北京 一 新 gTLD 安全性、稳定性和灵活性 (SSR) 更新
2013 年 4 月 8 日，星期一 一 15:00 至 16:30
ICANN 一 中国北京

女士们、先生们，请欢迎 ICANN 首席安全官 Jeff Moss 发言。

[掌声]

JEFF MOSS： 首先我先把麦克风拿过来。现在有了，好的。下面我们正式开始。本次会议是对新 gTLD 安全性、稳定性和灵活性的更新。我们今天的任务是，让大家了解 ICANN 和网络普通用户群体是如何应对与新 gTLD 计划相关的风险的。

今天我们有许多专家组成员参与，他们将在接下来的会议中发表他们的观点并就具体问题进行讨论。然后，在会议结束时，大家可以随意提问。我希望，针对这些相关问题，我们今天的讨论和辩论是深入彻底的。

总而言之，我是说，这次会议是非常互动的。不过，由于在会议中途我们不接受任何提问，因此，如果有任何疑问，可以记下来，等到会议结束时一并提出。专家组成员会一直待到会议结束，到时我们再来一起解决这些问题。

今天，在台上的专家组成员分别有：gTLD 运营副总裁 Christine Willett、IANA 副总裁 Elise Gerich、VeriSign 首席安全官 Danny McPherson、ICANN 的 DNS 运营总监 Joe Abley、安全小组的安全性、稳定性和灵活性高级

主管 John Crain、SSAC 主席 Patrik Faltstrom、Google 的高级网络工程师 Warren Kumari 以及 ICANN 的高级技术分析师 Steve Sheng。这些就是大家看到的台上的专家组成员。

下面我要重申一些大家都知道的内容。在 ICANN 的核心使命中，安全性极为重要。这是在《ICANN 章程》2012 年 12 月 20 日的修订版中提出的。《章程》规定，我们的使命是，对全球互联网唯一标识符系统进行总体协调，特别是要确保该唯一标识符系统能够稳定安全地运行。如果大家查阅《章程》第 1 页的第 1 部分和第 2 部分，就会发现这一规定列在前面，我们对这个是非常重视的。

作为一个全球性多利益主体组织，我们将通过协调、协作和合作来促进互联网唯一标识符系统的安全性、稳定性和灵活性。

当然，这也是 ICANN 的技术使命之一。

正如我之前所说，接下来我们要将精力集中在新 gTLD 计划上。大家思考一下便会发现，对于这一计划，我们主要有三个职责。第一个是：ICANN 组织的内部管理，即 ICANN 的运营职责。第二个是机构群体的编址，ICANN 主要充当协调的角色。

最后一个是对全球机构群体进行考量，促进群体沟通并达成共识。可以看出，这三种职责都与运营协调和促进模式相关。

另外，我要指出的一点就是，世界上没有什么是 100% 安全的。若非要达到 100% 安全，很可能会崩溃或精神错乱。同样，互联网领域内也没有什么是 100% 零风险的。既然如此，那我们要怎么做？我们要做的就是管理风险。作为互联网安全专家，我们所做的任何事都是为了平衡风险回报或权衡成本。

在这之中，有些风险是我们已知的，这时我们需要制定相应的风险降低策略。例如，我们制定解决方案；我们分摊成本、可能性和影响；我们努力降低风险发生的可能性及其带来的影响。

但除此之外，我们还需要制定适当的程序来应对未知风险。我们都知道，在新 gTLD 计划的实施过程中，必然会出现一些我们无法预料到的风险。因此，ICANN 无论是作为单独运营商还是与机构群体协作，我们都必须要懂得变通，必须要足够灵活，必须要提出适应性较强的程序来帮助我们解决风险。

这也是我想让机构群体参与此次会议的原因，当问题发生时，我们所有人必须齐心协力解决问题。仅仅依靠 ICANN 是不太可能奇迹般地解决所有这些问题的。

虽然我们现在所谈论的 DNS 是一个非常复杂的生态系统，但它也并非完全无规律可循。我们在 DNS 系统运营方面拥有数十年的丰富经验。如果回过头来看，大家会发现，机构群体到目前为止已经实现了好几次扩展。我们新增了 AAAA 记录、TSIG 和 DNSSEC 等资源记录类型，修改了 EDNS0 协议，引入了 IDN，并将这些改进保持了多年。而且，当我们做出这些改变时，根系统并未崩溃。

同时，我们还完成了从路由到根的 BGP 任播分布的转换，使根系统变得更加灵活，并且我们像一个群体一样经受住了考验。

所以，我的意思就是，无论将来我们是否遇到任何问题，我们都要像一个群体那样共同面对，一起解决，然后继续前进。

接下来大家看到的这张幻灯片，是对之前 Fadi 在新 gTLD 月度更新会议中所展示的幻灯片的更新，请大家注意看幻灯片的下面，这个

有关 SSR 的砖块图。这个图片对 ICANN 的每项使命进行了分级，从中我们可以看出，互联网的安全性、稳定性和灵活性是我们的头号核心使命。其他所有使命都是建立在此基础上的。因此，任何可能危害 DNS 或唯一标识符系统的安全性、稳定性和灵活性的事情，我们都不可以做。绝对不可以！说到这里，Christine Willett 在此次会议前刚就运营准备问题发表了演讲。如果有人没有听到，那么我现在将麦克风递给 Christine，让他给我们做一个简短的更新并说说这张幻灯片。

CHRISTINE WILLETT： 谢谢 Jeff。这张幻灯片向我们呈现了，gTLD 计划应该具备哪些构件和组件，以达到运营准备就绪的状态。幻灯片开头是去年六月份公布和发布的申请。目前，我们已经完成了优先次序抽签，正处于初步评估阶段，并在每周公布初步评估的结果。

继续往下看，在蓝色文本框这里，我们看到准备 gTLD 运营须具备的另外几个构件，在签约阶段，我们会最终确定并批准注册管理机构协议。申请人一旦完成签约流程，将接受授权前测试。完成授权前测试后，根据新 gTLD 计划，便可说他们完成了，他们完成了自己在这一计划中的职责。然后我们会向申请人发出一份通知，同时通知 IANA 申请人已经完成。接着授予申请人一份认证证书作为证明，申请人便可拿着这份证明去寻求 IANA 的授权。

我们会部署商标信息交换机构。目前，商标信息交换机构的验证系统已经开放。我们会提供和执行预注册服务和索赔功能，预注册将从 7 月 1 日起生效，索赔将从 8 月份起生效。

作为计划的组成部分，我们的 URS 统一快速暂停程序将在 7 月底投入使用并开始运营。

EBERO 系统，即后方紧急注册管理执行机构服务将在 8 月份开始运营。另外，我们的 SLA 监控工具也将在 8 月份开始运营。这些都是《指南》中关于新 gTLD 计划的内容，也是我们目前正在构建的对象；同时也是我们准备 gTLD 运营的方式和时间表。

JEFF MOSS： 谢谢。运营准备完成后，申请人也就完成了上述所有步骤，接下来便是授权阶段，申请人应提出申请，请求 IANA 为新 gTLD 授权。关于授权请求流程，下面我们请 IANA 副总裁 Elise Gerich 谈谈他的看法。

Elise？

ELISE GERICH： 非常感谢 Christine 和新 gTLD 小组不畏繁琐，列出所有授权流程步骤。从 IANA 的角度来看，授权一个 gTLD 就像是在完成一套标准作业程序一样。过去，我们的授权准备工作要比现在多很多，大约相当于目前我们所授权 gTLD 数量的五倍。其中一项是，对我们现在拥有的自动化系统进行改进，即 RZM，根区域管理系统。该系统在 2011 年推出；从那时起，我们便一直与我们的根区域管理合作伙伴 NTIA 和 VeriSign 一起，共同致力于该系统的完善，希望在申请人申请将顶级域名授权到根区域时能及时准备就绪。

另一项准备工作是，摒弃以提交陈述式报告的方式来说明申请人已完成所有必需事项和符合所有标准，改用列清单的方法。在这方面，我们与 Christine 团队进行了非常紧密的合作。目前，该清单已在新 gTLD 流程中完成。

最后，我们还增聘了工作人员。

可以进入到下一张幻灯片吗？

关于我刚才说的自动化，可以说，我们基本上实施了一个新的工作流程，这一流程允许申请人创建新的 gTLD。而在过去，由于创建出的新 gTLD 少之又少，因此，完全不必将授权流程自动化作为优先解决的问题。

上周，我们的根区域管理合作伙伴已经完成了这一自动化流程的端到端测试。如今，我们已准备好于 5 月 1 日启用该流程。下面进入下一张幻灯片。

接下来，我要谈谈之前提到过的清单和报告。gTLD 申请人在完成新 gTLD 申请流程后，会面临许多评估小组成员的评估，这一点 Christine 今天曾花了一个多小时讲解，我想在座各位比我更清楚。

总之，评估人员会进行评估。每完成一项评估，评估人员会在一个小的复选框里面打勾。当所有复选框都勾选完以后，就会得到一张小的凭证，此时你便可以凭借着这张凭证以及网上的复选框清单，请求继续处理以获得 IANA 部门的授权。

可以进入下一张幻灯片吗？

这只是一个原型，与实际的 IANA 网站不完全一样。在座的要是视力好的话可能看得比较清楚。它大概是说，需要在网站底部输入你的新 gTLD 字符串。这里我们以 .example 为例。在字符串下面，需要输入在完成新 gTLD 计划时所收到的凭证信息。

到此就已经进入授权流程了。在授权过程中，我们要做的工作或标准做法就是，对所有 TLD 再进行一次技术检查，确保域名服务器可正常工作。另外，我们还需联系你的申请中指定的联系人以确保联系信息正确。这些都是标准的作业程序。

