有关加强互联网安全性、稳定性和灵活性的计划

已批准草案 – 2009 年 5 月 16 日

目录

执行摘要

互联网作为一种由多个利益主体构成的社会生态体系，正在蓬勃发展之中，这些利益主体通过有效合作，促进了全球互联网共同空间中的交流、创新和商业往来。全球互联网要实现互操作性，取决于互联网唯一标识符系统的运营和协调。[1] ICANN（互联网名称与数字地址分配机构）和这些系统的运营商都意识到，维护和增强该系统的安全性、稳定性以及灵活性是他们合作的核心内容。

《ICANN 2009-2012 年战略计划》(www.icann.org/en/strategic-plan/strategic-plan-2009-2012-09feb09-en.pdf) 中强调：“安全性、稳定性和灵活性始终是第一位的，确保互联网唯一标识符系统的安全性、稳定性和灵活性是 ICANN 为关注的使命，为此，ICANN 将与其他互联网利益主体展开有效的合作，力图增强并保护互联网的安全性和稳定性。”战略计划明确了 ICANN 在安全性、稳定性和灵活性责任方面的一系列目标。该战略计划在其第二个工作重点 － “互联网唯一标识符分配和指定的安全性、稳定性和灵活性”中阐述了安全性、稳定性和灵活性问题。第二个工作重点强调：ICANN 使命的一个核心是确保互联网唯一标识符系统安全、稳定而灵活地运行。目前，破坏性攻击及其他恶意行为愈加频繁，复杂性也日益增加，ICANN 及其群体必须不断提高 DNS 的灵活性并增强应对这些攻击和恶意行为的能力。鉴于攻击和恶意行为的类型日趋多样化，任何组织都无法凭一己之力解决这些问题，因此，ICANN 必须与其他利益主体密切合作，明确 ICANN 的职责，共同寻求解决方案。此工作重点的主要目标是确保互联网唯一标识符系统在本计划有效期内保持有效而稳健的运行。

该战略计划在其第二个工作重点中确定的具体目标为：

A. 提交计划以征询意见，计划中应阐明 ICANN 在确保互联网的安全性、稳定性和灵活性方面所扮演的角色；确定合适的合作伙伴并展开合作。界定 ICANN 的角色，以此阐明职责范围、成本及交付成果，并在 2009 年启动一项流程，促使机构群体与理事会之间达成共识。与合作伙伴开展有效合作，探寻多利益主体方式，开展有助于提高互联网安全性、稳定性和灵活性的项目。这些项目的评估标准将在 2009 年底之前确定，2010 年中期之前将进行首次项目评估。

B. 提供允许用户验证 ICANN 发布的互联网标识符真实性的机制，并广泛地开展技术工作，以提供更安全的互联网命名与编址系统。具体来说，ICANN 将与主要的利益主体倾力协作，确保在 2009 年底之前完成 DNS 根区域的 DNSSEC 签名，并促进 rPKI 的实施，以增强编址方案的安全性和稳定性。

[1] 按照 ICANN 章程，ICANN 主要协调以下三套互联网唯一标识符的分配和指定：域名（构成 DNS 系统）；互联网协议 (IP) 地址和自治系统 (AS) 号码；以及协议端口和参数号码。

C. 开展有针对性的项目，提高风险意识，并增强 TLD 群体相关组织的安全性和灵活性。具体项目包括：与合作伙伴协力在 2009 年底之前制定出一套有效的方案，以便在整个群体内分享最佳做法，并在本计划有效期内对群体开展持续的区域性培训和演习项目。

D. 在本计划有效期内，继续与整个 ICANN 群体中的利益主体密切协作，以此增强利益主体的风险意识，提高 DNS 的安全性与灵活性，有效防范各种威胁。ICANN 将与合作伙伴一起在 2010 年中期之前制定出衡量 DNS 及其用户运营风险的方式。

ICANN 有关加强安全性、稳定性和灵活性的计划提供了目标 A 所需的文档，进一步明确了 ICANN 在解决安全性、稳定性和灵活性问题方面的具体职责，概述了 ICANN 在这一领域的计划，并具体说明了为在下一运营年度更好地发挥 ICANN 的作用而计划采取的行动。本计划第一版旨在作为 ICANN 及其机构群体履行其职责的依据，同时建立相应的框架来组织开展其在安全性、稳定性和灵活性方面的工作。本计划不会为 ICANN 凭空添加在此领域的任何新的重大职责或计划。

ICANN 的职责

ICANN 通过执行由多利益主体参与的基于共识的流程来制定相关政策和计划（包括与安全性、稳定性和灵活性相关的政策和计划）时，需要按照其章程规定来采取相应行动。

- ICANN 的职责必须始终体现与唯一标识符系统相关的核心使命。
- ICANN 的身份不是网络警察，也不会在运营中直接与犯罪行为做斗争。
- ICANN 不会参与有关利用互联网从事网络间谍和网络战争的对话或活动。
- ICANN 不担当界定互联网违法内容的角色。
- ICANN 的职责包括与广泛的互联网群体共同参与各种打击滥用唯一标识符系统的活动。这些活动包括与相关政府部门合作打击利用这些系统实施的恶意活动，以加强对这些系统的保护。

ICANN 有关安全性、稳定性和灵活性的计划

- ICANN 负责互联网号码分配当局 (IANA) 的运营。确保 DNS 根区域功能的安全、稳定而灵活的运营，一直是且未来仍将是 ICANN 的首要任务。
- ICANN 推动着域名系统 (DNS) 和地址分配群体为加强系统的安全性、稳定性和灵活性基础而开展工作。这些工作包括对各种协议的制定和实施提供支持，以及为互联网名称和号码的验证提供技术支持。

- ICANN 是 DNS 注册管理机构、注册服务商及其他机构群体成员实施的安全性、稳定性和灵活性等相关活动的推动者和协调者。
- ICANN 负责自身资产和服务的安全、稳定和灵活运营。
- ICANN 是与互联网唯一标识符系统的安全性、稳定性和灵活性相关的多个论坛和活动的参与者。

有关加强安全性、稳定性和灵活性的计划

2009 至 2010 运营年度，ICANN 将执行下列各项计划和举措。附录 A 详细说明了具体的计划和活动目标、合作伙伴、交付成果以及资源投入。

- ***IANA 运营*** — 按照《ICANN 2009-2012 年战略计划》，ICANN 应为在权威根区域实施 DNSSEC 做好运营准备，并与互联网群体共同扫除采用 DNSSEC 的障碍。ICANN 愿意、能够并已准备好对根区域进行签名。本文的第 5.1.1.3 和 6.1.1.1 部分将介绍 ICANN 根据其 2008 年 9 月的提议而开展的当前工作和计划工作。其他措施包括通过自动化流程改善根区域管理；改进与 TLD 管理机构的通信认证。
- ***DNS 根服务器运营*** — 断寻求对角色和职责的相互认同，发动自发力量实施应急计划和演练。
- ***gTLD 注册管理机构*** — 确保继续对新通用顶级域名 (gTLD) 和国际化域名 (IDN) 申请人进行评估，以保证运营的安全性。ICANN 将推出成熟的 gTLD 注册连续性计划并测试数据托管系统。
- ***ccTLD 注册管理机构*** — ICANN 将加强与国家或地区顶级域名 (ccTLD) 注册管理机构的合作，进一步完善其与国家或地区代码域名支持组织 (ccNSO) 和各地顶级域名 (TLD) 协会联合制定的攻击事件及应急响应计划 (ACRP)。
- ***合同合规性*** — ICANN 将继续扩大涉及 gTLD 的合同履行活动的范围，作为实施《注册服务商委任协议》(RAA) 2009 年 3 月修正案的部分措施，对合同签约方启动审核事宜，并确定合同签约方参与恶意活动的的潜在可能，以便采取合规行动。
- ***应对 DNS 恶意滥用*** — ICANN 将基于多方力量共同打击利用 DNS 实施的恶意行为，同时促进信息共享以便有效应对恶意行为。
- ***ICANN 内部安全性和连续性运营*** — ICANN 将确保其安全计划在机构的整体风险管理、危机管理和业务连续性计划中执行。其重点在于为成文计划和支持流程打下坚实的基础。
- ***确保全球参与和协作*** — ICANN 将继续加强与互联网工程任务组 (IETF)、互联网协会 (ISOC)、地区互联网注册机构 (RIR) 和网络运营商团体 (NOG) 以及 DNS 运营、分析和响应中心 (DNS-OARC) 之间的合作关系。ICANN 还将积极参与全球性对话，以促进公众对整个互联网群体所面临的安全性、稳定性和灵活性等方面的挑战的理解，以及对如何通过多利益主体参与的方式来共同应对这些挑战的认识。

1. 目的和概述

1.1 本计划向广大互联网利益主体全面阐述了 ICANN 将如何围绕其协调互联网唯一标识符的使命，参与解决互联网面临的安全性、稳定性和灵活性等挑战的全球行动。本计划界定了 ICANN 在这一领域的职责及职能范围，概述了 ICANN 针对该领域已建立的计划，并详细说明了下一运营年度的计划活动和专项资源投入。本计划包括七个章节和一个附录：

- 第 1 章：目的和概述
- 第 2 章：挑战和机遇
- 第 3 章：ICANN 职责
- 第 4 章：ICANN 安全性、稳定性和灵活性工作的参与方
- 第 5 章：ICANN 与安全性、稳定性和灵活性相关的现行计划
- 第 6 章：ICANN 有关提高安全性、稳定性和灵活性的 2010 财年计划
- 第 7 章：总结
- 附录 A：ICANN 2010 财年安全性、稳定性和灵活性的计划目标、合作伙伴、重大事件/交付成果及资源投入

1.2 如执行摘要中所述，本计划基于《ICANN 2009-2012 年战略计划》中的愿景和目标而制定。本计划第一版旨在作为 ICANN 及其机构群体履行其职责的依据，同时建立相应的框架来组织开展其在安全性、稳定性和灵活性方面的工作。本计划不会为 ICANN 凭空添加在此领域的任何新的重大职责或计划。本计划每年与 ICANN 战略和运营计划同步更新。

2. 挑战和机遇

2.1 活跃的互联网环境所遭受的恶意活动正在不断升级，实施者来自多方，包括犯罪组织大量参与的诈骗、敲诈和其他网络违法活动，以及不断增加的拒绝服务 (DoS) 攻击和其他通过互联网进行的破坏性活动。人类的各种社会动机和行为，正在通过互联网活动日益得到体现。这类活动在一定程度上反应了互联网的开放特性，正是这种开放性，互联网才取得了今天的成功，才能促进互联网尖端技术的创新，才能实现全球互联网共同空间中的交流、创新和商业往来。但互联网的开放性也带来了许多缺陷：例如，通过趁机“欺骗”或“毒害”DNS 解析，误导不知情用户进行计算机连接的事件不断增加。同样，路由劫持以及地址注册和自治系统号码 (ASN) 注册劫持事件也在持续增加。拒绝服务 (DoS) 攻击对所有类型的用户都可能会造成干扰。过去几年里，互联网各阶层的利益主体，包括用户、企业、主权国以及参与以互联网和广泛信息社会为中心议题的各种讨论的组织，对此表示了日益深切的担忧。要解决这些问题，还必须消除安全性和稳定性的风险。这些风险的形成可能源自于使得网络稳定性难以实现的网络设计，或者源自于可能会被犯罪分子滥用的互联网管制新措施。

