草案计划制定速览 [1]

高安全区 TLD

咨询委员会

[1] 制定速览摘自 2010 年 2 月 17 日的 HSTLD AG 维客和电子邮件列表

本文档的来由状况

这是高安全区 TLD 咨询委员会（“HSTLD AG”）已完成或正在进行的活动的制定速览。本文档的起草工作反映了相关方为增强公众对于选择加入计划的 TLD 的信任，而围绕旨在支持控制标准和鼓励措施的志愿项目所做的持续制定工作。

摘要

作为新 gTLD《申请人指南》现行制定工作的一部分，本报告将提交给 ICANN 机构群体供征询公众意见。本报告所反映的工作被称作“正在进行的工作”，因为我们开展了高安全性 TLD 的志愿活动。

文件标准

作为制定速览，本文就 HSTLD 计划中正在制定的计划内容进行了简要说明并描述了其当前的实际状况。为了区分对计划内容的说明和实际制定的计划内容，前者采用正常的文本格式，而后者用斜体表示。

目录

1.0 执行摘要

在 ICANN 首尔国际公开会议之前，开始启动志愿计划的初步制定工作。该志愿计划由控制标准和鼓励性措施组成，旨在增强对选择参与该计划的 TLD 的信任。首尔会议之前的一段时间内，ICANN 工作人员创建了一份概念文件。文件针对如何完成该志愿计划的初步想法进行了概述。该概念文件是第 3 版的新 gTLD 《申请人指南草案》的一个组成部分。要参阅概念文件，请单击以下链接：

http://www.icann.org/en/topics/new-gtlds/high-security-zone-verification-04oct09-en.pdf

大多数机构群体都对概念文件持肯定意见。为了继续获得对这一概念的支持，ICANN 已邀请机构群体成员加入 HSTLD 咨询委员会（“HSTLD AG”）。HSTLD AG 目前是由 ICANN 工作人员、表示有意协助计划的机构群体成员以及该计划相关领域（如，安全、审计、认证计划）的各专家组成。HSTLD AG 定期召开会议，以原始文件中的概念为基础，起草控制要素和活动要求，并发布可执行计划以供机构群体审查讨论。本文介绍的是 HSTLD AG 目前正在审查或编制的最新材料。

HSTLD AG 通过公开透明的流程开展活动和制定计划。该制定速览就是这一流程中的一部分。请通过以下链接查询更多信息，其中包括组织的参与人员和 HSTLD AG 的每周会议记录：

http://www.icann.org/en/topics/new-gtlds/hstld-program-en.htm

2.0 制定活动

自 ICANN 在韩国首尔召开国际公开会议以来出现的最重要的发展活动包括：

- HSTLD AG 的成立以及 HSTLD AG 对原始概念文件的审查；
- HSTLD 最初要求和依据的说明文档；
- 改进原有概念文件内容（包括基础组件）的额外工作：
  - 组织目标声明
  - HSTLD 问题陈述
  - HSTLD 益处说明；
- 改进原有的概念文件的原则、主题、目标和样本标准的额外工作；以及
- 添加一个新的“报告单”概念。

本制定速览文件的其余部分将就上述每个活动进行解释，并以“速览”方式阐述其当前的发展状态。HSTLD AG 通过每周的会议、电子邮件、HSTLD AG 维客和其他协作工具编制 HSTLD 计划材料。最终，HSTLD AG 编制的材料将被用于创建可执行的 HSTLD 计划及其关键内容。届时 AG 将公布计划以征询公众意见。

2.1 HSTLD AG 的成立

最初的工作是，ICANN 赞助成立一个咨询委员会以改善志愿 HSTLD 计划概念。该咨询委员会是由 ICANN 工作人员和感兴趣的机构群体成员组成的。成立该咨询委员会的目的是继续编制志愿 HSTLD 概念材料。该材料最初是在 ICANN 韩国首尔国际公开会议上作为会议内容的一部分公布的。HSTLD AG 的首次会议已于 2010 年 1 月 6 日召开，咨询委员会继续每周召开一次会议，致力于 HSTLD 计划概念的制定工作。委员会制定工作的现状、制定速览更新以及最终编制的新的概念文件（如果考虑公布该计划）将在 ICANN 国际会议期间汇报。

