新通用顶级域名 (gTLD) 计划
解释性备忘录更新
减少恶意行为

背景 - 新通用顶级域名 (gTLD) 计划

ICANN 成立于十年前，是一个非营利性的多利益主体组织，致力于协调互联网的寻址系统。自从成立以来，其基本原则之一就是在确保互联网的安全性和稳定性的同时，促进域名市场的竞争，这一原则得到了美国和其他国家/地区政府的认可。通用顶级域名 (gTLD) 的扩展将为互联网的地址系统（现在由 21 个通用顶级域名 [gTLD] 表示）带来更多的创新、选择和变化。

在作出引入新通用顶级域名 (gTLD) 的决定后，将进入一个与各个利益群体（政府、个人、民间团体、企业和知识产权社群以及科技社群）代表的全球互联网社群的所有选区组织的详细而又冗长的咨询过程。同时，作出贡献的还有：ICANN 的政府咨询委员会 (GAC)、全体咨询委员会 (ALAC)、国家或地区代码名支持组织 (ccNSO) 以及安全性和稳定性咨询委员会 (SSAC)。咨询流程产生了针对引入由通用名称支持组织 (GNSO) 于 2007 年完成，并由 ICANN 董事会于 2008 年 6 月采用的新通用顶级域名 (gTLD) 的政策。该计划预计在 2010 日历年启动。

本解释性备忘录是由 ICANN 发布的一系列文档的一部分，以协助全球互联网社群理解《申请人指导手册》（目前还是草案）中提出的要求和流程。自 2008 年底以来，ICANN 员工一直通过针对申请人指导手册草案和支持文档的一系列公众意见论坛，与互联网社群分享计划制定过程。迄今为止，针对关键计划材料的咨询已超过 250 天。收到的意见继续得到仔细评估且用于进一步完善该计划，并且通告申请人指导手册最终版本的制定情况。

有关新通用顶级域名 (gTLD) 计划的最新信息、时间表以及活动，请访问

http://www.icann.org/en/tlds/select.htm

请注意，本文件只是讨论草案。潜在申请人不应依赖任何关于新通用顶级域名 (gTLD) 计划拟议的细节，因为此计划有待进一步的咨询和修订。

综述

在解决社群关心的减少与新通用顶级域名 (gTLD) 计划相关的恶意行为潜在增长可能性方面取得了重大进展。

此处介绍的解决方案将带来域名系统 (DNS) 环境的重大改进：为注册人提供保护以及更加稳定的环境和用于发现与打击潜在恶意行为的工具。始终需要在这些领域进行持续改进，这些改进将有助于新通用顶级域名 (gTLD) 流程的稳定启动。随着新通用顶级域名 (gTLD) 计划即将启动、最终实施并超越，处理不断变化的安全性、稳定性和可靠性问题仍将成为 ICANN 持续高度重视的问题。

在此方面进行了大量的卓越工作，大部分是由公众意见论坛或工作组中的社群志愿者进行的。他们因显著改善了域名系统 (DNS) 环境而广受赞扬。ICANN 在此对大家表示感谢。

本文件是于 2009 年 10 月 3 日发布的原“减少恶意行为”（“恶意行为备忘录”）备忘录的更新。可以单击以下链接获得原备忘录：

http://www.icann.org/en/topics/new-gtlds/mitigating-malicious-conduct-04oct09-en.pdf

在原恶意行为备忘录中，ICANN 征询了公众对建议的意见，以应所有注册机构的要求将具体措施增加到新通用顶级域名 (gTLD) 注册机构协议，从而降低新通用顶级域名 (gTLD) 中恶意行为的可能性。

为了推动这一过程，ICANN 完成了恶意行为研究，因为该行为与顶级域名 (TLD) 空间内的行为相关。在研究期间，ICANN 员工征询并收到了来自多个外部来源的意见，其中包括知识产权协会 (IPC)、注册机构互联网安全组 (RISG)、安全性和稳定性咨询委员会 (SSAC)、计算机紧急应变小组 (CERT) 和银行/财务成员以及互联网安全社群。这些团体阐述了若干潜在的恶意行为问题，并鼓励 ICANN 在新通用顶级域名 (gTLD) 注册机构协议中考虑解决或减少这些问题可能的方式，或者作为申请流程的一个组成部分。这些建议的措施旨在提高对注册人总体安全性和稳定性的益处，并得到这些新通用顶级域名 (gTLD) 区域中所有用户的信任。