2.2 ICANN 将在其职责范围内努力消除互联网安全性、稳定性和灵活性方面的风险。ICANN 章程第 1 款中将 ICANN 的使命描述为“对全球互联网的唯一标识符系统进行总体协调，确保互联网唯一标识符系统能够稳定而安全地运行”。ICANN 这方面的计划和活动主要在于使互联网唯一标识符系统实现三个主要特性：安全性、稳定性和灵活性。安全性是指保护互联网唯一标识符系统并防止其被滥用。稳定性是指确保系统能正常运行且唯一标识符系统的用户相信系统能够正常运行。灵活性是指唯一标识符系统能够有效应对和打击恶意攻击和其他破坏性活动，并能从中恢复。ICANN 与各责任方就唯一标识符系统的方方面面进行了通力合作，确保其负责任地正确执行各项政策和合同协议。作为一个由多利益主体推动的组织，ICANN 确保将与主要利益主体进行密切合作，明确战略、运营和财政计划的实施目标和绩效衡量标准，尽最大努力来有效利用机构群体在这一领域的一切可用资源。本计划就 ICANN 如何履行其职责这一问题为机构群体提供了一张路线图。本计划中的附录 A 详细说明了 2010 财年的活动计划、重大事件及相关资源。ICANN 负责安全事务的工作人员 2010 财年的目标主要在于，制定出相应的标准，以便开展更广泛的计划，来寻求改善唯一标识符系统整体的安全性、稳定性和灵活性。

3. ICANN 职责

3.1 ICANN 通过执行由多利益主体参与的基于共识的流程来制定相关政策和计划（包括与安全性、稳定性和灵活性相关的政策和计划）时，需要按照其章程规定来采取相应行动。ICANN 核心使命主要在于，通过多利益主体参与的方式，有效发挥 IANA 的职能，制定全球政策来协调 DNS、互联网协议 (IP) 地址分配和 IP 分配，并通过与 gTLD 注册管理机构和 ICANN 认可的注册服务商签订的合同体系，来促进 gTLD 环境中的竞争、增加消费者的选择。

3.2 过去 10 年来，作为其使命之一，ICANN 一直在履行其职责，为互联网唯一标识符系统的安全和稳定贡献着一己之力。ICANN 和唯一标识符系统的相关运营商都已意识到并承认，维护和增强服务的安全性和稳定性是他们合作的核心部分。这一原则在 ICANN 与运营商之间的合同和协议体系中，通过特定的合作关系、具体职责和共同责任，得到了充分的体现。ICANN 与相关运营商之间的这种合作和行动的落实为人们树立了必要的信心，它使人们相信，全球唯一标识符及其提供组织通过协调一致的合作体系，可确保互联网的安全性、稳定性和灵活性。

3.3 ICANN 计划继续投身于各种相关活动，使互联网命名和地址分配系统在面对不断变化的风险和威胁时能够安全、稳定和灵活地运行。同时，ICANN 还将确保其所有工作都围绕与唯一标识符系统相关的核心使命来开展进行。它扮演的不是网络警察的角色，不会在运营中直接打击犯罪行为、限制恶意行为参与者。ICANN 不参与有关利用互联网进行网络间谍活动和网络战争的活动或对话。同样，ICANN 也不会参与讨论如何界定存在于互联网或通过互联网传播的违法内容。ICANN 将继续与广泛的互联网安全群体一起参与相关的重要论坛，共同打击利用互联网唯一标识符系统的特定恶意活动（如网络钓鱼和发送垃圾邮件）。

3.4 ICANN 根据其所承担的角色（直接负责者、推动者/协调者和参与者），来组织、安排其在安全性、稳定性和灵活性等方面的工作。

- ICANN 直接负责 IANA 的运营，并与美国商务部和 VeriSign（威瑞信）共同负责根区域的系统编译和分发。确保 DNS 根区域功能的安全、稳定而灵活的运营，一直是且未来仍将是 ICANN 的首要任务。此外，ICANN 是 DNS 和地址分配群体验证互联网名称和号码工作的重要推动者。ICANN 认为，解决 DNS 安全性问题的重要一步是实施域名系统安全扩展 (DNSSEC)，其中包括在 DNS 根区域签名。ICANN 提议在 DNSSEC 运行过程中与 VeriSign、NTIA 和根服务器运营商进行合作，以确保 DNS 根区域分配机制的连续性不受影响。ICANN 提供了能从临时方法过渡到永久方法的灵活解决方案，并为履行这一职责做好了运营准

备。其他主要工作在于改善相关方对系统层面风险的理解，促进资源公共密钥基础架构 (rPKI) 根一级的实施工作，并与合作伙伴共同加强 TLD 群体在安全性和灵活性方面的实际工作。

- ICANN 是 DNS 注册管理机构和注册服务商开展的安全性、稳定性和灵活性相关工作的推动者和协调者。ICANN 的职责实质上取决于它与这些核心运营商关系的特定性质。除合作活动外，ICANN 已与所有 gTLD 注册管理机构和 ICANN 认可的注册服务商签定了合同。这些合同协议已逐渐成为改善 DNS 整体安全性、稳定性和灵活性的机制。确保这些协议条款的履行和正确实施将是 ICANN 未来工作的主要侧重点。对于 ccTLD 注册管理机构，ICANN 和 ccTLD 运营商承诺本着关系平等的原则，从本地及全球互联网群体的利益出发，进一步增强 DNS 的安全性、稳定性和互用性。信息共享、相互协助和能力培养将会是未来合作活动的主要侧重点。
- ICANN 与号码资源组织 (NRO) 和 RIR 以三方的共识为导向共同参与各种活动，即 RIR 与 ICANN 的共同目标是从本地及全球互联网用户的利益出发，维护和提高互联网的安全性、稳定性与灵活性。
- ICANN 直接负责自身资产和服务的安全、稳定和灵活运营，同时还承担 IANA 的运营和其他协调职能，并且还是 DNS L 根服务器的运营机构。
- ICANN 支持组织、咨询委员会和工作人员是更为广泛的一些论坛和活动的重要参与者，从提高应对破坏性攻击的灵活性到共同打击互联网恶意活动（例如，利用互联网唯一标识符系统实施的恶意软件传播和网络钓鱼行为），不一而足。ICANN 的使命之一是让公众信任其在协调互联网唯一标识符系统方面的职责，面对实现安全、稳定和灵活的互联网生态系统这一挑战，ICANN 将会扮演领导者角色，为全球对话、商业往来和创新维持一个积极活跃的环境。

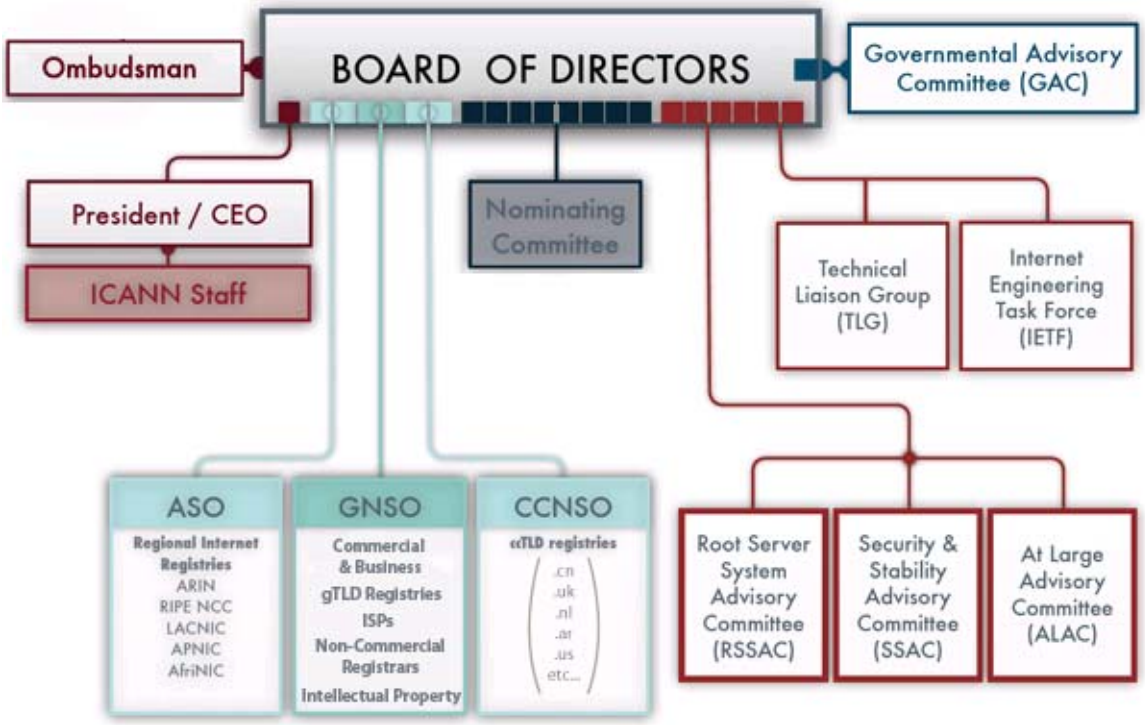
4. ICANN 安全性、稳定性和灵活性工作的参与方

ICANN 在安全性、稳定性和灵活性方面的活动包括该组织工作人员、支持组织和咨询委员会参与的活动。主要参与者包括：

- ***IANA 工作人员*** — 负责执行 IANA 职能，包括协调 DNS 根区域，负责 .arpa 注册管理机构的运营、分配 IP 地址空间以及登记协议参数。IANA 工作人员已制定了在根级实施 DNSSEC 的计划，并已为 ICANN 管理的 DNS 区域制定了相关计划。与安全性、稳定性和灵活性相关的具体活动将在下文列出。
- ***服务/合同合规性工作人员*** — 负责确保 gTLD 注册管理机构和 ICANN 认可的注册服务商配合并遵守协议。与安全性、稳定性和灵活性相关的具体活动将在下文列出。
- ***政策工作人员*** — 负责协助支持组织和咨询委员会开展与政策制定相关的活动，包括支持组织召集的工作组活动。与安全性、稳定性和灵活性相关的具体活动将在下文列出。
- ***全球合作部门工作人员*** — 负责与 ICANN 利益主体进行全球性和地区性合作，确保 ICANN 在全球范围内全面参与相关的运营和实施工作。ICANN 在这方面的安全性、稳定性和灵活性活动被归入到全球合作部门针对 ICANN 的整体工作中。
- ***企业关系/沟通工作人员*** — 负责确保 ICANN 规划和计划的有效宣传，在 ICANN 机构群体中代表该组织及其活动。ICANN 针对安全性、稳定性和灵活性的活动被归入到其企业沟通整体计划中。
- ***安全工作人员*** — 负责 ICANN 理事会和 CEO 在 ICANN 战略和运营计划的实施过程中要求开展的与安全相关的运营工作的日常计划和执行。该团队协调 ICANN 所有工作，确保有效参与与安全相关的主题活动（包括计算机安全）以及其他与安全性、稳定性和灵活性相关的研讨会。
- ***安全与稳定咨询委员会 (SSAC)*** — ICANN 的一个咨询委员会，负责向 ICANN 董事会和机构群体明确 ICANN 在确保互联网唯一标识符系统的安全性和稳定性时面临的重大问题和挑战。委员会根据 ICANN 董事会的要求，根据其使命（如下所述）对重大问题展开研究，并与通用名称支持组织 (GNSO) 等其他 ICANN 组织通力合作。
- ***根服务器系统咨询委员会 (RSSAC)*** — ICANN 的一个咨询委员会，负责针对根名称服务器的运行要求提出建议，检测根名称服务器系统的安全性以及系统整体性能、耐用性和可靠性并提出相应建议。
- 从更广泛的意义来说，与安全性、稳定性和灵活性相关的活动包括所有 ICANN 支持组织和其他咨询委员会的相关活动，详细情况如下文所述。