2.2 HSTLD 最初要求和依据的说明文档

HSTLD AG 组建过程中，委员会列举了 HSTLD 概念文件的最初的要求和依据，以帮助制定核心材料。请通过以下链接，参阅这些收集的材料：

http://mm.icann.org/pipermail/hstld-ag/2010-January/000094.html

2.3 编制材料概况

HSTLD AG 的首要重点领域之一就是 HSTLD 组织目标、问题和益处。这些领域是 HSTLD 计划顺利执行的基础，同时还是 HSTLD 计划所依据的总体指导方针。HSTLD AG 的讨论目前已经超越了这些范围，但在整个 HSTLD 制定工作中还将根据需要对其进行重新讨论。

在目标、问题和益处声明的编制过程中，HSTLD AG 的成员提出了供有意成为 HSTLD TLD 的 TLD 使用的新报告方式。新的报告方法基于“报告单”概念。它为 TLD 自行验证其自身是否符合 HSTLD 计划提供了方法。AG 将对这一报告方法进行评估，并且与其他认证、信任标识以及相似的验证程序相比较。

创建并讨论了 HSTLD 目标、问题和益处材料之后，HSTLD AG 的重点集中在原则、主题、目标和样本标准上。这些材料是最近讨论过并且仍处于积极编制状态的材料。

下面对每部分进行简要介绍，普通文本格式代表该材料，斜体文本代表 HSTLD AG 工作草案材料。

2.4 组织目标声明

HSTLD AG 承担的第一份制定任务是起草 HSTLD AG 组织目标声明。HSTLD AG 组织目标声明向机构群体提供了 HSTLD AG 总体目标的章程。还提供了与机构群体和 HSTLD AG 成员就总体目标和方向进行沟通的方法。当前的 HSTLD AG 目标声明草案如下：

“高安全区顶级域名咨询委员会的目标是将各机构群体代表聚集在一起，共同评估一项支持控制标准和鼓励性措施的志愿活动的可行性。这些控制标准和鼓励性措施可提高基本注册管理控制的信任度和安全性。”

2.5 组织问题声明

在 HSTLD AG 开始制定适合的目标声明时，一些 AG 成员提出，应当界定 HSTLD AG 的成立目的是解决哪些问题，因此这些问题被记录下来以供机构群体审查。由于制定了旨在减少这些问题的控制措施，这类材料有助于 HSTLS AG 不偏离重点。HSTLD AG 问题声明如下：

“某些个人/组织为已经试图利用 DNS 技术的漏洞以及某些注册管理机构的商业惯例，达到不当的和/或非法目的。”对这些漏洞的利用已经威胁到了互联网的安全和稳定，并且对用户在使用互联网时的信任度产生了负面影响。

利益相关方包括：

1. *注册人想要确定其注册的域名不会因为受累于注册服务商/注册管理机构/自己的账户而被劫持。（包括 DNS、WHOIS 等）*
2. *注册服务商希望能够向注册人合理保证第 1 条所述的情况不会出现，因为他们采取了控制措施。为了做到这一点，他们要求注册人和注册管理机构共同合作。*
3. *注册管理机构也希望满足第 1 条，这需要注册人与注册服务商的合作。*
4. *最终用户希望知道当他们输入某一类型的域名，或通过书签导航时，进入了正确的域，而且 DNS 等未被劫持。*
5. *最终用户希望了解在特定 gTLD 中注册的域名符合旨在减少注册人恶意行为的注册标准、政策和程序。”*

2.6 组织益处声明

到目前为止，计划制订的最终基础领域是制定 HSTLD AG 益处声明。这种益处材料的最终目的是让机构群体了解通过遵守 HSTLD 计划可以获得哪些益处。该材料并不是全面的商业利益分析。相反，它所提供的是整体的群体利益，并按受 HSTLD 计划影响最大的组织对其进行分解。当前的 HSTLD AG 益处材料如下：

