stability” can mean “unchanging” or it can mean “freedom from liability to fall or be overthrown.” *See* Oxford English Dictionary, “Stability,” online edition. In engineering terms, when applied to a system, “stability” generally means the latter, *i.e.*, that the system is free from a failure or from being overthrown. *Id.* By mixing the two usages, the Report engenders confusion and deviates inappropriately from its limited delegated mission. Only the latter meaning is appropriate here. Only that which causes failure in the system should be considered. Applying that meaning, the Report fails to demonstrate how or why Site Finder threatens the stability of the DNS system or the Internet overall, much less that it actually ever did.

per second at peak times, totaling more than 10 billion queries per day. This performance is the result of the tens of millions of dollars VeriSign has invested in the .com and .net infrastructure, the hundreds of thousands of employee hours dedicated to constant monitoring of that infrastructure, and VeriSign's continued willingness to deploy additional capacity to exceed anticipated demand. It is this investment, by VeriSign, that ensures the deterministic, robust, reliable, and highly scalable infrastructure of the Internet. It is undisputed that Site Finder had no impact on this infrastructure.

## **VI. SITE FINDER DID NOT VIOLATE "FUNDAMENTAL" INTERNET ENGINEERING PRINCIPLES**

As stated above, SSAC was unable to fault Site Finder on security or stability grounds. Indeed, SSAC member Paul Vixie has expressly admitted as much. In response to an email stating that "I think recent events prove pretty well that VeriSign GRS no longer gives a crap about stability. Have we forgotten \*.COM so quickly?," Mr. Vixie conceded:

[I] was . . . publicly critical of \*.COM and \*.NET, but that's a *policy problem, not an operational problem*.  
[V]eriSign has a very good record for name server uptime both at the TLD and root level.<sup>60</sup>

Nonetheless, SSAC proceeded to perform a policy assessment of Site Finder. SSAC evaluated the Site Finder service against an ill-defined set of "principles" of Internet engineering. These "principles" were primarily derived from the SSAC members' personal, philosophical views of the Internet. The Report's policy discussion is beyond the scope of SSAC's mandate, outside its area of expertise, and inappropriate. It also is flawed.

First, as explained above, SSAC acknowledges that Site Finder was fully compliant with all applicable RFCs, protocols and specifications. But, notwithstanding these critical admissions, the Report makes the conclusory statement that "Good practice regarding wildcards has evolved," and then implies that *any* wildcard implementation is in fact bad practice.<sup>61</sup> The Report provides *no support* for its statements and fails to describe "good practice." Given that wildcards are clearly anticipated, and even

---

<sup>60</sup> Email message posted by Paul Vixie to [nanog@merit.edu](mailto:nanog@merit.edu) dated June 17, 2004 (emphasis added). A copy of this email is attached as Exhibit. H.

<sup>61</sup> Report at p. 12.

specified, in the RFCs, any claim that the adoption of a wildcard by VeriSign was unexpected or non-compliant is disingenuous. Moreover, the implication that a DNS level use of wildcards is “bad practice” is inconsistent with the RFCs and reflects merely a differing philosophy, not a technical issue or an issue of security or stability.

SSAC’s use of the principle of “stability” to critique Site Finder also is misplaced.<sup>62</sup> SSAC is using “stability” to mean nothing more than “unchanging.” But innovation and experimentation are the true founding principles of the Internet. A verbatim quote from RFC 1034 underscores this point:

. . . The official protocol includes standard queries and their responses and most of the Internet class data formats (e.g., host addresses).

. . . However, the domain name system is *intentionally extensible*. Researchers are continuously proposing, implementing and experimenting with new data types, query types, classes, functions, etc. Thus while the components of the official protocol are expected to stay essentially unchanged and operate as a production service, *experimental behavior should always be expected* in extensions beyond the official protocol. (Emphasis added.)

SSAC’s conception of “stability” would limit any implementation of new standards compliant functionality, solely on the basis that it had not been done in the past. This is not stability; it is rigidity. By equating stability with “unchanging,” SSAC has set itself up as the enforcer of the *status quo*. SSAC’s conception of its role is thus antithetical to the experimental and innovative nature of the Internet, as recognized by the RFCs themselves.

The other “principles” referenced in the Report likewise are inapplicable here. The Report states that “[t]he authoritative servers for these two zones (.com and .net) no longer give out ‘no such name’ responses for any possible name in these two zones”<sup>63</sup>

---

<sup>62</sup> The Report describes a “set of core protocols” which SSAC asserts must remain stable: “[T]he diversity and complexities that can arise from the commitment to an open architecture are enabled by an equally deep commitment to a discipline of a minimal set of core protocols that are kept very stable. *This core includes the Internet Protocol (IP), the routing system and the domain name system. . . .*” *Id.* at p. 8 (emphasis added). The Report includes *no evidence* that these “core protocols” were affected by Site Finder.

<sup>63</sup> Report at p. 12, citing IAB Commentary.

and asserts that this violates two other alleged principles: “Be conservative in what you send and liberal in what you receive”<sup>64</sup> and “Do what you think the other party is expecting.”<sup>65</sup>

The first principle alleged, as generally understood, means that a program or user should not expect an expansive interpretation by the recipient of what it sends, but that it should be prepared to receive a relatively broad range of responses. This “principle” applies to clients as well as servers. Thus, an application asking for an “A Record” should be prepared to interpret any form of response described in the applicable RFC. Site Finder always produced a standards compliant response defined by the RFC. It supplied an IP address for every possible query, in exactly the prescribed format. In fact, Site Finder is an example of being liberal in what is received. Instead of rejecting outright a request for an uninstanitated domain name, Site Finder made an effort to respond most liberally to the sender’s request.

The second purported principle, the so-called principle of “least astonishment,” invoked by SSAC for the purpose of critiquing Site Finder, is described by SSAC as “traditional.” However, nowhere in the Report is the origin of the “principle” identified, nor are examples given of its application. Moreover, this “principle” is inherently subjective and difficult, if not impossible, to apply predictably to any real system. Indeed, it is difficult to discern what the Report claims *is* unexpected. As stated above, a wildcard response is clearly contemplated by the applicable RFCs and, thus, can hardly be characterized as “unexpected.”

The Report also asserts that Site Finder “implicitly” violated the “principle of layering” by assuming that “all – or at least the vast preponderance – of queries involving uninstanitated names were intended to be HTTP (Web) queries or SMTP (e-mail) transactions.”<sup>66</sup> The Report fails to mention that this “assumption” is actually correct. Nearly 86% of all traffic to Site Finder was from HTTP queries or SMTP transactions.<sup>67</sup> Moreover, multiple widely accepted technologies used on the Internet, and not criticized by ICANN, including Network Address Translators and firewalls, clearly “violate” the “layering” of address resolution in a way that Site Finder did not. With Site Finder, the

---

<sup>64</sup> This principle is in fact set forth in RFC 793, section 2.10, authored by Jon Postel.

<sup>65</sup> Report at p. 9.

<sup>66</sup> *Id.* at p. 14.

<sup>67</sup> See Hollenbeck, note 8, above, VeriSign Site Finder Technical Review Panel Summary, slide 7. Many of the other protocols using the DNS are automated and, therefore, less prone to the user error that results in a query involving an uninstanitated domain name.

boundary between an Internet application and the application resolution process remained unchanged. If a resolver did not find an entry for a second level domain name in its cache, it queried root zone and TLD name servers in exactly the same fashion as it did before the launch of Site Finder. Site Finder did not require resolvers to change their procedures in order to respond to application-layer queries for IP addresses.

Further, SSAC itself recently approved VeriSign's processing of internationalized domain names ("IDNs") at the DNS level, a technical innovation that, according to the Report, would "blur" the boundaries between architectural layers. VeriSign's IDN technology replaced the error code that otherwise would be received by a user with a wildcard response that attempts to match the IDN with its ASCII equivalent.<sup>68</sup> For purposes of SSAC's "layering" critique, this is functionally equivalent to Site Finder. Nonetheless, even though SSAC *endorsed* VeriSign's IDN implementation, it has chosen to condemn Site Finder. SSAC's own inability to apply these supposed "principles" in a consistent manner undercuts its rationale for using them to constrain implementation of VeriSign's RFC-compliant wildcard.

The Report also asserts that Site Finder reduced "coherency" on the Internet.<sup>69</sup> SSAC defines coherence as follows: "One of the fundamental objectives in the design of the domain name system is to give the same response no matter where the queries are initiated. This attribute is called *coherence*."<sup>70</sup> SSAC does not contend, nor can it, that Site Finder introduced incoherence into VeriSign's DNS query responses. Before, during, and after the launch of Site Finder, VeriSign's DNS name servers responded to identical queries with identical responses, no matter where the queries were initiated.

In fact, the Report contends that incoherence was created, not by VeriSign and Site Finder, but by certain software vendors and ISPs when they began modifying intermediate systems to intercept and alter the RFC-compliant DNS responses returned from VeriSign's servers. This type of incoherency, however, is common and existed before the launch of Site Finder: Many ISPs routinely intercept and alter traffic on their network in such a way that their users experience different application behavior than other Internet users. SSAC fails to recognize or address this.

---

<sup>68</sup> See SSAC's *Comments on VGRS*, note 41, above, Exh. D.

<sup>69</sup> Report at p. 20. As noted, SSAC's only "evidence" for this assertion is the opinion of Paul Vixie. *Id.* at p. 20 n. 60.

<sup>70</sup> *Id.*

## **VII. THE REPORT FAILS TO QUANTIFY OR SUPPORT ITS PURPORTED EVIDENCE OF SITE FINDER'S ADVERSE EFFECTS**

The Report identifies no adverse impact on responses to HTTP requests, which constituted the majority of the requests received by Site Finder. Instead, the Report focuses on alleged effects of Site Finder on a narrow range of applications that are not themselves a part of the Internet infrastructure, but which in some way interact with that infrastructure. Specifically, the Report focuses on potential implications for non-standards compliant applications when a standards-compliant wildcard is deployed. As explained below, the Report fails to quantify these alleged problems or, with the exception of one unverified anecdote, to provide any evidence to support its description of these “problems.”

The Report begins by criticizing the manner in which Site Finder dealt with requests from email applications. After a criticism of the initial Site Finder software, however, the Report, proceeds to discount its own criticisms, eventually, and accurately, pointing out that the second version of the Site Finder SMTP server did *not* refuse a connection, thereby triggering further connection attempts. Rather, its response was equivalent to “no user at this address.” The SMTP client response was not to continue to try to transmit, but rather to terminate the effort and report the error. Thus, no messages were lost in transit.

The actual operation of Site Finder was technically straightforward. When presented with an uninstantiated domain name in the .com and .net top level domains, VeriSign’s authoritative name server returned the IP address of a server complex VeriSign had configured specifically for the Site Finder service (“Response Server”). An authoritative name server never knows what application will use the IP address thereafter. It does not make any assumptions in that regard, nor need it make any such assumptions. Applications that queried for an uninstantiated domain name would naturally transmit their requests in exactly the same manner as prior to the launch of Site Finder.

In the case of queries using HTTP protocols and directed to port 80, the Response Server responded with a web page identifying potential alternative spellings and web addresses, as well as providing enhanced searching capability. In the case of service requests using SMTP protocols and directed to TCP port 25, the Response Server did not refuse a connection, even in its initial deployment. Rather, it established a TCP connection. Once the connection was established, the user’s SMTP client application transmitted the addressee information, at which point the Response Server would indicate unequivocally that no such user was known. The uniform and proper response of a client application to a “no such user” reply is to report the error immediately, *not* to queue up retries as implied in the SSAC Report. Further, the Response Server received no more

header information than for any other misdirected e-mail. VeriSign did not catalogue or collect any header information.

In the case of the remainder of application protocols or requests directed to other ports, the Response Server explicitly rejected connection attempts using protocol-standard responses, allowing applications to note the refused connection without undue delay. Significantly, the Report includes no examples of any problems with these protocols.

The Report also asserts that the second iteration of VeriSign's Response Server "bounced" messages in excess of ten megabytes with a "message too large" error. This is incorrect. VeriSign's Response Server never was set to reject messages larger than ten megabytes, and it did not, in fact, reject messages on that basis. Although the Response Server "advertised" a maximum message size of 10 megabytes, if the client indicated it wanted to send a larger message, the Response Server did *not* issue a 5xx error code as it would have if it were actually rejecting messages larger than 10 megabytes but, rather, issued a 550 error with the text explanation "Client host rejected: The domain you are trying to send mail to does not exist." A test of the Response Server would have confirmed this. SSAC did not attempt to perform such a test. In the absence of such a test, its assertion is not only incorrect, but irresponsible, and underscores its questionable approach.

The Report next speculates that VeriSign "*might* be collecting information that users would not expect them to collect . . ." <sup>71</sup> The Report, however, fails to identify any information VeriSign collected. In fact, as SSAC knows, VeriSign did not collect any private information. Because of the way VeriSign structured its SMTP response, no message content should ever have been transmitted to VeriSign. The sender's email address and the email addresses of message recipients were transmitted initially, but nothing more. VeriSign has stated publicly and unequivocally that it did not record and collect even that much information, and it did not do so. <sup>72</sup> Any and all SMTP requests (port 25) were summarily responded to with the "no such user" response and nothing was recorded. The implications of the Report to the contrary are simply unfounded.

---

<sup>71</sup> Report at p. 16 (emphasis in original).

<sup>72</sup> See, e.g., VeriSign Response to IAB Commentary: Concerns on the use of DNS wildcards, October 6 2003 at p. 6 (<http://www.icann.org/correspondence/verisign-response-iab-06oct03.pdf>); see also VeriSign Privacy Policy FAQs ([http://www.verisign.com/products-services/naming-and-directory-services/naming-services/site-finder-services/page\\_002700.html](http://www.verisign.com/products-services/naming-and-directory-services/naming-services/site-finder-services/page_002700.html)).



The spam filter issue raised in the Report is even more specious. Any spam filter can check for the IP address of the Site Finder server (which is published), just as easily and quickly as it can check for a Name Error code. Spam filters typically are installed on servers, not clients, and they are updated frequently. As the Report notes, spam filter companies quickly added the capability of treating the Site Finder IP address as equivalent to a DNS Name Error response for filtering purposes.<sup>73</sup>

The so-called “web bug” is yet another baseless attack on Site Finder and VeriSign in the SSAC report. Virtually every web server includes a program to log every inquiry, recording the host name making the request and the full URLs requested. Information about the type of browser, transmission speed and other purely technical information is received as well. These logs are used by almost every web site operator to monitor which portions of a web site are most used and to correct configuration errors. Because VeriSign is concerned only with usage of the Site Finder web site, the standard logs (which would cover all protocols) were over-inclusive and not particularly helpful for usage monitoring functions.

Accordingly, VeriSign engaged Omniture to collect the equivalent information by means of a small Javascript program placed in the Site Finder page. That way, only instantiations of the Site Finder web page would be reported. That Javascript program relayed a small amount of information, substantially equivalent to that contained in a usage log, to Omniture’s server. Omniture then produced summary, aggregate statistics and relayed them back to VeriSign. Omniture is specifically precluded from using any individual items of information other than to report them back to VeriSign.

VeriSign did not use the information in any fashion other than it would use normal web usage log information. This web usage log information gathering also was fully disclosed in VeriSign’s Privacy Policy.<sup>74</sup> Moreover, VeriSign did not “install” anything on user’s computers, and specifically did not install any program that would continue to operate after a Site Finder page ceased to be active. The Javascript employed by Site Finder ceased to be active as soon as the user exited the Site Finder page.

---

<sup>73</sup> Spam filters that rely primarily or exclusively on name error responses are exceedingly rare, and process less than 3% of spam. *See* Hollenbeck, note 8, above, VeriSign Site Finder Technical Review Panel Summary, slide 11; *see also* Review of Technical Issues and VeriSign Response, slide 7, presented by Matt Larson, VeriSign Principal Engineer, at 15 Oct 2003 SSAC Meeting.