ICANN 安全工作人员将总体把握 ICANN 各项活动的有效协调，并针对这些活动制定完整的计划和跟踪流程，并确保各部门和利益主体的一致和融合。图 1 描绘了 ICANN 结构内部的基本组织关系。

图 1 — ICANN 组织结构



5. ICANN 与安全性、稳定性和灵活性相关的现行计划

本章节详细说明了 ICANN 针对互联网唯一标识符系统的安全性、稳定性和灵活性已实施的主要计划和活动，明确了主要的运营合作伙伴，并为目前的工作提供了实施依据。本章节的目的是简要说明 ICANN 开展的促进唯一标识符系统的安全性、稳定性和灵活性的各项活动。为使 ICANN 能够有效履行其在此领域的职责，大多数主要工作人员以及支持组织和咨询委员会都参与了这些活动。本章节提供相关的背景信息，并说明这些计划和活动如何在 ICANN 组织结构内部协调安排以及如何与外部组织接轨。

本章节围绕第 3.4 章节中所建立的框架进行阐述，首先阐明主要的 DNS/地址分配职能，随后介绍与 TLD 注册管理机构和注册服务商群体的合作，然后分别描述与 NRO 和 RIR 的密切合作、机构安全性和连续性计划、支持组织和咨询委员会的活动以及对全球及地区互联网安全性、稳定性和灵活性活动的参与情况。

5.1 核心 DNS/地址分配的安全性、稳定性和灵活性职能

5.1.1 IANA 运营

5.1.1.1 ICANN 通过美国商务部、VeriSign、互联网工程任务组 (IETF)、地区互联网注册机构 (RIR) 和顶级域名 (TLD) 运营商的配合来执行 IANA 职能（详见下文）。有效开展这些活动是 ICANN 为实现互联网稳定性和灵活性所做的基本工作。通过执行 IANA 职能，ICANN 可协调并管理关键标识符的注册管理机构，从而实现全球互用的互联网构想。

5.1.1.2 尽管互联网以非集中协调形式的全球性网络而著称，但关键唯一标识符系统的运行须进行全球性协调，目前这一协调任务由 ICANN 承担。具体来说，通过 IANA 职能，ICANN 负责技术标准（“协议”）中所用的唯一代码和编码系统的分配和维护。这些技术标准正是互联网发展的推动力。IANA 职能所涉及的各种活动可大致分为三类：

- ***域名*** — 通过 IANA 职能，ICANN 管理 DNS 根、.int 和 .arpa 域名以及国际化域名 (IDN) 实施资源。其管理工作确保了这些区域的任何变动都会得到评估，以确定其对特定的顶级域名和根区域整体稳定性和安全性的影响。通过执行 IANA 职能，ICANN 还可在 DNS 和地址分配系统的根区域部署和维护信任锚，从而发挥巩固 DNS 和 IP 地址系统安全性的作用，这样便大大增强了唯一标识符数据的完整性以及 DNS 系统内响应的完善性。

- ***号码资源*** — 通过 IANA 职能，ICANN 协调全球 IPv4 和 IPv6 地址空间池以及 ASN，并负责向 RIR 提供这些资源。ICANN 通过 IANA 职能实施这一协调活动，并以 RIR 群体通过其政策制定流程而制定的流程和程序作为行动指南。通过这一参与式政策制定流程，全球范围的号码资源最终接受者将共同认识到，ICANN 和 RIR 的行动方式是公平、稳定且可预知的。
- ***协议分配*** — 互联网协议和参数注册管理机构由 ICANN（通过 IANA 职能）和 IETF 共同管理。ICANN 对 700 多个协议和参数注册管理机构进行管理和支持，其依据的标准是在长期实行的基于共识的征求意见书 (RFC) 发布流程中制定的。通过与 IETF 和 RFC 的起草者密切合作，IANA 工作人员可确保采用一致的流程建立注册管理机构，并对其提供支持以确保其运行方面的准确性和可用性。有关 IANA 工作人员与 IETF 的关系在 RFC 2860 和服务水平协议中有记录。

5.1.1.3 ICANN 认同在根级实施 DNSSEC 的需求，于 2008 年 9 月就 IANA 在根级签名方面的职责问题向商务部递交了一份提案，并做好了履行该职责以及在 .int 和 .arpa 域签名的准备。这些准备工作包括：自 2007 年 6 月起试验实施 DNSSEC，与 TLD 和其他 DNS 运营商合作实施 DNSSEC，提高运用符合相关标准的密码分析法的技术熟练度，以及确保 DNSSEC 的实施工作在运营计划和预算内进行。ICANN 已成立了专门的工作小组负责运营和保障 DNSSEC 的实施，其中还包括对 icann.org 和 iana.org. 的签名。最后，为进一步全面实施 DNSSEC，ICANN 建立了 IANA 顶级域名信任锚存储库 (ITAR)，确保已实施 DNSSEC 的 TLD 的 DNSSEC 密钥能用于目前正在部署 DNSSEC 的 TLD。

5.1.1.4 此外，ICANN 与 RIR 和 IETF 合作开发了 rPKI 技术，以便推广对已分配的号码资源的认证。为应对 2008 年夏季发现的 DNS Cache Poisoning（DNS 缓存投毒）漏洞，IANA 工作人员与 TLD 群体通力合作，对 TLD 系统内全面缓解措施的实施进行了跟踪。（参见“2008 年 DNS 缓存投毒漏洞”介绍，访问地址：http://www.iana.org/about/ presentations/davies-cairo-vulnerability-081103.pdf）。ICANN 将确保其计划和活动可提高根区域变更/添加流程以及 DNS 内部查询信任锚运营的安全性、稳定性和灵活性（详见下文）。

5.1.1.5 ICANN 每年都会向美国商务部提供一份信息安全计划，说明如何按照 ICANN 与商务部签订的 IANA 职能合同执行 IANA 职能，该计划也是 ICANN 自身机构安全及应急计划的组成部分。

5.1.2 DNS 根服务器运营

5.1.2.1 ICANN 就根区域的安全和稳定协调与根名称服务器运营商进行了通力合作，以确保有相应的应急计划并维持明确的根区域变更流程。ICANN 将就根服务器系统安全性和稳定

性的协调工作继续与根名称服务器运营商和其他机构进行合作。RSSAC 已成为有关协议变更（例如在根区域中添加 IPv6 记录）如何影响系统的重要咨询机构。

5.1.2.2 ICANN 将会继续推进与根名称服务器运营商关系的正式化，以便履行 2006 年度 ICANN 理事会批准的《ICANN 私营管理的责任认定》中的承诺。2008 年，ICANN 与互联网系统联合会就 F 根 (F-root) 的运营达成了一项共同责任协议，协议重申了“本着关系平等的原则，从全球视角着眼，从本地及全球互联网群体的利益出发，以创新的方式进一步增强互联网域名系统 (DNS) 的稳定性、安全性和互用性的承诺”。

5.1.2.3 此外，ICANN 还负责根名称服务器指定的 l.root-servers.net 的运营。由于这一运营职责，ICANN 工作人员与其他根服务器运营商还会进行运营层面上的互动。作为 L 根 (L-root) 运营机构，ICANN 还积极参与 DNS 群体活动，包括为群体工作贡献己力，例如在域名系统方面，参加了运营、分析和研究中心 (DNS-OARC) 与互联网数据分析协作组织 (CAIDA) 组织的“Day in the Life of the Internet”（互联网时代）研究项目。ICANN 致力于通过自身的运营，促进最佳实践的多样化以及对最佳实践的认识，努力吸取和宣传各种实践经验。

5.2 TLD 注册管理机构和注册服务商的安全性、稳定性和灵活性

ICANN 与互联网整体安全性、稳定性和灵活性有关的一项直接的基本职责是，管理与 gTLD 注册管理机构和 ICANN 认可的注册服务商的协议以及用于管理与 ccTLD 注册管理机构关系的框架性协议结构。ICANN 与 16 家 gTLD 注册管理机构、900 多家认可的注册服务商签有合同，它们主要负责协调域名的注册并确保域名可通过 DNS 进行解析。这些签约方的职责在注册管理机构协议 (RA) 和注册服务商委任协议 (RAA) 中有明确规定。通过上述协议中的条款，ICANN 致力于保护注册人的利益，并以此维护 DNS 和更广泛的互联网领域的安全性、稳定性和灵活性。在过去的十年中，ICANN 一直致力于加强这些协议，包括制定可改善稳定性和灵活性的条款（详见下文）。

5.2.1 gTLD 注册管理机构

5.2.1.1 ICANN 就 TLD 的安全和稳定协调与 gTLD 运营商进行通力合作。此外，所有 gTLD 注册管理机构都与 ICANN 签定了合同。虽然这些合同中的某些部分可能会有所不同，但与安全性、稳定性和灵活性相关的条款都是一致的。这些协议中都含有一条特定条款，要求注册管理机构运营商必须实施由 ICANN 制定的临时性规定或政策以及由通用名称支持组织 (GNSO) 制定并由 ICANN 采纳的共识性政策。协议中的其他条款还要求 DNS 服务、共享注册系统和名称服务

器运营需要第三方数据托管并建立相应的服务水平协议，以此来确保注册管理机构安全和稳定运营。ICANN 与 gTLD 的合同具体规定了可用性、运行水平和数据中心要求。2007 年，ICANN 启动了一项 gTLD 连续性计划，并由此制定了工作计划，承诺每年要实施一系列演练，以便提高 gTLD 注册管理机构群体应对注册管理机构或注册服务商系统内部问题或故障的能力。

5.2.1.2 2006 年，ICANN 推出注册管理机构服务评估流程 (RSEP)，以此促进相应流程的及时性和可预测性，便于引入新的注册管理机构服务。RSEP 的一个重要作用就是确定所提议开展的服务是否会造成安全性或稳定性问题。如果确定所提议的服务可能会造成安全性或稳定性问题，则该服务议案会被提交给一个名为注册管理机构服务技术评估小组 (RSTEP) 的独立技术专家小组。RSTEP 会对提议的服务进行审核，并向 ICANN 理事会提出是否予以批准的建议。

5.2.2 新 gTLD 和 IDN

5.2.2.1 鉴于 ICANN 准备开放新 TLD（包括 IDN）的申请流程，ICANN 认为有必要采取相应措施，以确保新开放的域名能够在 DNS 和整个系统中安全、稳定和灵活运营。新 gTLD 的申请和审核流程包括根据“应用程序中的域名国际化”(IDNA) 协议和 IDN 指南对申请机构运营注册管理机构的能力以及字符串是否符合 RFC 中规定的技术要求进行技术评估。IDN ccTLD 的引入流程将会遵循不同的流程，此次引入作为首次引入，仅限于与现有 ccTLD 对应的、代表国家和区域名称的无争议字符。SSAC 在 2007 年 7 月的通知性实施计划和测试流程中就 IDN 对 DNS 根级的安全性和稳定性的影响给予了评价。