这项研究的结果以及相应的公众意见征询期形成了旨在提供工作重点的九项建议，从中控制措施可以降低制定的通用顶级域名 (gTLD) 内恶意行为的可能性。计划中将实施的九项建议如下：

1. ***审查注册机构运营商*** – 该建议要求对新通用顶级域名 (gTLD) 申请人注册机构运营商进行相应审查，以确定申请人注册机构运营商是否具有犯罪或恶意历史记录。
2. ***展示域名系统安全协议 (DNSSEC) 部署的计划*** – 这是强制性建议，需要新通用顶级域名 (gTLD) 申请人展示域名系统安全协议 (DNSSEC) 部署的计划，以降低欺诈域名系统 (DNS) 记录的风险。
3. ***禁止通配*** – 此建议要求适当控制域名系统 (DNS) 通配，降低域名系统 (DNS) 重定向至恶意网站的风险。
4. ***删除孤立粘附记录*** – 该建议要求通用顶级域名 (gTLD) 在系统从通用顶级域名 (gTLD) 删除时删除名称服务器记录，以降低这些残留记录被恶意操纵者使用的风险。
5. ***要求充分的 WHOIS 记录*** – 该建议要求新通用顶级域名 (gTLD) 维护“充分的 WHOIS”记录，以提高 WHOIS 数据的准确性和完整性。使用充分的 WHOIS 记录通过提供顶级域名 (TLD) 内行为的更完整链，提供了一个打击恶意使用新通用顶级域名 (gTLD) 的关键机制。从而，这会允许在确定恶意行为活动后，对其进行更快的数据搜索和解析。

6. ***区域文件访问集中化*** – 该建议要求获取注册机构区域数据的访问凭据通过集中来源提供，以允许更准确快速地确认每个顶级域名 (TLD) 内的联系关键点。这将减少在出现恶意活动的顶级域名 (TLD) 内采取矫正措施所需的时间。
7. ***记录注册机构级别滥用联系人和程序*** – 该建议要求通用顶级域名 (gTLD) 建立负责处理滥用投诉的单个联系点，且注册机构提供旨在打击滥用的政策的说明。这些要求被视为成功打击新通用顶级域名 (gTLD) 内恶意行为取得成效的基本步骤。
8. ***参与快速的注册机构安全申请流程*** – 该建议通过建立专门流程以审查和批准加快安全请求，使新通用顶级域名 (gTLD) 能够在发现域名系统 (DNS) 的系统威胁时快速有效地采取行动。
9. ***高级别安全区验证的草案框架*** – 该建议推荐建立旨在指定想要建立的顶级域名 (TLD) 并证明安全和信任增强级别的自愿计划。该计划的总体目标是为需要将其确认为安全可信任的顶级域名 (TLD)、可以从此差异中获益的顶级域名 (TLD) 业务模式提供一个机制。

本备忘录的其余部分将确定有关每个建议的具体工作状态。

九项恶意行为建议的状态

本部分提供旨在降低新通用顶级域名 (gTLD) 内恶意行为可能性的九项建议的当前状态和/或更新（如果有），如原恶意行为备忘录中所述（请参见上文的“文件要点综述”）。每项建议都分为详述针对建议的显著更新的“当前状态和/或更新”部分，以及“新通用顶级域名 (gTLD) 流程的具体建议改进”，作为 2009 年 10 月 3 日恶意行为备忘录中发布材料的参考。

1. 审查注册机构运营商

- 当前状态和/或更新

该建议要求“审查”或回顾调查注册机构运营商是否有一个增强新通用顶级域名 (gTLD) 申请人的申请流程的指导原则。新通用顶级域名 (gTLD) 申请流程现在包含要求新通用顶级域名 (gTLD) 申请人提交若干背景调查的具体标准，作为申请流程的一个组成部分。此外，根据原恶意行为备忘录中所述，针对合格申请人未能通过指定审查流程的情况，《申请人指导手册草案》模块 2 包含特定内容来陈述拒绝这些申请人的权利。《申请人指导手册草案》模块 2 中标准和语言的详细信息可以参考下面的内容或以下链接：

http://www.icann.org/en/topics/new-gtlds/draft-evaluation-criteria-30may09-en.pdf