<sup>74</sup> A copy of VeriSign’s Site Finder Privacy Policy is attached as Exhibit I.

Finally, the Report evocatively but falsely implies that Site Finder made it easier for end users to access websites featuring adult content. It states that many sites “have strong filters in place to protect its end users from accessing inappropriate sites,” and it implies that Site Finder would permit users to bypass those protections. The Report does not explain how this would occur,<sup>75</sup> and indeed, it could not occur. Site Finder was incapable of altering the function of a content filter in the manner described by SSAC. When Site Finder’s HTTP server displayed a list of alternatives to the erroneously typed URL, the links displayed on a Site Finder response page did *not* bypass any content filter that otherwise would operate on a user’s computer. In other words, if a content filter prohibited a user from visiting a specific link, Site Finder in no way provided a “back channel” through which to access that link. Moreover, Site Finder included the *added* functionality for a user to set individual Site Finder preferences such that future Site Finder pages received by that user would not include links to sites featuring adult content.<sup>76</sup> The Report’s insinuation that Site Finder increased the likelihood of access to adult content is false.

## **VIII. CONCLUSION**

As the foregoing discussion demonstrates, the Report is fundamentally flawed in its process, analysis and recommendations. SSAC had a single, limited mandate with respect to Site Finder – to assess quantitatively the *technical* effect of Site Finder on the stability and security of the DNS and the Internet. SSAC mustered no evidence that Site Finder adversely impacted the security of the DNS or Internet. SSAC found no evidence that Site Finder adversely impacted the stability of the DNS or Internet. SSAC was forced to acknowledge that Site Finder did not cause DNS or Internet failures or outages. These facts should have ended SSAC’s Site Finder process.

Instead, having concluded before it had even begun its investigation that Site Finder should be suspended, and having been stacked during its purported technical evaluation with Site Finder opponents, SSAC proceeded in the absence of evidence or quantification to formulate the biased and unsupported conclusions and recommendations appearing in the Report. Those conclusions and recommendations do not follow from

---

<sup>75</sup> The only purported support for this comment appears to be a couple of “personal communications” between Dr. Crocker and Ms. Woolf, and someone named “Collie,” who appears to have asserted that Site Finder provided “an alternative pathway to reach objectionable content” to students in Tennessee school districts. SSAC Report at pp. 19 n. 57, 20. No further information is provided regarding this purported problem.

<sup>76</sup> Site Finder Preferences, Content Filtering, formerly available at <http://sitefinder.verisign.com/help.jsp>, a copy of which is attached as Exhibit J.

any evidence or technical analysis by SSAC. Rather, they derive from and reflect the purely personal philosophies and preferences of SSAC's conflicted membership. As SSAC member Paul Vixie recognized: "[I] was publicly critical of \*.com and \*.net, but *that's a policy problem, not an operational problem.*"<sup>77</sup> (Emphasis added.) SSAC's conclusions and recommendations should thus be recognized for what they are – *policy* recommendations by a body that was not charged with, and has no expertise in, policy-making.

Indeed, SSAC's policies espoused in the Report are misguided and wrong-headed. They equate "stability" with a total lack of change. However, as the RFC's themselves recognize, the history of the Internet is change, and the future of the Internet is change. To remain vibrant and responsive, the Internet must change, at its core as well as at the periphery. By aligning itself with an immutable status quo, SSAC has done a thorough disservice – to Site Finder, to the Internet, and to present and future Internet users who expect innovation to keep the Internet expanding and responsive to their needs.

VeriSign reserves all rights and remedies it has with respect to the actions of ICANN and SSAC regarding Site Finder or any other matter, including those rights subject to claims in the pending litigation VeriSign has commenced against ICANN. A statement of the violations of VeriSign's rights by reason of the conduct of ICANN and SSAC, including in connection with the Report, is beyond the scope of this letter.

---

<sup>77</sup> Vixie, note 60, above, Exh. H.



# **EXHIBIT A**

> Recommendations Regarding Verisign's Introduction of Wild Card  
> Response to Unregistered Domains within .com and net

> ICANN Security and Stability Advisory Committee

> BACKGROUND

> [3] On September 15, 2003, Verisign changed the way its .com and .net  
> servers respond when presented with an unregistered domain name.  
> Previously, such queries returned NXDOMAIN ("non-existent domain"),  
> the negative response defined in the official DNS protocol  
> specification, RFC xxx. Verisign changed this to return an IP  
> address for a special server it had set up, thereby making it appear  
> the requested domain name exists. The special server would then handle  
> the subsequent requests for application level service, e.g. web, mail,  
> etc. For web requests, the special server would notify the user that  
> the domain name wasn't registered and offer search services and/or  
> registration services to the user. For mail, the special server would  
> simply close the connection and appear to be unresponsive  
> (unreliable?).

> [3] Although Verisign explained this change as a way to improve the  
> user's experience when he mistypes a domain name, it is widely  
> understood as a way of finding additional revenue from such mistakes.  
> Related but not identical approaches have been fielded before. For  
> several years(?) some browsers have given the user a search page  
> and/or a commercial sales pitch when the domain query returned  
> NXDOMAIN. Also, Verisign had earlier fielded a much narrower and  
> smaller version of this scheme for queries which contained  
> unrecognized codes in the query. In that case, Verisign's software  
> examined the unrecognized codes to determine if the query might be  
> representing a domain name in another language, usually Chinese,  
> Japanese or Korean, which had been sent to its servers before being  
> mapped into one of the standard encodings used for those languages.  
> Nor was Verisign the first top level domain system to try this more  
> general approach of substituting a single virtual host for all  
> unregistered domain names. Several other top level domains, including  
> .museum, <list of country codes> have been doing the same thing.  
> However, there is a sharp difference in the sizes of these domains  
> compared to the .com and .net domains, and the impact on the user  
> community in those cases has been far less.

> [3] There has been strong negative reaction throughout the community  
> to these changes. These reactions have included claims that some  
> services have stopped working or have become degraded, that the  
> overall domain name system is now less stable, that trust within the  
> community has been damaged, and that more regulation is needed.

> SECURITY AND STABILITY ISSUES

> [1] The Security and Stability Advisory Committee has examined the  
> situation from several points of view.

> - Conformance with the protocol specifications as defined by the  
> engineering community

- > - Conformance with accepted best practices and operational procedures
- > as defined by the engineering and operational communities
- >
- > - Consideration of the technical stability and security of the domain
- > name system and the Internet as a whole in light of the both the
- > changes introduced by Verisign and the corresponding changes being
- > introduced by others.
- >
- > - Procedural and governance controls in place to assure review and
- > analysis of changes to the critical components of the Internet
- >
- > - Public confidence in the stability and reliable operation of the
- > Internet
- >
- > We particularly note that security and stability is not confined to a
- > narrow interpretation of the technical specifications of the protocol
- > documents, but also includes engineering, operational, business and
- > political issues.

> ANALYSIS

- > <<This is where we need to include the factual information to support
- > the opinions and recommendations that follow. PAUL VIXE and SUZANNE,
- > AMONG OTEHRS, please dump stuff into this section.>>

> OPINIONS

- > [1] Verisign's change constitutes a material change in the base
- > service. That is, it is neither an introduction of just a value-added
- > service nor is it an immaterial change to the base service. (This
- > point intentionally relates to the language in an MOU between Verisign
- > and the US Dept of Commerce regarding review of changes in service.
- > I've requested details so we can state this accurately. We'll need to
- > say something in the analysis section to support this point if we wind
- > up including it.)

- > [5] Verisign's change has materially interfered with some number of
- > existing services which depend on the accurate, stable and reliable
- > operation of the domain name system. Treatment of misaddressed mail
- > and anti-spam services are among the most commonly cited complaints.
- > (We should expand this list but we don't have to include every
- > possible
- > claim.)

- > [3] Other groups, notably ISC, are introducing changes to thwart
- > Verisign's new service. The end result of a series of changes and
- > counterchanges is likely to lead to added complexity and instability
- > in the overall system. From a systems analysis perspective, this
- > sequence leads in exactly the wrong direction. Whenever possible, the
- > systems should be kept simple and the architectural layers cleanly
- > separated.

- > [1] Verisign's sudden introduction of this service has undermined the
- > community's sense of confidence that the critical services of the
- > Internet are being managed in a responsible manner.

- > (Additional opinions? Objections to the above list?)

> RECOMMENDATIONS

- > [3] Verisign should roll back the change and explore this matter more

- > broadly.
- >
- > [1] ICANN should examine the procedures in place concerning changes in
- > service. Even if Verisign simply rolls back their change, this issue
- > has triggered a strong concern as to whether the critical parts of the
- > Internet are being governed properly. Changes in procedures might
- > include changes in contracts, changes in review processes within ICANN
- > and/or broader community involvement.
- >
- > [1] The IAB and IETF should examine the specifications for the domain
- > name system and consider whether additional specifications could
- > improve the stability of the overall system. The role of error
- > responses and separation of architectural layers may be useful areas
- > of focus.



# **EXHIBIT B**



**VeriSign, Inc.**  
487 East Middlefield Road  
Mountain View, CA 94043

**Via FedEx and Facsimile**

October 3, 2003

John Jeffrey, General Counsel  
Internet Corporation for Assigned Names and Numbers  
4676 Admiralty Way #330  
Marina del Rey, CA 90292

**Re: VeriSign Wildcard Implementation**

Dear Mr. Jeffrey:

I am writing in response to the report submitted to the ICANN Board of Directors by ICANN's Security and Stability Advisory Committee ("SESAC") entitled, *Recommendations Regarding VeriSign's Introduction of Wild Card Response to Uninstantiated Domains within COM and NET* ("SESAC Report"), dated September 22, 2003 and to express concerns regarding the upcoming SECSAC meeting scheduled for October 7, 2003 on this subject.

On September 15, 2003, VeriSign implemented a wildcard initiative, which is fully standards-compliant as that term is defined in the applicable specifications. As part of this initiative, VeriSign launched its Site Finder service; a service already offered by 11 other TLD registries at the time of launch. Prior to implementing the service, VeriSign completed extensive research and testing. Our findings indicated that Internet users worldwide receive more than 20 million cumulative error messages a day during navigation with mistyped domain names or domain names that for technical purposes do not resolve on the Internet. With the launch of Site Finder, rather than receiving an error message with no useful information, users now receive a helpful web page with a clear message that what was entered could not be found and, offering helpful links to possible destinations and allowing an Internet search.

The service has been well received by millions of Internet users who appreciate receiving navigation tools as opposed to the 'dead end' of an error message. Indeed, growing numbers of Internet users are utilizing the navigation tools available through the service.

In reviewing the SECSAC Report, the SECSAC recommended suspension of the service based on what the Report claimed to be the "apparent" impact of the service. The SECSAC Report, and the recommendation, did not provide any data or facts on which to

VeriSign Wildcard Implementation

October 3, 2003

Page Two

base the recommendation. We understand that the October 7, 2003, SECSAC meeting in Washington DC will be an attempt by SECSAC to gather data to support the conclusions and recommendations already issued in its report. Unfortunately, and despite our requests, we were not given the opportunity to provide any input or supply any information to the SECSAC prior to the issuance of the report.

We had hoped to have a meaningful opportunity to describe the Site Finder service at the October 7 meeting as well as to provide information, to explain the services functioning and implementation, and to debunk some of the misconceptions currently being forwarded. We were informed yesterday by SECSAC Chair, Steve Crocker, that VeriSign will only be permitted to make a thirty-minute presentation. Respectfully, given the issues to be addressed and the structure of the meeting, this limited time will not be sufficient.

As with the issuance of the initial report, we are concerned regarding the organization of the meeting, the conclusions that appear already embedded in the agenda, the lack of structure around how the meeting will be conducted, and the lack of any terms of reference for the meeting. Further, we learned yesterday that the meeting will consist of a series of speakers, each of whom has already come out publicly against the service, followed by an unstructured open microphone session. We do not believe that this format is appropriate to objectively gather and substantiate the data upon which the SECSAC seeks to base the conclusions in its report. Further, given the speakers that SECSAC has selected, we have grave concerns that the meeting can be objective, constructive, or fair.

Prior to the meeting, please provide us with the committee's documented processes and procedures for conducting the type of meeting proposed for October 7, and any related proceedings. We have been unable to locate such documentation. We believe that these procedures at a minimum, should form the basis for the conduct of the meeting.

Furthermore, we believe that the meeting and any related proceedings should be conducted in accordance with the committee's charter and that the scope of the meeting will be limited to matters within the committee's charter. If this is not correct, please let us know.

In addition, we request that the meeting and any related proceedings be conducted in a manner consistent with ICANN's Bylaws. In this regard, at a minimum we would request that, in an effort to obtain broad and informed participation, the committee: 1) disseminate an objective description of the service and related technology beforehand; 2) disseminate the results of any investigations undertaken by the committee to date, including a description of the committee's investigative methodology, techniques, and sources of information; and 3) disclose the applicable standards for wildcard, and the

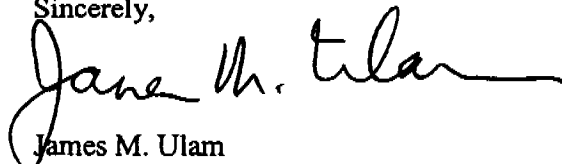
VeriSign Wildcard Implementation  
October 3, 2003  
Page Three

conclusions in the IAB report that the VeriSign wildcard is compliant with those standards.

Finally, given our discussion today, the circumstances surrounding the SECSAC report, and the limits on VeriSign's participation, I am concerned that certain basic steps to ensure an objective, open, transparent, and constructive meeting have not been taken. At a minimum, to plan and conduct a meeting such as this neutrally, objectively, and with integrity and fairness, the following conditions should have been present: 1) refraining from making public statements concerning VeriSign's wildcard initiative before the meeting; 2) discouraging the exertion of any influence on participants before the meeting; 3) encouraging open-mindedness and refraining from orchestrating the content presented at the meeting; 4) requiring committee members or any participants in the meeting to disclose their commercial affiliations prior to making any contributions during the meeting; 5) documenting the committee's process for establishing the meeting agenda, conducting the meeting, and considering any related matter; 6) ensuring that issues that are outside the proper scope of the meeting or the committee's charter are not considered; 7) establishing terms of reference for the meeting; 8) providing VeriSign an opportunity to respond to statements or data presented during the meeting; 9) requiring contributors to submit to the committee documents or other substantiation supporting the statements made during the meeting; and 10) requiring ICANN's manager of public participation and a representative of ICANN's Office of Ombudsman to be present to assist in ensuring fairness and no irregularities during the meeting. Given actions over the course of the last several weeks, it is apparent that certain of these conditions cannot now be met. We would hope that every effort will be made to conduct the meeting in a manner that can at least meet some of them.

I trust the committee will consider these issues before continuing down the course it has chosen for this meeting. However, we remain troubled by the manner in which the SECSAC issued its original report and the manner in which the October 7 meeting has been organized, the agenda formed, and VeriSign's participation limited.

Sincerely,



James M. Ulam  
Senior Vice President, General Counsel  
VeriSign, Inc.

cc: Paul Twomey, President and CEO, ICANN  
Steve Crocker, SECSAC

# **EXHIBIT C**



October 9, 2003

**VIA ELECTRONIC MAIL AND  
FACSIMILE**

John Jeffrey, General Counsel  
Internet Corporation for Assigned Names and Numbers  
4676 Admiralty Way #330  
Marina del Rey, CA 90292

**Re: VeriSign Wildcard Implementation**

Dear Mr. Jeffrey:

I write to express our objection to ICANN's groundless interference with VeriSign, Inc.'s ("VeriSign") business. In order to force VeriSign to shut down its Site Finder service, ICANN has threatened termination of our registry agreements without any sufficient legal or factual basis – while at the same time improperly excluding VeriSign from all of ICANN's deliberations. Representatives of ICANN also have made false public statements that VeriSign is violating the registry agreements and interfering with the stability of the Internet. Despite the fact that Site Finder is fully compliant with all applicable standards and the Registry Agreement, ICANN's wrongful conduct has left VeriSign with no practical alternative but to suspend temporarily the Site Finder service. ICANN's actions, however, constitute a clear breach of the Registry Agreement and unprecedented interference with VeriSign's existing contractual and other business relationships, for which ICANN and those acting in concert with it will be held fully responsible.