5.2.2.2 独立专家小组将会对申请机构及其申请的 TLD 进行技术评估。此外，在新 gTLD 流程前会先进行一个 RSEP 流程，以便评估 gTLD 申请中所申请的新注册管理机构服务可能存在的安全性或稳定性问题。对于 IDN TLD，有关字符串的技术要求以及相关的评估与 IDN gTLD 和 IDN ccTLD 相同。

此外，所有的申请机构都需要通过一个授权前的技术核查，以确定他们符合运营注册管理机构方面的技术要求。

5.2.3 gTLD 注册服务商

5.2.3.1 ICANN 还就安全性、稳定性和灵活性问题与注册服务商进行通力合作。根据所签定的合同，ICANN 与注册服务商的关系受标准的《注册服务商委任协议》(RAA) 的约束。RAA 对数据收集、保留及托管设定了特定的标准。RAA 还引用了 ICANN 机构群体制定的共识性政策，例如，注册服务商之间的转让政策、Whois 数据提醒政策以及已恢复名称的准确性政策，等等。这些政策多方面地支持了 DNS 的安全性、稳定性和灵活性。

5.2.3.2 ICANN 的注册服务商联络人员作为第一关卡，负责对注册服务商是否符合 RAA 要求进行日常监督，包括对注册人投诉和注册管理商之间的纠纷进行非正式处理，并定期审查委任资格（例如，在注册服务商续签 RAA 时）。

5.2.3.3 为支持更为稳定的域名系统，ICANN 制定了多套计划和流程来应对注册服务商无法提供服务的情况。例如，ICANN 实施了注册服务商数据托管计划，要求注册服务商每天或每周进行一次注册备份数据托管。丧失认可资格的注册服务商数据交接流程方便了丧失认可资格的注册服务商与 ICANN 认可的注册服务商之间及时交接注册数据。此外，ICANN 工作人员利用多个内部运营流程来帮助维护健康的域名注册环境，防止因注册服务商无法提供服务而造成注册人和互联网用户的服务中断。

5.2.4 Whois

5.2.4.1 通过 Whois 服务，公众可访问与注册域名相关的数据，目前这些数据包括域名持有人的联系信息。ICANN 负责管理由机构群体制定的 gTLD 内的 Whois 系统规则。在注册域名时收集的注册数据的数量以及获取这些数据的方式在 ICANN 为 gTLD 中的注册域名制定的协议中均有规定。例如，ICANN 要求经过认可的注册服务商收集并让公众免费查看注册域名及其名称服务器和注册服务商的名称、域名创建日期、过期日期、注册域名持有者和技术联络人以及管理人员的联系信息。

5.2.4.2 不同的机构群体将 Whois 用于各种用途，包括促进技术协调，帮助提供可能涉及滥用 DNS 的组织和个人的信息。ICANN 活动重点在于确保 gTLD 注册管理机构和 ICANN 认可的注册服务商履行了它们的合同义务。考虑到与 Whois 相关的政策变化，ICANN 机构群体认为在努力平衡广大利益主体在 Whois 系统运营方面的利益的同时，还应合理利用 Whois 系统以帮助打击 DNS 滥用行为。同时，对于一些人提出的 Whois 会泄露其个人信息的隐私和安全性问题，ICANN 表示认同。

5.2.5 合同合规性

5.2.5.1 合同合规部门负责确保 ICANN 及其合同签约方履行双方协议中列出的要求。该部门的活动包括管理 ICANN 投诉受理系统。这个系统登记公众提出的可能涉及安全性、稳定性和灵活性问题的域名投诉。请访问网址 http://reports.internic.net/cgi/registrars/problem-report.cgi 。合同合规性工作人员会调查对可能存在的违反 RAA 情况的投诉，一旦发现有违反合同情况，将会采取合规行动。虽然该系统接到的投诉大多数都是 ICANN 管制范围之外的问题（例如，垃圾邮件、网站内容、注册服务商的客户服务），但 ICANN 会将这些投诉转发给注册服务商进行处理。

5.2.5.2 合同合规部门还管理 Whois 数据问题报告系统 (WDPRS)，该系统可通过 http://wdprs.internic.net/ 访问。WDPRS 用于协助注册服务商履行其义务，调查所报告的 Whois 数据误差情况。该系统于 2002 年开发而成，登记公众对 Whois 数据误差的投诉，这些投诉将会转发给注册服务商进行适当处理。经与注册服务商和知识产权社群 (IPC) 协商，WDPRS 于 2008 年进行了重新设计，解决了互联网群体提出的若干问题，包括功能受限、能力受限以及缺乏合规性跟进措施。重新设计的 WDPRS 于 2008 年 12 月启用。合规小组将本着提高 Whois 数据准确性的目的不断改善这一系统。

5.2.6 保护 gTLD 注册人

5.2.6.1 ICANN 还采用各种保护办法竭尽所能地确保注册人对 DNS 安全性、稳定性和灵活性的信心。这些保护办法包括在 ICANN 合同、协议及履行计划中设立相关条款。ICANN 向注册人提供了许多相关信息，包括注册服务商在 RAA 下的义务以及通过 InterNIC 网站 (http://www.internic.net/) 的投诉方式。ICANN 还与注册服务商群体进行了更多的互动，鼓励他们对域名注册人提供 IPv6 支持。

5.2.6.2 此外，ICANN 支持组织和咨询委员会的工作主要侧重于注册人的安全性、稳定性和灵活性问题。SSAC 对注册服务商的建议对其实践有着指导意义，有助于他们提高对域名的保护，加大对于 fast flux、Whois 数据滥用和域名劫持问题的关注，并消除注册人对续用等问题的担忧。除 SSAC 之外，网络普通用户咨询委员会 (ALAC) 也提到关于保护注册人的几个问题。ALAC 首先提到了域名体验问题，针对该问题，GNSO 委员会和理事会批准了一项新的共识政策来防止滥用域名体验延长宽限期。最近，ALAC 向 GNSO 委员会提出了关于注册人恢复过期域名的问题。GNSO 目前实施了不少新举措，例如，注册服务商之间的转让政策的增强措施（该措施考虑了电子认证需求和 Fast Flux Hosting 方面的政策制定需求）和滥用注册政策，这些举措有望提高对注册人的保护。

5.2.7 ccTLD

ICANN 与 ccTLD 注册管理机构之间的合作以双方的共识为导向，即 ccTLD 注册管理机构与 ICANN 的共同目标是从本地及全球互联网用户的利益出发，维护并提高 DNS 的安全性、稳定性与灵活性。这一点体现在责任性框架计划中，从而为各 ccTLD 注册管理机构与 ICANN 之间达成广泛共识打下了基础。ICANN 在增强 ccTLD 的安全性、稳定性和灵活性方面主要侧重于通过与其他组织机构的协同工作，打造相应平台，针对攻击事件及应急响应计划进行信息共享、采取一致行动以及开展提高意识的技术培训和能力培养。ICANN 工作人员与 TLD 运营商密切合作，通过 IANA 职能、攻击事件及应急响应计划 (ACRP) 和全球合作部门地区联络人员向他们通报安全性问

题。通过与 TLD 运营商群体更全面、广泛的接触，ICANN（通过 IANA 职能）与 TLD 运营商建立了相互信任的关系，在需要针对 DNS 进行全球协调时，TLD 运营商群体可协助 IANA 共同应对。

5.2.8 IANA 技术要求

ICANN 通过管理 IANA 职能，还有助于确保 TLD 符合支持稳定和安全运营所需满足的技术要求。具体的名称服务器要求可确保 DNS 域名的可用性，而 IANA 工作人员则与 TLD 管理人员密切合作，致力于解决维护这些技术标准时可能遇到的各种问题。ICANN 虽然不直接参与 ccTLD 的运营，但随时准备在必须快速、可靠地变更其根区域数据时提供协助。ICANN 的一个重要目标就是确保 TLD 区域和根区域的稳定性和安全性。

5.2.9 共同应对恶意滥用域名系统的行为

ICANN 与众多机构组织通力合作，致力于确保利益主体能够分析可能涉及 DNS 滥用的活动。自 2008 年后期起，利用 DNS 进行的恶意软件活动数量猛增。ICANN 正与注册管理机构和注册服务商积极合作，以保持警惕性并促进信息的传播。ICANN 在这一领域中的使命有限，因此只作为兄弟组织参与讨论在出现特定的运营情况时如何有效地应对。

5.2.10 实现 DNS 整体安全性和灵活性

5.2.10.1 虽然 ICANN 工作人员、支持组织和咨询委员会中没有任何一个实体单独承担主要的职责，但都在增强 DNS 整体的安全性、稳定性和灵活性方面发挥了促进作用。自 SSAC 成立以来，它一直在向 DNS 群体提供分析数据和建议。它的主要工作包括对 DDoS 攻击、通过在 DNS 根中添加 IPv6 记录实施 DNSSEC、抢先注册域名、Fast Flux Hosting 以及域名劫持进行分析，并提供相关建议。此外，SSAC 成员还参与了反网络钓鱼工作组 (APWG) 的互联网政策委员会，并联合编写了有关网络钓鱼者如何利用域名和子域名的白皮书。

5.2.10.2 ICANN 计划继续加强这一职责，努力寻求与广泛机构群体的合作机遇，确定并缓解系统面临的风险。在 2009 年 2 月与乔治亚理工学院信息安全中心 (GTISC) 共同举办的 Global DNS Security, Stability and Resiliency Symposium（全球 DNS 安全性、稳定性和灵活性研讨会）上，ICANN 发起了提高对 DNS 整体风险的认识以及采取相应缓解措施的行动。该研讨会的主要目的是促进对大型企业内的 DNS 相关风险的认识，以及对 DNS 在发展中国家进行安全、可靠、灵活运营所面临的挑战的认识，解决利用 DNS 开展恶意活动的问题。相关报告可从 http://www.gtisc.gatech.edu/icann09 获取。

5.2.10.3 此外，ICANN 工作人员、支持组织和咨询委员会还加大了与多利益主体机构组织的合作，目的是提高 ICANN 有效制定政策、促成合同履行和采取其他举措的能力，以应对 DNS 所面临和带来的安全性和灵活性挑战。

5.3 与号码资源组织 (NRO) 及地区互联网注册管理机构 (RIR) 合作

ICANN 与 NRO 及 RIR 之间的合作以三方的共识为导向，即 RIR 与 ICANN 的共同目标是从本地及全球互联网用户的利益出发，维护和提高互联网的安全性、稳定性与灵活性。ICANN 与这些组织共同参与了多个有关互联网安全性、稳定性及灵活性的活动。具体来说，ICANN 一直在与这些组织共同推动 DNS 树中反向区域的 DNSSEC 签名措施。作为 IP 地址注册管理机构，RIR 正通过实施根级公钥基础架构 (rPKI) 直接促成地址及边界网关协议路径的认证，ICANN 将在这一方面继续与其进行密切合作。

