新通用顶级域名（New gTLD）计划

说明书

减少恶意行为

公布日期： 2009 年 10 月 3 日

背景：新通用顶级域名计划

作为一个致力于协调互联网寻址系统的非盈利、多方共同管理的组织，ICANN自十年前成立之日起便确立了一条基本原则，即促进域名市场的竞争，同时互联网运行的安全性和稳定性，该原则同时得到美国及其他政府的认可。目前全球通用顶级域名（gTLD）仅有21种，扩张通用顶级域名将考虑到更多创新、机会及对互联网寻址系统的改变。

引入新通用顶级域名的决定经历了一个详细而漫长的咨询过程，咨询对象为全球各种互联网团体用户，包括政府、个人、民间社团、知识产权支持者及技术团体。同时作出贡献的还有CANN的政府咨询委员会（GAC）、一般会员咨询委员会（ALAC）、国家代码域名支持组织（ccNSO）及安全和稳定咨询委员会（SSAC）。咨询过程导致引入新通用顶级域名（New gTLD）政策的出台，该政策由通用名称支持组织（GNSO）于2007年拟定，2008年6月在ICANN董事会获得通过.该计划有望于2010年推出。

本说明书是ICANN公布的系列文件的组成部分，旨在协助国际互联网团体理解《申请指南》中规定的要求和程序，目前为草案形式。自2008年末，ICANN员工举行了一系列研讨会，就申请指南草案及支持文件邀请公众评议，藉此与互联网团体分享计划的进展过程。至此，就计划关键资料征求意见的时间已超过250天。收到的评议继续得以仔细评估，并用于进一步推敲计划和帮助发展《申请指南》最终稿。

如欲了解有关新通用顶级域名计划的最新信息、进度及活动，请访问：http://www.icann.org/en/topics/new-gtld-program.htm。

请注意，本文件仅是一个讨论草案。潜在申请人不应依赖新通用顶级域名计划提议的任何细节，因为该计划还有待进一步咨询和修订。

要点总结

ICANN就在新通用顶级域名注册协议中增加具体措施的提案征求意见，所有域名注册局都需执行这些措施，以减少潜在恶意行为。

在研究恶意行为的过程中，ICANN寻求并收到了外界多方面反馈，包括反钓鱼工作组（APWG）、网络注册安全组（RISG）、安全和稳定咨询委员会（SSAC）、计算机紧急响应小组（CERTs）和银行/金融团体及网络安全团体。他们提出了数个潜在恶意行为问题，并鼓励ICANN在新通用顶级域名注册协议中考虑解决或缓和的途径。这些措施旨在帮助注册人提高整体安全性和稳定性并增进新通用顶级域名全体用户间的信任。

《申请指南草案》（第二版）中包括在悉尼会议和咨询会上收到的意见，在此基础上，将在新通用顶级域名注册协议中增加恶意行为缓解措施及控制。以下是在建议准备过程中考虑的反馈及遵循的流程总结。

建议在九个方面提出了缓和恶意行为风险的措施：

1. 审查域名注册营运商
2. DNSSEC 部署示范方案
3. 禁止通配符方式
4. 删除域内的名称服务器项目后，同时删除孤立粘帖记录
5. 要求 WHOIS 记录
6. 域文件访问认证
7. 记录域名注册局层面的滥用联络及程序
8. 参与域名注册安全快速请求流程
9. 拟定高安全域认证计划

综上所述，我们相信这些措施将大大有助于缓解新通用顶级域名导致的恶意行为增加风险。有关这些问题的政策工作及减少恶意行为的具体措施还在继续进行。ICANN也可能尝试设立一个由安全领域和ICANN团体组成的工作组，以帮助发展并评价缓解措施解决方案及其具体执行。

前言

作为一个致力于协调互联网寻址系统的非盈利、多方共同管理的组织，ICANN自十年前成立之日起便确立了一条基本原则，即促进域名市场的竞争，同时互联网运行的安全性和稳定性，该原则同时得到多国政府及其他股东的认可。扩展将为寻址系统带来创新、机会和积极的改变在一个拥有15亿互联网用户的多元化世界里，机会和竞争是保证全球网络持续成功和延伸发展的关键。