From the beginning, ICANN's proceedings in this matter have failed to comport with basic principles of fairness, openness or transparency, and have represented arbitrary action beyond any contractual or other jurisdiction ICANN might claim to possess. Through the date of ICANN's demand that the service be shut down, ICANN completely shut VeriSign out of ICANN's deliberations on Site Finder. Rather than consider the hard data and facts VeriSign tried to present, ICANN chose to conduct its affairs secretly and without the facts, relying instead on unsupported complaints of VeriSign's competitors and others in the community. For reasons discussed more fully below, it has become apparent to us that the desired outcome for VeriSign's wildcard initiative has been preordained from the beginning, driven in substantial part by the personal agendas of VeriSign's competitors and a few ICANN representatives.



ICANN's conduct constitutes a naked attempt to create "regulatory" jurisdiction for itself in violation of the Registry Agreements, the MOU, ICANN's bylaws, and applicable federal and state law. VeriSign calls on the ICANN Board of Directors immediately to convene a meeting with VeriSign to attempt to limit the ongoing and serious injury to VeriSign that ICANN has caused. We believe that an immediate and proper assessment of the true facts about Site Finder may allow this matter to be resolved now, before it escalates further beyond the control of the parties. Absent such a resolution, VeriSign will hold ICANN, and those acting in concert with it, fully responsible for damages incurred as a result of their actions.

### **VeriSign's Wildcard Implementation**

Applicable DNS standards have long recognized the existence and legitimacy of wildcard functionality. *See, e.g.*, RFC 1034 (1987). Wildcards are a well established feature of the DNS landscape, as demonstrated by the fact that the following top-level domains had supported wildcard functionality in their zones prior to VeriSign's introduction of Site Finder: .cx, .io, .mp, .cc, .museum, .nu, .ph, .td, .tk, .tv, and .ws. In its agreement with the registry operator for the .museum TLD, ICANN specifically permits the implementation of a wildcard. We are not aware of any significant concerns raised by ICANN or the Internet community with respect to the wildcard implementations within these TLDs. As operator of the registries for the .cc and .tv TLDs, we have not received significant expressions of concern or criticism in connection with supporting the wildcard functionality.

Through similar implementation of a standards-compliant "wildcard", as that term is defined in the applicable specifications, VeriSign's Site Finder service assisted millions of Internet users who appreciated receiving navigation tools and a clear message that what was entered could not be found, as opposed to the 'dead end' of an error message. Indeed, up until ICANN's demand that the service be shut down, large and growing numbers of Internet users were utilizing the navigation tools available through the service.

Moreover, the operational stability and security of the DNS and the Internet are of paramount concern to VeriSign, as clearly demonstrated by our longstanding record of operating the largest registries in the world. We have taken great care to ensure that our deployment of a wildcard within the .com and .net zones is fully compliant with applicable standards. By definition, therefore, such a deployment should not be the cause of any operational instability. Indeed, our wildcard implementation has had no adverse impact on the critical elements of the DNS infrastructure. Domain name registration and resolution services across all TLDs were occurring without any effect, the root server system continued to operate as usual, and there were no indications that the Internet's backbone was being affected in any way.



### The IAB Commentary

On September 19, 2003, the Internet Architecture Board ("IAB"), apparently acting in its capacity as a member of ICANN's Technical Liaison Group, issued a Commentary entitled, *Architectural Concerns on the use of DNS Wildcards* (the "IAB Commentary"). The IAB Commentary addresses what the IAB believes are various possible implications of implementing standards-compliant wildcards in a zone, with particular emphasis on the IAB's understanding of VeriSign's wildcard implementation.

It is first worth noting what the IAB Commentary did not say. The IAB found no inherent weaknesses in any components of the Internet's infrastructure, including the DNS or the presence of a wildcard in DNS standards. The Commentary explicitly acknowledges and recognizes the legitimacy of a wildcard within relevant DNS protocols. Further, the IAB did not find that the introduction of a wildcard within a zone necessarily has any significant adverse effects on the Internet infrastructure, or that the VeriSign wildcard failed to conform to applicable standards. In fact, the IAB emphasized that "technically, this was a legitimate use of wildcard records that did not in any way violate the DNS specifications themselves." Finally, the IAB did not suggest that VeriSign should change its implementation in any way or that ICANN should consider adopting any policies concerning the use of wildcards.

Further, the IAB commentary did not appear based on data relevant to the subject it was considering. Accordingly, the concerns expressed in the IAB Commentary, like those appearing in the SECSAC Report, would appear to be founded more on abstract theories and possibilities than on hard data.

The primary focus of the IAB Commentary is on a narrow range of applications and protocols that are not themselves a part of the Internet infrastructure, but which in some way interact with that infrastructure. More specifically, the IAB focused on potential implications for certain non-standards-compliant applications when a standards-compliant wildcard is deployed. On October 6, 2003, we submitted a technical response to the IAB Commentary that addresses the IAB's limited technical concerns.

While we felt the need to provide a technical response to the IAB Commentary, we question the appropriateness of the Internet Architecture Board assessing the implications of what is concededly a standards compliant wildcard implementation on protocols and applications that are not part of the Internet's architecture. We do not believe the IAB is the appropriate body to address these issues. Moreover, the very purpose of having standards would be undermined if those who are implementing the standards must yield to and accommodate those who choose to deviate from them. Yet this is precisely what the IAB seems to be suggesting in its Commentary. We therefore have reservations about the IAB's assessment of these applications issues.





The IAB, like SECSAC, has not disclosed the data on which its analysis rests, the methods by which the IAB collected such data, or the sources of the data. To the extent that ICANN has relied on the IAB, we request a copy of all information on which the IAB based its analysis and conclusions.

### **The SECSAC Report**

One week after VeriSign launched Site Finder, ICANN's Security and Stability Advisory Committee ("SECSAC") on September 22, 2003, submitted a report to the ICANN Board of Directors entitled, *Recommendations Regarding VeriSign's Introduction of Wild Card Response to Uninstantiated Domains within COM and NET* ("SECSAC Report").

In light of circumstances leading to the publication of this report, it would appear that SECSAC's conclusions and recommendations were prejudged from the outset. The committee's Chairman, Mr. Steve Crocker, supplied the most persuasive evidence of this when he circulated to committee members a draft report that already included the committee's opinions and recommendations. Mr. Crocker circulated this draft on September 19, 2003, just four days after VeriSign launched its wildcard initiative.

The analysis of the report, consisting of the facts and analysis section, did not exist, except for a bracketed comment that reads:

This is where we need to include the factual information to support the opinions and recommendations that follow. PAUL VIXE [sic] and SUZANNE, AMONG OTEHRS [sic], please dump stuff into this section.

SECSAC committee members apparently were unwilling or unable to supply any backfill to prop up the committee's opinions and recommendations prior to publication of its report. As a result, the final version of the report does not include any facts concerning the effects of VeriSign's wildcard implementation or any analysis to support the report's opinions and recommendations. Unable to provide any supporting "factual information," SECSAC was forced to abandon most of its pre-formed opinions and recommendations. The final report, nevertheless, states that there is evidence to support its recommendation to suspend Site Finder. To date, no such evidence has been produced.

SECSAC apparently was determined to publish its report without the benefit of VeriSign's input. Hours before the report was to be published, Mr. Crocker solicited VeriSign's feedback on a draft, but only concerning "small factual nits." In an affront to ICANN's stated core values and its commitment to operating in a fair and transparent fashion, Mr. Crocker stated that he had made this meaningless gesture in the "spirit of operating in an open, surprise-free mode."



In addition to limiting VeriSign's feedback to "small factual nits," SECSAC had previously declined VeriSign's offer to provide relevant data before the report was published, including: (1) a description of the methods and technologies used by VeriSign to implement its wildcard initiative; (2) the extensive body of data that VeriSign had developed in the course of researching and testing its wildcard implementation; (3) the views of VeriSign's senior DNS engineers on the subject; (4) the operational data that VeriSign collected since launching the initiative; and (5) the feedback that VeriSign had received from the Internet community since the launch.

Similarly, ICANN declined to consider this data when both SECSAC's Chairman and the Chairman of ICANN's Board abruptly cancelled scheduled meetings with VeriSign representatives to discuss the service prior to the SECSAC Report's publication.

Because SECSAC had not tested for any effects of VeriSign's wildcard implementation, had not collected a full set of relevant data, and had not analyzed such data, it could not make the statement that it wanted to make -- that the Internet's stability had been weakened. Instead, the final report concludes that VeriSign's wildcard implementation "appears to have considerably weakened the stability of the Internet" and "introduced ambiguous and inaccurate responses in the DNS." Not a single fact or piece of technical data was cited in support of these statements. Nonetheless, the report went on to call on VeriSign to suspend Site Finder.

ICANN adopted SECSAC's drastic recommendation to require a shut down of the Site Finder service, despite the fact that the committee itself was forced to acknowledge that it lacked any factual basis for believing that the Internet's stability had been weakened and when all of the data we have reviewed indicates that VeriSign's wildcard implementation has had no significant adverse operational impact on the DNS or the Internet. The opinions and recommendations contained in the SECSAC Report, and ICANN's subsequent actions based on the Report, are arbitrary and capricious, were not produced in an open and transparent manner, and unfairly and unjustifiably single VeriSign out for disparate treatment.

Further evidencing the unreliability of the SECSAC report and the unfairness of the committee's work were the lack of documented mechanisms to ensure that the committee's decision making was fair, reasonable, open, and transparent. Indeed, the manner in which SECSAC operated itself should have raised questions for the ICANN Board as to whether the SECSAC Report fairly represented the views of the committee or resulted from a fair and impartial consideration of VeriSign's wildcard implementation.

Based on the lack of evidence supporting the conclusions of SECSAC and the inherently unreliable and unfair processes followed by the committee, ICANN immediately should rescind its demand that Site Finder be shut down based on the SECSAC Report and direct SECSAC to retract the Report and conduct an objective,



independent review of VeriSign's wildcard initiative. The report certainly cannot form the basis for proper action by ICANN to shut down VeriSign's Site Finder service.

### **The October 7 SECSAC Meeting**

On September 30, 2003, SECSAC published an announcement on the ICANN web site that it would hold a special meeting on October 7, 2003, for the ostensible purpose of gathering input regarding VeriSign's wildcard implementation. We suspect, however, that the real purpose of this special meeting was to obtain the backfill needed to support the conclusions that Mr. Crocker had wanted to make in SECSAC's initial report. As with the formulation of the SECSAC response, Mr. Crocker's conclusions for the October 7, 2003 meeting also appear predetermined. In fact, in an email discussing the SECSAC meeting topics, Mr. Crocker listed the following items, among others, as "the main point of what we have to do:"

- RFCs are important but not definitive. (This needs to be expanded and supported.)
- Although other registries (museum, cc, tv and a few others) use this scheme, the magnitude of the change in this case makes it qualitatively different.... This matter should have been reviewed, and there have been discussions about limiting the use of wildcards in TLDs.
- All of the technical details are important, but so is the broader notion of trust. To what extent has this episode changed the expectations and level of trust in the Internet?

These statements do not represent an open, transparent, and objective consideration of VeriSign's Site Finder service. Rather, they demonstrate an arbitrary singling out of VeriSign for disparate treatment and, again, we are concerned, a preordained conclusion. Further, as addressed separately, we request that you adopt fair procedures for these and any other meetings, as distinct from the kind of staging demonstrated by Mr. Crocker's "agenda."

Although we participated in this meeting, we did so with reservations, as addressed in separate correspondence. Regardless, as a result of that meeting no hard data was presented in support of SECSAC's position.

In response to our criticism of the SECSAC process, ICANN on October 6, 2003, for the first time, offered to allow VeriSign to present information concerning Site Finder. VeriSign appreciates ICANN's belated recognition of VeriSign's concerns regarding the decision-making process with respect to Site Finder, and has responded separately.



### **Consequences for Improperly Interfering With Site Finder**

In the event that ICANN does not immediately rescind its direction to shut down the Site Finder service, VeriSign will suffer serious injury in the form of lost revenues and costs, and an interference with VeriSign's contractual relationships and prospective business advantage associated with the service. Furthermore, ICANN will have liability to VeriSign for these losses under explicit terms of the Registry Agreement as well as applicable federal and state laws.

For example, Section II.6 of the .com Registry Agreement, titled "Protections from Burdens of Compliance with ICANN Policies", provides:

ICANN shall indemnify ... and hold harmless Registry Operator ... from and against any and all claims, damages, liabilities, costs, and expenses ... arising solely from Registry Operator's compliance as required by this Agreement with an ICANN specification or policy ... established after the Effective Date....

The provisions of Section 6 are not subject to damage limitation provisions in the Registry Agreements.

Furthermore, under Section II.4 of the Agreement, as well as federal antitrust laws, ICANN is precluded from undertaking acts or policies that unreasonably restrain competition, from acting other than in an "open and transparent manner," or acting arbitrarily or inequitably against VeriSign, among other applicable legal obligations of ICANN. VeriSign believes that ICANN's actions violate each of these principals.

Finally, ICANN has used its actions with respect to VeriSign's Site Finder service to further delay other VeriSign services, including VeriSign's Wait List Service and Internationalized Domain Names service. These services already have been held up by ICANN for two years, at significant expense and injury to VeriSign, its partners, and to users. Nevertheless, ICANN informed us that it would make no progress on these services until the Site Finder service was taken down. Such arbitrary and cavalier interference in VeriSign's business, and disregard of ICANN's obligations under the Registry Agreement, only exacerbates the injury to VeriSign and raises additional questions as to whether ICANN sees its role as fostering innovation or stifling it.

Continued interference with VeriSign's business shall subject ICANN, and those individuals and companies who act in concert with it, to liability for the serious and continuing injuries resulting to VeriSign. In order to limit such ongoing injury to VeriSign, and in an attempt to resolve these important issues, we request an immediate negotiation of our differences. Absent a prompt resolution of these disputes, VeriSign



will be forced to seek other appropriate redress for ICANN's baseless interference with our business.

VeriSign does not waive, and hereby expressly reserves, any and all rights, claims and defenses that are in any way related to VeriSign's wildcard implementation.

Sincerely,

A handwritten signature in black ink that reads "James M. Ulam". The signature is fluid and cursive, with a long horizontal flourish extending to the right.