2. 需要进行域名系统安全协议 (DNSSEC) 部署

- 当前状态和/或更新

针对域名系统安全协议 (DNSSEC) 部署的计划证明仍然是新通用顶级域名 (gTLD) 申请流程中的必要组成部分，以及用于每个新通用顶级域名 (gTLD) 预授权测试的组成部分。可以在《申请人指导手册草案》模块 5 中参考针对要求的文档。与原恶意行为备忘录一样，注册机构协议第 3 版的规范 6 包含有关域名系统安全协议 (DNSSEC) 的内容（见下文）。第 3 版第 6 款的第一句已修改为“注册机构运营商应签署其实施域名系统安全扩展（‘DNSSEC’）的顶级域名 (TLD) 区域文件”。

注意：RFC 4310（如下文所述）已更新为 RFC 5910。

3. 禁止通配

- 当前状态和/或更新

禁止域名系统 (DNS) 通配符的相关内容仍然是注册机构协议第 3 版第 6 款的一部分（请参见下文的“原恶意行为备忘录的状态”）。此外，ICANN 于 2009 年 11 月 24 日发布了一份标题为“注册机构级别中 NXDOMAIN 取代（域名系统 [DNS] 通配符和类似技术）造成的危害和问题”的解释性备忘录。该解释性备忘录介绍了注册机构级别 NXDOMAIN 取代（通常通过使用域名系统 [DNS] 通配符来实施）造成的危害和问题。该文件是由主题专家发布的调查结果的集合。可以单击以下链接参考实际备忘录：

http://www.icann.org/en/announcements/announcement-2-24nov09-en.htm

ICANN 董事会在 2009 年 6 月于悉尼举行的公开会议上，决定新的顶级域名不能使用域名系统 (DNS) 重定向和综合域名系统 (DNS) 响应。

为响应董事会决议，ICANN 员工在新通用顶级域名 (gTLD) 的注册机构协议草案中加入了禁止重定向和综合域名系统 (DNS) 响应。ICANN 还在拟议的条款和条件以及 ICANN 与国际化域名 (IDN) 国家和地区代码顶级域名 (ccTLD) 经理之间的三项拟议关系选项中，加入了类似承诺作为新国际化域名 (IDN) 国家和地区代码顶级域名 (ccTLD) 的一部分。

最后，董事会还指示 ICANN 员工报告因使用重定向和综合域名系统 (DNS) 响应（都属于 NXDOMAIN 取代）而造成的危害和问题。

4. 鼓励删除孤立粘附记录

- 当前状态和/或更新

安全和稳定咨询委员会 (SSAC) 组建了工作组研究该问题。该工作组目前正在检查当前所有通用顶级域名 (gTLD) 的区域文件以普查孤立名称服务器，并且确定这些孤立名称服务器用于恶意或犯罪用途的程度（如果可能的话）。由安全和稳定咨询委员会 (SSAC) 工作组生成的建议会为注册机构提供针对如何管理孤立记录的额外指导，并为关键通用顶级域名 (gTLD) 流程中的包含内容进行评估。

正如原恶意行为备忘录中所提到的，注册机构必须提供如何在名称服务器从区域删除时删除孤立粘附记录的说明（见下文）。

5. 充分的 WHOIS 的要求

- 当前状态和/或更新

现在已经有了为所有新通用顶级域名 (gTLD) 制定“充分的 WHOIS”的要求的建议。根据最新的注册机构协议，所有新通用顶级域名 (gTLD) 都将必须实施充分的 WHOIS 要求。