这里，我想向大家保证，我们已经准备就绪。通过与根区域管理合作伙伴 VeriSign 和 NTIA，以及 gTLD 小组的密切合作，现在，我们已准备好在 5 月 1 日正式启用自动化系统。谢谢大家。

JEFF MOSS： 好的，谢谢 Elise 的发言。

在说完授权流程后，接下来我想谈谈新增的所有这些 gTLD 会对根服务器系统产生什么影响，以便解决调整、测量和监控相关问题。关于这一点，我打算让 ICANN 的 DNS 运营总监 Joe Abley 谈谈他的看法。我有预感，Joe 会将 VeriSign 的 Danny 拉入这一讨论。

那么 — 哦，我需要回到上一张幻灯片，可以吗？好了。

JOE ABLEY： 谢谢 Jeff。我们现在看到的是一张很老的幻灯片，来自思科，它已经被流传了很多年。从该幻灯片可以看出，互联网流量的增长真正依赖于我们所拥有的 TLD 的数量。我们并不认为流量一定会与日俱增。

但我们希望根服务器上的流量从总体上能带来更多的流量。我们也希望流量的增长可以不受根区域大小的限制。

大家可能很难看清楚，我们所说的是根区域内授权域名数量在过去 10 年左右的增长情况。抱歉不能放到更大。可以看出，在过去 10 年时间里，新增了将近 100 个新 gTLD，增长速度非常平缓。图表中标出了增长趋势，看起来要比实际数据更为生动一些。不过，区域的实际绝对大小仍然非常小。因此，尽管在座的许多都是经验丰富的注册管理执行机构和运行根服务器的专业人士，但在运行比这大得多的区域以及区域分配比根区域广泛得多的时候，我们仍有必要感到担忧。很明显，根区域非常重要。根服务器系统也非常重要。因此，我们必须采取稳健保守的原则，确保根服务器始终保持稳定。

JEFF MOSS： Danny，你认为 Joe 的说法准确吗？

DANNY McPHERSON： 绝对准确。我认为，这里需要注意的一个事实是，在过去 14 年左右的时间里，一共新增了 67 或 68 个授权，换言之就是每年授权了 4 1/2 或 5 个域名。再看看现在，这一情况突然加速，每 36 小时左右便会新增 4 1/2 或 5 个域名。

从过去较为平缓的增长速度到现在的急剧增长，这中间必然存在一些我们需要认识到的问题。

如果回过头来看看 2009 年，大家应该会注意到，当时 ICANN 曾委托相关机构开展了一项研究，即根区域调整研究，旨在确定要调整的根区域系统的一些功能和不同影响，以及调整后可能引发哪些问题。

这里有一些事实，其中一个关键的事实就是，编址群体中的很多成员都具备在整个根服务器系统中建立基线的能力。这样，我们便可以知道所有根服务器中的延迟类型、查询数量和（听不清）以用户为中心的态度，以及根服务器是如何运作的。若没有这些基线，突然加速授权域名将会带来更高的风险。

SAC 46 曾谈及这一点，另外，SAC 46 建议 4 还提议建立一个提前警告系统，这也是根区域调整研究的一部分。目前，负责根区域运营的 RSSAC 已经在这一方面取得了一些成绩，但我认为仍然有改进的余地。

我认为 —

JEFF MOSS： 等等。在整个会议中都可以表达自己观点。

DANNY McPHERSON： 抱歉。

JEFF MOSS： 在整个会议中都可以表达自己观点，不必一次讲完。

DANNY McPHERSON： 由于根区域调整研究和 SAC 46 中的这些内容都与根服务器系统相关，因此 ICANN 有必要让大家大概看到整个系统的运行情况。我认为，在大家可以看到的情况下，SSAC 和根区域调整研究专家小组所提出的许多建议都能够向前推进。

在完全加速授权域名之前，我们必须要达到这一目标。虽然在达到目标之前便加速授权可能也是可行的，但我认为，正如机构群体所认可和讨论的那样，这绝对是我们最终要追求的目标之一。

JEFF MOSS： 谢谢 Danny 的发言。

下面，Joe，L 根服务器已经收集到一些统计数据。

JOE ABLEY： 是的。目前，RSSAC 内部仍在对起草一套度量和衡量标准进行讨论。可以很公平地说，此时此刻这些标准中大多数都相当稳定。讨论的目标在于，尝试建立一套能被每个根服务器运营商连续收集并发布的衡量标准，以便确定根服务器系统性能的长期变化趋势。

为实现这一目标，正如 Danny 所说的，第一步是建立基线，了解在当前增长水平下根服务器的基线效率。

接下来，鉴于我们已经开始添加新 gTLD，我们需要做的就是监测根服务器系统，确定是否存在任何表明系统运行艰难的趋势。我之前说过，我们不希望看到这样的情况。这个系统极其重要，我们必须要谨慎、负责任地运行它。

于是，在 4 月 3 日当天，基于最初由 IAB 与 RSSAC 的联络人 Peter Cock 编写的最初草案建议，我们开始发布过去两个月收集到的数据。

正如我所说的，这一点曾在 RSSAC 内部讨论过。举个例子：返回到上一张幻灯片，我们可以看到，幻灯片上链接引用的公告可链接至每周更新的实时统计数据。任何人都可访问该链接，跟踪我们所收

集的根区域内各个方面的增长情况以及 RSSAC 建议的各个衡量标准的情况。这里再强调一下，这仅适用于 L 根。

L 根是首个发布此类统计数据的根服务器，但我们知道，其他根服务器也在收集这些数据。而且我们打算将它们发布出来。我们刚好有个例子。我通常认为，当人们展示这样的图表时，他们往往会力求指出图标上的显著特征。但这确实是两个月以来的收集成果。它向我们展示了在整个 L 根系统内分布一个新的根区域所花的时间，此 L 根系统在全球大约有 300 个任播节点，包括位于几乎无联系的偏远区域的一些节点。在最坏的情况下，组合分布时间为 4 秒左右。图表左侧的比例尺为毫秒。

但毫无疑问，随着时间的推移，图表中肯定会出现峰值。到那时，我们会看到上升和下降的情况。这是因为我们在互联网上分布服务器，而互联网的环境每天都会变化。

对这个图表而言，重要的不是所看到的头两个月的数据特征，而是跟踪图形随着时间的变化，跟踪首个授权以及后续授权时的分布时间，以确定新的根区域在整个互联网变化过程中的分布时间。

在了解了这些之后，我们现在看到，对于每天发布两次数据的根区域，分布时间为 4 秒。即 12 小时中有 4 秒分布时间，我认为这还不算太糟。这就是我们现在面临的情况。

以下是来自另一组统计数据的例子。共有两组数据。一组是根据 RSSAC 统计数据的 L 根性能，另一组是以不同方式测量的根区域的实际大小。依我看来，图上的根区域的大小是以千字节计。不过究竟是字节还是千字节？真的很难说清楚。

这里，2010 年 7 月，大家所看到的是根区域签名阶段。这一阶段是利用加密签名、加密密钥及类似东西对根区域进行拓展。此前，我们曾就根区域大小问题使用过 net 函数。大家可以想象一下，橙色这根线沿着现有轨迹持续上升，在开始授权新 gTLD 后，此上升速度将会加快。

好了。下面我将把这一问题交给 John Crain。

JOHN CRAIN： 这里我想向大家简单展示一些数据，或者说让大家大概看一下我们根服务器系统上的数据。这些数据来自一个全球性计划。该计划由欧洲的区域互联网注册管理机构 RIPE NCC 运作。ICANN 在早些时候曾是这一计划的发起方之一。

大家请看这上面，由于我们只想展示我们自己的测量结果，因此上面显示的图表仅针对 L 根服务器。但实际上，这张图适用于所有根服务器。这里是根服务器的查询时间，即查询根服务器的速度能有多快。图上的这些点并不是指根服务器，而是互联网上发起查询请求的小型机器。这些点也可以慢慢被追踪，并将所有数据储存在数据库中。这是数据的一种图形化显示。除此之外，测量机构还测量过许多其他参数。

实际上，数据库中这几年测量的数据就是我们建立基线的依据。测量数据的机构既不是 ICANN，也不是根服务器运营商，而是第三方机构。因此，收集这类数据的目的在于 — 幻灯片底部有一个 URL。当然，大家都可以查看这些幻灯片。我会向大家提供更多 URL，以便大家从其他地方获取数据。

请换下一张幻灯片。

下面我们谈谈 L 根服务器上的统计数据。我们真正要向大家展示的是 RSSAC 文档中提到的数据格式，我们要以什么样的格式呈现数据才能让所有人得到类似的观点？

JOHN CRAIN： 有关根服务器，这里我不会详细介绍。大家如果有兴趣可另外找时间了解。

除 L 根服务器以外，其他字母服务器也会发布统计数据。据我所知，所有这些服务器都会收集数据。但实际上，这些服务器已构成公共接口，你可访问服务器以查看数据，或进入拥有大量数据的域名系统运行分析研究中心 DNS-OARC 查看数据。但这些数据格式与 RSSAC 文档规定的格式不同。也就是说，发布尚未完成，但数据却可以查看。

请换下一张幻灯片。

此外，我们与一些根服务器运营商达成了合作协议，是一些而不是所有，但实际上我们与所有此类机构都进行了合作。例如，对于 F 根服务器，我们与 ICANN 不仅达成了一项共同责任协议，还就他们要做的事签订了意向书和协议书。ICANN 曾对外宣布：“这是我们的责任，我们将认真对待，并且我们非常愿意一起合作和完成这些事项。”其他字母服务器的网站上也提到了这件事。他们都与 ICANN 进行了一些合作。