5.4 ICANN 的机构安全性及运营连续性

5.4.1 在管理 DNS 和编址系统的过程中，ICANN 通过 IANA 的工作及其执行的其他核心职能来确保自身运营的安全性、稳定性和灵活性，并以此履行机构责任，为互联网唯一标识符系统的整体安全性、稳定性和灵活性做出贡献。

5.4.2 ICANN 正致力于制定一套全面的安全计划，用以控制其在信息、人员以及物理资产方面存在的风险。2008 年秋季，ICANN 聘请了一位安全运营理事来负责实施此计划。ICANN 通过提供信息、处理敏感数据并借助信息技术 (IT) 来实施相应操作。ICANN 的《信息安全计划》以 ISO 27002 标准为基准，目前此计划的支持程序/流程正在不断改进。ICANN 的《信息安全计划》还包括向美国商务部提供 IANA 信息安全计划，并管理其计划的外部审核活动。人员安全计划旨在保护 ICANN 工作人员在 ICANN 主要工作场所中的安全，以及他们在开展 ICANN 全球活动时的安全，包括在 ICANN 会议上的安全。ICANN 已设立了一套用以控制人员安全风险的计划流程，同时也通过内部安全团队和安全顾问的支持来管理风险。此外，ICANN 也设立了一套用以控制物理设施风险的计划流程，包括其位于美国加利福尼亚州玛丽娜德尔瑞的总部设施、中心办事处的设施以及后备设施。

5.4.3 ICANN 的安全计划符合 ICANN 理事会监督的机构总体风险控制计划以及互助式机构业务连续性计划。随着 ICANN 不断发展，其全球活动及公共档案的规模日益扩大，机构的资产库也在随之扩大。ICANN 的机构安全环境面临的挑战将不断增多，为此，ICANN 将继续加大风险控制力度、提高业务连续性和安全性，为机构各项流程的有效运转奠定基础。

5.5 ICANN 支持组织和咨询委员会的活动

5.5.1 在 ICANN 通过“自下而上”的政策流程，确保互联网唯一标识符系统的安全性、稳定性和灵活性的过程中，ICANN 的广泛群体发挥着至关重要的作用。ICANN 有三个支持组织 — 通用名称支持组织 (GNSO)、国家或地区代码域名支持组织 (ccNSO) 和地址支持组织 (ASO)，这些组织负责制定相关的安全性和稳定性政策。如需了解各支持组织及其流程的详细信息，请访问 http://gnso.icann.org 、http://ccnso.icann.org/ 和 http://aso.icann.org/。这些组织提出的建议必须获得 ICANN 理事会的批准，方可通过各种合同、协议、谅解备忘录 (MoU) 和工作人员的活动付诸实施。GNSO 的主要职责范围是：制定与 gTLD 注册管理机构和注册服务商协议相关的政策（包括考虑是否应修改 gTLD Whois 政策）；研究 Fast Flux Hosting 引起的问题、域名过期问题、注册服务商之间转让域名的问题以及滥用注册政策等。

5.5.2 ICANN 目前正与各机构群体共同修改现有的 gTLD 政策制定流程 (PDP)，使其能更有效、更迅速地满足 ICANN 的政策制定需求。对于现有 PDP，预计的修改之处包括：让更多的专业技术人员、研究人员以及调查人员在早期参与流程，以更明智、更专业的方式帮助界定并应对政策难题；确立更好的评估新政策效力的方式。

5.5.3 ccNSO 负责促进 ICANN 与 ccTLD 之间的合作，包括共享与安全性、稳定性和灵活性相关的信息。

5.5.4 ASO 负责制定有关向 RIR 分配 IPv4 和 IPv6 地址段、自治系统 (AS) 号码段的政策。

5.5.5 此外，ICANN 还有四个咨询委员会 — 网络普通用户咨询委员会 (ALAC)、政府咨询委员会 (GAC)、根服务器系统咨询委员会 (RSSAC)、安全与稳定咨询委员会 (SSAC)，这些委员会负责向理事会和 ICANN 群体提出建议。如需详细了解这些委员会各自的职能、流程和活动，请访问 http://www.icann.org/en/committees/gac/。这些咨询委员会不仅相互合作，还经常与 ICANN 支持组织进行合作，其中 SSAC 与各组织之间的合作尤为活跃。咨询委员会在 ICANN 政策工作人员的支持下开展研究活动、进行审议和提出建议。

5.5.6 SSAC 负责就与互联网名称和地址分配系统的安全性和稳定性相关的事宜向 ICANN 机构群体和理事会提供建议。这些事宜包括：根名称系统正确可靠的运行；地址分配和互联网号码分配问题；gTLD 注册管理机构和注册服务商的服务（如 Whois）。SSAC 参与当前的互联网名称和地址分配服务的威胁评估和风险分析，评估哪里会存在严重的稳定性和安全性威胁，并据此向 ICANN 机构群体提供建议。要详细了解 SSAC 的活动，请访问 www.icann.org/en/committees/security。

5.5.7 除上述活动之外，各支持组织和咨询委员会目前正在开展的活动包括：在 ICANN 会议上讨论各方共同关注的安全性和稳定性问题；就安全性和稳定性问题组织研讨会、编制简报；通过每月发布的《政策更新》向群体传达政策活动信息（http://www.icann.org/en/topics/policy/）。

5.6 全球共同参与提高安全性、稳定性和灵活性

5.6.1 全球合作伙伴和活动

ICANN 与安全性、稳定性和灵活性相关的全球参与战略的核心是巩固并充分利用全球合作伙伴团队的现有工作成果。ICANN 一直积极参加世界各地各种与互联网相关的论坛，其中就包括以互联网的安全性、稳定性和灵活性为主题的讨论会。下文仅列出了 ICANN 的部分合作伙伴和活动；ICANN 还将在机会合适时积极参加其他活动。主要的全球合作伙伴包括：

- 互联网工程任务组 (IETF)/互联网架构委员会 (IAB)：领导开展相应工作，着重于开发更稳健的协议和运营方式，寻求相应技术方法来提高互联网的安全性。ICANN 与 IETF 共同制定与命名和编址相关的协议，并努力确保这些协议在互联网的核心基础架构内得到部署，以帮助提高整个互联网环境的安全性。具体来说，ICANN 将参与协议的制定工作（尤其是 DNSSEC 和 rPKI 协议的制定），为互联网提供更安全的基础。
- 互联网协会 (ISOC)：提高公众对于计算机安全问题的意识，宣传全球用户群体（尤其是发展中国家的用户群体）对互联网建立信任的必要性；与其他机构合作，提供有关如何增强互联网安全性和灵活性的技术培训。ICANN 与 ISOC 合力增强公众对于安全性、稳定性和灵活性的意识，并提高他们在这方面的能力。ICANN 计划与 ISOC 共同完善正在开展的 ISOC/ICANN 联合项目，为 TLD 运营商提供培训，包括有关如何提高安全性、抵御计算机网络攻击和破坏的培训。
- 互联网监管论坛 (IGF)：IGF 倡导各利益主体之间就网络安全性和信任问题进行沟通。此外，IGF 还关注互联网关键资源的管理问题以及网络犯罪问题。ICANN 将继续参加 IGF，包括在该论坛中

阐明自身在维护互联网唯一标识符系统的安全性、稳定性和灵活性方面的职责，并增进全球利益主体在论坛上的相互沟通。

- DNS 运营、分析和响应中心 (DNS-OARC)：ICANN 将继续以支持组织的身份积极参与 DNS-OARC 的各项活动。

5.6.2 区域合作伙伴和活动

ICANN 已通过多个合作伙伴和活动与各区域建立了紧密联系。ICANN 区域性活动的主要方面包括：

- ***区域 ccTLD 协会*** — 除与各区域的 ccTLD 协会合作开展 ACRP 计划（见下文）之外，ICANN 还将继续为这些组织主办的活动提供协助和专业技术。
- ***区域网络信息中心 （NIC）/网络运营组织 （NOG）*** — ICANN 将继续参加这些组织主办的论坛，并协调 IANA 的职能，以确保 ICANN 的活动能最大程度增强网络运行的安全性和灵活性。
- ***亚洲*** — 2008 年 5 月，ICANN 在吉隆坡与亚太地区 TLD 协会 (APTLD) 共同启动了 ccTLD 安全性和灵活性培训计划，并且在亚太地区实施该计划时不断获得大力支持。ICANN 将继续参加“互联网资源管理纲要”等区域论坛，在机会合适时提供有关 DNS 安全性和灵活性的建议和培训。
- ***欧洲*** — ICANN 将与欧洲网络和信息安全署 (ENISA) 就 DNSSEC 问题和提高 DNS 灵活性继续进行合作，这也是欧盟委员会在关键基础架构保护领域开展的更大规模工作的一部分。ICANN 将与欧洲国家顶级域名注册管理机构委员会 (CENTR) 合作开展 ccTLD 安全性和灵活性培训课程，本课程是 ICANN 在 RIPE（欧洲 IP 资源）第 58 届会议（2009 年 5 月在阿姆斯特丹举行）中启动的。ICANN 将继续与莫斯科国立信息安全学院 (IISI) 共同促成有关网络安全性的全球对话。具体来说，在德国/美国的马歇尔战略研究中心的支持下，ICANN 和 IISI 于 2008 年和 2009 年在德国 Garmisch 联合举办了多场研讨会，且双方均计划进一步开展合作。
- ***非洲和拉丁美洲*** — ICANN 将继续与 ISOC 的区域组织共同开展与网络安全有关的活动，并继续参与其他相应的论坛。在 2009 年 3 月的 ICANN 第 34 届国际公开会议召开之前，ICANN 与 LACTLD 协会联合举办了 ccTLD 安全性和灵活性培训，并计划与 LACTLD 继续开展相关培训。ICANN 还将与非洲顶级域名协会 (AfTLD) 和 ISOC 非洲分会联合提供 ccTLD 培训。这些活动是在 2009 年 4 月于坦桑尼亚阿鲁沙举行的非洲顶级域名组织 (AFTLD) 会议上发起的。

5.6.3 与政府合作

在确保互联网唯一标识符系统的安全性、稳定性和灵活性的过程中，ICANN 与全球政府进行了密切合作。ICANN 将继续向各国政府提供关于如何提高互联网唯一标识符系统的安全性、稳定性和灵活性的技术见解和运营建议。ICANN 认为这些系统必须被视为关

键的基础架构。在 ICANN 内部，政府咨询委员会 (GAC) 会定期收到有关 ICANN 在安全性、稳定性和灵活性方面所做工作的最新动态，并按照战略计划流程对这些计划提出建议。对于政府间组织，ICANN 将继续在以安全性为主题的全球讨论中积极阐明自身的职责，并说明提高唯一标识符系统的安全性和灵活性的潜在意义。ICANN 在此方面的主要活动包括：