引入新通用顶级域名的决定经历了一个详细而漫长的咨询过程，咨询对象为全球各种互联网团体用户，政府、个人、民间社团、知识产权支持者及技术团体等各界代表均参与了为期超过18个月的讨论。2007年10月，通用名称支持组织（GNSO）——ICANN负责协调全球互联网政策的小组——完成了新通用顶级域名政策发展工作，并接受了一系列建议。2008年6月，在ICANN巴黎会议上，ICANN董事会决定通过该政策。有关政策过程和结果摘要，请访问：http://gnso.icann.org/issues/new-通用顶级域名s/。

本文件是ICANN发布的系列说明书之一，旨在协助互联网团体更好地理解《意见请求书》（RFP），也称《申请指南》。在《申请指南》和这些文件的公众评议阶段，对有关构想作了详细的评审和改善。在准备《申请指南》最终稿时，将利用这些评议对有关文件作出修订。

请注意，本文件仅是一个讨论草案。潜在申请人不应依赖新通用顶级域名计划提议的任何细节，因为该计划还有待进一步咨询和修订。

有关恶意行为问题的团体反馈

ICANN已从多个领域收到大量公众意见，响应其扩张顶级域名以授权新域名（包括）IDN顶级域名的提议。其中，有几方提出一个共同的问题，即新通用顶级域名有可能导致恶意行为增多。为解决这个问题，ICANN征求了有关专家的意见及受现有通用顶级域名恶意行为影响的股东的意见。

第一、二版《申请指南草案》收到的反馈是发展第三版中所含建议的主要来源。

有关该问题的第二个反馈来源是安全和稳定咨询委员会（SSAC）针对恶意行为提交的报告，即《SAC038：域名注册服务商恶意联络》（SAC038: 域名注册服务商 滥用联络(pdf)）和《SAC040：域名注册服务非法利用或误用防范措施》（SAC040: Measures to Protect 域名注册 Services Against Exploitation or Misuse (pdf)）。这些报告及SSAC开展的其它工作为域名注册局和域名注册服务商提供了指导，同时对改进《申请指南草案》和新通用顶级域名注册协议也有指导意义。

第三个来源是反钓鱼工作组（APWG）备制的报告草案。APWG是一个行业协会，致力于清除网络钓鱼和电子邮件欺诈引起的身份盗用和欺诈。该报告由APWG互联网政策委员会（IPC）协调整理，委员会包括90多名成员，在APWG具广泛代表性。值得一提的是，ICANN的许多股东（包括通用顶级域名及国家和地区顶级域名、域名注册局和域名注册服务商、互联网服务供应商、知识产权所有人及安全和金融机构）都是APWG和APWG IPC的成员，详

见：http://www.antiphishing.org/sponsors.html。APWG IPC将通用顶级域名扩张视为一件大事，认为会给对电子犯罪空间带来潜在影响。针对众多恶意行为问题，APWG IPC报告为ICANN提供了大量全面而有建设性的信息，APWG IPC认为这些是在引入新通用顶级域名过程中值得注意和需要预作规划的。

第四个来源是由网络注册安全组（RISG）提供的，这是一个全球性的互联网负责组织，其使命是各成员通力协作共同打击网络身份盗用，尤其是网络钓鱼和恶意程式。RISG在报告（pdf）中列举了注册数目增加可能导致的几个问题。

第五个来源是银行和金融机构的意见。许多行业组织都贡献了他们的专长，包括减少BITS欺诈计划（Fraud Reduction Program）、美国银行联合会（American Banking Association）、金融服务信息分享与分析中心（Financial Services Information Sharing and Analysis Center，简称*FS-ISAC*）、金融服务技术联盟（Financial Services Technology Consortium，简称FSTC）等。从他们保护网络和敏感数据的独特视角和经验出发，该团体针对注册应采取的措施提出了高贵的建议，包括安全操作规程，以增进用户信任，同时降低恶意攻击导致的损害风险