请换下一张幻灯片。

虽然大家可能未曾接触过根服务器运营商的相关负责人，但他们确实参加过 ICANN 的会议。目前，他们正在讨论将根服务器系统咨询委员会的会议纳入 ICANN 的会议中，以便大家能够与他们多多接触。不过另一方面，他们都是运营人员。在运营 DNS 服务器的同时，他们也定期开展合作。实际上，他们每年会举行三次会议，讨论相关运营问题。

JEFF MOSS： 他们同时还在试运行响应系统。

JOHN CRAIN： 确实如此。他们做了所有你能想到的事情。而且，共同完成试运行等工作也是合作的一部分。实际上，来自 VeriSign 的朋友是我们最大的合作伙伴，向我们提供资助，并举办一些技术讲座等等。

过去，我们曾经历过各种各样的事情。我们经历过改变。但如今互联网似乎仍然正常运行。这是个好消息。这样，我们便不用担心，在新增几百个 TLD 后互联网会发生崩溃。

下面有请 Danny 继续？

JEFF MOSS： 好的，Danny，请继续。

DANNY McPHERSON： 我想要补充一点。John 刚才忽略了 13 台根服务器中的 A 和 J 根服务器，此两者由 VeriSign 运作。可以很肯定地说，我们意欲在今年下半年建立起相应的公共网站，发布与 A 和 J 根服务器相关的统计数据。目前，我们正在广泛收集这些数据。

在合同方面，我们确实与美国商务部签订了根服务器协议。

从目前与 ICANN 签订的协议来看，许多承诺书都与 ICANN 的合规性框架相违背。我是说，作为 VeriSign 的首席安全官，我负责管制 8 个合规性框架中 1,385 项不同的内容。这些合规性框架受到高安全性 FISMA 到 SOX 等等的审核和连续监测。对于 ICANN，我们显然具有一些合同义务，这不仅关系到根服务器的运营，还关系到什么样的性能、数据发布或其他方面是可以接受的。我认为，严格遵守这些框架对基线建立一定有好处，并且这也是基础架构和收集等工作的常见方法。

JEFF MOSS： John？

JOHN CRAIN： 麦克风被关了，抱歉。

这里的这些图是真正的根服务器。它与我们之前看到的那张图很像。这两张图都是我们大家非常熟悉的地图提供商而作的。

这张图向大家呈现了根服务器系统的分布范围。可能有时会听到有人担心根服务器是否具备足够大的容量。这是肯定的，虽然我不知道具体有多大容量，但我可以告诉大家，L 根服务器共有 300 个节点。而

且（听不清）由我们运营。每一个节点都由 18 个单独的机器构成，具有很大的负载容量。而且，除了这 300 个节点以外，我们还拥有其他具有类似基础架构的运营商。所以，如此大的基础架构还会不断升级，这就是目前的状况。

如果再过 6 个月，我们可能还会拥有更多。而在多年前，在根服务器遭受 DDOS 攻击的时候，由于技术限制，我们只有 13 个物理位置。

这就是发展。而且，随着 DNS 和互联网不断发展，根服务器系统还会越来越强。我们要将这一优势保持下去，希望永远走在需求和要求前面。

JEFF MOSS： 谢谢 John。

下面我们将进入另一个环节，讨论 ICANN 采用何种方法来处理未知问题。此类未知问题的出现，既可能会让我们措手不及，也可能会平添一个新的问题。但我们不得不面对它。我们必须想出一个万全的缓解计划。

在讨论下一案例之前，我们先谈谈在座各位很多人都比较熟悉的 SAC 57 报告。这一报告阐述了 ICANN 在发生未知情况时的处理方式。

下面我把发言权交给 SSAC 的主席 Patrik Faltstrom。

Patrik？

PATRIK FALTSTROM：

非常感谢。下面我想先大概解释一下，我们是在什么背景下提出 SAC 57 的，然后再将麦克风交给 Warren Kumari，让他给大家详细讲讲这份报告。

首先，SSAC 的运作是基于行动的，这种行动既可能由我们从理事会或 ICANN 其他任何部门或机构群体处获得的外部问题引起，也可能是某 SSAC 成员半夜醒来思考出的自发行动。

这份报告就是这样一种自发性质的行动。我不知道 Warren 在想起这个问题的时候做了些什么，但我知道，他将这一问题提交给了 SSAC，并且我们都一致认为这是一个非常严肃的问题，必须认真对待。

关于这份报告另外一点我可以说的是，我们都知道，这类问题是我们针对早期别人所谈论的进行调查和风险分析时就应该察觉的，但我们也都知道，同安全问题打交道时，无论调查和分析报告有多深入或详尽，也无论你理解得有多彻底，总会存在一些其他问题有待发掘。因此，能够采取实际行动是非常非常重要的。

所谓的准备就绪，不是指百分之百肯定不会存在风险，而是当问题发生时，具备处理这些问题的能力。

我们发现问题后就提出这个报告。

第三，就这一报告而言，与常规做法略有不同的是，此次我们并没有立即将报告公诸于众，而是先将其送交给 ICANN 安全小组处理。因为在我们看来，这一问题非常严肃，ICANN 有必要制定一项披露政策。至于如何来做，我们待会在回来讨论。

由于这份报告的缘故，现在许多事情我们都不得不设法采用新的方式进行解决，但正因为如此，我认为，目前各机构群体应该准备好向前迈进了。

我的发言到此结束，下面有请 Warren Kumari 讲讲 SAC57 报告的具体内容。

WARREN KUMARI： 好的。我准备了很多材料，不过我打算非常迅速的过一遍就好，不会占用大家太多的时间。

下一张幻灯片。

在与 Web 服务器之间建立 SSO 或 TLS 安全连接时，基本上是以 HTPS 开始，然后浏览器将得到一个公钥并用其进行加密。此公钥位于证书认证机构签发的证书内，一旦认证机构对证书进行签名，即将公钥绑定到相应的身份上。此类身份类似于 www.example.com。当浏览器使用这一身份时，服务器会对身份进行认证，确保证书的签名正确，并且是服务器所知道的认证机构的签名；还要确保证书未过期，仍然有效；以及要连接的浏览器名称与证书中的身份一致。

认证机构颁发证书后，当他们签名时，他们需首次验证证书是否颁发给了正确的人。验证时，尤其是 — 或者只是在验证域名验证证书时 — 认证机构会向请求认证的域名地址发送一封电子邮件，即向（音频故障）example.com 或 WHOIS 中所列的电子邮件地址发送邮件。此邮件中包含一个口令，接收邮件的人须向认证机构回复这一口令，证明他确实控制或（音频故障）拥有此域名（音频故障）。

除上述证书以外，还有另外一种仅适用于内部连接的证书，称为内部服务器名称证书。是的，名称。这类证书通常用于 Microsoft Exchange、Active Directory、邮件服务器和其他许多服务器（音频故障）。这些证书中的身份形式是 www.corp 或 www.accounting 或 mail.test。与常规证书不同的是，对内部服务器名称证书而言，互联网上的其他服务器无法从 TLD 中获取用户身份。这就是说，用户无法在互联网上使用这类证书，而且，没有可供认证机构发送验证邮件的地址。

既然这样，如果某一内部服务器名称证书的结束标签突然变为一个真实存在的 TLD 会怎么样？也就是，如果结束标签被授权为真的 TLD，会产生什么样的后果？

简单说就是：糟糕的事情发生了。

现在，为了向大家示范，我为域名 www.site 申请了一个内部服务器名称证书。我知道有人会对这一证书进行验证，于是我取了一个有趣的名称 Dulles Steel and Forge，该名称（音频故障）。下一张幻灯片。

接着，我将请求提交给认证机构，这时会显示一个小的弹出框，提示说“警告：通用域名 www.site 无法连接到互联网。你是否了解这一点？

然后我点击“是”。下一张幻灯片。

三、四个小时后，认证机构给我发来了证书。大家可以看到，邮件中，（音频故障）名称是我，主题是 www.site。另外还有两个名称，或者说其实还有一个包含 www.site 和 .site 的主题（音频故障）。

好了。现在我已经拥有内部服务器名称了。那么，我能用这个名称做些什么呢？

为了向大家示范，我在实验室内创建了一个假的根域名服务器，并将 .site 域名授权给我自己。然后，我配置了 Web 服务器（音频问题），在 Safari 浏览器的地址栏中输入上述域名，果然，不出所料，Safari 弹出一个锁定图标，显示此证书有效。我是说，这样才比较公平。证书实际上是有效的。它起作用了。

后来，我分别在 Chrome、Internet Explorer、Firefox、Opera 以及许多其他浏览器上进行了同样的操作。

那么，这还意味着什么呢？

这还意味着，攻击者可能会利用上面两个有人申请过的 TLD，提出请求并获得这些 TLD 中众所周知的名称的证书。然后，攻击者要做的就是手持证书，等待这两个 TLD 获得授权。

一旦 TLD 获得授权，攻击者就会在当地的星巴克、咖啡店或旅馆转悠，利用（音频故障）名称或（音频故障）一大堆其他（音频故障）发起攻击。这时，如果用户浏览那些证书为攻击者所持有的网站，攻击者就会展示证书，让用户得到锁定图标，然后便拿着用户的所有钱、银行凭证、Cookie 文件或者他能得到的其他任何东西逃之夭夭。