- ***国际电信联盟 (ITU)*** — ITU 正在实施《全球网络安全议程》(GCA)，打造一个“旨在增强信息社会信心和安全性的国际合作框架”。在这一广泛框架下，ITU 的电信发展部门 (ITU-D) 已制定了一个覆盖范围较广的计划，目的是与发展中国家携手共同提高有关加强网络安全性的国民意识，并开展相关的能力培养计划。ICANN 将继续尝试与 ITU 就提高网络安全性进行合作，共同开展外展活动、提高公众意识、培养能力，并体现其在确保 DNS 安全性和灵活性方面的技术作用。
- ***经济合作与发展组织 (OECD)*** — ICANN 将继续参加有关网络安全性的论坛，如 OECD 正在开展的打击恶意软件的活动。ICANN 还将与 APEC 在这一领域进一步开展相关工作。
- ***其他国际组织和联合国区域经济委员会*** — ICANN 将继续与其他国际组织和联合国区域经济委员会进行合作，工作重点是开展旨在提高 DNS 安全性和灵活性的区域活动。这些活动的开展将以 ICANN 与各组织签署的谅解备忘录为基础。

6. ICANN 有关提高安全性、稳定性和灵活性的 2010 财年计划

ICANN 在开展有关提高安全性、稳定性和灵活性的活动以及为这些活动分配资源时，是以战略和运营计划流程为指导的。ICANN 计划对 2009－2010 运营年度做出了规划，并要求各方实施多项重要举措，包括：

- ***IANA 运营*** － 按照《ICANN 2009-2012 年战略计划》的要求为 DNSSEC 的根级执行进行支持、教育和准备，同时通过自动化流程改善根区域管理；改进与 TLD 管理机构的通信认证
- ***DNS 根服务器运营*** －不断寻求对角色和职责的相互认同，发动自发力量实施应急计划和演练
- ***gTLD 注册管理机构*** － 确保继续对新 gTLD 和 IDN 申请人进行评估，以保证运营的安全性。ICANN 将推出成熟的 gTLD 注册连续性计划并测试数据托管系统。
- ***ccTLD 注册管理机构*** － ICANN 将会增强与各方的合作，进一步完善与 ccNSO（国家或地区代码域名支持组织）和各地 TLD 协会共同制定的攻击事件及应急响应计划 (ACRP)。
- ***合同合规性*** － ICANN 将继续扩大涉及 gTLD 的合同履行活动的范围，作为实施《注册服务商委任协议》(RAA) 2009 年 3 月修正案的部分措施，对合同签约方启动审核事宜，并确定合同签约方参与恶意活动的的潜在可能，以便采取合规行动。
- ***应对域名系统恶意滥用*** － ICANN 将基于多方力量共同打击利用 DNS 实施的恶意行为，同时促进信息共享以便针对恶意行为做出有效反应。
- ***ICANN 内部安全性和连续性运营*** － ICANN 将确保其安全计划在机构的整体风险管理、危机管理和业务连续性计划中执行。其重点在于为成文计划和支持流程打下坚实的基础
- ***确保全球参与和协作*** － ICANN 将加强与互联网工程任务组 (IETF)、互联网协会 (ISOC)、地区互联网注册管理机构和网络运营商团体以及 DNS 运营、分析和响应中心 (DNS-OARC) 之间的合作关系。ICANN 还将积极参与全球性对话，以促进对整个互联网群体所面临的安全性、稳定性和灵活性等方面的挑战的理解，以及对如何通过多利益主体参与的方式来共同应对这些挑战的认识。

下文将进一步介绍各项活动。附录 A 详细说明了 2010 财年的具体目标、合作伙伴、交付成果及资源投入。

6.1 核心 DNS/编址职能

6.1.1 IANA 运营

ICANN 将继续执行 IANA 职能，同时与美国商务部、威瑞信、RIR 和 TLD 运营商展开合作，不断改进运营绩效。

6.1.1.1 与全球互联网群体协商，并与根区域管理合作伙伴、美国商务部和 VeriSign 共同实施根区域的 DNSSEC 签名流程。ICANN 将继续执行其在 2008 年 9 月提案中列出的流程。根据《ICANN 2009-2012 年战略计划》中列出的工作重点，ICANN 将于 2009 年年底做好在根区域部署 DNSSEC 的运营准备。ICANN 提议在 DNSSEC 运行过程中与 VeriSign、NTIA 和根服务器运营商进行合作，以确保 DNS 根区域分配机制的连续性不受影响。ICANN 提供了能从临时性方式过渡到永久方法的灵活解决方案，并为扮演这一角色做好了运营准备。

ICANN 还将继续开展一系列活动，推动 DNSSEC 在全球 DNS 系统中得到更广泛的实施。ICANN 将确保其各项计划（包括注册服务商之间的转让和托管计划）有助于 DNSSEC 的实施，并继续与各利益主体讨论实施 DNSSEC 的相关问题。ICANN 将继续维护 IANA 顶级域名信任锚存储库 (ITAR)，直至根区域已签名。ICANN 将继续寻求 .int 和 .arpa 区域的签名许可。ICANN 将对由 ICANN 管理的区域（包括 icann.org 和 iana.org）签名，并开展实施测试，促进参与 DNSSEC 实施的各方之间的经验交流，以此支持 DNSSEC 的实施。

6.1.1.2 其他改善 IANA 职能的具体措施包括：

- 通过自动化流程（IANA/RZM 软件）改善根区域管理；改进与 TLD 管理结构的通信认证；审核流程和操作以利于安全性和优化职能
- 通过 rPKI 或 RIR 和互联网路由群体采用的其他机制促进 IP 地址的安全分配和指定，包括继续为 IETF 安全智能数据储存库 (SIDR) 工作组提供支持
- 与技术和运营群体共同确定和分析提高 DNS 安全性、稳定性和灵活性的其他技术需求或标准，并在可行时落实这些需求或标准

6.1.2 DNS 根服务器运营

6.1.2.1 在履行协调 DNS 的总体职责的过程中，ICANN 将继续寻求与根服务器运营机构之间互相认同对方的角色和职责。作为根服务器运营机构群体的一分子，ICANN 还将继续针对有助于提高安全性、稳定性和灵活性的措施建立更可靠的协调机制。作为 L 根运营机构，ICANN 计划与其他根服务

器运营机构进行合作，发动各方自发开展旨在提高根服务器系统灵活性的计划和演练，以应对各种重大突发事件。

6.1.2.3 ICANN 计划继续改善 L 根服务器的运营。另外，ICANN 已与 DNS-OARC 签订了合作协议，共同研究各种改革（包括实施新 gTLD 和 IDN、实施 IPv6 以及可能会实施的根区域 DNSSEC 签名）对基于 L 根模型的单个根服务器运营带来的影响。除此之外，RSSAC 和 SSAC 也正在共同研究第 6.6 部分详述的各项预期改革对根服务器的安全性和稳定性的影响。

6.2 与 TLD 注册管理机构和注册服务商之间的关系

6.2.1 gTLD 注册管理机构

ICANN 将继续按照与 gTLD 注册管理机构签订的合同协调 gTLD 的运行，包括通过 RSEP 审核增设新服务的申请。ICANN 预计的审核范围包括需要 RSTEP 评估安全性、稳定性和灵活性问题的提案。ICANN 将继续鼓励各机构群体进行合作，继续举办 ICANN 区域性注册管理机构/注册服务商研讨会、参与各种群体论坛，并通过自己的网站分享信息，以此促进机构群体采用有关安全性、稳定性和灵活性的最佳实践做法。此外，ICANN 还计划与 DNS-OARC 共同设立一个门户网站，在其中分享有关安全性、稳定性和灵活性的最佳实践以及合作成果的信息，供全体注册管理机构群体使用。

6.2.2 新 gTLD

由于 ICANN 可能会实施与引入新 gTLD 相关的流程，因此安全性、稳定性和灵活性问题将成为明年公众关注的焦点。2009 年 2 月，ICANN 理事会要求 RSSAC 和 SSAC 共同研究 DNS 内部可能实施的一系列改革（包括在未来 18 个月内实施新 gTLD 和 IDN 以及可能会在根区域实施 DNSSEC 签名）对根服务器系统的整体安全性、稳定性和灵活性的潜在影响。这项研究的报告预计将在 2009 年 9 月公布。ICANN 还将制定有关申请人评估的规定，以确保申请人实施的运营活动具有技术安全性且符合 Whois 规定，确保申请人能提供妥善的应急计划，同时也确保注册人得到保护。ICANN 将继续完善 gTLD 注册管理机构的业务连续性计划和演练计划，并对数据托管系统进行现场测试。此外，ICANN 还将确保 TLD 自动申请系统能安全地建立和运行。

6.2.3 IDN

与 gTLD 一样，ICANN 也将努力促进 IDN TLD（ccTLD 和 gTLD）实施，确保这些以本地语言字符组成的新域名具有安全性、稳定性和灵活性。制定互联网协议是 IETF 的常规职责，ICANN 将继续与其进行合作，确保协议得以定案，并确保所批准 IDN 协议的安全性和稳定性。如果 IETF 制定的协议未获得完全批准，ICANN 可能

会借鉴技术群体的建议进一步设立有关 IDN TLD 的具体要求，以确保当协议定案时，这些要求仍会长期有效。ICANN 将继续为注册管理机构与供应商的合作提供便利，以确保 IDN 表能最大程度地防止字符串冲突和混淆，并减少恶意滥用系统的机会。对于希望成为 IDN TLD 运营商的注册管理机构以及需要现场协助和专业技术的注册管理机构，ICANN 将为其提供针对 IDN 的支持。

6.2.4 ccTLD

ICANN 将继续与 ccTLD 运营商进行合作，共同提高 ccTLD 的安全性、稳定性和灵活性。ICANN 明年的工作重点是完善其与 ccNSO 和各地 TLD 协会联合制定的攻击事件及应急响应计划 (ACRP) 研讨会计划。ACRP 计划的主要内容是：通过预先计划和迅速的响应能力应对各种破坏性威胁和风险，以此提高安全性和灵活性。而且，该计划将在明年扩大技术培训范围，增加有关如何提高安全性和灵活性以应对不断演化的威胁的技术培训，以及如何帮助相关方为 ccTLD 安全和应急计划制定演练和评估计划的技术培训。明年，ICANN 将培养工作人员以非英语语言提供 ACRP 课程的能力，并与卡耐基-梅隆大学的软件工程协会进行合作开展一项志愿活动，利用该协会的灵活性工程框架 (REF) 评估提高 TLD 安全性、稳定性和灵活性的工作的完善性。

6.2.5 注册服务商

ICANN 将继续制定相关政策，通过改进 RAA 来提高注册服务商委任要求和数据托管要求。除为这些工作提供支持外，ICANN 工作人员还将继续在现有的合同和政策框架内制定相关程序和流程，以保护注册人的利益，最终达到提高 DNS 安全性、稳定性和灵活性的目的。具体来说，ICANN 工作人员目前正在加强对委任申请流程的控制，设立更严格的 RAA 合格要求和资格取消规则，并制定一套使注册服务商以负责任的态度退出注册服务商市场的程序。在此之前，ICANN 已开始制定数据托管程序和注册服务商终止委任程序，这些工作也将巩固 ICANN 目前以及将来开展的合规执行工作，使得当注册服务商的行为威胁到 DNS 的安全性和稳定性时，ICANN 能终止对该服务商的委任。ICANN 将继续开展有利于分享行业最佳实践的外展活动，以此构建一个强大的注册服务商群体；同时也将着手开辟新的沟通渠道，及时帮助注册服务商报告严重的安全威胁并采取应对措施。