第六个来源是商标保护议题评估小组（IRT）的工作。在确立新通用顶级域名时，ICANN已将商标保护和防止恶意滥用作为有待解决的另一个突出问题，在补救方法上与减少恶意行为有很多交叉之处。IRT在2009年5月29日的"IRT工作说明公开信"中对其工作成果作了总结。IRT由CANN知识产权社群（Intellectual Property Constituency）应团体寻求商标注册人潜在风险解决方案的请求，依据2009年3月6日的ICANN董事会决议（链接）组成。IRT团队提交的报告（pdf）反映其18名成员和两名候补成员在经验和地理上的多元化。

此外，网络安全第一响应者团体的成员也提供了反馈意见。应急响应和安全小组论坛（FIRST）等组织的成员提供了宝贵的建议。FIRST由计算机和网络应急响应小组构成，这些团队来自美、亚、欧和大洋洲多达180家公司、政府部门、大学及其它机构，旨在齐心协力打击网络犯罪。各种执法机构的成员在定义重要问题方面提供了协助，并未域名注册运营变革提出建议，这些都将有利于打击网络犯罪。

除上述来源外，ICANN还在悉尼、纽约、伦敦、香港和阿布扎比举办公共咨询会，广泛征求公众意见，包括就降低恶意行为可能性的问题专门召开会议。

ICANN还在icann.org站点上开设了维客（wiki）专区，以便针对新通用顶级域名中的恶意行为寻求可能的解决方案。上述报告已经张贴在维客上，欢迎公众参和评论。

确认的关键问题

在ICANN的工作过程中，各种参与者确认了大量有关潜在恶意行为的问题。尽管其中许多问题暴

露出独特和复杂的技术缺陷，需要利用各种控制措施并顾及诸多考虑因素，但仍可将它们总结为下列关键主题类目：

A. 如何防止害群之马经营域名注册局？

有反馈要求ICANN采取措施降低如下风险，即扩大域名注册的数目有可能致使不可靠的营运者或不法之徒进入团体，从而导致恶意行为的发生。

B. 怎样确保域名注册信息的完整性和实用性？

有反馈鼓励ICANN利用创建新通用顶级域名的机会，提高域名注册和域名解决方案服务的质量，同时限制从事恶意行为的机会。

C. 如何保证采取更有效的措施打击验证滥用行为？

既然已存在恶意行为且对所有顶级域名都有影响，有反馈呼吁ICANN在设立新顶级域名的过程中，改进现有的流程和工具，以减少网络犯罪及对域名服务系统（DNS）和域名注册系统的滥用。

D. 对于本身有可能被滥用的顶级域名，如何强化控制结构？

某些新顶级域名可能涉及电子服务交易，需要高信赖性基础设施（如电子金融服务或电子投票），也可能涉及重要资产和基础设施（如支撑能源基础设施或医疗服务），必须加强保护，防止不法之徒利用域名系统从事恶意行为。有反馈建议ICANN创建一个系统，以提升在该等领域运营的信任。

建议缓解措施：

为解决上述恶意行为问题，ICANN认为应采取综合措施，作为新通用顶级域名实施计划的组成部分。除了在合同中强化新通用顶级域名注册局的义务外，ICANN鼓励新域名注册局在与获授权域名注册服务上的磋商中，提高商业和安全规程的标准。具体而言，新通用顶级域名注册局有能力要求域名注册服务商采取具体措施减少恶意行为，以在他们的域内注册商标。

此外，ICANN将继续与团体共同努力，对现有政策发展加以补充，并携手工作组，拿出可在域名注册服务商-注册人界面实施的缓解措施。

当前版本《申请指南草案》中的建议缓解措施基本类目如下：

1. 审查域名注册营运商
2. DNSSEC 部署示范方案
3. 禁止通配符方式

4. 删除域内的名称服务器项目后，同时删除孤立粘帖记录
5. 要求 WHOIS 记录
6. 域文件访问认证
7. 记录域名注册局层面的滥用联络及程序
8. 参与域名注册安全快速请求流程
9. 拟定高安全域认证计划