因此，（音频故障）咨询委员会和我们曾建议，安全小组应成立 CA/B 论坛，即认证机构和浏览器论坛，（音频故障）旨在确定一个关于如何处理安全漏洞信息的漏洞披露政策。CA/B 论坛是一个代表

认证机构的行业组织，是所有相关方沟通的平台，同时也是我们在想出缓解措施前的一个应急计划（音频故障）。

下面我把话筒交给安全小组，让他们讲讲是如何执行的。

JEFF MOSS： 谢谢 Warren。下面有请 Steve Sheng 发言。

STEVE SHENG： 谢谢 Jeff。当 DNSSEC 在一月初向 ICANN 提出这个问题时，我们就非常重视。做完电话会议简报后不久，我们就成立了一个跨部门的缓解小组。

缓解小组会定期召开会议，按照 SSAC 报告制定缓解步骤。

这就是我们在 1 月份到 2 月份之间所做的事。我们举行了多次电话会议，包括与 CA/B 主席以及与主要认证机构的电话会议，提醒他们注意这个问题，同时他们还邀请我们在 2 月份召开的会议上发言。在那次会议上，我们正式向他们提出了这个问题。

他们也非常重视。这里我想说明一点，这个问题并不是最近新出现的问题。早在 2010 年，电子前沿基金会就指出了这个内部名称证书问题。

在这一问题上，我认为，认证机构的行动非常迅速。他们很快便通过了 Ballot 96，这点我将在下一张幻灯片讲到。

2 月 20 日，这一天非常关键，这一天认证机构执行了投票程序，并通过了 Ballot 96。这大大缩短了这一问题的漏洞时段。

在那之后，SSAC 最终确定了报告。正如 SSAC 建议的那样，在 3 月 15 日，我们便将这一问题告知了所有新 gTLD 申请人。

请换下一张幻灯片。

上一张。好的。Ballot 96 强烈建议认证机构立即停止发放内部证书，并在 ICANN 批准新 gTLD 运营后 30 日内撤销相应证书。这就意味着，ICANN 与运营商签订了合同，认证机构必须停止发放这些类型的证书，并在合同公布后 120 日内，撤销所有以新 gTLD 后缀为结束标签的证书。

在跟进这些工作的同时，我们设置了一项通知服务，用以通知认证机构哪些字符串被申请为 TLD，以及 ICANN 何时与 TLD 运营商签订合同。我们会向认证机构发布通知，帮助他们注意这些大事件发生的时间。

下一张幻灯片。

尽管如此，关于这一问题仍然存在一些残留风险。那么，下面我就用几张幻灯片谈谈这些风险究竟是什么，以及我们如何缓解这些风险。

同时，我也希望机构群体能给我们提出意见和建议。

第一类风险是，尽管我们预计大多数认证机构会遵守 Ballot 96，但由于并非所有认证机构都是 CA/B 论坛的成员，因此，某些认证机构在正式成为（音频故障）前很可能不会遵守 Ballot 96 的规定。例如，北美的 WebTrust 和欧洲的 ETSI，如果主流浏览器符合他们的标准，那么这两者都会将其纳入根证书列表中。

要缓解这一风险，我们的策略是沟通，目前我们正与能改变这一状况的相关各方积极沟通。

如果我们积极沟通的对象中有浏览器发行商，那么我们会说服他们主动要求认证机构遵守 Ballot 96。

我们认为，此流程能缓解这一风险。

下一张幻灯片。

第二类残留风险是，由于种种原因，这之中我认为主要是性能原因，一些浏览器版本不会进行实时的撤销检测。

这样，即使认证机构撤销了证书，如果浏览器没有及时检测是否撤销，则该证书仍然有效，从而导致仍然会存在漏洞时段。

针对这类风险，我们的策略依然是沟通。目前，我们已经就这一问题与相关浏览器发行商进行过沟通，并讨论如何最好地解决问题。

沟通过程中所提出的各种各样的考虑，我们都一一和发行商讨论过。

下一张幻灯片。

第三，除上述两类风险以外，在 ICANN 和 TLD 运营商签订合同与 TLD 运营商激活二级域名之间仍然可能存在漏洞时段。

下面我给大家看一个时间表。如果大家把 120 天粗略计为 17 周的话，那我们将合同签订阶段定为第 0 周。合同签订完成后，便是授权前测试，然后是 IANA 授权，接下来有一个为期 30 天的预注册通知期，通知期结束后便是预注册阶段。

我认为，这整个时间安排都告诉我们，签订合同和激活二级域名之间很可能会存在漏洞时段，关于这一问题，请翻到下一张幻灯片，我们真心希望机构群体能够提供一些意见和建议，告诉我们作为协调者，我们应该如何做才能最好地缓解这一风险。

正如 Jeff 和 Patrik 前面所提到的，有时候，要提前预测所有风险是不可能的。所有我们需要做的就是，时刻准备好采取应对措施，并拥有一套应对流程。我要讲的就是这些，下面有请 Jeff。

JEFF MOSS： 谢谢 Steve。

我希望这张图能稍微大一些。实际上，这是我们协调漏洞披露流程的流程图，此披露流程已经被 ICANN 采纳，我们还在上个月公布了这一流程，并将其应用在了 SAC57 报告上。这次应用相当于为确保流程起作用而进行的试运行，以便发现有什么不足的地方再进行微调。

今后，我们便要按照这一流程执行漏洞披露。

流程中包括多种处理漏洞披露的方式。

下面先来看这一种：作为机构群体成员，你发现了根服务器、根服务器软件或域名服务器存在某一问题，并将此问题报告给了 ICANN。

接下来，我们便要根据漏洞披露流程，决定如何将此问题信息披露给各相关方。

另一种情况，当我们 ICANN 也是相关方之一时，如果你发现我们某一 Web 服务或 Web 应用程序存在漏洞，并跑来告诉我们说：

“ICANN，我发现了你们的一个问题。这个到底是怎么运作的？你们会公布我的名字吗？这个过程是否是透明的？”或许我不希望我的名字被公布。这样的话，我们就会按照漏洞披露流程来披露我们自己的漏洞信息。

可以看出，处理漏洞披露问题的一个通用方法就是，通知相关各方，并与不希望直接与相关方联系的人们或机构进行协调。

好了。

接下来，这是一张最近发布在 SSR 上的图片，希望各位机构群体成员之前都看过，但以防有人没机会看到，我在这里大概说一下，这张图片形象化地向大家呈现了 ICANN 应对风险和与机构群体沟通的总体方法。好了，这是本演示文稿中的最后一张幻灯片，相信在座各位都有一些疑问并将它们记下来了，下面请大家随意提问。

我知道，听众席中有一些代表是来自 — 好的，Danny —

DANNY McPHERSON： 我只是想在回答大家的开放式问题前，先返回到内部名称证书那一部分。实际上，针对第 45 张幻灯片，我想说几句。

JEFF MOSS： 好的。那下面我们先返回到前面。哪一张？这一张吗？

DANNY McPHERSON： 或许可能是第 44 张。

JEFF MOSS： 这一张吗？

DANNY McPHERSON： 对，就是这一张。

JEFF MOSS： 好的。很好。

DANNY McPHERSON： 这里我想指出一点，我相信 Warren 在 ccNSO 或 ALAC 会议上也曾提到过，如果我说错了，Patrik 作为 SSAC 主席可以纠正我，我觉得对于从总体上是否可接受这一点并没有与 SSAC 达成协议，与广泛的机构群体也是一样。

另外，我认为漏洞时段实际上是未知的。如前所述，由于许多申请实际上并不支持证书撤销，或者当存在中间人攻击时，攻击者必然会阻止那些撤销功能继续运行，因此，我认为，要实现这些至少要等到 2016 年，这一点我想 DigiCert 的 Jeremy 在 ccNSO 上也曾提到过。Jeremy 可能也在场，如果我有说错，他可以进行澄清。

另外一方面我想要说明的是，想必大家都知道，面对任何风险，我们可以有四种选择。

那就是：规避风险、控制或缓解风险、接受风险、转移风险。

任何不能彻底解决问题的做法最终都会是单方面地将风险转移给用户，我说的对吗？因此，我们在 gTLD 中引入新的域名空间和相应事物后，最终受到影响的必然是那些在该域名空间里消费的人们。

也就是 Warren 所举例子中那些在星巴克上网更新财务记录或健康档案而遭受中间人攻击的人们。

因此，关于 Fadi 早些时候的讨论，我认为，这世上并没有可以立即解决这一问题的灵丹妙药，机构群体唯一能做的就是进行大量的协调，执行大量的工作。

目前，我们的工作看似突飞猛进，但这却是 ICANN 负责安全事务的工作人员在过去三个月努力的结果，大家知道，就是 Jeff 刚才提到的那些工作。我认为，这些工作真的非常繁重，而且目前仍然 一 大家知道，由于目前仍然存在大量未知的残留风险，因此，如果我们不顾这些风险继续向前，最终势必会把这些风险转移到用户身上，这是我们需要担忧的问题。

我要说的最后一点是，在 Patrik 和许多其他同事所负责的 RSST 研究中，以及在 SAC45、SAC46 和 SAC57 等报告中，存在许多有关跨学科研究的讨论。这些研究所讨论的内容正是 DNS 允许用户在互联网上访问的内容。

理想情况下，用户访问互联网内容是安全、稳定、可预测和可靠的。大家都知道，在互联网上，用户通常不会去访问 DNS 中的内容，而是利用 DNS 访问其他地方。因此，如果出于安全和可靠的目的，回头将这些依赖系统与全球 DNS 绑在一起，那么在未与用户协调前，我们不应该单方面地更改这些系统，以免影响系统的安全性和可用性。