“注册管理机构得益于：

Ry1. *通过审计流程证明其具备有关连续性、安全性和运营完整性的高标准*
Ry2. *证明其业务运作已经过审查并符合组织、运营和财务完整性的标准*
Ry3. *证明其具备满足数据保密性、准确性、完整性和数据恢复等高标准的数据处理和存储方法*
Ry4. *证明其已经采取了措施，以减轻域名服务和域名注册服务的滥用行为*
Ry5. *满足 (Ry1) 到 (Ry4)，培养最终用户和注册人对其业务和财务状况的信任，并确保为注册管理执行机构执行注册过程的注册服务商实施其降低恶意注册域名发生率的措施*

注册服务商得益于：

Rr1. *通过审计流程，证明其满足了从 HSTLD 注册管理机构“滴入”的所有连续性、安全性和运营完整性的标准。（“滴入”的意思是，注册服务商执行任何强加于注册管理机构的条件，如果没有注册服务商的协助，则无法满足这些条件，例如影响注册服务商和注册人之间的业务接口的条件）*
Rr2. *证明其业务运作已经过审查而且符合 HSTLD 注册管理机构“滴入”的组织、运营和财务完整性标准*
Rr3. *通过 Ry3“滴入”*
Rr4. *通过 Ry4“滴入”*
Rr5. *满足 (Rr1) 到 (Rr4)，培养了用户和注册人的信任，使其相信 HSTLD 委托注册服务商代表注册管理机构执行注册。较高的注册程序标准也向用户和注册人保证了注册数据的准确性，以及对滥用问题投诉的处理符合标准做法等。*

注册人得益于：

Re1. *证明其愿意递交与 HSTLD 注册管理机构有关的严格验证措施*
Re2. *证明其愿意维持准确的注册数据（并遵守确保数据准确性的验证措施）*
Re3. *证明其愿意同意服务和 AUP 条款，AUP 列举了禁用和滥用情况，并授权注册管理机构/注册服务商在处理违背 TOS/AUP 的情况时采取暂停服务或其他应对措施*
Re4. *实施减少恶意域名注册行为的措施：许多这样的措施增加了攻击者损害合法注册人账号的难度*
Re5. *实施减少 DNS 滥用情况的措施：许多这样的措施增加了攻击者损害合法注册人账号并改变 DNS 配置信息的难度。*

用户得益于：

U1. *更准确的注册数据*
U2. *HSTLD 中注册的域名的恶意注册事件和 DNS 滥用事件发生率降低*
U3. *明确定义的滥用问题处理程序”*

2.7 “报告单”概念

由于 HSTLD AG 编制了上述的基础材料，出现了有关最初验证概念文件的认证过程的问题。最初的概念文件将第三方验证方式作为向整个机构群体报告 TLD 采用 HSTLD 计划控制措施的机制。通过组织讨论过程，引入了一个 TLD 采用 HSTLD 控制措施的替代方法（尽管并不互相排斥）这一替代

方法是基于报告单的概念，TLD 能够填写该报告单向机构群体报告其 HSTLD 控制措施的合规程度。对于该概念的概述如下：

“TLD 安全记分卡

目前，对于如何让注册人做出关于其域名注册选项的知情决策，ICANN 没有提供任何标准。安全记分卡将作为可纳入 ICANN 当前仪表板特征的概念。

该记分卡将包括一个以约定的安全控制标准为 Y 轴，“所有”TLD 注册管理执行机构为 X 轴的矩阵。矩阵中每个方块将符合以下配色方案：

- *白/空方块：注册管理执行机构未提供与该控制元素相关的任何数据。*
- *黄色阴影方块：注册管理执行机构已经“自行认证”其自身与该控制元素的符合性。*
- *50% 绿色阴影方块：第三方已证实注册管理机构在某一特定时间点符合该控制元素，但是未能确定长期的符合性。*
- *100% 绿色阴影方块：第三方已证实注册管理机构能长期符合该控制元素。*
- *红色阴影方块：注册管理机构就某一具体控制标准进行了“自行认证”，但是随后被发现并不符合。有关自行认证的任何虚假声明都是违反注册管理机构协议的行为，将接受 ICANN 合规性团队工作人员的调查。”*