6.2.6 合同合规性

6.2.6.1 ICANN 将继续扩大合同执行活动的范围，包括增加合同合规团队的工作人员。新的主要活动领域包括，在实施《注册服务商委任协议》(RAA) 2009 年 3 月修正案的过程中启动对合同签约方的审查活动。此外，合同合规团队的工作人员将在 2009 年与 ICANN 安全团队合作，确定可能参与恶意行为的合同签约方。如果合同签约方参与了恶意行为，将对其采取相应的合同强制措施。在所有其他情况下，为妥善处理这一类问题，ICANN 将通知执法部门和其他相应机构。

6.2.6.2 合同合规部门目前正在开展相关研究，评估 gTLD 系统中 Whois 联系信息的准确性，同时评估注册人可在多大程度上利用隐私和代理服务掩盖其身份。为促进签约方遵守合同并加强公众信心，合同合规部门正在开发一套公开确定投诉方的系统。目前这套系统正处于开发的初步阶段，合同合规部门将在实施系统之前咨询注册服务商和注册管理机构群体。

6.2.7 共同应对恶意滥用域名系统的行为

自 2008 年底开始，ICANN 工作人员与各合作伙伴共同应对了多起有关域名系统的事件，如 2008 年底/2009 年初分别针对 Szirbi 僵尸网络和 Conficker 蠕虫病毒开展的活动，ICANN 将进一步巩固这些合作成果。此外，ICANN 还计划与 DNS 注册管理机构和注册服务商、安全研究群体以及软件供应商和防病毒软件供应商展开这类合作。具体来说，ICANN 将与注册管理机构和注册服务商群体协同来改进合作方式，共同打击利用 DNS 进行传播和控制来散布恶意软件、蠕虫病毒以及僵尸网络。ICANN 将开展相关工作，澄清有关注册管理机构和注册服务商活动的沟通和验证程序，并确立自身与安全研究人员、技术供应商以及执法部门共享信息的方式。ICANN 将公布其开展共同应对活动的程序，以征询公众意见。这些程序将提交理事会批准。这些方式将确保 ICANN 能对寻求 ICANN 参与和合作的全球各利益主体及时做出响应。

6.2. 8 实现 DNS 整体安全性

ICANN 工作人员将协助主要合作伙伴降低 DNS 运营商和用户面临的运营风险，以此巩固 2009 年 2 月举行的有关“DNS 安全性、稳定性和灵活性”研讨会的成果。相应的计划包括：每年召开一次有关 DNS 整体风险的研讨会；增加合作机会，持续关注在确保发展中国家 DNS 安全性和稳定性方面所面临的挑战。ICANN 还计划与 DNS-OARC 及应急响应与安全小组论坛 (FIRST) 开展合作，重点研究如何对 DNS 群体中的重大意外事故和事件做出有效反应。此外，ICANN 工作人员还将继续跟踪有关建立对象命名系统 (ONS) 的计划的进展情况，并跟踪这些计划对 DNS 可能造成的影响，及早发现有关安全性、稳定性和灵活性的潜在问题。

6.3 与 NRO 和 RIR 合作

ICANN 计划与 NRO 和 RIR 继续合作，并参加与三方共同关注的有关安全性、稳定性和灵活性问题的活动。ICANN 工作人员将与 RIR 讨论可以改进的合作活动，以确保 DNS 的安全性、稳定性和灵活性。讨论内容包括：理解 RIR 关于打击滥用传统 IPv4 地址空间的计划设想；是否需要通过全球政策来解决已确定的问题。

6.4 ICANN 的机构安全性及运营连续性

6.4.1 ICANN 工作人员将确保其安全计划在机构的总体风险管理、危机管理和业务连续性计划中得以执行。其重点在于为成文计划和支持流程打下坚实的基础。2010 年中期进行的改善 ICANN 风险管理和连续性工作方式的具体举措包括：正式制定 ICANN 业务连续性/危机管理计划；与其他活动一同开展 ICANN 内部演练活动，包括 gTLD 连续性演练活动、会议筹备等。作为执行 IT 连续性计划的组成部分，ICANN 将加大对替代网站的使用力度。其中一个工作重点是建立一个 IT 安全中心和后备设施，为 ICANN 连续性计划提供支持。ICANN 计划在 2009 年中期之前开展一次机构安全性风险评估。

6.4.2 明年，ICANN 工作人员将确保建立一套覆盖其运营活动的全面的信息、人员和安全流程。和风险管理和连续性计划一样，其重点也是为相应的成文计划和支持流程打下坚实的基础。2010 年中期进行的提高 ICANN 安全水平的具体举措包括：改善逻辑和物理访问控制；提高工作人员的安全意识，举行应急响应培训；制定差旅人员安全计划、会议安全和应急响应计划。ICANN 将不断加强与各机构群体的合作，开发和部署外展 IT 工具，同时确保相应的安全控制措施就位。

6.4.3 ICANN 工作人员计划与卡耐基-梅隆大学的软件工程协会 (SEI) 进行合作，利用 SEI 的灵活性工程框架 (REF) 确保安全性、连续性和风险管理计划融入了最佳实践，同时利用该框架来衡量就完善性而不断进行的改进工作。ICANN 计划在 2009 年底之前对照 REF 方式评估其基本流程的完善性。此外，ICANN 还计划在 2010 年上半年对其安全性和连续性计划开展一次外部审查和审核。

6.5 ICANN 支持组织和咨询委员会

6.5.1 SSAC 计划将下一步的工作重点放在部署 DNSSEC、保护域名注册、减少滥用域名以及维护地址系统稳定等方面。

6.5.2 2009 年 1 月，GNSO 委员会发布了一份*关于 Fast Flux hosting 的初步报告*，向公众征求意见，以便委员会采取进一步行动。同时，委员会也在考虑开展多项关于 Whois 的研究。GNSO 委员会计划制定六项相关政策，并设立了一个工作组专门负责其中第二项政策的制定工作，这些政策旨在解决注册商之间转让域名的各方面问题。GNSO 已设立了一个滥用注册工作组，同时也在考虑针对过期域名恢复问题采取相应举措。为了将对这些问题感兴趣的各利益主体召集起来，ICANN 在其第 34 届国际公开会议（2009 年 3 月于墨西哥城召开）上举办了一场电子犯罪扩展研讨会，并针对滥用注册问题举办了一场专项研讨会。

6.6 全球合作

6.6.1 拓展现有合作关系

ICANN 与安全性、稳定性和灵活性相关的全球参与战略的核心是巩固并充分利用全球合作伙伴团队的现有工作成果，同时进一步拓展稳固的合作关系。ICANN 计划在 2010 财年与这些合作伙伴开展以下活动：

- ***互联网协会 (ISOC)*** — ICANN 计划与 ISOC 共同完善正在开展的 ISOC/ICANN 联合项目，为 TLD 运营商提供培训，并增加有关如何提高安全性、抵御计算机网络攻击和破坏的技术培训的计划。
- ***DNS-OARC*** — ICANN 将资助 DNS-OARC 创立一个门户网站，该门户网站用于 TLD 群体内部交流信息，分享关于安全性、稳定性和灵活性的最佳实践。ICANN 还将与其他组织合作提供教育和培训计划，让公众更好地了解唯一标识符系统的功能、控制这些系统的风险所面临的挑战以及 ICANN 的职责。
- ***亚洲*** — ICANN 计划与马来西亚政府支持的新国际计算机网络安全中心建立合作关系，重点是探讨 ICANN 如何协助全球合作伙伴共同打击威胁互联网唯一标识符系统的计算机网络恶意行为。

6.6.2 商业企业

2009 年 2 月，ICANN 举办了旨在了解企业对 DNS 的期望以及与 DNS 有关的风险的“DNS 安全性、稳定性和灵活性”座谈会。明年，ICANN 将以此次座谈会的成果为基础，广泛采纳各类企业的意见，继续增强 DNS 的安全性、稳定性和灵活性，这也是 ICANN CEO 外展计划的一部分。

6.6.3 参与全球计算机网络安全对话

ICANN 将积极参与这些对话，以确保深入全面地了解自身的职责和作用。ICANN 计划在明年与多家机构进行此类对话，包括：

- ***国际战略研究中心 (CSIS)*** — ICANN 计划在 2009 到 2010 年期间与该机构共同筹办一系列研讨会，讨论的议题包括多利益主体组织在全球计算机网络安全领域中的角色。ICANN 还将与 CSIS 在美国之外的合作机构开展合作。
- ***大西洋理事会*** — 在日益猖獗的计算机网络攻击和破坏行为面前，较小国家和组织的防线变得越来越脆弱，有鉴于此，ICANN 计划携手大西洋理事会开展一系列活动，以期解决这一问题。ICANN 的职责主要是确保 DNS 在遭遇此类攻击和破坏时的灵活性。

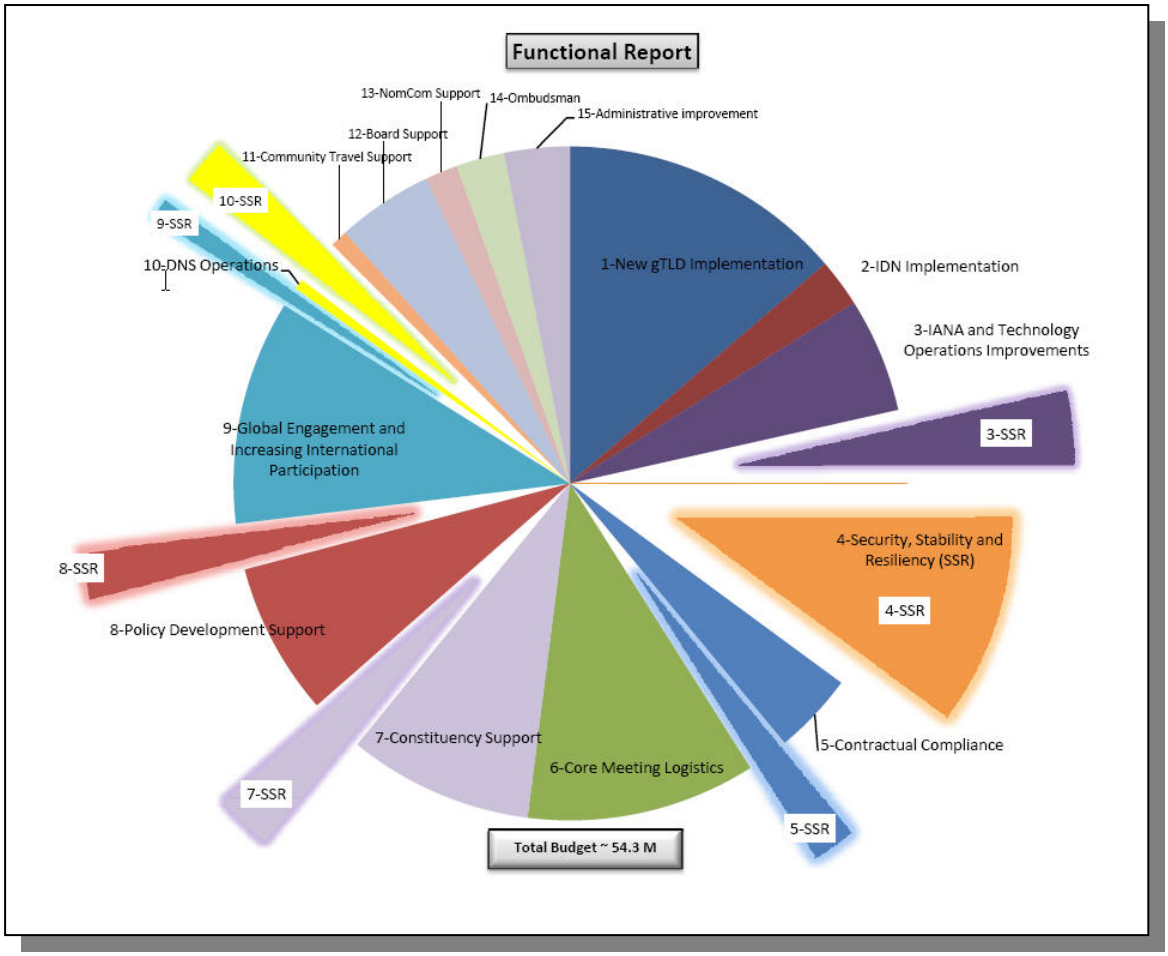
ICANN 将积极寻求与其他智囊团和学术机构合作的机会，共同引导公众如何确定与安全性、稳定性和灵活性相关的挑战。