好了，以上就是我想就这一问题指出的几个关键点，Jeff，谢谢！

JEFF MOSS： 谢谢，Danny。

我还要指出一点，我们在其他根服务器运营商、CA/B 浏览器论坛和 CA 的受众中也有一些代表，所以我希望能和本机构群体中的其他专家一起进行热烈讨论。

那么现在我们一起来看关于问题的幻灯片。大家可以使用左侧的麦克风提问。请大家在提问的时候先说一下自己的姓名、来自哪里，然后再提问。

JEFF NEUMAN： 好的。我叫 Jeff Neuman。我来自 NeuStar。我昨天问过 Faltstrom 先生一个问题。我想应该是昨天。我在时间上有些混乱。也许是两天前。有一次在针对 GNSO 委员会的 SSAC 演示中，Faltstrom 说道，作为理事会的咨询委员会，SSAC 并没有建议 ICANN 理事会推迟或放慢新 gTLD 计划。

从 McPherson 之前提出的意见来看，你似乎仍然相信存在着重大风险，我相信我们大家都听到你说的了，那么我要向 McPherson 先生提这样一个问题：

关于降低风险，是否能在会上提出些具体的建议？我的意思是，既然注意到有一些风险，那么你下一步打算怎么做呢？多久能解决好这个问题？如果正在实施降低该风险的计划，那么你都会做哪些工作呢？

DANNY McPHERSON： 好吧。我将与 ICANN 特许专家研究团队从 2009 年起针对不同学科间的相关性所提出的要求一样，开始研究问题空间。

我觉得，在过去的两三个月里，人们很认真地观察，然后说“嘿！我们马上就要实施这个新 gTLD 计划了，这样做会带来什么影响呢？”人们开始纷纷说“如果授权了这个 TLD，而且我在内部使用并入网了，那意味着什么呢？”这是个很有趣的情况。或者人们会说“整体上根服务系统的可见度如何？我们是否具备提前警告的能力，使我们可以识别威胁？可不可以假设说我们开始实施这个计划时就会具备这个能力？”

所以说，我对此并没有什么灵丹妙药。我知道机构群体中有很多聪明能干的人，而且在与那些依赖 DNS 的相关系统的协作下已经取得了很多不错的成就。我也知道对此还需要做一些工作。

至于时间表或任何在此之后的事情，当然需要整个机构群体的努力来确定，以及是否需要推迟。

但是我觉得对于我的组织，如果我有决定权的话，我当然会考虑其影响。从我个人角度来讲，为了我的个人健康、金融交易或其他方面，我不会使用新 gTLD。也就是说，如果我想到我正在使用的基础设施内部隐藏着这些问题，我是不会选择使用新 gTLD 的。

我将会使用更稳定的服务，这样我们才能享有可预测的、安全的性能。这就是我的回答。

JEFF NEUMAN： Patrik 有什么想说的吗？

PATRIK FALTSTROM： 是的。我想澄清一下。针对你问的这个问题，我已经从两方面做出了回答。

其一，SSAC 是否在着手进行该工作的后续工作，答案是在当时并没有。

第二个问题是，我们在接到 VeriSign 的来信后，是否采取了什么措施。对于这个问题，答案依旧是没有。

JEFF NEUMAN： 好的。我还要简短地再说一句，如果可以的话。

JEFF MOSS： 好的。

JEFF NEUMAN： 这是关于所有的 TLD 还是你只关心诸如 .site、.corp、.home 之类的一小部分域名？

我的意思是，理论上讲，如果有人要做的话，所有域名都可能出现这样的问题，所以我想知道你真的关心所有域名吗，还是只关心其中一小部分？

DANNY McPHERSON： 我认为有些域名的问题更大。我相信如果没有由所有认证机构发布的证书全集，大家永远也不会想到这些，这只是我的想法。另外，在这些新 gTLD 的使用上可能会有不同的级别。

大家知道，还牵扯到其他方面，我想来自 PayPal 的 Bill Smith 等也提到了一些。所以我认为简单地说确实有不同级别。

事实上 Warren 做了一些分析，所以在此事上他应该有话要说。

WARREN KUMARI： 是的。在对被公开的证书库的 EFF SSL 观察数据做分析时，我们发现了一些关于 .home 和 .corp 等可以在根服务器的查询副本中看到的域名。不过还有关于 .ads 的一大堆东西，我们也不知道那些是什么。最后，我们认定这是 Active Directory 服务。但是只有你真正看到那里的证书才真正知道是些什么东西。

所以除非你能从所有认证机构得到具有代表性的样本，否则是不可能知道已发布的内容的。

JEFF NEUMAN： 那么国际化字符是不是也是同样的威胁呢？还是主要是 ASCII 呢？

WARREN KUMARI： 不清楚，不过我想坐在你身后的人或许能回答这个问题。

JEFF MOSS： 我得先走到这个麦克风前才能发言。

CHRIS WRIGHT：

我叫 Chris，来自 ARI Registry Services。

我也有个类似的问题需要问 Jeff，不过问题可能稍有些不同。

会议对我们快速处理引入新 gTLD 期间存在的 SSR 问题很有帮助。我们可以在同一个地方看到所有信息资料，而且这些资料经过简化后更易于我们看懂，这一点是很好的。

不过，我没能从本次会议中了解到 ICANN 的行动计划是什么；我也不知道 ICANN 将会进行或亟待进行什么样的活动去解决这些问题，这些活动的时间范围是怎样的，我们该用什么指标来衡量每一个问题对我们的影响、我们对问题的掌控程度以及继续下去是否安全，我们需要达成的具体目标有哪些，最后就是关于新 gTLD 计划的所有这些问题的总体影响有哪些？

所以我要从另一个角度来提问，或许比 Jeff 的问题少一点政治性的东西。我的问题是，ICANN 在每个问题上的立场分别是什么？ICANN 此时是否已经妥当地缓和了这些安全问题？残留风险是否也已经在令人满意的程度上被接受或被转移了？

JEFF MOSS：

那我现在开始回答你的一系列问题。如果我走题了可以纠正我，我觉得这样说应该没错，那就是技术群体对于提出的技术问题都理解得相当好，没有一人觉得吃惊。我想，如果大家回想上个月发生的事情，就会发现所有的问题都一直在逐渐得到改进。那么，举例而言，人们曾经有过这样一个担心，即 ICANN 没有合适的系统可以在签署合同时通知认证机构。现在这样的系统已经于几天前开始启用了。有人担心没有选定 EBERO 提供商。而事实是他们已经选定了。

而且，我们有一个清单用来跟踪每一个问题，针对每一个问题我们都有相应的补救措施或应对预案。此外，我们每次都会选择解决其中一个问题。

目前，在 ICANN 运营的领域中，我们可以掌控我们自己的命运，这在我的管理范围内，是我负责缓和这些问题的。比如我们在 SAC 57 的情况下与机构群体进行合作，那么我们将会有很多合作。Steve Sheng 谈到了他与主要操作系统和浏览器发行商共同开展的所有工作，但是只有当我们与他们的合作告一段落的时候，我们才能告诉大家。也许看起来好像是有一段空白，浏览器没有变化。我们取得了一个解决方案，然后我们再就此进行宣布，这与 CA/B 浏览器论坛很像。但这些并不是我们正在做的唯一一件事。我不知道大家对这点有没有想补充的。没有吗？好的。那么由 Jeremy 来说吧。

JEREMY ROWLEY： 我是 Jeremy Rowley，来自 DigiCert，代表认证机构。我想建议大家采用漏洞报告机制，如果能增强该机制的功能并且让该机制更加公开，那就更好了。抱歉，我是不是讲得不够清楚？因为我们是在你们找我们解决问题不久前才发现的这个问题，而且我们不确定应该由谁来解决这个问题，因为它确实不能算是异议或类似的什么东西。所以，如果你有更好的途径汇报此问题，那么识别这些类型的问题就会变得更简单。

我现在要回答之前那位先生提出的问题，事实上，只要攻击者能满足浏览器的要求，即显示自己可以控制域名，就能得到任何他们想要的域名。而且他们确实能控制域名，因为他们有带服务器的机盒，并不是一个 gTLD。所以这个问题存在于每个 gTLD 上。是的。

每个单独的域名都可能存在这个问题。我们已经看到了排名前四的问题域名，它们分别是 .corp、.ads、.mail 和 .bank。这个问题就是这样。

还有，我要简单发表一下我对于撤销问题的看法。我认为如果大家开始使用 OCSP stapling 的话，该问题是需要首先解决的，因为你无法在此基础上阻止撤销回应。

JEFF MOSS： 有没有使用 OCSP stapling 的浏览器？

JEREMY ROWLEY： 有，我想所有主流浏览器都支持 OCSP stapling。这要看客户的服务器上是否开启了该功能，而且我相信按照国际标准是默认开启的，所以说只需在 Apache 和 Genex 上将其开启就可以了。如果没有开启，很多行业组织目前就会将此作为解决方案进行推广。