此外，为注册机构协议草案的注解临时增加了有关 WHOIS“搜索功能”的新条款。该条款包含以下内容：

“为了在统一域名争议解决政策 (UDRP) 下协助投诉人确定特定注册人是否表现出‘恶意’的方式，将根据相应的隐私权政策在公众可访问的数据库中提供 WHOIS 信息，可以按域名、注册人名称、注册人邮政地址、联络人姓名、注册管理人联系 ID 和互联网协议地址不受限制地搜索该数据库。为了提供一个有效的 WHOIS 数据库，可能会提供布尔搜索功能。”

该条款为涉及确定和面临名称空间中恶意行为的人提供了额外的工具，同时提供了用于执行具有控制结构的、旨在减少搜索功能本身恶意使用的搜索的方法和标准。本条款存在于当前的一些注册机构协议（.ASIA、.MOBI、.POST）中，并包括在新通用顶级域名 (gTLD) 注册机构协议的本草案中供讨论。作为一个参考点，.NAME (http://www.icann.org/en/tlds/agreements/name/appendix-05-15aug07.htm) 自发布以来就提供了“广泛 WHOIS”搜索功能。该搜索功能基于有助于减少潜在恶意使用功能的分层访问模型。尤其针对该要求如何帮助确定某些类型的恶意行为征询意见，为已注册名称使用 Whois 数据的替代性解决方式是新通用顶级域名 (gTLD) 中减少恶意行为背景下的有效工具。如果支持要求，还会为存在的搜索功能征询制定统一征询技术规范的建议。

6. 区域文件访问集中化

- 当前状态和/或更新

ICANN 接受了建立机制以支持集中化访问区域文件记录的建议，并组建了名为“区域文件访问咨询小组”（“ZFA AG”）的咨询小组，其任务是与社群合作以提出支持区域文件访问集中化机制的建议。ZFA AG 已完成其有关战略建议的工作，可以单击以下链接参考：

http://www.icann.org/en/topics/new-gtlds/zfa-strategy-paper-12may10-en.pdf

区域文件访问集中化的下一步是实施建议中概述的建议。

7. 记录注册机构级别滥用联系人和政策

- 当前状态和/或更新

该建议要求新通用顶级域名 (gTLD) 记录特定注册机构滥用联系人，并提供其特定反滥用政策的说明，该建议是所有新通用顶级域名 (gTLD) 的要求。该建议自原恶意行为备忘录制定以来并未发生变化（见下文）。

8. 参与快速的注册机构安全申请流程

- 当前状态和/或更新

根据原恶意行为备忘录中的简介，ICANN 发布了名为“快速的注册机构安全申请流程发布”的解释性备忘录（见下文）。本解释性备忘录定义了名为“快速的注册机构安全申请”(ERSR) 流程的流程。它代表了 ICANN 与通用顶级域名 (gTLD) 注册机构之间协作努力，以制定快速行动流程，其中通用顶级域名 (gTLD) 注册机构：

- 通知 ICANN 存在或即将发生对其顶级域名 (TLD) 和/或域名系统 (DNS) 的安全事件，并
- 针对为缓解或消除事件而可能采取或已经采取的措施申请合同放弃。

合同放弃是在响应事件的必要时段内，从与注册机构协议具体条款的合规中免除。

现在提供 ERSR 基于网络的提交程序，可以在附录 A 中参考，或单击以下链接：

http://www.icann.org/en/registries/ersr/。

这一新流程由通用顶级域名 (gTLD) 注册机构针对需要由注册机构立即行动的事件独家使用，以避免对域名系统 (DNS) 稳定性和安全性造成有害影响。为了域名系统 (DNS) 的稳定性起见，该流程在 2009 年 10 月 1 日立即生效。有关 ERSR 流程的额外信息，可以单击以下链接访问：

http://www.icann.org/en/announcements/announcement-01oct09-en.htm

9. 高级别安全区验证的草案框架

- 当前状态和/或更新

银行和财务利益主体团体（如 BITS）提出了建立高级别安全区验证的草案框架的建议，并且发出了名为高级别安全区顶级域计划（简称“HSTLD 计划”）的倡议。该倡议起草了针对高级别安全区验证的建议控制框架。为了分析此框架的可能方法并推动建议进行社群审查，ICANN 组建了高级别安全区顶级域咨询小组（“HSTLD AG”）。HSTLD AG 的任务是通过自下而上的发展模式与社群合作，提议由控制标准和动机组成的自愿计划的方法，以提高在选择参与此计划的顶级域名 (TLD) 中的安全性和信任度。