James M. Ulam  
Senior Vice President, General Counsel  
VeriSign, Inc.

cc: Ivan Moura Campos  
Vinton G. Cerf  
Lyman Chapin  
Mouhamet Diop  
Tricia Drakes  
Masanobu Katoh  
Veni Markovski  
Thomas Niles  
Michael D. Palage  
Alejandro Pisanty  
Hualin Qian  
Njeri Rionge  
Paul Twomey  
Steve Crocker  
Roberto Gaetano  
Francisco A. Jesus Silva  
John Klensin  
Mohamed Sharil Tarmizi

# **EXHIBIT D**

>  
>  
> SECSAC comments on VGRS  
>

> EXECUTIVE SUMMARY  
>

> We have followed the exchange between the IAB and Verisign in which  
> the IAB has raised particular technical issues regarding Verisign's  
> announced support for international domain names. Verisign has  
> responded that it is in the process of changing what it is doing to  
> address those concerns. This committee has no issue with what  
> Verisign is doing.  
>

> BACKGROUND  
>

> This is a brief description of what Verisign is currently doing and  
> plans to do.  
>

> Any DNS query to a Verisign server with an eighth bit set in an octet  
> within the second label of a domain name would receive an IP address  
> record (A RR) in its response, i.e., the address of a special purpose  
> Verisign server. The resulting action by the client would be to make  
> a connection (or use UDP to deliver its data) to the indicated  
> address. The current behavior of the Verisign server is to ignore  
> (silently drop) all connection requests and packets received other  
> than tcp/80 (HTTP).  
>

> Upon receiving a tcp/80 connection request, the Verisign server uses  
> the additional information in the HTTP request (it would also contain  
> the same domain name with an eighth bit set that was received in the  
> DNS  
> query) to identify the various international domain names (IDNs) that  
> could match the domain name. The client web browser will receive a web  
> page that presents the various alternatives and an opportunity to  
> download a plug-in that fixes the incorrect behavior, i.e., the plug-in  
> ensures that future DNS queries are properly encoded before being sent  
> to a DNS server. If the user chooses not to download the plug-in they  
> can simply select the desired site from the list offered and they will  
> be redirected there immediately.  
>

> Verisign has indicated that the planned behavior (scheduled for  
> deployment sometime after mid-May) in response to connection requests  
> to the special purpose server is as follows:  
>

- > - Connection requests to tcp/25 (SMTP) will be accepted but any mail  
> sent will be rejected with a 550 response code with human-readable  
> error message text. This will have the have effect of stopping the  
> attempted delivery of undeliverable messages.  
>
- > - Any TCP connection attempts to ports other than 80 (HTTP) and 25  
> (SMTP) will be reset, i.e., the same behavior any ordinary host would  
> exhibit when receiving a connection to a port without a listening  
> process.  
>

> - Any UDP packets received will result in an ICMP port unreachable  
> response, i.e., the same behavior any ordinary host would exhibit when  
> receiving a similar packet to a port without a listening process.

>  
>  
> DISCUSSION

>  
> The technical issue is that the DNS protocol requires that when names  
> as presented (QNAMEs) do not exist the correct reply is "non-existent  
> domain" (NXDOMAIN). However, as an operational matter, we also know  
> that a significant fraction of all queries are for NXDOMAINs (in the  
> case of the root servers it is the majority). Verisign is simply  
> observing that some number of the queries it gets are not really for  
> NXDOMAINs but are presented incorrectly because the software making  
> the query is "broken."

>  
> In that context they are providing a service for those users with  
> broken software. They are both providing a way for the user to get  
> the answer they actually want and providing a plugin that ensures the  
> user will not have this problem in the future (bootstrapping the  
> deployment of IETF standards).

>  
> The downside is that some number of users who do such broken things  
> (make queries for a non-existent domain name with the eighth bit set  
> in one of its octets) get a response with an address in it. If the  
> application being used by the client user is web-based (e.g., a  
> browser), then they will get the web page described above. All other  
> applications will not get the most desirable response, since preferred  
> response should have been NXDOMAIN from the DNS. This is not a  
> technically correct interpretation of the DNS protocol.

>  
> More generally, what Verisign is doing is deploying a mapping layer on  
> top of the DNS, in this case primarily to assist some number of users.  
> Similarly, the following registries are providing a mapping layer on  
> top of the DNS:

>  
>     <http://steve.tv>  
>     <http://k.mark.nu>  
>     <http://www.doron.cc>  
>     <http://dnssac.museum>

>  
> Specifically, they are returning "wildcard" address records for  
> non-existent domain names. The web page they display when attempting  
> to connect to a non-existent domain name is a sales pitch attempting  
> to sell it to you. In some cases the sales pitch is an auction  
> offering the domain name to the highest bidder.

>  
> The critical difference between what these example sites are doing and  
> what Verisign is doing is that Verisign is providing a service that  
> facilitates the use of the web by users, without offering a "sale."  
> The example sites above are using the opportunity to sell domain names  
> to the highest bidder.

>  
> If we are to take issue with what Verisign is doing, then it seems  
> reasonable to take issue with the others as well. However, although  
> the practices give us some discomfort, we can't really see a technical  
> basis for objecting to what Verisign is doing.

>  
>  
> BIBLIOGRAPHY



- > Verisign's original announcement:
  - > VeriSign Enables Companies to Enhance Their Online Brands in
  - > Virtually Any Language Using Internationalized Domain Names
  - > [http://www.verisign.com/corporate/news/2003/pr\\_20030114b.html](http://www.verisign.com/corporate/news/2003/pr_20030114b.html)
  - >
  - >
  - > IAB's response to the request:
  - > <http://www.iab.org/Documents/icann-vgrs-response.html>
  - > <http://www.icann.org/correspondence/iab-message-to-lynn-25jan03.htm>
  - >
  - >
  - > Verisign's response to the IAB response:
  - > <http://www.icann.org/correspondence/lewis-letter-to-lynn-07feb03.htm>
  - >
  - >
  - > Verisign's followup announcement:
  - > VeriSign Confirms Support for IETF IDN Standard
  - > [http://www.verisign.com/corporate/news/2003/pr\\_20030216.html](http://www.verisign.com/corporate/news/2003/pr_20030216.html)
-

# **EXHIBIT E**

To: Johan Ihren <johani@autonomica.se>  
cc: Mark Kosters <markk@verisignlabs.com>, secsac@icann.org  
Subject: Re: [secsac] wildcards in gtld servers  
From: Jaap Akkerhuis <jaap@sidn.nl>

Mark Kosters <markk@verisignlabs.com> writes:

> Looks like .biz is now running a wildcard in its zone much like  
.cc  
> and .tv. What do people think about this?

I think wildcards are a bad mistake that should be avoided  
(religious  
pov), but as others have commented it is not up to us or anyone  
else  
but the zone owner to decide the contents of the zone as long as  
these  
contents adhere to relevant RFCs.

So while I think this is bad I cannot claim that it is wrong.

A wildcard as in the normal DNS is within the protocol. If people  
do that, there is not a lot you can do. And, to make things worse,  
for .muesum it is a a requirement according to the contract they  
have with ICANN:  
<http://www.icann.org/tlds/agreements/museum/sponsorship-agmt-att13-16oct01.htm>

In a discussion on the centr-tech mailing list that started yesterday,  
it was noted by Scott Hollenbeck <shollenbeck@verisign.com>:

<quote>  
Prior to anything done by VeriSign, there were (and continue  
to be) at least 11 TLDs (.cc, .cx, .io, .mp, .museum, .nu, .ph,  
.td, .tk, .tv, and .ws) that have been using DNS wildcards for  
quite some time to offer either domain registration services  
or to provide web navigation assistance.  
</quote>

The discussion (about wildcards) started to spread around over other  
cctld related lists. I include here a reaction from .us/.biz on the  
centr-ga list, which includes parts of the discussion. Note, that  
people are confused. A "pure" wildcard as in:

```
*.tv.          60      IN      A      65.201.175.144
```

is different then a somewhat smarter redirecting, such as VGRS  
system. The latter one is a special form of wild carding (only when  
an eith bit is set). About the general case is not an IAB statement  
as far as I know, only on the VHRS system.

And yes, I'm with Johan here. I don't like wildcards either.

jaap



# **EXHIBIT F**

**[COVER and TITLE PAGE (DON'T NEED BOTH FOR PDF)]**

## **Redirection in the COM and NET Domains**

### **A Report from the ICANN Security and Stability Advisory Committee (SSAC)**

**1 July 2004**

**Prepublication copy; not for citation without permission from the  
Committee**

**Embargoed, July 1, 2004**

Table of Contents

<b><u>Preface and Acknowledgements</u></b> .....	3
<b><u>Executive Summary</u></b> <b><u>1.0 Introduction</u></b> .....	5
<b><u>1.0 Introduction</u></b> .....	6
<b><u>2.0 Summary of Events and Issues Raised by the Community</u></b> .....	7
<u>2.1 Events of September – October 2004</u> .....	7
<u>2.2 VeriSign’s Perspective</u> .....	10
<u>2.3 Design principles and good practice in the Internet technical community</u> .....	11
<u>2.4 ICANN, IP Addresses, Domain Names, Wildcards and Error Messages</u> .....	13
<u>2.5.1 Protocol Independence and the Effects on Mail Systems</u> .....	17
<u>2.5.2 SiteFinder</u> .....	19
<u>2.5.3 Workarounds and inconsistencies: Implications for end-users</u> .....	20
<u>2.6 Discussion and conclusion</u> .....	22
<b><u>3.0 Findings and Recommendations</u></b> .....	24
<b><u>Appendices</u></b> .....	26

## Preface and Acknowledgements

This is a report about a sequence of actions undertaken by VeriSign, Inc., the reactions of the Internet community, and the implications of the chain of events for the stability and security of the Internet. The Security and Stability Advisory Committee (SSAC)<sup>1</sup> is an advisory committee to ICANN (the Internet Corporation of Assigned Names and Numbers). The Committee advises “the ICANN community and Board on matters relating to the security and integrity of the Internet's naming and address allocation systems” (Appendix 1). As an advisory committee, SSAC offers independent advice to the ICANN board, the ICANN staff, and the various ICANN supporting organizations, councils and committee as well as to the technical community at large. The Committee has no official authority to regulate, enforce or adjudicate. Those functions belong to others, and the advice offered here should be evaluated on its merits.

Formed in the wake of the events of September 11, 2001, the Committee is drawn from industry, academe, and non-profit organizations in the U.S. and abroad (Appendix 1) and reports directly to the ICANN Board. The Committee is composed of volunteers, who serve without pay, each a technical contributor in his or her own organization and in the community at large. There is broad representation of all segments of the domain name system community. We have members who operate root servers, top level domain servers (both generic and country code), registrars and address registries. Some of our members are network security experts or conduct network security research. The Committee draws from the commercial and not-for-profit sectors, has broad geographic representation and has broad representation across industry and academe.

Because the Committee is composed of people actively working in the field, conflicts of interest arise from time to time. Committee members are expected to declare conflicts of interest, whether actual, potential or apparent, but Committee members are not required or expected to recuse themselves. In the current activity, several members work for VeriSign or for companies doing business with VeriSign or work for companies competing with VeriSign. In all cases, the members have made their situations clear and have been careful to provide technical information without attempting to influence others on the Committee. SSAC's policy concerning conflict of interest is posted to the committee's Web site (<http://ssac.icann.org/conflict-of-interest.htm>). Biographies and declarations of potential sources of conflict of interest are included in Appendix 2.

Like any such effort, preparing this report owes much to many:

- Two public meetings were held in Washington, D.C. on 7 October 2003 and 15 October 2004 and chaired by Stephen Crocker. We are grateful for venues and logistical support provided by the Center for Strategic and International Studies (CSIS) and the Academy for Educational Development and their staffs. Arnaud

---

<sup>1</sup> <http://secsac.icann.org/>. We note that the original acronym “SECSAC” denoting this Committee has been changed to “SSAC”.



de Borchgrave, Senior Adviser and Director at CSIS, hosted the CSIS meeting on 7 October and gave the welcoming talk.

- Both meetings benefited from considerable organizational help from Marilyn Cade and Elana Broitman. TK provided transcription services, and Steve Conte, John Crain and TK supplied network support.
- Paul Ott and Ari Elias-Bachrach.com ordered and analyzed the comments received on "secsac-comment" (now called SSAC-COMMENT).
- Fourteen scheduled speakers offered analysis and made presentations at these meetings: Steven Bellovin, AT&T; Benjamin Edelman, Harvard University; Chuck Gomes, VeriSign; Hakon Haugnes, Global Name Registry; Scott Hollenbeck, VeriSign (7 and 15 October 2003); John Klensin, John C. Klensin and Associates; Matt Larson, VeriSign; Rusty Lewis, VeriSign; Geir Rasmussen, Global Name Registry;; Anthony Renzette, VeriSign; David Schairer, XO Communications; Richard Smith, privacy consultant; Ben Turner, VeriSign; Paul Vixie, ISC. kc claffy also made substantial contributions as did Mike St. John and Suzanne Woolf. James Galvin, Principal at eList express, provided continuous staff support to the committee during the process,
- Many people attended or listened in on the meetings where they offered thoughtful comments and observations. Many more participated in the online discussions. To list them all would overwhelm this document so however inadequately, the Committee offers its blanket thanks to the community.

Doug Maughan, Cyber Security Program Manager at HSARPA, U.S. Department of Homeland Security, and SRI, International under contract xxxx-xx-xx-xxxx, provided financial support for this report. We are grateful to Victoria Stavridou, Steven Cheung and Lori Truitt for their assistance.

Stephen Crocker and Amy Friedlander wrote and edited this report under the general direction of the Committee.

**Executive**

**Summary**

## 1.0 Introduction

On 15 September 2003, VeriSign, Inc. changed the way that NET and COM registries responded to domain names that were non-existent either because the name had been mis-entered, the name had lapsed, or the name had never been registered. In so doing, the company changed the way that the domain name system (DNS), a fundamental component of the Internet architecture, works for two large top-level domains. VeriSign's actions consisted of a period of private research followed by a launch of service on 15 September 2003. The changes in service were aimed at the World Wide Web (HTTP) but had unexpected effects on the other parts of the Internet. VeriSign refers to this set of changes as the introduction of its SiteFinder service, focusing attention on the functionality provided to Web users who mistyped domain names and were routed to VeriSign's servers. Our primary focus is not SiteFinder, per se. Rather, our focus is two-fold: that core registry operations were modified, thereby changing existing services, and that the change was introduced abruptly without broad notice, testing, refinement or community agreement. Since our concern here is on both the change itself and the method of introducing the change, we refer to both with the terse shorthand "VeriSign's action".

The effects rippled through multiple communities who depend upon predictable operation of the Internet including registrars, registrants, system administrators, Internet service providers (ISPs) and, most specifically, end-users. Outcry from the technical community, which is described in more detail in Section 2.1, as well as formal advisories prepared by the Internet Architecture Board (IAB) and the ICANN Security and Stability Advisory Committee (SSAC) identified a series of issues arising from VeriSign's action and the reaction to it that affected security and stability. VeriSign took the position that its action was compliant with protocol specifications and therefore did not affect security and stability of the Internet. But as SSAC's advisory observes, "Security and stability [are] not limited to a narrow interpretation of the technical specifications of the protocol documents; it also includes engineering, operational, business, and policy issues" (Appendix 3). How technology and organization have intertwined in the development of protocols, codes of conduct and good practice to build a robust Internet is addressed in more detail in Sections 2.3 and 2.4.

During the development of the Internet over the last 30 years, the technical community has grappled with the tension between regulation of infrastructure services on behalf of the public and promoting competition among the private sector interests who provide these services. These relationships derive from three sets of policy considerations, technological innovation, economic competition and reliable infrastructure service. How these relationships will play out at national and international levels have yet to be fully articulated. As part of the information and communications infrastructure and also a source of and basis for innovation, the Internet and discussions about the Internet go to the intersection of all three policy areas.

Ultimately, the matter is one of fostering and sustaining trust. Most Web and e-mail end-users have seen error messages when a name fails to resolve. These error messages

usually come either as a Web page displayed on their browsers, perhaps supported by a well-known search service, or as a bounced message in their e-mail in-boxes. And many, if not most, end users know the rough contours of the explanation: That the name is supposed to correspond to a sequence of numbers that represent an address and that the registry databases maintain the relationship between the name and the address. The sophistication of the addressing system and the complexities of how this communication actually works across a range of heterogeneous platforms, devices and networks are typically and intentionally hidden (that is, the typical user does not see all of the steps in the transmission). Most users outside the technical communities rely on intermediary services, such as Internet Service Providers and technical services units in their organizations, to keep their systems up and running so they can go about doing interesting things.<sup>2</sup> For the public, information technology systems require trust: “They [the systems] must do what they are required to do – and nothing else.”<sup>3</sup>

## **2.0 Summary of Events and Issues Raised by the Community**

The section describes the events of September/October 2003 presents a brief summary of VeriSign’s SiteFinder; provides an overview of Internet design principles, naming, IP (Internet Protocol) addresses and wildcards; and offers an analysis of the issues that have been raised.