2.8 原则、主题、目标、样本标准

原概念文件的第 3.2.1 节包含了有关 HSTLD 计划核心要求的具体内容。本节阐述了原则、目标和标准的集合，它们是旨在改善 TLD 安全性和信任度的实际控制措施的基础所在。HSTLD AG 一直致力于改善本节。最近，对最初的原则进行了审查并且正在对一份附加的原则草案（目前列为“原则 4”）进行讨论，希望最终将其添加进原则中。HSTLD AG 目前也在评估“可能的标准主题”，争取就实际标准和支持说明性控制示例达成一致。全部完成时，每个标准主题将有一个或多个说明性控制示例，针对为符合标准要求而必须采用的适当的控制措施提供指导。本节当前的制定速览如下：

“原则 1：通过执行以下措施，注册管理机构保持有效的控制措施以合理地确保支持注册管理机构关键 IT（即，注册服务、注册管理机构数据库、区域管理和提供域名解析服务）和业务运营的系统和信息资产的安全性、可用性和保密性得到维护：

- *确定系统运营目标、政策和标准以及信息资产安全性、可用性、保密性和隐私性并就这些问题进行沟通；*
- *利用程序、人员、软件、数据和基础架构，按照既定的政策和标准达到确定的目标；以及*
- *监测系统和信息资产并采取行动以达到确定的目标并遵守既定政策和标准。*

序号	主题	目标	可能的标准主题	标准	说明性控制
1.1	注册管理机构 IT 基础架构安全	保护支持 TLD 基础架构的 IT 组件的关键元素，禁止未授权的物理和逻辑访问。	· 安全管理 · 人员安全 · 物理访问控制 · 媒介存储和处理 · 系统采购和发展控制 ·安全事件管理控制 · 安全事件响应和报告 · 接口控制 · 系统访问控制 · 网络安全 · 应用安全 · 加密要求 · 定期漏洞检测和响应演练 · 系统软件发布流程 · 域名解析服务管理控制（即，DNS 区域完整性和名称服务器可用性监测……） · DNSSEC 部署计划 · 安全通信通道（与注册服务商之间的认证加密连接） · 信息资产管理（区域、注册和其他用户数据的数据库准确性/完整性/可用性服务）		
1.2	注册管理机构 IT 基础架构可用性	根据合同或承诺可使用 TLD 服务。	· 服务水平协议 · Whois 服务可用性 · Whois 服务性能水平 · Whois 服务响应时间 · Whois 准确性和完整性 · 可用性监测 · 注册和交易数据托管，包括托管时间表、规格、转让和安全验证 · 灾难恢复和业务连续性计划（故障转移策略，包括在业务出现问题时维持域名解析服务的计划）和演练 · 环境控制（电源和空调、防火、发电机） · 布线安全控制		
1.3	敏感数据的保密性和隐私性	依照承诺或协议保护 TLD 拥有或由 TLD 管理或转让的被指定为机密的信息。TLD 运营商收集的个人信息是按照注册管理	· 适当的机密和个人身份信息分类 · 数据收集、使用、保存、访问和披露政策 · 在途和静止数据		

		机构运营商管辖区的相关数据保护法律进行收集、使用、保留、披露和毁坏的。	*· 第三方访问信息的途径* *· 加密要求* *· 签名密钥的管理控制* *· 物理和逻辑访问控制* *· 职责分离* *· 系统监控* *· 人员安全控制*		