JEFF MOSS： 所以也许你会建议我们采用这样的方式减小风险，即与服务器制造商合作，让他们默认开启 OCSP stapling。

JEREMY ROWLEY： 是的，这将是很好的解决办法。我们正在为之努力，如果其他人也在为之努力，那么此事将会进展得更快。我想说的就这么多。

JEFF MOSS： 先生，请讲。

BILL SMITH： 我是 Bill Smith，来自 PayPal。是的，PayPal 确实向 ICANN 发过一封信，信中内容基本上是关于排名前 13 的私营顶级域名，且这些域名在发出 DNS 解析请求的根服务器流量中占约 10% 的份额。这个数字很庞大。我们的建议是不要授权这些域名。大家知道这也许会导致一些问题。我们也关注其他域名，不过我们尤其关注这些域名。而且现在还没有确定转移这种突然出现的风险所带来的影响。我们无法解析这些域名。该问题不会发生。那么突然间，我们开启某个功能，10% 向根提出的解析请求就可能会被解析错了。是不是？这是几十年来这些私营 TLD 一直都在经历的事情。所以，我们认为这是个严重的问题。事实上，我们建议 ICANN 和 CA/B 论坛尽快回应此事。虽然我们给予了关注，但是我们对此的关注度还是不够。我想我的问题核心还是在于此，即我们如何确保这个解决方案在所有参与者的 DNS 系统、证书授权系统以及所有其他系统上都能起作用。最后就是，我们讨论了浏览器供应商所做的工作，这很好，但是我们之前并不是只通过这些人或这些应用程序来上网的。我们仍然要考虑所有那些问题。所以说这是个重大的问题。事实上，对于这个问题，大家在相当一段时间前就已经意识到了。所以，大家都知道，我的问题其实是 一 我们怎样才能确保自己不再重复出现这些问题呢？

JEFF MOSS： 那么，有个问题要问你。首先，我想说明一点。在我们给你的信中说了，ICANN 仍在继续调查情况，尚未做出最后决定。所以不如我们跳出这个“二选一”的思维框架，即不要考虑是授权还是不授权，而是想一想两者之间是否有另外的解决方案。或者头两年先不要授权，给大家时间进行修正？

BILL SMITH： 那我谨代表我个人来就这点发表下看法，因为我知道 PayPal 可能在此事上有不同决定或不同观点。我想答案是肯定的。我觉得我们不必非要“二选一”。但是如果我们确实要做出决定的话，那么应该是更倾向于“不授权”，而且“不授权”的范围要更广些，至少要包括这 13 个顶级域名。而且，我们对其他域名的处理也要持谨慎态度。正如 Jeremy 指出的，真正的问题是因为我们没有任何可查阅的记录，所以我们不知道对所有顶级域名或任何其他字符串已经发出了哪些作为私营 TLD 的证书。即便我们立即采取措施，我们也要在一段时间内面临这个问题。因此，我认为在“绝不授权”和“立即授权”之间还有其他选择，不过这个选择应该更倾向于“不授权”。

JEFF MOSS： 嗯，你的答案比较保守。

BILL SMITH： 我们对类似于 .corp 这样的域名处理起来更要保守一些。这是有道理的，这是常识。务必不要立即授权此类域名。在所有对根服务器的请求中，有 10% 的请求都属于此类，而且都会被视为无效请求。所以若是能解析，也将会是错误的解析。

JEFF MOSS： 好。首先我要问一下，有没有人想继续就此事发表意见？没有吗？请 Patrik 发言。

PATRIK FALTSTROM： 好的，我要谢谢你给我表达意见的机会。我还要感谢你参与了那次对话，因为正如你在信中提到的一样，当 SSAC 谈到这些问题时，我们在 2010 年 11 月 15 日发布的 SAC 45（听不清），答案是肯定的，我们确实与 Jeff 和其他人开展了对话，对话主要是关于我们和 SSAC 是否应该重新编写 SAC 45 或其他文件以便研究调查这些灰色地带的问题。所以我觉得机构群体中大家都站出来发言是非常好的，如果你们没有时间、来得比较晚或者有什么别的问题，也一定要找机会和我们进行交流。我们齐聚一堂就是为了达到这个目的，就是为了想办法解决这个问题。谢谢。谢谢。

RUBENS KUHL： 我是 Rubens Kuhl，我要说的是关于 .br 的事。我有个问题想问问 Steve Sheng 和 Warren。你们是否考虑过修改浏览器的事情呢？比如说检查一下证书的发布日期。如果该发布日期在我们所知的 TLD 授权日期之前，那么这就是内部证书，我们现在就可以忽视该证书，因为此域名现在已经得到授权了。所以说这也是个选择。

STEVE SHENG： 谢谢你的问题。当我们与浏览器供应商进行交流时，他们确实向我们提供了这个可选方案。我们现在就是要研究可行性的问题。因为，大家是知道的，当域名得到授权的时候，我们需要让供应商们看到这个可行性。所以我们正在研究该措施的可能性，而且我们会在这方面为你提供更多的新信息。

WARREN KUMARI： 大家要记住的是，仍有相当多的人在 Windows XP 系统上使用 IE6 浏览器。

RUBENS KUHL： 这样的话他们就会有安全问题。

WARREN KUMARI： 他们还有很多其他方面的问题。不过只需要设法不让人们在某个特定日期提前得到证书。我们要面对许多旧域名，而且也不是所有事物都在互联网上。如果大家仔细阅读了整个 RFC 系列，就会发现其中约有 850 处提及了证书，还约有 870 处提及了 TLS。还有例如 AAA、电子邮件和 Jabber 等其他协议以及所有其他东西都依赖着证书。所以说大家在这方面也有同样的问题。

RUBENS KUHL： 好的。谢谢。

MIKEY O'CONNOR： 你好，Jeff。我叫 Mikey O'Connor。这里大多数人都只知道我是工作组中最热衷宣传的人，不过在此我还要向大家展示我的另一面，其实我对 ICANN 也很有兴趣。我拥有 corp.com 这一域名，无论我为该域名开放哪种路由，流量都很多。我面对的流量太多，以至于在约 20 分钟后，我的 ISP 中的虚拟链路就饱和了。我非常愿意为任何想要研究这种情况的人提供这些流量数据。我可以告诉大家这不是网络请求。这涉及到各种各样的活动目录、交换服务器、奇怪的端口和用于未知事物的未命名端口。流量大得惊人。这不是在根服务器导致问题时出现的，而是在 .com 级别上的问题。所以我只能想象开

始将 .corp 路由到互联网上的其他地址时会发生什么情况。所以我愿意加入来自 PayPal 的 Bill 的行列，我也会很高兴为那些想了解一下情况的人们提供数据流。

JEFF MOSS： 所以说你认为在 .corp 上不存在自动完成 .com 的情况？

MIKEY O'CONNOR： 是的，我认为不存在。原来在很多关于如何设置小型服务器的 Microsoft 文档中，默认的都是 corp.com。这就是在涉及到 .corp 时会遇到的一类问题，因为按照惯例 .corp 就是那么使用的。不过，大家都知道，举例来说，Microsoft FrontPage 多年来都默认解析为 company.com，当时我恰巧也使用的是这一默认值。关于此事的继发效应，我有很多相关的处理经验。关于这种情况会导致什么问题，我手头有个很好的例子，那是当我第一次为 corp.com 架设电子邮件服务器的时候，发布前，我花了大约十分钟的时间才将寄错地址的电子邮件发到包含 SEC 备案的 joecorporatefinance@sun.corp.com 中。为此，我不得不对 DNS 服务器进行过滤，还得关闭所有此类服务器，因为很明显它们将导致包括我在内的许多人遇到各种各样的问题。幸好我是个遵纪守法的好人，如果是个心存邪念的坏人，那就会产生各种问题，而且现在会发生什么样的状况我们都不得而知。

JEFF MOSS： 谢谢你将其提供给研究员而不是有组织的犯罪集团，因为也许他们会比我们出的价钱还要多。

MIKEY O'CONNOR： 是的。不过，无论如何，我都很乐意在保护措施合理的情况下为大家提供这一服务。但是我想指出一点，这是现实世界中碰到的问题，而不是不值一提的虚拟世界发生的事情。要知道，流量非常大。

JEFF MOSS： 谢谢。有没有人想就此发表意见？有人吗？没有吗？好的。

ANDREW SULLIVAN： 我是 Andrew Sullivan。在上一次会议中，有一个关于授权前测试的演讲，演讲中建议我们需要让受试人和测试人之间有互动，因为很明显这并不是一个仅关乎“测试通过”或“测试失败”的完全机械的过程。而且，我们通过观察知道大家都突然间意识到我们从开始行动到现在仅有几个月的时间，也许是时候开始考虑此问题了。我想知道我们此时发现的问题是否会比我们原本想的风险还要更大。我们要启用新域名，而人们在我们启用之前的几个月里却只是关注实际风险的问题。所以我想知道专家小组是否从这个已经非常棘手的认证机构问题出发，更进了一步，也就是说是否对于该领域的一般风险有什么分析见解；还有，关于不考虑其他方面的影响就授权这么多新的 TLD 会引发的风险，我们是否要重新考虑我们的立场。谢谢。

CHRISTINE WILLETT： 在某种程度上，我想我可以就授权前测试说说我的看法。想要让测试人和申请人之间进行更多互动并将这一互动作为授权前测试的一部分，这种想法要建立在确保申请人有能力为启动测试提供必要文

件的基础上。这并不是说缺少自动化或无法进行自动测试，而是沟通问题，或许是语言障碍。所以我们要通过努力扩展 G 空间并且让需要的文件清晰化、具体化。况且，我尚未得到任何反馈说工具或自动测试有问题。我只是想针对你意见中授权前测试这部分说一下我的看法。

JEFF MOSS： 我得说，这不是我们第一次扩展 G 空间，而是第三次。所有这些问题从我们第一次为系统添加新 G 的时候就已经存在了。我认为现在存在的情况是可路由的空间大小比过去更大了。现在我们授权的可能是比较倾向于 .bank 这种域名，而且这会比 .info 更吸引那些怀有恶意的人。我们现在面临的问题与我们一直以来都有的问题是一样的，不过我们只是更清楚地看到这些问题的存在罢了。Danny 你觉得呢？