### 2.1 Events of September – October 2004

---

<sup>2</sup> Systems administrators can run traces on the system to assess performance and identify errors so the system is both seamless and transparent.

<sup>3</sup> Computer Science and Telecommunications Board, National Research Council, *Making IT Better: Expanding Information Technology Research to Meet Society’s Needs* (Washington, DC: National Academy Press, 2000), p. 114.

VeriSign, Inc.'s corporate Web pages describe the company's products and services. According to the company's Web page, VeriSign's COM NET Registry "is the authoritative registry for .com and .net domain names and supports registrars who offer these registrations to their customers." VeriSign's COM NET Registry "manages relationships with more than 100 ICANN-accredited Registrars who submit over 100 million domain name transactions daily" (Key terms and concepts will be described hereafter in section 2.3.).<sup>4</sup> On 15 September 2003, VeriSign changed the way the COM and NET registries responded when presented with uninstantiated names. That is, names that did not exist because the name had been misspelled, had lapsed or had never been registered. Instead of returning the standard error code, the name server responded with the address of one of VeriSign's servers. Web browsers were directed to a site called SiteFinder.com; everything else either failed or, as in the case of mail, behaved in ways unexpected by the sender.

News of VeriSign's action was reported in the Wall Street Journal (5 September 2003) and Computer Business Review (9 September 2003), before the actual release, and on the day itself by the New York Times (15 September 2003). It was characterized in the press as a potentially highly lucrative business venture that affected Web users. "VeriSign Mulls Way to Make Money from Typos" read the headline in Computer Business Review. And the story began, "VeriSign Inc. is testing changes to its domain name system services, which could generate tens of millions in revenue a year for itself and partners, and which would impact the way almost every internet user surfs the web."

Response from the technical community to VeriSign's change was swift in both formal communications to ICANN from organizations in the U.S. and abroad and on the mailing list servers.<sup>5</sup> A petition to ICANN garnered approximately 18,000 signatures, and 220 messages were sent to ICANN's wildcard-comments address between 27 September and 9 October 2003, three days after VeriSign disconnected SiteFinder. By 19 October, comments to ICANN totaled 330. An analysis of the comments received by 9 October cited specific problems with the network, patches, user interfaces, e-mail, link checkers, configurations that rely on a domain name that is not registered, and non HTTP/SMTP protocols. The problems clustered into four broad topics: trust, registration, "Things Break" and user services and choice. In the analyses that followed, the topics raised by the broad technical community have consistently re-occurred.<sup>6</sup>

On 19 September 2003, four days after the release of SiteFinder.com, ICANN issued its first advisory requesting VeriSign suspend the service voluntarily given concerns that had been expressed about the threat that VeriSign's actions posed to stability and security. VeriSign declined to do so in a communication dated 21 September 2003, arguing that such action was "premature", absent collection and review of available data. On 3

---

<sup>4</sup> Naming and Directory Services, VeriSign COM NET Registry; <http://www.VeriSign.com/nds/naming/registrar/index.html?sl=070406>; verified 21 April 2004.

<sup>5</sup> VeriSign's Wildcard Service Deployment, Internet Community Comments; <http://www.icann.org/topics/wildcard-history.html>; verified 21 April 2004.

<sup>6</sup> Thomas Roessler, SiteFinder: Community Comments, At-Large Advisory Committee, Carthage, October 2003; <http://www.icann.org/presentations/roessler-wildcard-carthage-27oct03.pdf>; verified 22 May 2004.

October and following preliminary reports by SSAC and the Internet Architecture Board (IAB), ICANN more forcefully demanded that VeriSign suspend “the changes to the .com and .net top-level domains introduced on 15 September 2003 by 6:00 PM PDT on 4 October 2003.”<sup>7</sup> On the same day that the letter was sent to VeriSign, ICANN also issued a public advisory, noting widespread concern expressed about the implications of the changes for the stability and security of the Internet, stating:

For all these reasons, ICANN has today insisted that VeriSign suspend the SiteFinder service, and restore the .com and .net top-level domains to the way they were operated prior to 15 September 2003. If VeriSign does not comply with this demand by 6:00 PM PDT on 4 October 2003, ICANN will be forced to take the steps necessary to enforce VeriSign's contractual obligations.<sup>8</sup>

Despite its objections, VeriSign complied. The service has been suspended, ostensibly temporarily, and the matter remains unresolved. Relevant correspondence is included as Appendix 4.

As of October 4, the suspension was characterized as “temporary, pending full review of the technical issues by IAB and SSAC.”<sup>9</sup> On 22 September, SSAC had issued a preliminary advisory as a first step in its examination of this situation (Appendix 3). In this document, the Committee outlined a series of considerations:

- Conformance with the protocol specifications as defined by the engineering community.
- Conformance with accepted best practices and operational procedures as defined by the engineering and operational communities.
- Consideration of the technical stability and security of the domain name system and the Internet as a whole in light of the both the change introduced by VeriSign and the corresponding changes being introduced by others.
- Current procedural and governance controls to assure review and analysis of changes to the critical components of the Internet.
- Public confidence in the stability and reliable operation of the Internet.

The Committee further opined, “VeriSign's change appears to have considerably weakened the stability of the Internet, introduced ambiguous and inaccurate responses in the DNS, and has caused an escalating chain reaction of measures and countermeasures that contribute to further instability.”<sup>10</sup>

---

<sup>7</sup> Letter from Paul Twomey to Russell Lewis, 3 October 2003; <http://www.icann.org/correspondence/twomey-to-lewis-03oct03.htm>; verified 22 May 2004; included in Appendix 3.

<sup>8</sup> Advisory, 03 October 2003; <http://www.icann.org/announcements/advisory-03oct03.htm>; verified 22 May 2004; included in Appendix 3.

<sup>9</sup> Letter from Paul Twomey to VeriSign, 6 October 2003; <http://www.icann.org/correspondence/twomey-to-verisign-06oct03.htm>. Included in Appendix 3.

<sup>10</sup> Message from Security and Stability Advisory Committee to ICANN Board, 22 September 2003; <http://www.icann.org/correspondence/secsac-to-board-22sep03.htm>; verified 4 June 2004.

The Committee then called for inputs and held an open meeting on Tuesday, 7 October 2003, in Washington, DC at which there were presentations from industry representatives as well as opportunities for questions. A second meeting was scheduled on Wednesday, 15 October 2003, also in Washington, D.C., to provide VeriSign with an extended period of time to present information and research it had developed in reference to its service. Representatives from VeriSign offered a vigorous explanation of its actions. Both meetings were Web cast and questions taken from remote participants by telephone and e-mail. Transcripts for both meetings are available at <http://ssac.icann.org/>. Presentations are available at <http://www.icann.org/presentations/>.

## 2.2 VeriSign's Perspective

From the outset, beginning with the article in *Computer Business Review*, VeriSign consistently described SiteFinder as an aid to end users that provided Web search assistance for those who were potentially stymied by an apparent dead end. In its presentations on both 7 October and 15 October, representatives of the company emphasized customer satisfaction, while acknowledging refinements to their service that they had instituted in response to problems that had arisen. In this section and Appendix 5, we summarize the main technical points of VeriSign's position; critiques that surfaced in the public meetings are discussed in Section 2.5.2

At the 7 October public meeting, Scott Hollenbeck, Director of Technology for the VeriSign COM NET Registry, described SiteFinder as follows: Users who entered a URL ending in NET or COM that could not be resolved to a Web site were offered a page, hosted by a VeriSign server, offering alternative sites that seemed similar to the unresolvable address. The Web page also offered users "the ability to surf the web or something else or to search a list of fairly well-known categories, "From the DNS perspective," he began his presentation, "it [SiteFinder] involved putting a wildcard A record in the com and net zones as described in RFC 1034."<sup>11</sup> For protocols, other than HTTP, "we provide a protocol-defined response."<sup>12</sup>

VeriSign argued that its changes to DNS were compliant with the relevant protocols, pointing to other top-level domains such as MUSEUM in which wildcards were used, and that the service was useful to end users. The company expanded on these points in four separate presentations at the 15 October meeting in which they described a lengthy process of research and development, examination of relevant protocols and user studies. Presentations addressed concerns that had been raised by the technical community since the launch and the steps that they with their technical review panel of outside experts had taken to address these concerns.

VeriSign had assembled a Technical Review Committee (TRC) composed of seven industry experts drawn from outside the company together with four of VeriSign's

---

<sup>11</sup> SSAC Meeting Real-Time Captioning, 7 October 2003, [p. 7].

<sup>12</sup> SSAC Meeting Real-Time Captioning, 7 October 2003, [p. 7].

engineers, who described their role as to “listen and answer questions.”<sup>13</sup> The TRC reviewed the consequences of VeriSign’s action by examining the effect on different protocols. In the “Summary of TRC Findings” as presented by Hollenbeck (see Appendix 5, slide [9]), the effects on the top 10 protocols were listed: HTTP, SMTP, DNS, IRC, epmap, pop3, microsoft-ds, netbios-ns, netbios-ssn, ftp. The summary characterizes the user experience before SiteFinder and the user experience with SiteFinder, provides a judgment of the change, and suggests a remedy, if applicable.

In all cases except HTTP and SMTP, the user experience before the change is that “‘Name error’ from DNS is presented to the user through their application”. In the case of HTTP, the user received either an error message or a search page from a local application. In the case of SMTP, mail addressed to an uninstantiated name is rejected as having an invalid recipient address. After the change, VeriSign’s Technical Review Committee noted that for HTTP, there was an improvement for some users. In all of the other protocols except netbios-ssn, VeriSign’s Technical Review Committee commented, “users may notice a delay compared to previous behaviour.” VeriSign’s TRC did not comment on netbios-ssn. VeriSign’s Technical Review Committee further suggested a number of remedies, generally requiring either that users change their software or change their behavior.<sup>14</sup>

But at this meeting as in the 7 October meeting, the focus of VeriSign’s position rested on the usefulness of the service to end-users and the levels of satisfaction that end users had expressed. Ben Turner, Vice President of VeriSign, cited survey research in which 76 percent of the respondents rated the SiteFinder site excellent or very good and only 4 percent rated it poor.<sup>15</sup> Finally, Rusty Lewis, Executive Vice President, closed the series of presentations that senior members of the company gave on October 15, by acknowledging that advanced notice was appropriate and that if the service were to be re-launched, there would be at least 30 to 60 days of notice. He emphasized the importance of adhering to accepted best practice and concluded, “[W]e believe that encouraging innovation at the core is just as important as encouraging innovation at the edge.”<sup>16</sup>

### 2.3 Design principles and good practice in the Internet technical community

To much of the user public, the Internet is variously conceived as a cloud, a network of networks, or a souped-up telephone system with sound and images, delivered via a home computer or some other device. To the technical community, it is a set of protocols that

---

<sup>13</sup> VeriSign Site Finder: Technical Review Panel Summary, Scott Hollenbeck, Director of Technology, VeriSign, in Site Finder Review, SECSAC Meeting, 15 October 2003, Washington, DC, slide [4]; <http://www.icann.org/presentations/turner-secsac-dc-15oct03.pdf>; verified 26 May 2004; included in Appendix 5.

<sup>14</sup> The summary page of this presentation (slide [8]) claims “no catastrophic problems” and “no identified security or stability problems.” Additionally, “most issues deemed minor or inconvenient.” The summary page acknowledged some software changes might be required. This summary does not reflect our reading of the Technical Review Committee’s specific findings.

<sup>15</sup> SSAC Meeting Real-Time Captioning, 15 October 2003, [p. 14].

<sup>16</sup> SSAC Meeting Real-Time Captioning, 15 October 2003, [p. 16].



enable signals to be transmitted over heterogeneous devices and multiple systems.<sup>17</sup> Historically, the achievement has been both organizational, embodied in the IAB and the Internet Engineering Task Force (IETF), and technological, embodied in the logical architecture as well as in the lines, routers, servers and multitude of end-user devices. The assumptions, values, expected codes of conduct and practice have proved as important as the hardware and software engineering.

Much has been made of the “open” character of the Internet, and with time and success, the notion of “open” has taken on a broad range of meanings in diverse contexts. Within context of the engineering, the Internet is based on the notion of an open architecture, meaning that an implementation can “plug in” if it meets the relevant protocol, and is an “open data network,” meaning that it can operate over and support highly heterogeneous technologies and applications, including those yet to be imagined.<sup>18</sup> This commitment to openness does not mean some version of “anything goes.” Rather, the diversity and complexities that can arise from the commitment to an open architecture are enabled by an equally deep commitment to a discipline of a minimal set of core protocols that are kept very stable. This core includes the Internet Protocol (IP), the routing and the domain name system, which shall be explained further in the next section.

The stability at the core supports innovation both above and below this set of core protocols. Below it is where new transmission technologies and new signaling protocols have been introduced, including the Ethernet, the increase of speeds from 50k bits per second to multi-gigabit technologies and the use of both wired and wireless transmission media. Above it are the new protocols, new applications and new services, such as the World Wide Web and many other innovations large and small, such as search engines, e-commerce, voice over IP (VoIP) and so on. We emphasize these innovations above and below the core require the core to be kept under very tight discipline and to be both small and stable.

Often this arrangement of a robust active set of innovations above the core and equally robust set of innovations below are pictured as an hourglass figure in which the least number of required elements appear at the narrowest point with more and more choices – and complexity – above and below. In this hourglass image, applications and services above the core are at the edge of the network not at the control of the network operators. As a result, innovation, intelligence and complexity occur at the periphery or the edge, and the network, or the core, provides only simple, basic levels of service. Known as the “end to end argument,” this design posed a radical challenge by the original Internet architects to existing principles behind the public switched telephone network (PSTN), where intelligence was concentrated in the center where network operations were controlled and “dumb” devices were located at the periphery where end users had access to them.

---

<sup>17</sup> We recognize that the key breakthrough was packet switching and the conversion of the signal from analog to digital.

<sup>18</sup> This history is well known. We rely in part on the summary provided by the Computer Science and Telecommunications Board; see Computer Sciences and Telecommunications Board, National Research Council, *The Internet's Coming of Age* (Washington, DC: National Academies Press, 2001), pp. 36-40.

The original architects of the Internet made a second fundamental decision: to divide the complexities of the network by employing the principle of layering. Application developers may build on the lower layers. As a result, there has been a profusion of innovation on a stable base. Conversely, innovative applications have respected the boundary between applications and core services, which remain stable and unaffected by the ferment of creativity the network can support. Thus, making changes to the center is necessarily difficult, slow and predictable.

At the heart of this logic is the robustness principle, summed up in the maxim: “Be conservative in what you send and liberal in what you receive.”<sup>19</sup> Related to the robustness principle is the principle of least surprise: “Do what you think the other party is expecting.” As a practical matter, given the challenges of networking across heterogeneous systems and technologies and the requirements of robustness and simplicity, there has arisen a careful process of review, discussion, testing and refinement. This is part of the popular notion of the Internet’s “open” character: That these discussions take place publicly and with broad input from concerned communities within the framework of the IETF and the resulting protocol reflects consensus among those concerned. The process serves the highly practical purpose of enabling change to occur in a heterogeneous technological environment in a way that preserves both heterogeneity and stability. The results of these consensus deliberations are protocols that set forth the agreed upon conditions that an implementation must meet to work.

#### 2.4 ICANN, IP Addresses, Domain Names, Wildcards and Error Messages

As the preceding section suggests, the “Internet” is an organizational phenomenon as well as a set of logical relationships and configurations of equipment. The issues raised by VeriSign’s action lies precisely in the intersection of these three elements, in particular in the relationship between domain names and the associated IP addresses and the way that this relationship is managed.

Outside the technical communities of network engineers and software developers, the IP address is typically thought of as the sequence of numbers that identifies the physical server connected to the Internet; the subtleties of hosts, networks and routers are usually glossed over. More precisely, the IP address refers to the numbers that identify each sender or receiver of information that is sent in packets. It has two parts: the identifier (or string of numbers) associated with a particular network on the Internet and the identifier (or string of numbers) associated of the specified device or machine or within that network.