联系问题与缓解措施

A. 如何防止害群之马经营域名注册局？

1. 审查域名注册营运商

B. 怎样确保域名注册信息的完整性和实用性？

2. 要求 DNSSEC 部署
3. 禁止通配符方式
4. 鼓励清除孤立粘帖记录

C. 如何保证采取更有针对性的措施打击验证滥用行为？

5. Thick WHOIS 要求
6. 域文件访问认证
7. 记录域名注册局和域名注册服务商层面的滥用联络及政策
8. 域名注册安全快速请求流程的可用性

D. 对于本身有可能招致恶意行为的顶级域名，如何强化控制结构？

9. 高安全域认证计划

新域名注册局合同中将要执行的具体措施

《申请指南》中包含下列措施，它们体现了对所有新域名注册局的要求。《申请指南草案》使用的语言得以确定。每条具体措施附有简短的说明（斜体）。

1. 审查域名注册营运商

申请人问题（模块2附件）规定：

如申请涉及如下情形，即便在其它方面合格，ICANN也可予以拒绝：

申请人或任何官员、合伙人、总监、或经理或其他成员或拥有（或受益享有）申请人百分之十五或以上份额的任何人或实体：

a. 在过去十年内，曾被宣判重罪或有关金融或企业管治失当行为的轻罪，或曾被法庭判决欺诈或违反诚信义务，或曾是司法裁决的对象且 ICANN 认为其性质相当于前述行为；

b. 在过去十年内， 曾因欺骗或滥用资金或其它而被政府或业内监管机构处罚；

c. 目前卷入任何法律诉讼或调查，且可能招致与（a）或（b）项下同类罪行、判决、裁决或处罚；

d. 曾被 ICANN 剥夺资格且该处分在考虑其申请时仍然有效；或

e. 申请时，未能向 ICANN 提供确认身份必需的验证信息；

f. 曾被确认为须对有关域名注册的不诚实行为负责或屡次发生此类行为，包括：

(i) 获取域名的目的主要是为了向商标或服务标志所有人或竞争对手出售、租赁或转让，且价格远远超过与域名直接相关的实际成本；或

(ii) 注册域名的目的是为了阻止商标或服务标志所有人在对应域名中体现其标志；或

(iii) 注册域名主要是为了干扰竞争对手的生意；或

(iv) 利用域名将互联网用户吸引到一个网站或其它在线场所，以获取商业利益，方法是制作与以下商标或服务标志混淆的可能性：网站或在线场所的出处、赞助、联号或背书，或网站或在线场所上的产品或服务的出处、赞助、联号或背书。

注意： 申请时，将考虑在背景审查过程中收集的信息，包括以往的犯罪活动记录。

申请流程包括对公司及个人（如重要官员）进行标准、严格的背景和参考审查。该措施有助于防止已知的重罪犯、犯罪团伙成员或有不良营业历史的人参与域名注册局运营或取得域名注册局的所有权或控制其代理权。

2. 要求 DNSSEC 部署

要求域名注册营运商提供成熟的方案以签署其域文件且在开始运营时确保DNSSEC部署到位。

根据技术评论，《域名注册协议》（第三版）第6条项下增加了下列语言；

“域名注册营运商应执行域名系统安全协议（‘DNSSEC’）。在协议有效期间，域名注册营运商及其继承人应遵循RFCs 4033、4034、4035、4509及4310，且采用RFC 4641中规定的最优方法。如域名注册营运商执行DNSSEC哈希认证否定存在，则该营运商及其继承人应遵循RFC 5155。 域名注

册营运商应按照业内最优方法，从子域安全地接受公共密钥材料。同时，域名注册局应在其网站中公布规程和政策文件（又称DNSSEC政策声明或DPS），说明其密钥材料及注册人信任锚材料的储存、访问及使用。”