DANNY McPHERSON： 是的，所以我希望回应一下 Andrew 和 Christine。从运营的视角来看，我们公司已经拥有了与运营注册管理机构相关的大量基础设施和系统知识，而且，退一步说，我们找到了授权前测试问题的大量相关文件。事实上，我认为你们感兴趣的那些文件都反映在我们分别于 2 月 8 日、3 月 18 日发出的信中，以及 Akram 和注册管理机构利益主体组织之间的交流中。二者间的交流为众多正在解决中的问题进行了分类汇总，但还有很多遗留问题尚未包括进去，比如说试授权前测试的相关问题。我只是想授权我们公司的一个区域，我们此刻正好有 110 个任务，对吧？看上去这恰恰是发生在各个方面的情况。我们在为我们自己的内部运营工作进行序列部署计划和项目

规划时，这样的严格程度是很重要的。我们当然也希望在授权前测试的各方面也能达到相似的严格性。我认为情况当然会变得越来越好，而且我们很高兴看到目前有所进展，也希望能看到更多进步。

对于 Andrew 的意见，我要说，从某种角度上来说，我完全同意你的观点。我想我这么说仅仅是因为你为了后退一步真的付出了努力，还指出有迹象表明我们正在让当前的系统发生改变，也就是说让系统变得让用户更加想去访问其内容或更加注意互联网等等。要不是你真的后退一步去仔细研究那些方面，你是不会有这么多发现的。而且我认为那的确是我们所看到的产物。看上去这有些晚了，但是其实是因为人们最终才看到我们的运营带来的效果。因为，坦白讲，不是每个人都会追随 ICANN、DNS 或 IETF 等机构，而是每天忙着自己的工作。对于我们以及在座各位中的大多数人来说，我们的工作就是围绕网络和 DNS 展开的。这就是我们的工作。我们投身于这个行业。我们关注，我们用心。但对于这个行业以外的人员，那又是另外一回事了。

JEFF MOSS： Joe 你有什么看法？

JOE ABLEY： 那么，既然大家比较关注根系统，我觉得我还是谈谈我对其规模的看法吧。比之过去，我们在结构上有了很大变化，我想，注意这点是很重要的。我们现在面对的情况是这样的：根区域发展的规模相对于现在来讲较大，但从绝对意义上来说又非常小。我们并不是说要添加新的资源记录，也不是要改变初始时期，更没有说要改变协议或返还签名等。我们谈论的是和平常一样的根区域业务，不过根

区域比之前稍大一些。如果我们想象一下我们正在讨论目前的根区域，或许也会在这里结束相关讨论，那么其实我们已经在这里充分讨论过 .info 和 .org 了。这些都使用了相同的协议。它们也使用了相同的软件。所以，我认为我们应该采取所有对本基准的建立有必要的防范措施，并在发展该根区域的同时进行测量，还要跟踪性能变化，这点很重要；而且，我相信 Danny 当然也会同意这个观点的。我认为，事实上，根服务系统的变化并不太大。我们听到了一些与根区域没多大关系的其他事情，我们所关注的事情是针对非常重要的系统。而且，Danny 当然可以就此发表看法，不过我想我们更期待相对于这一发展而言可以忽略的系统的反应。

JEFF MOSS： 先有请 Patrik 发言，Warren 可以随后发言。

PATRIK FALTSTROM： 好的。只是因为有不同的（听不清），我也在运营 L 根，我想要补充一点，Joe 说我们也不仅仅是在运营根区域，还运营着若干 ccTLD。所有这些 ccTLD 都要比根区域大很多倍，所以在任何情况下，这都绝对没问题。

JEFF MOSS： Warren 请发言吧。

WARREN KUMARI： 事实上，我要对 Jeff 刚刚说的问题作出回应。是的，我们以前推出了新 gTLD。不过推出之后我们经常会碰到一些问题。比如说，Ram 在 .info 上有问题，它推出的时候实际上并没有得到人们的认可。而且看上去我们现在的关注点实际上是 DNS 本身和其他系统之间的互动。也就是 SSAC 曾经要求过的跨学科研究。

JEFF MOSS： 在 ICANN 语言中，这些是得到普遍认可的问题是吗？

WARREN KUMARI： 嗯，这些属于 Ram 谈及的 .info 一类问题。不过其实更倾向于 DNS 和预期会消耗 DNS 的申请之间的互动。所以是的，它们确实是普遍认可的问题，但同时也是跨申请的问题。所以我现在认为普遍认可问题可能快要得到解决了，不过将会对依赖于 DNS 的其他事物造成不良影响。

JEFF MOSS： 所以在那些情况下，我想大家会期望看到当我们无法控制 python 如何解决问题或无法控制 Microsoft 应用程序如何查找域名时，ICANN 能越来越多地作为推动者或协调者进行运营。不过，我们当然也可以向他们指出，我们已经决定目前是存在问题的，如果他们能着手解决该问题我们将不胜感激，并且我们可以派出专家协助他们解决问题。所以我认为在处理 ICANN 运营并有直接影响的问题的同时，大家将会看到我们越来越多地扮演推动者或协调者的角色。抱歉。先生，请讲。

PAUL STAHURA： 好的，我叫 Paul Stahura。我来自 Donuts。我饶有兴趣地阅读了 SSAC 的报告，其中引用了一份 2009 或 2010 年的调查。然后，我…

JEFF MOSS： 你是说 EFF SSL 观察报告吗？

PAUL STAHURA： 是的，我觉得其中引用的调查太旧了。大家知道，现在是 2013 年了，所以说那份调查已经大概是四年前的了。

JEFF MOSS： 好的。他们没有及时更新。

PAUL STAHURA： 我更新了。

JEFF MOSS： 哦，好。

PAUL STAHURA： 那么我现在来报告一下结果。我们检查了 com 和 net 区域，检查了这两个区域的每一个域名，然后检查了那些域名指向的每一个服务器并且观察了 2500 万个证书。我们还对这些证书中的每一个都进行了仔细检查，并且发现了顶级标签。我们发现在 2500 万个证书中本轮共有 51 个新提出的 gTLD。2500 万个证书中发现了 51 个 TLD。我们得出的结论是最大的是 .corp，和调查报告中的一样。然后我们检查了 .corp 中提到的子域名，我们发现在 .corp 域名所有可能出现的

巨大空间中共有 102 个特殊的子域名。另外，我们发现空间第二大的是 home，其中有 42 个特殊子域名。Offline 排名第三，Inc. 排名第四。我也有 .corp 的清单。我们发现的 .corp 中有 park.corp、digi love.com 等，共有 102 个。我们为什么不阻止这些域名一段时间呢？或许可以像那位来自 VeriSign 的先生所说的一样，阻止到 2016 年怎么样？我们可以只阻止那些带 .corp 的子域名，而不必阻止整个 .corp 域名空间。我们现在可以停止发放这些证书，然后阻止一些域名，知道以后某个时间再解除阻止，这样做是不是可行呢？

JEFF MOSS： 谢谢。

DANNY McPHERSON： 我能回应一下吗？

JEFF MOSS： 是的，

DANNY McPHERSON： 你是叫 Pete 吗？

>> 我叫 Paul。

DANNY McPHERSON： SAC 57 中有个很有趣的事儿，从 2010 年起，其中一个数字就始终是 37,000，从未变过。我认为做出更新是件非常棒的事情。我将很高兴看到该成果能发布出来。

>> 听上去不错，我会发布的。

DANNY McPHERSON： 但是，我想指出的一件事是，那些其实是内部域名证书，而且实际上不会在互联网中使用，对吗？所以你们在互联网上找到的是人们泄露到互联网上的。因此那绝对是下限，你得寄希望于人们能正确配置他们的系统并且拥有比那些多出几个数量级的证书。所以在没有认证机构证书库的情况下，确认针对哪些数据流发放了怎样的证书范围是不可能的。

>> 我同意，样本量是非常巨大的。

DANNY McPHERSON： 对于面对内部证书的互联网，确实是这样。我表示完全赞同。

JEFF MOSS： Jeremy，请发言。

JEREMY ROWLEY： 好的。我想说的是，Bill Smith 发现的问题在大多数这些域名中与认证机构问题有关，但也有不同之处。很多架设起来的网络都是内部的，所以即使在域名可解析的情况下，它们也无法被解析。我的意思是，这些是内部网络。因此，大家在互联网上将会与所有这些架设的内部服务器或其他类似事物发生很多冲突。人们会去咖啡店上网，并且会想着使用 .corp 的电子邮件服务器；他们将不再使用他们不想用的那些新 gTLD。大家将会遇上许许多多的那类问题。而且它们与为这些域名发放的证书是不同的。因为，从某种程度上说，认证机构可以处理好证书问题。这些网络已经将它们的整个运营工作都集中在这些内部网络中，以便让运营工作进行重新配置，从而避免它们产生所有这些问题。但是我想知道的是，大家为了连入这些网络都做了哪些工作？我不确定是否已经做了任何外展工作。你们大家确实在报告中确认了该事，但是你们最终还是找到我们认证机构解决问题。不过，确实有向他们进行外展的需要。大家是否已经在这方面已经开展工作了呢？

JEFF MOSS： 有没有哪位想就此话题给出意见？Patrik 先讲吧，然后我再讲。

PATRIK FALTSTROM： 我想你指出的问题是非常合理的。即便情况是这样的，即某个域名确实属于内部网络，正像你所说的那样，确实可能发生这样的情况，结果当然也会不同。这取决于域名的解决方案是基于内部区域之内还是之外，这不仅仅是涉及到你使用的是否是外面的公司网络，还有，比如说，你的 VPN 连接是否成功，因为有时候 VPN 的连接会不太可靠。当然，这就是我们目前在 SSAC 关注的问题。不过，