The domain name is the term associated with an institution, organization, entity or even individual and is also the term that is more widely recognized. Again, many of the distinctions and implications of root, top level, second level and sub-domains, are generally not well understood outside the technical communities. Indeed, many end-users probably confuse the familiar second level domain (for example “un” for the United

---

<sup>19</sup> CSTB traces the articulation of this maxim to Jon Postel in 1979; see Ibid, p. 39, n. 15.

Nations) with the domain name itself, not realizing that the fully qualified domain name is un.org. The hierarchy is reflected in the sequence from right to left with the top level domain name to the right of the ".", the familiar second level domain immediately to the left of the ".", and the sub-domain (if any) to the left of the second level domain. A "zone" is one or more levels in the hierarchy (root, top level, second level, and so on) handled by a name server.<sup>20</sup>

ICANN manages the distribution of IP addresses and domain names through an organizational system of registries, registrars and registrants.<sup>21</sup> ICANN accredits domain name registrars<sup>22</sup> and has the ultimate responsibility for ensuring that domain names are uniquely assigned. The operation of the registry databases and the actual work of registering domain names and maintaining the relationships fall to the registries themselves. VeriSign operates the registry for the very large NET and COM top level domains (TLDs).

The domain name system (DNS) is a set of databases and programs that allow the fully qualified domain name to be translated into or linked to an IP address through a series of queries. The fundamental concepts behind DNS are well-established and were set forth

---

<sup>20</sup> SSAC has recently set forth a set of recommendations concerning delegation of zones and sub-zones; see DNS Infrastructure Recommendation of the Security and Stability Advisory Committee SAC 005 Document 005 Version 1, 1 November 2003; <http://www.icann.org/committees/security/dns-recommendation-01nov03.htm>; verified 26 May 2004.

<sup>21</sup> The glossary provided by ICANN (<http://www.icann.org/general/glossary.htm>; verified 25 May 2004) provides the following definitions for potential registrants, that is, those who wish to register a domain name. For *Registrar*: "Domain names ending with .biz, .com, .info, .name, .net or .org can be registered through many different companies (known as "registrars") that compete with one another. A listing of these companies appears in the Accredited Registrar Directory. The registrar you choose will ask you to provide various contact and technical information that makes up the registration. The registrar will then keep records of the contact information and submit the technical information to a central directory known as the "registry." This registry provides other computers on the Internet the information necessary to send you e-mail or to find your web site. You will also be required to enter a registration contract with the registrar, which sets forth the terms under which your registration is accepted and will be maintained." For *Registry*: "The 'Registry' is the authoritative, master database of all domain names registered in each Top Level Domain. The registry operator keeps the master database and also generates the "zone file" which allows computers to route Internet traffic to and from top-level domains anywhere in the world. Internet users don't interact directly with the registry operator; users can register names in TLDs including .biz, .com, .info, .net, .name, .org by using an ICANN-Accredited Registrar."

<sup>22</sup> "Accredit' means to identify and set minimum standards for the performance of registration functions, to recognize persons or entities meeting those standards, and to enter into an accreditation agreement that sets forth the rules and procedures applicable to the provision of Registrar Services." (See <http://www.icann.org/faq/#WhatisICANN>; verified 23 May 2004.)

in Requests for Comment (RFCs) 1033, 1034 and 1035, dated November 1987.<sup>23</sup> As described in RFC 1034, DNS has three major components: the domain name space and resource records, which are stored in what computer scientists call a “tree structure”; name servers, which have information about the domain’s tree structure; and resolvers, which obtain information from name servers in responses to a query from a client. The tightly defined operation wherein an unambiguous name is presented to the system and the system returns a unique IP address is called “Lookup”. A broader operation in which the system responds to a query by presenting a set of connections is a “Directory” operation.

RFC 1034 allows for flexibility in the way that DNS can respond to queries for uninstantiated names. It describes wildcards as “instructions for synthesizing” information associated with a name. The original specifications are not clear when it is appropriate to use wildcards, but at the time, wildcards were anticipated for use in mail applications: “This facility is most often used to create a zone which will be used to forward mail from the Internet to some other mail system. The general idea is that any name in that zone which is presented to server in a query will be assumed to exist, with certain properties, unless explicit evidence exists to the contrary.”<sup>24</sup>

Good practice regarding wildcards has evolved. But as a commentary on the use of wildcards prepared by IAB and released 19 September 2004 observes: “Even after twenty years of experience with the DNS, the effects of unexpected uses of wildcards can still be quite surprising, because the small but fundamental way in which they change the record lookup rules has a nasty way of violating implicit (or, sometimes, explicit) assumptions in deployed DNS-using software.” The report has been included as Appendix 6 and its principal points summarized in the following paragraphs.

The IAB acknowledged that the wildcard mechanism had been a part of the DNS protocol since the specifications were originally written. However, the mechanism was also understood to be tricky, especially when more than one protocol is invoked. DNS returns one of three responses to a query: success, no data (which means that the name exists but the does not have information about it), and no such name. When wildcards are present, the success and no data responses can be conflated and the no such name response cannot occur. Hence, in the instance of SiteFinder and other similar services, mistakes in typing can be processed, rather than rejected, and the user re-directed to a page that provides information. But this may be, in a sense, a false positive since the system appears to work when in fact it is masking an error, and an error is a legitimate

---

<sup>23</sup> Requests for Comment (RFCs) are both a system of communication and a way of documenting developments and proposed developments within the Internet technical community. They may be found at <http://www.ietf.org/rfc.html>. RFC 1033 is the “Domain Administrators Operations Guide” (M. Lottor, SRI International, November 1987). RFC 1034 is “Domain Names – Concepts and Facilities (P. Mockapetris, ISI, November 1987). RFC 1035 is “Domain Names – Implementation and Specification (P. Mockapetris, ISI, November 1987). These have been updated over the years. A useful introduction to DNS for non-experts is the Internet Society’s briefing by Daniel Karrenberg, The Internet Domain Name System Explained for Non-Experts, ISOC Member Briefing #16. It is available at <http://www.isoc.org/briefings/016/>; verified 23 May 2004.

<sup>24</sup> RFC 1034, Section 4.3.3.

form of information. Applications that rely on the “no such name” response fail since the “no such name” no longer occurs.

The IAB analysis identified two main problems:

- the authoritative servers for these two zones no longer give out "no such name" responses for any possible name in these zones, and
- every possible name rooted in one of these zones which, until this change, did not exist at all, now has a synthesized address record pointing at a "redirection server" run by the operator of this zone.

A series of implications was then identified that affected Web browsers, e-mail, spam filters, automated tools, error messages, interaction with other protocols, charging, single point of failure, privacy, use of reserved names, and undesirable work-arounds. From an architectural point of view, the mechanism violated two fundamental principles: Robustness and the Principle of Least Astonishment (see discussion in Section 2.3). It is possible to use wildcards in certain situations, the commentary concluded, and the Museum Domain Management Association claims to have done so (Appendix 7). However, theirs may be relatively rare case where the domain is restricted to a “clearly bounded community.” “Warning flags”, the IAB cautions, were that the action:

- affected more than one protocol, and
- was done high enough up in the DNS hierarchy that its effects were not limited to the organization that chose to deploy these wildcard records.

## 2.5 Issues

VeriSign’s action consisted of a change to the registry operations and a change to the operation of those servers. It had two adverse effects. First, it changed the way the registry functioned by returning seemingly legitimate addresses for domain names which really did not exist. Second, it introduced this change abruptly, without public notice, without coordination, and without independent testing and refinement. Each of these, the fact of the change and its abruptness, violated community standards and caused harm to large numbers of people and enterprises. In this section, we describe those changes and those effects in greater detail.

Prior to VeriSign’s action, when the name server<sup>25</sup> received a query for an uninstantiated name (which might be a name that had not been registered, one that had previously existed but did so no longer, or a misspelling of an existing name), the standard error code RCODE3 was returned, thus alerting the requester that the name was not instantiated. After VeriSign’s action, the VeriSign registries responded to queries for an uninstantiated name by returning the IP address of one of its servers as if the requested name were instantiated and fully in operation. Instantiated names were not affected.

---

<sup>25</sup> We note that only NET and COM were affected by VeriSign’s action; other domains were unaffected. However, for purposes of simplicity, we have described the events in this section without introducing this qualification.

However, the change in the way that errors were reported – or not reported – to the end user had substantial and destabilizing effects. As described in the previous section, the response, no such name, possesses important meanings. We emphasize the point that error responses contain information upon which other systems then act. Consequently, effectively eliminating the “no such name” response has ramifications through the system, preempts the expected behavior, and, in this instance, provoked localized efforts to work around or restore the system. In addition, the burden of work was, in many cases, shifted to system administrators and help desks, who suddenly had to cope with unanticipated changes and reactions from bewildered end-users.<sup>26</sup>

### *2.5.1 Protocol Independence and the Effects on Mail Systems*

It is important to understand that when a DNS query is made to a name server, the purpose of the query is not included. That is, there is no way for the name server to tell whether that query is for the purpose of looking up a Web page, sending mail, initiating a file transfer, logging in remotely to a machine, or initiating a network management action. Each of these services, and many others not mentioned here, are embodied in their own protocols. All of them require the translation of domain names into IP addresses. But the DNS look-up message does not include the name of the protocol that has triggered this look-up. Specifically, the operation of the name server is independent of the functionalities of the query submitted to it.

VeriSign’s action implicitly violated that separation. It assumed that all – or at least the vast preponderance – of queries involving uninstantiated names were intended to be HTTP (Web) queries. Thus it made assumptions about the protocol initiating the query.

When the requester made the connection to a VeriSign server, if it was, indeed, a Web request, then it reached the SiteFinder service. If it was not a Web query, the VeriSign server refused the connection. In the first release, VeriSign simply refused all connections except for Web connections thus ignoring other protocols. In the particular case of mail, this behavior turned out to be problematic.

Most mail systems interpret a refused connection as a temporary impediment, not as a permanent obstacle, and over the 30 years in which mail systems have operated, strategies have developed within the e-mail community to overcome temporary inability to reach distant mail servers. Having already gotten a successful positive response to the look-up of the domain name, they expected that there was actually a mail server ready to accept the connection at that address. Thus, when a mail system attempted to deliver mail to a VeriSign server and found that its attempt to connect was refused, it re-queued the message that it was trying to send and persisted with subsequent attempts usually for some number of days (typically three) before finally reporting back to the sender that it was unable to reach the intended mail system. Further, its error report would necessarily

---

<sup>26</sup> One comment reported to ICANN’s mailing list server: “I mistyped a URL and VeriSign’s wildcard service suggested I visit a porn site with a similar name! I find this highly offensive.” As quoted in Roessler, October 2004, Slide 4.

state that it had been *unable* to reach that system rather than the more accurate report that the mail system did not exist or that the domain name was misspelled. Prior to VeriSign's action, a bounced message would have been returned immediately because the domain name would not have resolved, thus giving the end user an immediate response and providing an error message stating that the domain name does not exist.

There is a further subtlety. In some environments, particularly corporate environments, there is sometimes a list of mail addresses to try to reach someone. If the first address fails, then the system that is trying to deliver the mail tries the next one. Subsequent to VeriSign's action, the mail system's attempt to go down the list was interrupted because the first attempt looked good. Not only did the end-user not realize what has happened for three days, the logic of the system is that that address exists and the system does not ever proceed down the list and the logic of using a range of addresses is defeated. From the perspective of mail systems, David Schairer, Vice President, Software Engineering for XO Communications, concluded at the October 7 meeting, there were network impacts and operational costs. Specifically:

- Bounced messages increased traffic and costs;
- Undeliverable mail increased costs for mail server farms; and
- Mail queuing reduced performance.<sup>27</sup>

After the launch of SiteFinder, VeriSign sought to ameliorate the impact of its HTTP-focused strategy by changing the ways its servers dealt with e-mail. In its subsequent operations, it accepted e-mail operations and then in the course of processing attempts to deliver mail to specific users, sent back "no such user" for each one of those. This is better from the sense that it gave a more immediate response. However, it confuses a "no such user" response with the more accurate "no such domain" response.

It also created additional concerns. As a result of this new strategy, names of users in e-mail headers entered VeriSign's computers, thus allowing a possible analysis of who is sending mail to whom, unbeknownst to either sender or receiver. VeriSign strongly asserted that the company was not keeping that information or making use of it. Nor is there any evidence that they did so or would do so. However, there is no opportunity under this strategy to observe independently what the facts might be. That is, in the first case, when the connection was refused, one could at least observe that this information was not collected. In latter case, although VeriSign was able to give the much prompter, albeit incorrect response, of "no such user", the "fix" raises the concern that VeriSign *might* be collecting information that users would not expect them to collect nor architecturally was there any way for the user to have given permission for this information to be collected. Thus, an ambiguity was created for the end-user knowledgeable enough to recognize the implications.

VeriSign's action also affected certain spam filters. One of the strategies used by some spam filters is to check whether the domain name of the sender exists. For example, prior

---

<sup>27</sup> David Schairer, Consequences I: What Was Affected, Washington, DC, 7 October 2003; see especially Slide 9; <http://www.icann.org/presentations/shairer-secsac-dc-07oct03.pdf>; verified 23 May 2004.

to VeriSign's action, if a message putatively from user@madeupdomainname.com had been sent, the spam filter would have tested the existence of madeupdomainname.com and would have gotten the response, "no such domain name". Subsequent to VeriSign's actions, it would have received the address of a server for madeupdomainname and thus presumptively – and potentially erroneously -- classified the message as legitimate. Thus, in one action, VeriSign disabled all of those spam filters.

It may be argued that only a small number of spam filters employ this strategy. Further, that this strategy is not the most effective one for eliminating spam. It is beyond the scope of this report to make judgments on the relative merits of different spam filters. We simply note here that VeriSign's action did have the effect of disabling this class of spam filters.

### *2.5.2 SiteFinder*

As reported earlier, VeriSign offered copious evidence showing that a majority of users were pleased with SiteFinder.<sup>28</sup> However, some critics pointed out problems in usability (for example, that the site was only in English and was not broadly accessible to certain populations, such as the visually impaired). Moreover and of greater concern from the perspective of this Committee are two effects on end-users: substitution for existing services and removal of choice. The SiteFinder service substituted itself for equivalent services already existent at the desktop; MSN and AOL offer similar services in the form of plug-ins for browsers so that when the error message "no such domain name" is returned, a comparable search takes place. Thus, VeriSign's action had the effect of disabling existing services and depriving users of a choice as to which service, if any, is to be provided at the desktop and how to configure it. All those choices were removed.

Some critics have viewed this imposition of a service as a lack of opportunity for end-users to participate, that is, the lack of an opportunity to refuse or to "opt out". We note here that the actual effect is broader: not only were users not able to opt out but if they had already had an existing service, it was replaced by VeriSign's SiteFinder service. Thus, in addition to the often heard complaint that VeriSign did not provide a way to opt out of this service, they also pre-empted decisions users had already made.

There was a further problem beyond the unilateral imposition of this service. It also subjected end users to potential scrutiny of which they were unaware and about which they had no control. Analysis of SiteFinder showed that a "web bug" had been embedded in the page operated by a company named Omniture which monitors Web traffic. Information about users of SiteFinder was thus passed off to a third party, again without the consent of the users and perhaps without their knowledge.

---

<sup>28</sup> In response to specific questions from social science researchers about the overall methodology and the release of the survey instrument, which are customary among academic researchers, VeriSign refused to disclose either. Moreover, Benjamin Edelman offered evidence of push-back, based on analysis of data provided by Alexa. See Benjamin Edelman, *Measuring ISP Response to VeriSign SiteFinder*, Washington, DC, 15 October 2003; <http://www.icann.org/presentations/edelman-secsac-dc-15oct03.pdf>; verified 23 May 2004.