HSTLD AG 当前由对协助计划表示出兴趣的社群成员组成，还包括与 ICANN 员工成员支持的计划（例如安全、审计、认证计划、金融服务代表）相关的准则方面的专家。HSTLD AG 会定期举行会议并以最初在 2009 年 10 月文件中提出的概念为会议基础，起草控制要素和计划要求以及发布行动计划供社群考虑和审查的计划。HSTLD AG 通过公开和透明的过程安排其活动和计划制定。包括 HSTLD AG 每周会议的组参与者和记录的其他信息，可以单击以下链接获得：

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

计划不是由 ICANN 开展。独立实体将建立标准并根据这些标准认证顶级域名 (TLD)。他们将负责监控和更新认证并公布认证。

附录 A

快速的注册机构安全申请流程

目前已制定了快速的注册机构安全申请流程 (ERSR)，以为通知 ICANN 存在或即将发生对其顶级域名 (TLD) 和/或域名系统 (DNS) 的安全事件（下文简称“事件”），以针对为缓解或消除事件而可能采取或已经采取的措施申请合同放弃的通用顶级域名 (gTLD) 提供一个流程。合同放弃是在响应事件的必要时段内，从与注册机构协议具体条款的合规中免除。ERSR 旨在允许在事件中维护运营安全性，并相应地通知相关各方（例如 ICANN、其他受影响的提供商等）。

事件可能是以下一项或多项：

- 在域名系统 (DNS) 的范围及严重性方面威胁到顶级域名 (TLD) 或域名系统 (DNS) 的系统安全性、稳定性和灵活性的恶意活动；
- 未经授权披露、篡改、插入或破坏注册数据，或通过按照所有适用标准运行的系统，在互联网上未经授权访问或披露信息或资源；
- 造成通用顶级域名 (gTLD) 注册机构一个或多个关键功能临时或长期故障的潜在情况，如 ICANN 通用顶级域名 (gTLD) 注册机构持续性计划 [PDF，96K] 中定义。

ERSR 专用于事件，即需要注册机构立即采取行动，并在 3 个工作日内获得来自 ICANN 的快速响应。该流程的目的不是要取代通过注册机构服务评估政策 (RSEP) 发出的请求。

在某些特殊情况下，不会要求注册机构立即采取行动以防止或解决事件。在此类事件的情况下，注册机构应尽快提交 ERSR，以便 ICANN 以追溯放弃进行回应（如果适用）。

注册机构可以填写请求表来提交 ERSR，地址为：http://www.icann.org/cgi/registry-sec。提交的请求将进行如下处理：

- ERSR 将自动转发给 ICANN 安全响应小组，副本将提供给请求者。安全响应小组包括来自以下部门的员工：安全部、通用顶级域名 (gTLD) 注册机构联络部、总法律顾问和合规部。
- 安全响应小组的指定成员在逐案基础上，负责在 1 个工作日内联系注册机构，以确认事件和请求其他信息（如有必要）。
- 安全响应小组可以请求其他信息进行审查（如有必要）并考虑 ERSR，并且将要求请求者迅速提供此类信息。
- 安全响应小组将集中利用 2 个工作日接收请求（以及任意请求的其他信息），以审查并确定响应。

- ICANN 将在收到请求者或其指定代表的 ERSR 后 3 个工作日内，作出口头和书面响应。
- 安全响应小组的指定成员将在整个事件持续期间保持与注册机构主要联系人的联系。
- 如果注册机构已响应事件后收到请求，ICANN 将尽力在 10 个工作日内作出响应，以提供请求的书面追溯放弃（如果适用）。
- 对 ERSR 作出响应后，与受影响注册机构协作的安全响应小组将制定可向社群提供的行动后报告 (AAR)。如果要发布 AAR，ICANN 以及受影响注册机构将共同审查 ERSR 请求和 AAR 的哪些部分应重新编写，以确保保护机密和专有信息。ICANN 和注册机构可以重新编写相应视为机密和专有的此类信息。