执行DNSSEC对互联网整体安全性和稳定性的益处已有很好的说明。ICANN致力于在2009年内签署根域，并保证在创建新通用顶级域名时，启用这一重要手段，以提高DNS的安全性。

3. 严禁通配符方式

SSAC（经ICANN董事会批准）的SAC041报告及其他评议组织的报告均建议ICANN在新顶级域名中应严禁使用DNS重定向及合成DNS响应。

考虑到当前与网站提供广告关联的恶意软件趋势，域名重定向至广告站点有可能导致恶意行为增多。对于非由注册人亲自注册的、或注册人未提供NS记录等有效记录或没有获准在DNS中公布的域名，严禁使用RFC 4592规定的DNS通配符资源记录或其它方法或技术合成DNS资源记录或使用DNS重定向 。具体而言，当查询该等域名时，官方名称服务器必须回复“名称错误”响应（又称NXDOMAIN）、 RFC 1035及有关RFC规定的RCODE 3。

该规定适用于DNS树所有层面的所有DNS域文件，域名注册营运商（或提供注册服务的分支机构）为其保存数据、允许保存数据或从中收费。

《域名注册协议》（第三版）第6条项下增加了以下通配符禁止规定：

“对于非由注册人亲自注册的、或注册人未提供NS记录等有效记录或没有获准在DNS中公布的域名，严禁使用RFC 4592规定的DNS通配符资源记录或其它方法或技术合成DNS资源记录或使用DNS重定向 。当查询该等域名时，官方名称服务器必须回复‘名称错误’响应（又称NXDOMAIN）、 RFC 1035及有关RFC规定的RCODE 3。该规定适用于DNS树所有层面的所有DNS域文件，域名注册营运商（或提供注册服务的分支机构）为其保存数据、允许保存数据或从中收费。“

SSAC（经ICANN董事会批准）的SAC041报告（pdf）及其他评议组织的报告均建议ICANN在新顶级域名中应严禁使用DNS重定向及合成DNS响应。重定向与合成响应不仅对顶级域名，而且对DNS子层也存在威胁。新域名注册合同中作此规定是为了在域名注册局层面解决这一问题。

4. 鼓励清除孤立粘帖记录

作为公布的防止滥用政策的一部分，域名注册局必须说明从域删除名称服务器项目时，怎样清除孤立粘帖记录。以下段落摘自《申请指南草案》模块2申请人问题：

“滥用预防及缓解：申请人应说明将采取何种政策及程序，在最大程度上减少滥用注册及其它活

动，以免给互联网用户带来消极影响……答案应包括快速卸下或中止系统及对于名称已从域中删除的孤立粘帖记录的管理和清除的建议措施。”

APWG研究估计，约有3%用于网络钓鱼的域名使用“孤立名称服务器”记录，即已被域名注册局删除的域名的残余痕迹。这就可能为该等域文件中的名称服务器项目提供避难所，滥用者可藉此支持恶意域名注册。

5. Thick WHOIS 要求

域名注册营运商必须按照《域名注册协议》（第三版）第4条的要求，利用thick Whois数据模型为注册数据保留并提供公共访问路径。

“WHOIS服务：在ICANN作出不同的格式和协议规定前，域名注册营运商将按照RFC 3912的要求，通过端口43和<whois.nic.(TLD)>运营提供注册数据公布服务，以下列各式至少提供下列要素的免费公共访问路径。ICANN保留规定替代格式和协议的权利，包括互联网注册信息服务（‘IRIS’–RFC 3981及相关RFC）。一旦有此规定，域名注册营运商将尽快执行该等替代规定。”

在心域名注册协议提案中，ICANN曾建议修改Whois要求，要求所有域名注册局按照说明书（pdf）的规定提供thick Whois信息。此外，由ICANN知识产权社群组成的商标保护议题评估小组的报告草案（pdf）规定，“IRT相信在域名注册局层面，以Thick WHOIS的方式提供WHOIS信息，是保护消费者和知识产权所有人的关键，且该方法具成本效益”。实施Thick WHOIS可增进可达性并可提高记录访问的稳定性，从而有助于减少恶意行为。