Further, many sites, most notably public school systems, have strong filters in place to protect its end users from accessing inappropriate sites. The SiteFinder service as initially launched included partial but not stringent controls on what sites could be looked up. It was quickly discovered that users connected to SiteFinder could then reach sites that they could not otherwise have reached. Managers in charge of public schools and libraries in the U.S. were then faced with adding additional controls to their existing systems to protect against SiteFinder. That is, SiteFinder itself had to be added to the list of prohibited sites.

### *2.5.3 Workarounds and inconsistencies: Implications for end-users*

Ameliorating VeriSign's action and dealing with end-users' responses to it created work for system operators. Between launch and suspension of the service, patches were released by ISPs and by vendors of DNS resolver software, most notably by Internet Systems Consortium (ISC), the providers of BIND, the most commonly used DNS resolver software. This solved certain problems on a relatively limited basis. In quite a few cases, system operators, some at the ISP level, some at the enterprise level, sought to intercept VeriSign's synthesized response and then to retransform that response back to the original "no such domain" error code. This approach required identifying the specific address, for example, 1.2.3.4, and then blocking it.

In Tennessee, 132 of the 139 public school districts are provided Internet service through a common provider. In aggregate, there are 1884 end sites, 900,000 students, 60,000 teachers/administrators and 250,000-plus computers. VeriSign's action triggered both a noticeable increase in help desk calls and an alternative pathway to reach objectionable sites. The system administrators installed the ISC patch to counteract the VeriSign change.<sup>29</sup>

This action on the part of ISPs and name resolvers provided an immediate salve but is considered poor engineering. First, the list of server addresses that VeriSign might return can change over time. More awkwardly, addresses that are filtered out might be configured at some later time for legitimate sites and there would be no obvious reason to the user why those sites are unreachable. In this hypothetical example, the ISP or the name resolver would return the message "no such domain" when, in fact, the domain exists. Second, this strategy adds to the workload and complexity to systems maintained by ISPs and name resolvers. It now introduces the network or resolver operator into the decision process, further removing users from exercising choice. Thus, if users were happy with SiteFinder, there would be no way to choose it and "opt-in" is precluded in this case just as "opt out" was precluded before.

From a broader perspective, this strategy has opened the door to network operators making decisions about content, that is, interfering or modifying the traffic going through

---

<sup>29</sup> Personal communications, Collie to Woolf, 20 October 2003 (e-mail); Collie to Crocker, 24 May 2004. This action was taken by the provider before the SiteFinder matter came to the attention of state officials or the media.

their systems and doing so under the rubric of protecting users. The general principle that the Internet has operated under from its inception is that the lower layers of the network should be exclusively focused on accurate, reliable, efficient transmission of the messages sent from end-user to end user. This experience raises the possibility that some network operators will see other opportunities for so-called “participation” in the end user experience.<sup>30</sup>

Good practice has always required extensive testing, engineering refinement and public comment from the community. In marked contrast, these “fixes” were hustled into operation quickly. Instability results from abruptness, whether from VeriSign’s action or from the urgent responses to it. Whereas VeriSign had the benefit of months of preparation, albeit out of public view, the responses were instituted very quickly, and, of necessity, these responses, workarounds and fixes did not have the benefit of extensive testing and engineering refinement. Additionally, they were introduced locally and therefore not uniformly. Consequently, the end user experience varied depending on which resolver or which ISP had instituted these changes and when. Moreover, the end user experienced one kind set of responses for errors in NET and COM but other kinds of responses in, for example, ORG or one of the other top level domains.

One of the fundamental objectives in the design of the domain name system is to give the same response no matter where the queries are initiated. This attribute is called *coherence*. Local introduction of countervailing changes necessarily resulted in varying responses at different locations and a loss of coherence.<sup>31</sup> We note further that VeriSign’s single change triggered multiple countervailing reactions. That is, a significant number of man hours were spent across multiple organizations to undo a change introduced by one organization. We offer up no quantitative measures of the magnitude of this change and its potential differential impacts among different populations of users around the world with different levels of connectivity and access to infrastructure services, but as a qualitative matter, this effect is inescapable.

Finally, some have suggested that the introduction of countervailing changes is comparable to the introduction of VeriSign’s action. In particular and as previously mentioned, Internet Systems Consortium (ISC) released a modified version of its widely used BIND resolver with the capability to be configured to reverse or undo VeriSign’s synthesized response. We note here however that two actions were required to install such a change: First, vendors such as ISC provided software to make it possible to undo

---

<sup>30</sup> We note that this argument also cuts the other way. Once the door to content is opened, there exists potential for liability. We recognize that these issues best dealt with by the legal community and are outside the scope of this Committee. We simply note that in introducing engineering changes of this sort, the clean bright line that had previously been in place has become muddled.

<sup>31</sup> Paul Vixie’s comment at the 7 October meeting is telling. He is President of Internet Systems Consortium, Inc. (ISC), which supplied one of the work-arounds. He concluded: “From my perspective as a protocol and software person, the total result of this [sequence of patches] is incoherence and growing incoherence. The people who are responding to this are responding by making DNS response less coherent than they were. And that’s not a direction I’d like to see us go in. So I think that the total result in terms of DNS incoherence is that we’ve seen some instability. And there will be more if the service is turned back on.” SSAC Meeting Real-Time Captioning, 7 October 2003, [p. 34].

the change. Second, network or site operators explicitly chose to install and put into operation those changes.

There was no opportunity for a single organization, ISC or any other entity, to unilaterally counteract VeriSign's action. Rather, a natural check-and-balance or propose-dispose cycle existed, even with in the very short time of these actions. The decision to intercept and reverse VeriSign's action required a decision on behalf of the users and not solely a response from a direct competitor to VeriSign.

## 2.6 Discussion and conclusion

The Committee concludes that VeriSign's action violates fundamental and well-tested principles of the Internet architecture and good practice. It interferes with long standing design principles of robustness, supporting intelligence and innovation at the edges by maintaining stability at the core, and introducing changes and improvements at the core only after careful, public scrutiny, consensus, testing and refinement. In addition, VeriSign's action violates well-established principles of layering as was made very obvious in the initial treatment of protocols other than HTTP. It muddies the distinctions between operations at the core and operations performed elsewhere in the system. Finally, it increases the potential control of single operators that were previously kept carefully distinct.

Second, the method of introduction of the change also raised its own set of issues. The lack of review and need for refinement initiated a set of countervailing changes that were in their totality incoherent and created a different set of costs for yet another group of people compelled to make changes to reverse or compensate for unanticipated behaviors.

Third, economic as well as the technical costs were borne by third parties. Although shifting costs to third parties is not necessarily a security or stability issue, the fact that such changes and cost shifting may be imposed unilaterally without either consensus among affected parties or a viable alternative creates ambiguity for users and is therefore a source of instability.

Fourth, in addition to disrupting stability, end users were potentially exposed to invasions of their privacy of which they were unaware. Information embedded in e-mail headers ended up in VeriSign's servers and Web users re-directed to SiteFinder were watched and information sent to a commercial third party.

In aggregate, perhaps the greatest casualty involves trust. Previously, threats to security and stability were perceived to be primarily external, arising from acts of nature, possible business failures or the behavior of malicious outsiders. This sequence of events has shown that the stability of the Internet can also be affected by the actions of trusted operators of core services acting in their own self interest. In section 2.4 of this document, we identified three classes of people directly associated with operating the domain name system: registry operators, registrars, and registrants. All of them were affected by VeriSign's action, but there is also a fourth set of people who count on the

reliable operation of the domain name system – the users. As the Tennessee example shows, they can be system administrators or end users. They are the largest constituency. Yet they are the ones with the least say. Users who have no direct relationship with registry operators can fairly ask what are the rules governing stability of the core services? That question has more salience and urgency today than it did prior to VeriSign's action.

### **3.0 Findings and Recommendations**

In the previous sections, we described the events that transpired in September-October 2003 and the technological consequences of those events in the context of fundamental concepts, principles and accepted good practice. In this section, we set forth specific findings relative to questions of stability and security and make recommendations concerning future actions. The Committee offers these findings and recommendations in the spirit of open review, comment and evaluation in the expectation that they will be mulled over, parsed, dissected, and tested before they result in action. Overall, the Committee acknowledges that VeriSign's action did not cause network shattering and readily understandable failures or potential failures on the scale of the electricity grid's black-out in the Northeast United States last summer. Nor did it conjure up the specter of widespread failure in the public consciousness in the way that Y2K did. However,

Finding (1): VeriSign introduced changes to the NET and COM registries that disturbed a set of existing services that had been functioning satisfactorily. Names that were mistyped, had lapsed, or had never been registered were resolved as if they existed. As a consequence, certain e-mail systems, spam filters, and other services failed resulting in direct and indirect costs to third parties, either in the form of increased network charges for some classes of users, a reduction in performance, or the creation of the work required to compensate for the eventual failure.

Finding (2): The changes violated fundamental engineering principles by blurring the hitherto bright and well-defined boundary between architectural layers. Queries to the name server were assumed to be HTTP conformant whereas the DNS protocol, in fact, makes no assumptions – and is neutral – regarding the protocols of the queries submitted to it. As a consequence, more control was moved toward the center and away from the periphery, in particular, away from end-users, thus violating the long-held end-to-end design principle.

Finding (3): The mechanisms proposed by VeriSign to ameliorate the undesirable effects of their diversion on protocols other than HTTP put VeriSign in the development path of every new protocol that uses DNS. For every such protocol, it would be necessary to consult with VeriSign to figure out how to simulate the response of the protocol to “no such domain”. This is an unacceptable invasion of clear layering.

Finding (4): Despite a long period of internal research and development, the system was brought out abruptly. The abruptness of the change violated accepted codes of conduct that called for public review, comment, and testing of changes to core systems; this process exists to ensure that changes are introduced with minimal disruption to existing services and hence with minimal disruption to the stability and security of the Internet.

Finding (5): A series of work-arounds and patches was abruptly introduced, cumulatively reducing the overall coherence of the system and again violating the established practices of evaluation, testing, discussion and review before core services are

implemented and deployed. These work arounds shifted the name resolution function from DNS servers to name servers and ISPs, created additional work for third parties, and blurred the functional layers intrinsic to the Internet's robust architecture.

**Finding (6):** End-users were subjected to potential invasions of their privacy. Information contained in headers for e-mail was inadvertently but necessarily stored on VeriSign's servers without either the knowledge or consent of either sender or receiver.

**Finding (7):** End-users re-directed to the Web site were essentially "observed" by a service embedded in that site and users were deprived of choice, to accept the service, reject it, or substitute another similar service for it.

**Finding (8):** The initial set of changes, the responses they provoked and the responses to the responses collectively undermined expectations about reliable behavior and in so doing reduced trust in the stability and security of the system. Spam filters that suddenly stop working; e-mail that bounces three days after it is sent; and re-directions over which end-users have no control all contribute to a loss of confidence. The implications of that reduced confidence remain to be seen.

On the basis of these findings, the Committee makes the following recommendations:

**Recommendation (1):** Redirection of lookups to uninstantiated names should not be introduced into any existing or future registries. The wildcard mechanism for redirecting uninstantiated names is documented in the defining RFCs, but it was generally intended to be used only in narrow contexts, generally within a single enterprise.

**Recommendation (2):** Existing use of the wildcard in top level domains like MUSEUM should be phased out and the specifications re-written so that they cannot be used at the registry level. In small domains such as MUSEUM, alternative strategies can be employed.

**Recommendation (3):** Changes in registry services should take place only after a substantial period of notice, comment and consensus involving both the technical community and the larger user community. This process must (i) consider issues of stability and security, (ii) afford ample time for testing and refinement, and (iii) allow for adequate notice and coordination with affected and potentially affected system managers and end-users. This ensures not only robust engineering but also engenders trust in the systems and the processes surrounding maintenance and development of the systems.

## Appendices

- 1: Members of the Committee (bios and COI)
- 2: Security Committee Charter; approved 14 March 2002.  
<http://www.icann.org/committees/security/charter-14mar02.htm>; verified May 26, 2004
- 3: Message from Security and Stability Advisory Committee to ICANN Board, 22 September 2003; <http://www.icann.org/correspondence/secsac-to-board-22sep03.htm>; verified May 26, 2004
- 4: Correspondence between ICANN and VeriSign, Inc.
- 5: VeriSign Site Finder: Technical Review Panel Summary, Scott Hollenbeck, Director of Technology, VeriSign, in Site Finder Review, SECSAC Meeting, October 15, 2003, Washington, DC; <http://www.icann.org/presentations/turner-secsac-dc-15oct03.pdf>; verified May 26, 2004
- 6: IAB Commentary: Architectural Concerns on the use of DNS Wildcards, 19 September 2003; <http://www.iab.org/documents/docs/2003-09-20-dns-wildcards.html>; verified May 26, 2004
- 7: Museum Domain Management Association, Statement Concerning Wildcard “A” Records in Top-Level Domains, 6 October 2003; <http://musedoma.museum/policy/wildcard/>; verified May 26, 2004
- 8: Names of individuals mentioned in this report [with caveat noting that citation or reference in this report does not confer or reflect special recognition by the Committee.]

# **EXHIBIT G**



From: "Steve Crocker" <steve@shinkuro.com>  
To: ssac@icann.org  
Subject: [ssac] FW: GNR's comments to SSAC report  
Date: Thu, 17 Jun 2004 11:47:43 -0400

Folks,

Here's some comments from Hakon Haugnes of GNR. He is taking issue with the breadth of our recommendations.

I think it would be helpful if someone familiar with GNR and the registry they represent, .name, can refresh our understanding of what their issues are with respect to redirection of uninstantiated names. Is someone able to do so easily and quickly?

We need to decide whether we want to adjust our recommendations in light of these comments. I don't think we're under any obligation one way or the other. Hakon's comments imply we should restrict ourselves to speaking about the COM and NET domains. While the events there triggered this work, it's perfectly appropriate and arguably required that we look at security and stability issues across the spectrum of registries.

Please comment quickly.

Thanks,

Steve

-----Original Message-----

From: Steve Crocker [mailto:steve@stevecrocker.com]  
Sent: Thursday, June 17, 2004 10:20 AM  
To: hhaugnes@gnr.com  
Cc: 'James M Galvin'; 'Geir Rasmussen'; 'Philip Colebrook';  
steve@shinkuro.com  
Subject: RE: GNR's comments to SSAC report

Hakon,

Thanks. I appreciate the input and the time you've taken to review the draft report.

Your comments ask us to restrict our attention to the redirection in the COM and NET domains. Although that was the event that triggered our examination of this area, we felt it was necessary to give some attention to the question of redirection in registries in general.

That said, I'll share your comments with the committee and we'll consider them.

Again, many thanks.

Steve

> -----Original Message-----

> From: Hakon Haugnes [mailto:hhaugnes@gnr.com]

> Sent: Thursday, June 17, 2004 7:55 AM

> To: steve@stevecrocker.com

> Cc: James M Galvin; Geir Rasmussen; Philip Colebrook

> Subject: GNR's comments to SSAC report

>

>

>

> Dear Steve Crocker and James Galvin,

>

> Thank you for the opportunity to comment on SSAC's draft report  
> concerning redirection in the .COM and .NET TLDs. We believe that the  
> report is a thorough document and represents a great effort of the  
> many involved parties to understand the consequences of the  
> redirection of the .COM and .NET TLDs. We have read it with great  
> interest and have several comments in the following.

>

>

> As a general comment, GNR feels that it is appropriate that the  
> objective of the report is to focus on the redirection in the .COM and  
> .NET TLDs, yet the report extrapolates factual considerations and  
> conclusions to cover other registries.

>

> We would therefore submit that SSAC has not sufficiently considered  
> the fundamental distinguishing factors between different registries,  
> including size, purpose, market, usage patterns, user communities and  
> user expectations. In our belief, the report needs to be confined to  
> the specific facts surrounding the redirection of .COM and .NET TLDs  
> and should not follow a policy of equivalence amongst registries.