原则 2：注册管理机构保持有效的控制措施以合理保证注册管理机构核心职能的处理符合既定的政策和标准，经过授权，且准确完整、实施及时。参与实体的身份经过确定和认证。

序号	*主题*	*目标*	*可能的标准主题*	*标准*	*说明性控制*
2.1	*注册管理机构安全验证*	*注册管理机构运营商有权证实运营 TLD 的法人实体身份。*	*· 对注册管理机构组织的审查包括：* *- 负责人背景* *- 可验证的地址* *- 可验证的电子邮件地址* *- 可验证的电话号码* *- 公司章程* *- 注册证书* *- 章程文件* *- 营业执照* *- 经营名称（即，名称）* *- 商标注册* *- 合股文件* *- 营业执照* *·保险范围* *· 财务能力* *· 重新验证要求* *· 员工的筛选流程*		
2.2	*注册服务商安全验证*	*在开始运营前指定并证实注册服务商身份。*	*· 关于审查注册服务商组织的主题同 2.1* *· 注册服务商委任状态* *· 重新验证要求*		
2.3	*注册管理机构流程完整性*	*在 TLD 注册管理机构层级的 TLD 数据是一致且正确的。*	*· 域名注册和维护* *· 公共 Whois 数据的维护、准确性和完整性* *· 新注册服务商的审查* *· 进行中的监测流程* *· 注册服务商数据 QA/质量审查（和托管数据审计结果）* *· 争议解决程序*		

2.4	*反滥用政策和执行*	*建立有效的控制措施以减少注册服务商或注册人的恶意行为。*	*· 针对新 TLD 的反钓鱼反欺诈控制措施* *· 由著名的反钓鱼和反恶意软件分析师和实验室完成的独立的第三方评级* *· 基于每个注册“度量单位”（例如，1000、5000、10,000 个域名）的恶意域名百分比的 SLA* *· 孤立的名称服务器政策（采取何种措施来确定和纠正孤立的名称服务器的声明）* *· 记录了及时的可审计的响应过程的滥用联系人* *· 服务协议的注册人条款中对恶意使用（行为）进行定义，并明确禁止恶意行为* *· 快速域名暂停过程* *· 详细的 Whois 程序和支持* *· DNSSEC 和 IPv6 部署计划* *· 实时区域监控（即，针对恶意活动，如 fast flux）* *· 报告给注册管理机构的恶意活动月报（例如钓鱼和僵尸网络），如果恶意活动较严重，还包括解决问题的承诺（相对于与该注册管理机构有业务来往的其他注册服务商）*		

原则 3：注册管理机构应保持有效的控制措施以合理保证注册服务商核心职能的处理符合既定的政策和标准，经过授权，且准确完整、实施及时。参与实体的身份经过确定和认证。

序号	*主题*	*目标*	*可能的标准主题*	*标准*	*说明性控制*
3.1	*注册人安全验证*	*在注册服务商提供域名之前确认并证实注册人的身份。*	*· 关于组织主题的审查参见 2.1* *· 在 TLD 中注册的注册人的管理机构* *· 免于代理/匿名注册的商业用户（申请人必须提供证据证明申请人为自然人，机构必须出示匿名的原因或理由）*		
3.2	*注册服务商流程完整性*	*在注册服务商层级的数据一致且正确。*	*· 注册服务商通过已达成一致的程序认证新注册人* *· 注册服务商确认注册数据准确完整* *· 注册服务商监控注册数据以确保其准确完整* *· 注册服务商验证每笔交易的注册数据* *· 注册服务商确认注册日期的更改* *· 因故拒绝/暂停注册数据（不完整、错误/不准确）* *· 详细的 Whois* *· 注册服务商删除注册数据* *· 进行中的监测流程* *· 定期对注册人数据进行 QA 审查* *· 关闭流程和及时性目标（如 MTTR）*		

原则 4：高安全区的注册人应维持最新的准确信息，并承诺避免意在混淆或误导互联网公众用户的行为。

序号	*主题*	*目标*	*可能的标准主题*	*标准*	*说明性控制*
4.1	*注册人数据准确性*	*注册人提供最新的准确的身份和位置信息*	*WHOIS 数据提供给注册管理机构的注册人位置信息提供给注册管理机构的联系信息没有代理*		
4.2	*注册人行为*	*注册人将明确承诺遵守 ICANN 政策以及在 HSTLD 标准应用过程中产生的任何其他义务*	*行为准则*		

3.0 后续措施

HSTLD AG 将继续编制材料，努力改善最初的 HSTLD 概念文件。接下来的步骤包括但不限于继续每周会议、在内罗毕召开会议和继续制定重要计划材料，其中包括：

- 基础材料；
- “报告单”概念对应供选择的方案；
- 原则、目标、标准和说明性示例；以及
- 计划的整体管理和实施者。

如前所述，将在 ICANN 国际会议上公布制定速览和对初始概念文件的更新。