6. 域文件访问认证

ICANN将要求域名注册局允许对域文件数据的访问，以便通过认证供应商实现其可用性。

《域名注册协议》第4条规定域名注册营运商将允许团体访问该等数据：

“2.2.1. 通用访问：域名注册营运商应按照ICANN可能不时规定的方式，为ICANN或其指定人员持续提供顶级域名注册域文件的访问路径。

“2.2.2. 中央域文件备份：如ICANN或其指定人员建立了中央域文件备份，域名注册营运商将应ICANN的请求，为ICANN或第三方营运商提供ICANN指定的该等备份。如建立该等中央域文件备份，ICANN可自行决定放弃遵守本文件第4条2.1项下的规定。[摘录2.2.2是为了便于团体讨论。根据该规定，ICANN指定人员可接管目前由域名注册营运商履行的责任，即审查和监督责任方对域文件数据的合法访问。]”

为便于访问注册域文件数据（目前由域名注册局掌管），ICANN（或其指定行使该职能的当事人）将从新通用顶级域名注册局收集域文件数据，并为订户提供该等数据的电子访问路径。同时，

希望访问ICANN管理的注册域文件的当事人须签署一份合同。ICANN将在现有模式的基础上拟订访问合同，并传输系统予以管理/支持。

通过中央协调，防止滥用团体可有效获取在各个域中创建的新域名更新信息。

7. 记录域名注册局和域名注册服务商 层面的滥用联络及政策

域名注册营运商应为顶级域名内的所有域提供一个滥用联络。该滥用联络负责解决验证方的滥用投诉并及时作出响应，该等验证方包括其他域名注册局、域名注册服务商执法机构、防止滥用团体的成员等。此外，域名注册局必须就其打击滥用的政策作出说明。

域名注册营运商可要求所有与其签约的域名注册服务商提供滥用联络。该措施与SSAC报告SAC038（pdf）中的建议一致。同时，域名注册局可要求域名注册服务商公布与域名注册局一致的防止滥用政策。根据两个层面的政策规定的程序，可以：

1. 中止涉及商标滥用、网络钓鱼、故意传播恶意软件或其它非法或欺诈活动的域名；
2. 解决与其控制下服务转售商或其他经销商有关的问题；
3. 清除与恶意行为相关的孤立粘帖记录；
4. 确定滥用联络及其通信方式。

《注册协议》（第三版）第6条中增加了以下规定：

“域名注册营运商应在其网站中提供详细准确的联络资料，包括有效的电子邮箱、邮寄地址及处理顶级域名恶意行为质询的主要联络人；如该等联络资料有任何变动，营运商应及时通知。”

此外，以下段落摘自《申请指南草案》（第三版）模块2:

“…要求每位域名注册营运商在自己的网站上建立并公布联络资料，负责解决需要特别注意的问题，并针对涉及顶级域名内一切名称的投诉作出及时响应，包括牵涉转售商的投诉。”

新域名注册局可能在很大范围内需要明确的控制措施，并在注册过程中定义职责。域名注册局和域名注册服务商层面的滥用联络及政策是将来打击恶意行为的基本步骤。

8. 域名注册安全快速请求流程的可用性

经咨询通用顶级域名注册局、域名注册服务商和安全专家，ICANN基于从蠕虫响应中学到的教训，发展出一套补充程序：ttp://www.icann.org/en/announcements/announcement-01oct09-en.htm，通过该程序，域名注册局可以通知ICANN某通用顶级域名当前或即将发生的事态，并请求依据合同放弃本应采取或已经采取的旨在缓和或消除安全问题的措施。

将安全事态定义为以下一或多种情形：

a. 涉及 DNS 的恶意活动，且其范围和严重性威胁到 DNS 的系统安全、稳定性及适应性；

b. 潜在或实际非法披露、更改、插入或销毁域名注册资料，或非法访问或披露系统依据有关标准运营的信息或资源；

c. 不希望发生的潜在或实际后果，且该后果可能导致或威胁致使ICANN"通用顶级域名注册持续性方案"（pdf）中定义的通用顶级域名注册局的一或多项重要职能暂时或长期失效。