>

> More specifically, with regards to the findings and recommendations  
> that the report makes, we would like to make the following  
> observations:

>

> Finding (5)

> We believe that this finding does not make it sufficiently clear that  
> at least some of the patches and workarounds were released by third  
> parties who have a de-facto responsibility for the stability and  
> functionality of the DNS. As you may remember, we commented on this  
> specifically in one of the SECSAC's meetings, as .NAME was  
> specifically impacted by third parties' actions. This finding(5)  
> appears in the context it is placed to have a different meaning than  
> it to our knowledge, factually should.

>

> Recommendation (1)

> We believe that this recommendation, whilst carefully predicated on  
> the consequences of redirection of .COM and .NET, draws too wide a net  
> in that it assumes that future introductions of a registry service on  
> other TLDs will have a comparable effect to that of the redirection of  
> the .COM and .NET TLDs. That there may be factual considerations in  
> the future that will be sufficiently distinguishable from the  
> scenario of redirection on .COM and .NET and that a blanket  
> restriction may in fact stifle valuable innovation in the

> operation of future TLDs.  
>  
> Recommendation (2)  
> Whilst GNR does not have sufficient knowledge of the operations of the  
> .MUSEUM TLD, we believe that the report has made this recommendation  
> on the basis of factual circumstances that assume the parity of  
> .MUSEUM TLD with .COM and .NET. As noted above, we believe that there  
> are several criteria in assessing a TLD that point to the assumption  
> of parity not necessarily being valid. On this basis, without  
> wanting to pre-empt any comment from the operators of  
> .MUSEUM, we would be in favour of striking this recommendation(2).  
>  
> Recommendation (3)  
> In our opinion, this recommendation is too wide and goes outside the  
> scope of considering the consequences of redirection in the .COM and  
> .NET domains. While the SSAC report is well researched on redirection  
> consequences on .COM and .NET, we feel that it does not provide a  
> foundation to make recommendations on the complex topic of "changes to  
> registry services". We would therefore draw SSAC's attention  
> to the ongoing GNSO Policy Development Process ("PDP")  
> concerning the introduction of new registry services. The  
> genesis of this PDP was in the reaction to the redirection of  
> the .COM and .NET TLDs, and the substance of the process will  
> almost certainly address the matters raised by SSAC under  
> this recommendation. We would therefore submit that this  
> recommendation(3) be changed to limit its scope to  
> redirection on .COM and .NET.  
>  
>  
> To conclude, GNR in general supports the efforts of SSAC in  
> this matter. We feel, however, that the submissions herein  
> are necessary in order to distinguish the events around the  
> redirection of .COM and .NET from different, and future,  
> registry services, and we are concerned that all registries  
> may be "tarred with the same brush" because of the assumption  
> that all registries or top-level domains are comparable.  
>  
> Finally, we thank SSAC for the opportunity to present this  
> submission and look forward to the final report.  
>  
>  
> Yours truly,  
>  
> Hakon Haugnes  
> President  
> Global Name Registry

# **EXHIBIT H**


[Home](#)
[Michigan](#)
[Networking R&D](#)
[Learning Systems](#)




## North American Network Operators Group

[Date Prev](#) | [Date Next](#) | [Date Index](#) | [Thread Index](#) | [Author Index](#) | [Historical](#)

### Re: Pushing GTLD zones [WAS: Akamai DNS Issue?]

- *From:* Paul Vixie
- *Date:* Thu Jun 17 14:04:34 2004

> > think stability.  
>  
> I think recent events prove pretty well that Verisign GRS no longer gives  
> a crap about stability. Have we forgotten \*.COM so quickly?

oh please. i was an publically critical of \*.COM and \*.NET, but that's a policy problem, not an operational problem. verisign has a very good record for name server uptime, both at the TLD and root level. if you're going to complain about their wildcard policies, please be specific.

(note that verisign has amended their complaint against icann (since the court dismissed the first one) and i'm now named as a co-conspirator. if you reply to this message, there's a good chance of your e-mail appearing in court filings at some point.)

--  
Paul Vixie

- **Follow-Ups:**
  - [Re: Pushing GTLD zones \[WAS: Akamai DNS Issue?\]](#) *Jeroen Massar*
  - [Re: Pushing GTLD zones \[WAS: Akamai DNS Issue?\]](#) *D'Arcy J.M. Cain*
- **References:**
  - [Re: Pushing GTLD zones \[WAS: Akamai DNS Issue?\]](#) *Michael Loftis*
- **Prev by Date:** [Re: Pushing GTLD zones \[WAS: Akamai DNS Issue?\]](#)
- **Next by Date:** [Re: Pushing GTLD zones \[WAS: Akamai DNS Issue?\]](#)
- [Date Index](#)
- [Thread Index](#)
- [Author Index](#)
- [Historical](#)

Merit Network, Inc.

4251 Plymouth Road  
Arbor Lakes, Bldg. 1  
Suite 2000  
Ann Arbor MI 48105-2785

734.764.9430

# **EXHIBIT I**

## **Why A Privacy Policy?**

VeriSign, Inc. ("VeriSign") respects your individual privacy. This Privacy Policy ("Policy") embodies our commitment to its protection through adherence to fair electronic information practices. You have our promise that we will not electronically process your personal information in any way that is incompatible with this Policy.

## **This Privacy Policy protects your privacy by:**

### **Informing you about:**

- The types of information VeriSign collects through the VeriSign Site Finder ("Site Finder");
- How it collects that information;
- The general purposes for which it collects such information;
- The types of organizations to which it discloses the information.

**Ensuring accountability** to individuals who believe that VeriSign has not complied with these privacy principles.

**Privacy** is of concern to most users of the Internet, and is an important part of an enjoyable and satisfactory user experience. We at VeriSign are aware of and sensitive to the privacy concerns of visitors to our Site Finder.

## **Information We Gather from You**

### **Personal Information**

We do not collect any personal information from visitors to our Site Finder. Under no circumstances do we collect any personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, or sex life.

### **Statistical Information About Your Visit**

When you visit our Site Finder, our computers may automatically collect statistics about your visit. This information does not identify you personally. We may monitor statistics such as how many people visit our Site Finder, the visitor's IP address, which pages a visitor views, from which domains our visitors come and which browsers and browser settings visitors use.

### **Use of Cookies**

We only use "cookies" as described in this Section. A "cookie" is a piece of information that our Site Finder sends to your browser, which then stores this information on your system. If a cookie is used, our Site Finder will be able to "remember" information about you and your preferences either until you exit your current browser window (if the cookie is temporary) or until you disable or delete the cookie. Many users prefer to use cookies in order to help them navigate a Web site as seamlessly as possible. You should be aware that cookies contain no more information than you volunteer, and they are not able to "invade" your hard drive and return to the sender with personal or other information from your computer.

Our uses of "cookies" are limited to the following specific situations. We may use temporary cookies in order to determine whether your browser accepts cookies. This

is set upon your arrival to our Site Finder. We may use permanent cookies for the purpose of remembering and enabling your indicated preferences for content filtering. Your preferences are set when you change the default settings. Our third party web site analytics vendor also may send a permanent cookie in order to track click behavior and gather aggregate information, including information to define new visitors, analyze site path data, and track historical commerce information.

Most browsers can be set to notify you when you receive any cookie, giving you the chance to decide whether to accept it in each situation in which one is sent. To find more information about cookies, if you are using Microsoft Internet Explorer® as your browser, go to the Microsoft Web site at <http://www.microsoft.com/info/cookies.htm?RLD=291> or if you are using Netscape Navigator® as your browser, go to the Netscape Web site at <http://home.netscape.com/security/basics/privacy.html#cookies>

### **How We Use and With Whom We Share the Information We Gather**

We assure you that the information we gather from you about your visit is in aggregate form and solely for the purposes of operating and improving the performance of our Site Finder.

### **Third Party Search Results and Cookies**

We use third-party companies to serve paid and unpaid search results and other content to our Site Finder. In the course of serving these results, these companies may place or recognize a cookie on your browser, and may use information (not including your name, address, e-mail address, or telephone number) about your visits to this and other web sites in order to serve content to our site, improve the services offered on our site, or measure advertising effectiveness of paid search results. For more information about this practice and to know your choices about not having your information used by these companies, please visit <http://www.content.overture.com/d/Usm/about/company/privacypolicy.html>.

In the event the terms of these third party privacy policies vary from or are inconsistent with the terms of this privacy policy, the terms of this privacy policy shall control. Furthermore, no third party will use any of the information collected in a manner that is inconsistent with this privacy policy.

### **How We Put Information to Good Use**

We use information about you for purposes of monitoring and improving our internal operations as well as to improve the experience of users on our Site Finder. For example, we may correlate Web site traffic information with data about individual users. This data helps us to determine how much our customers use parts of the Site Finder, allowing us to enhance it to fit the needs of as many of our customers as possible. We may also break down overall usage statistics according to customers' domain names, browser types, and MIME types by reading this information from the browser string (information contained in every user's browser).

### **Accountability**



If you feel that VeriSign, or any of our agents, representatives or employees, is violating this Privacy Policy, please contact us by postal mail at:

VeriSign, Inc.  
Attention: Legal Department  
21355 Ridgetop Circle  
Dulles, VA 20166

**Notification of Changes**

We will post any changes to this Privacy Policy 30 days before their effective date so you will always know what information we collect, how we use it, and under what circumstances, if any, we disclose it. You are responsible for periodically checking our web site for changes to this Privacy Policy.

**If you have any questions regarding this Privacy Policy, please contact**  
VeriSign, Inc.  
Attention: Legal Department  
21355 Ridgetop Circle  
Dulles, VA 20166

# **EXHIBIT J**

**Set Your Content Filtering Preferences**

**Filtering Preferences:**

Filtering attempts to block content containing explicit and adult material. While no filter is 100% effective, Site Finder uses industry-leading technology to identify explicit content and reduce undesired results.

Please choose your preference:

- Full filtering: Explicit content is removed from all results
- Partial filtering: Explicit content is removed from category results and presented last in search results
- No filtering: Do not filter my content



Note: Setting preferences will not work if you have disabled cookies in your browser.

Copyright © 2003 VeriSign, Inc. All Rights Reserved  
[Privacy Policy](#) | [Terms Of Use](#) | [Content Filtering Preferences](#) | [Help](#)

## Help

- [General Questions](#)
- [Search Tips](#)
- [Setting Preferences](#)
- [Application Developers](#)

## General Questions

### How did I get to Site Finder?

The Web address that you entered is not registered on the Internet or is inactive, and the Site Finder is designed to help you find what you are looking for.

This page may appear for a number of reasons. For example, you may have inadvertently misspelled the Web address. Or, the site you were looking for may have an expired Web address. By using the name that you originally requested, Site Finder looks for similar Web addresses and related categories.

### What are the different types of search results?

#### Did You Mean

The "Did You Mean" section displays Web addresses that are similar to the the address you entered. If you misspelled the name of a Web site, for example, it is likely that the correctly spelled name will appear here.

#### Related Categories

The "Related Categories" section contains topics or categories related to the information you originally looked for. By clicking on one of these categories, you will see a list of Web sites associated with the selected topic.

#### Popular Categories

The "Popular Categories" section contains topics or categories of common interest to users.

#### Sponsored Results

The "Sponsored Results" section lists links to information directly related to your search. These listings are sponsored by companies that pay to have a link to their sites appear in results for the specific search term you entered.

#### Web Results

The Web Results section displays links to sites that are listed in the order of relevance to the search terms you entered.

### How do I perform a search?

On any Site Finder page, type the words you want to search for in the search box. Then, click on the Search button or press the Enter key on your keyboard.

### Can I bookmark this page?

You can use your browser to bookmark any Site Finder page, searches that you perform frequently.

#### Netscape Users:

1. From the Location toolbar, select "Add to Favorites".
2. Select "Add Bookmarks".

#### Microsoft Internet Explorer:

1. From the Favorites menu, select "Add to Favorites".
2. Click "OK".

### Why do some links return an error?

Occasionally, when you click on some of the links on the results page, you may get errors such as "Permission Denied" or "Page Not Found". These errors may appear for a number of reasons:

- The site you are trying to visit may be busy or experiencing technical problems. This can happen when a site is very popular and overloaded with traffic.
- The site you are trying to visit is denying people access either intentionally or unintentionally. You might consider contacting the site's administrator directly via email or using other search results.

### Why is the Site Finder provided by VeriSign?

VeriSign provides the services that allow Internet users to find Web sites. Everyday, billions of Web address entries are handled by VeriSign. When users request a Web address that is not registered on the Internet or is inactive to VeriSign, they are forwarded to the Site Finder. The Site Finder provides information to users that may prove useful in locating the resources the user originally intended to access.

[Back to top](#)

## Search Tips

### Word Choice

---

Use obvious words first. For example, if you are looking for information on Maui, enter "Maui" rather than "Islands". Also, using specific search terms that are likely to appear on the site with the information you want will get more relevant results. The search term "Maui golf course list" will return better results than "really fun golf courses in Maui".

### Automatic And

---

By default, Site Finder only returns results that have all of your search terms. You do not need to include "and" between terms.

### Automatic Exclusion of Common Words

---

By default, Site Finder ignores common words such as "how" and single letter words such as "a" and "I" because they tend to slow down searches without improving results.

### Case Sensitivity

---

It is not necessary to capitalize your search terms. Searching for "Maui" will return the same results as searching for "maui".

[Back to top](#)

### Setting Preferences

---

#### Content Filtering

---

By default, Site Finder uses partial filtering to minimize explicit content from your results. You can apply full filtering of explicit content by clicking on the "Content Filtering Preferences" link and selecting the "Full filtering" option.

To turn off filtering, select the "No filtering" option. The filtering option you select on the Content Filtering Preferences page will remain on until you change and resave your preferences. While no filter is 100% effective, Site Finder uses industry-leading technology to try to identify and filter adult content and reduce undesired results.

Please note that setting preferences will not work if you have disabled cookies in your browser.

#### How Do I Enable Cookies?

---

To enable cookies, follow the instructions below for the browser version you are using.

##### Microsoft Internet Explorer 5.x

1. Select "Internet Options" from the Tools menu.
2. Click on the "Security" tab.
3. Click "Custom Level" button.
4. Scroll down to the "Cookies" section.
5. Set "Allow cookies that are stored on your computer" to "Enable".
6. Set "Allow per-session cookies" to "Enable".
7. Click OK.

##### Microsoft Internet Explorer 4.x

1. Select "Internet Options" from the View menu.
2. Click on the "Advanced" tab.
3. Scroll down to find "Cookies" within the "Security" section.
4. Select "Always accept cookies".
5. Click OK.

##### Netscape

1. Select "Preferences" from the Edit menu.
2. Find the "Cookies" section in the "Advanced" category.
3. Select "Accept all cookies" (or "Enable all cookies").
4. Click OK.

[Back to top](#)

### Application Developers

---

#### Application Developers

---

For a complete discussion of the impact of Site Finder functionality, please refer to the [Site Finder Developer's Guide](#).

[Back to top](#)

Copyright © 2003 VeriSign, Inc. All Rights Reserved  
[Privacy Policy](#) | [Terms Of Use](#) | [Content Filtering Preferences](#) | [Help](#)

http://www.verisign.com/pc/td-www.bookstore.com/td-www.bookstore.com

We didn't find: "www.bookstore.com"  
There is no Web site at this address.

Search the Web:

Did You Mean ?

We did find these similar Web addresses.

[www.bookstore.com](#)

[www.upbookstore.com](#)

[www.booksource.com](#)

Search Popular Categories:

[Travel](#)  
[Entertainment](#)  
[Gambling](#)  
[Shopping](#)  
[Gifts](#)

[Computers](#)  
[Autos](#)  
[Insurance](#)  
[Small Business](#)  
[Investing](#)

[Health & Fitness](#)  
[Home & Garden](#)  
[Career](#)  
[Education](#)  
[Reference](#)