正如我早先所说的，这并不是我们选出的工作议题。但是，鉴于我们在此进行的讨论，最好的情况就是会发生一些触发情况，能为我们充实一些工作内容。

STEVE SHENG： 而且，事实上我相信 SAC 45 中的一个建议就外展到了那些可能受到影响的事项，而且我认为那还是一个开放项目。

>> 我只想说，截止到 2011 年，文件显示大家实际上应该在多个项目上使用这些内部服务器域名，如 BlackBoard、Exchange 等。那么我想问问大家 CA/B 论坛选择 2016 年作为弃用日期的原因是什么；我们弃用整个这些域名是因为我们的很多客户，尤其是在教育领域的客户都反映说他们到了那时也无法做出改变，因为他们需要时间去升级他们的网络，以便让网络运营商得到恰当的培训并落实好其他事宜。你说过，不要在完全肯定与完全否定中二选一，而是选择可以得到授权，但要在 2014 年或 2015 年等我们有机会清除这些内部服务器域名证书的时候才能得到授权；另外的条件是我们得确信认证机构会在两年的时间里停止发放证书，而且不会再出现任何问题了。我赞成你的意见。你甚至还可以拥有可以提供支持的浏览器。此外，在该日期之前发放的任何证书都不可信。这就允许所有人都能有时间进行改变，从而完成转变。

当客户对你说“我的证书将在两个月后过期，我想买个新证书”的时候，基本上他们就会得到这样的回答“我很抱歉，先生，恐怕你不能购买新证书了，你得自己想办法。”

>> 该文件于 2011 年被采用，当时要求所有认证机构都要尽力去减轻风险。但是，客户总是在证书到期前两天左右联系你。他们会说：“太糟糕了，我得为我的服务器买个新证书，不然我的整个运营工作都会处于不安全的状态”。因此，我们会给他们一年的证书等等。

JEFF MOSS： 所以你一直都与他们有联系？

>> 是的，自 2011 年起，认证机构就应要求进行外展，避免他们使用该域名。

JEFF MOSS： 好的。Warren 请发言吧。

WARREN KUMARI： 我也要提一点，与更改人们的所有其他基础设施以便重命名相比，让人们将他们需要的服务器域名更改到完全合格要简单得多。所以让服务器域名改为 mail.corp，然后获得涵盖从 mail.corp 到 food.com 的证书，该方法与全部改为 .Corp 是不同的。那绝对是一个值得关注的问题。

>> 事实上，最高论坛早就围绕人们使用该方法的原因做过研究，也许我可以将该研究分享给大家。我得看看我是否能得到允许。他们得出的结果很有趣。很多人认为这些内部服务器域名都是必须的。他们并没有意识到自己可以使用一个 FTD，也不知道如何使用。

JEFF MOSS： 我们的时间还允许再提问一个问题。

CHRIS： 这次发言的还是我，Chris。恕我愚钝，我想问一下你们大家可否为我概括一下，在这种情况下，你们希望机构群体采取哪些行动？ICANN 又会采取怎样的行动呢？Fadi 曾表示，如果出现安全和稳定性方面的顾虑，他将会停止该计划。很显然，我们在座的很多人都对这两方面有顾虑，但并不想停止计划。那么我们怎么改善这一状况呢？ICANN 如何处理此事？你们大家又想从机构群体得到哪些帮助呢？

JEFF MOSS： 如果没有人想发表意见的话，我来说说吧。是的，我之前就觉得你会这么说。那么，正如我早先提到过的，我们正持续关注所有已经提出的风险，或许还有我们内部识别出来但并非来自机构群体的风险。而且我们也在不断研究如何减轻这些风险。如果我们遇到某个问题，如内部服务器问题、证书问题，而且这些问题会对现实世界有大规模的影响，这个问题就会让我们停步不前。

举例来说，如果我们不能和 CA/B 浏览器论坛合作，如果我们不能减轻该风险，那么这个风险就会变得非常严重，还会导致我们慎重考虑是否要修改计划。所以我们需要根据具体情况来考虑。

至于我们要求机构群体采取什么行动，如果大家想想我们在谈论的问题的本质，就会发现内部证书的问题其实是扩展可路由地址空间这个更大问题的表现。我确信与会的各位无法想象到每个可能发生的问题。但是，机构群体中的人们一直都在这方面下功夫，也许大

家会遇到需要我们察觉到的情况。总之，我们呼吁机构群体帮助我们辨识出其他任何我们应该察觉到的问题。我可不想听到有人嘴里说着“哦，是的。我五年前就知道了”，却在我们真正要面临问题前两分钟才告诉我们。

作为这个工作的一部分，如果你需要使用我们的协调披露流程，那就用吧；如果你想私下打电话以假名字跟我沟通，也没关系。不过，我们不会在进行调查之前就避开或拒绝任何问题。

CHRIS： 我明白。那么，照你刚才说的，我可不可以这样理解，即 ICANN 认为在这里提到的问题都已经得到了合理解决？

JEFF MOSS： 我得说现在没有哪个问题会成为阻碍计划实施的原因，因为我们现在正在着手解决这些问题。

DANNY McPHERSON： 作为个人以及运营商，我其实不太同意。我认为还有一些重大的遗留风险正在单方面地向互联网用户和客户转移。我们需要对这些风险的影响进行评估。我的意思是，如果你退一步考虑，就会发现新 gTLD 计划的一条承诺就是会让 gTLD 的运营方式比之前更安全。这与前面的情况恰巧是相反的。我请求 ICANN 能仔细研究这方面问题。我知道，经过飞速的成长与发展，我们已经与之前拉开了相当大的距离。但是我不相信现在的这种说法，不相信这些薄弱的地方都已经得到了合理改善。

JEFF MOSS： 那么对于机构群体来说，哪一个问题是阻碍计划实施的原因呢？

DANNY McPHERSON： 无论从单方面来看还是从整体来看，它们阻碍了计划的实施。这些问题中没有一个得到了解决。稍后我将听取其他专家组成员的意见。我知道我已经说过这个论断，但是我们用了 90 分钟的时间进行讨论，其内容是关于撤销没有起到任何效果。之后就可能发生这种情况。在其他域名空间上，这些影响都是怎样的呢？最终，我要说，我们作为机构群体，对 DNS 和用户 DNS 的相依系统负有责任和义务，不能单纯地去把风险转移给那些客户。

JEFF MOSS： 以 OCSP 为例，如果浏览器启动 OCSP 撤销检查，如果服务器默认启动该检查，那么情况就会与我们今天的情况在根本上有不同。对不对？所以其实并不是没有降低风险的措施。这种措施是有的。不过我们面临的挑战是让服务器将其设为默认行为，而不是…你们懂的。Steve 你有什么要说的吗？

STEVE SHENG： Danny，说明一下，我不同意你说的撤销没起到作用。谢谢。

WARREN KUMARI： 我不认为我们能避开所有风险。DNS 是个庞大而复杂的、互相关联的系统。当人们改变它的时候，就会有东西出错。我们已经有过这样的惨痛教训。当人们因为有人阻止个别域名而将整个域名服务器的清单列入黑名单时，我们见过这样的情况。我们需要确定我们能承受多少这样做带来的风险，还有事实上是由谁来承担该风险？

我们会把风险交给谁？他们准备好面对这样的风险了吗？他们有迎接这些风险的正确态度吗？

JEFF MOSS： 别人还有没有想说两句的？没有的话我们这一话题就就此打住了。Elise 你有想说的吗？John，你呢？都没有吗？好的。

这是我们关于此事的首次会议。如果你们大家认为这很有帮助，那么我将很高兴在未来每一次 ICANN 会议上都进行这样的讨论。我只是好奇想知道而已。那么认为这种讨论有帮助的请举手。显然，我们还可以再精简一些，也许可以提前接受提问，这样我们就可以更明确地解决大家关注的问题。很好。所以我觉得我们可以期待与大家在德班再次进行讨论。希望那时会有一些更新。好的，Mikey，我们都想听你讲讲。

MIKEY O'CONNOR： 我知道。我等着这个机会呢。那我就开始说吧。我不会像他一样敲话筒的，我知道你们戴耳机的各位一定难以忍受那种行为。怎么样？

我在这点上有不同的观点。从某种程度上来说，新 gTLD 计划是一众供应商提供的新产品。而我则是 ISP。我将是最后众矢之的那个人。因为当这个新产品出问题的时候，客户不会打电话给 ICANN。他们也不会联系 donuts。他们会找我。而且，作为 ISP，我请求大家一定要确保你们的产品运行良好。因为上次你们的产品运行不良，结果我受到了批评。而且我还要在客户支持呼叫服务上投入很大一笔资金。所以说，如果这次产品性能表现得更好的话，那将是一件可

喜可贺的事儿。现在，提供这一产品的人们正迫切盼望着能从 DNS 中获得大量收入。我也觉得收入多是件不错的事情。

但是这个产品给我的感觉还不够完美，我和 Bill 之前举出的关于 corp.com 的例子便是诸多不完美之处中的一个。因此，我的观点是不要对此太过漠不关心，而是应该让那些提供该产品的人负起一些责任，针对产品的不完美之处一一做出弥补与改善。

如果大家要说起该由谁去和浏览器供应商谈，那么我想应该是我去找他们谈。ICANN 不用和他们沟通。应该由那些生产产品的人来将产品做好做精，让产品在市场上卓尔不群。我说得情绪有些激动了。不好意思。

JEFF MOSS： 没关系，非常感谢。