ERSR专门针对需要域名注册局立即采取措施及ICANN采取快速响应（24-48小时内）的事故。该程序无意取代应通过域名注册服务评估政策（RSEP）（链接）作出的请求。

9. 高安全域认证计划

为满足在通用顶级域名内加强信任的整体需要，ICANN已拟定一个通用顶级域名认证计划框架。根据目前的建议，该认证计划遵循完全自愿的原则

申请新通用顶级域名时不选择认证，不会导致对申请人产生怀疑，也不会影响其在评估流程中的得分。认证计划旨在设定一系列可行的标准，藉由执行相应的营运和控制措施，加强获认证通用顶级域名内的信任度，同时根据控制措施评价通用顶级域名注册局和域名注册服务商的绩效。选择认证的通用顶级域名注册局将能够以某种公共展示的方法（如"标记"或可在通用顶级域名认证总清单中得到验证的标志）体现其认证。ICANN将保存并公布通用顶级域名认证总清单。

除保存通用顶级域名认证总清单外，ICANN的职能还在于设置、改进并控制计划的监管，及携手团体确定计划标准。通用顶级域名的实际评估将由独立实体依据计划标准实施。

为取得认证，域名注册局的运营必须遵循下列原则（见《指南》模块2）：

a. 域名注册局证明营运商采取有效控制措施，以资在如下方面提供合理保证，即其重要 IT 支持系统和信息资产的安全性、可用性、保密性和隐私性及有效的商业运营；

b. 域名注册局采取有效控制措施，以资在如下方面提供保证，即域名注册局的核心配置权威、准确、完整，且根据已确立的政策和标准得到及时执行，参与实体的身份经过确定和验证。

c. 域名注册局采取有效控制措施，以资在如下方面提供保证，即其域名注册服务商的核心配置权威、准确、完整，且根据已确立的政策和标准得到及时执行，参与实体的身份经过确定和验证。

获得认证必要的程序包括域名注册局及其域名注册服务商的营运认证。

如申请人希望申请认证，须分两个阶段进行。

第1阶段

在获得新通用顶级域名授权前,申请人须参加一项评估，包括：

- 背景信息
- 域名管理/卸下程序
- 滥用联络及响应
- 第三方保管记录程序

获得新通用顶级域名授权并开始运营后，申请人可以在规定的时间内实施所有预审流程及控制措施。

第2阶段

该阶段旨在检验第1阶段规定的流程、控制及程序，确认其有否按照计划运作。如发现缺陷，独立评估机构会通知ICANN。在认证请求前，域名注册营运商可以在规定的时间内将问题解决。域名注册营运商可在晚一点的时间重新申请认证。

如通过注册申请评估且获得顶级域名授权，域名注册营运商可在此时选择申请认证，然后在某个阶段完成上述检验。换言之，申请人也可选择在通过评估并开始运营后，获取认证。

支持认证必需的控制措施须定期接受审计评估，以保持通用顶级域名的认证状态。

ICANN相信，通过对域名注册局、域名注册服务商和注册人配置及域名注册局和域名注册服务商运营的控制措施提出额外的要求，该认证计划有利于在获认证通用顶级域名内加强信任。在信任和成本/利益间寻求平衡构成问题的关键，顶级域名注册将用作确定安全认证是否是要追求的业务需求的基础 。

安全认证计划适用于提升域名注册运营信任水平所必需的一系列支持活动。针对取得ICANN计划标记的通用顶级域名注册局，草案计划的重点集中在减少潜在恶意行为所必需的控制措施上。范围限制在域名注册局和域名注册服务商营运层面的互联网控制措施及活动上，并未延伸至注册人的运营。安全认证计划旨在提供一个合理但并非绝对的保证，即指定顶级域名已执行了有效运营控制措施，符合安全认证计划标准。确立认证标准，并对其有效性定期作独立审查/审计，从而得以提升并维持信任水平。