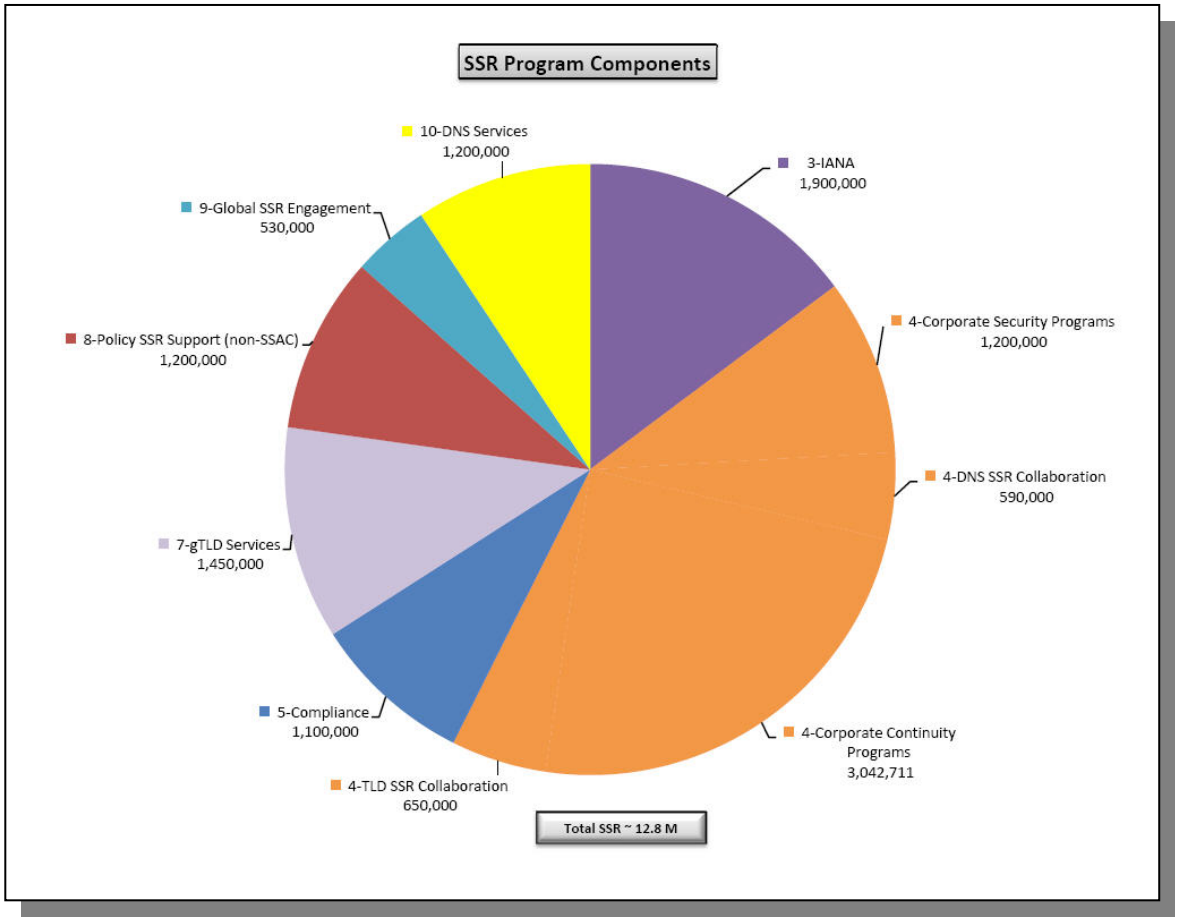
7. 总结

ICANN 深知：要赢得公众的信任，关键在于其计划和活动必须有利于将唯一标识符系统打造成更安全、更稳定、更灵活的互联网环境核心。随着挑战的不断升级，ICANN 这方面的工作力度也在不断加大。同时，ICANN 也认识到自身的作用和资源是有限的，因此在制定这方面的战略规划时高度重视与其他机构的合作。互联网的蓬勃发展来自其全球性环境的地位和对创新的促进作用，同时也有赖于多利益主体之间的相互协调。ICANN 也将借鉴这一成功经验来增强唯一标识符系统的安全性、稳定性和灵活性。

自成立以来，ICANN 已开展了各种增强互联网安全性、稳定性和灵活性的计划和活动，包括：改善核心 DNS/编址职能；与 TLD 注册机构和注册商群体合作；与 NRO 和 RIR 合作；制定机构安全性和连续性计划；通过支持组织和咨询委员会开展活动；参与有关互联网安全性、稳定性和灵活性的全球性和地区性活动。本计划第一版的宗旨是为制定 ICANN 的职责奠定基础，为 ICANN 安排与安全性、稳定性和灵活性相关的工作提供框架。作为 ICANN 战略和运营计划流程的一部分，ICANN 将会不断更新本计划，以确保自身的工作始终符合其核心使命，确保将其有限的资源集中用于履行最重要的责任，以期发挥最大的作用。

附录 A


Functional Report
13-NomCom Support
14-Ombudsman
15-Administrative improvement
12-Board Support
11-Community Travel Support
10-SSR
9-SSR
10-DNS Operations
1-New gTLD Implementation
2-IDN Implementation
3-IANA and Technology Operations Improvements
3-SSR
9-Global Engagement and Increasing International Participation
4-Security, Stability and Resiliency (SSR)
4-SSR
8-SSR
8-Policy Development Support
7-Constituency Support
6-Core Meeting Logistics
5-Contractual Compliance
7-SSR
5-SSR
Total Budget ~ 54.3 M


SSR Program Components
10-DNS Services
1,200,000
3-IANA
1,900,000
9-Global SSR Engagement
530,000
4-Corporate Security Programs
1,200,000
8-Policy SSR Support (non-SSAC)
1,200,000
4-DNS SSR Collaboration
590,000
7-gTLD Services
1,450,000
5-Compliance
1,100,000
4-Corporate Continuity
Programs
3,042,711
4-TLD SSR Collaboration
650,000
Total SSR ~ 12.8 M

Overview of Major Components of ICANN Security, Stability, Resiliency (SSR) Program

- IANA - $1.9 M
- DNS Services - $1.2 M
- DNS SSR Collaboration - $590 K
- gTLD Services - $1.45 M
- Compliance - $1.1 M
- TLD SSR Collaboration - $650K

OVERALL SSR – $12.8 M

- Global SSR Engagement - $530K
- Corporate Security Programs - $1.2 M
- Corporate Continuity Programs - $3.0 M
- Policy SSR Support (incl SSAC) - $1.2M

IANA Security, Stability and Resiliency (IANA)

Objectives	Deliverables (milestones)
- Automation of key elements in root zone change process - DNSSec operational readiness - Test rPKI implementation - Business continuity	- Implementation of automated RZM (date depends DOC approval; plan to have ready prior to implementation of new gTLDs) - Implement DNSSec signing of .ARPA (date depends on coordination with IAB and DOC) - Coordination with rPKI testers (currently underway) - IANA Continuity & Disaster Recovery Plan (approved by August 2009)
Key Stakeholders	**Resources**
- IANA, Security, IT - DOC/USG; Verisign - SSAC; RSSAC - IETF; DNS operator community, RIR communities; NRO	- Staffing – 6.5 FTE (including 2.5 FTE for related IT and other staff support) - Financial – $1.9M to support FTEs; staff support/travel; professional services; application development

ICANN DNS Services (IT Services)

Objectives

- Prepare for DNSSEC zone signing for ICANN zones, ARPA-related zones and the root
- Implement Trust Anchor Repository (TAR)
- Secure, resilient L-root operation

Deliverables (milestones)

- Trust Anchor Repository in full production: June 09
- L-root improvement (new design deployed at LA and Miami, 3rd node deployed at Prague): June 09
- Production infrastructure in place for signing root zone: Oct 09
- DNSSec signed ICANN zones: Oct 09

Key Stakeholders

- ICANN IT Services Team
- ICANN IANA staff, DoC, VeriSign
- ICANN Security & Resiliency Team

Resources (FY 10)

Human – 7.0 FTE (including related IT and other staff support)

Financial – $1.2M to support FTEs; planned capital investments for back-up services; DNSSec, L-root, improvements; backup facilities; professional services and travel

ICANN gTLD Registry/Registrar Services (Services)

Objectives

- Ensure implementation new gTLD/IDNs addresses SSR issues
- Continue maturing data escrow process & gTLD continuity procedures
- Conduct RSEP/RSTEP processes on registry services proposals

Deliverables

- Enhanced gTLD implementation process from SSR perspective
  - SSAC/RSSAC study complete (Fall 09)
  - Improved applicant guidebook (Aug 09)
- Conduct data escrow test (Aug-Sep 09 or Jan 10)
- Community failover exercise (Jan 10)
- RSEP/RSTEP studies as required

Key Stakeholders

- Registries/Registrars
- ICANN Services staff
- ICANN Security & Continuity staff
- GNSO/SSAC

Resources (FY 10)

Human – 2.75 FTE

Financial – $1.45M includes portion of evaluation staff/support for new gTLD/IDN activities to include TAS security; dedicated RSEP/RSTEP funds; support for testing/contingency exercise; staff travel/support

Contractual Compliance (Services)

Objectives	Deliverables

- Improved ICANN compliance process
- Improved compliant and WDPRS system
- Improved WHOIS data accuracy
	- Conduct audits as part of revised RAA implementation (50-100 by summer 2010)
	- Reporting improvements to WDPRS (by June 2010)
	- Conduct WHOIS related studies to further understanding of systems
	  - Proxy usage (Oct 2009)
	  - Data accuracy (Dec 2009)

Key Stakeholders - gTLD registry/registrars - ICANN Compliance staff - ICANN Security/Continuity staff	**Resources (FY 10)** Human – 3 FTE Financial – $1.1M support for FTEs, staff/travel support; professional services to conduct studies and support systems improvements

TLD Security, Stability & Resiliency Collaboration

(Security)

Objectives	Deliverables (milestones)
- Mature Attack & Contingency Response Program - Establish joint ISOC/ICANN tech training program - Establish TLD exercise planning workshops - Establish program metrics	- Conduct ACRP training sessions (5 in 2009); automate planning tool by Aug 09) - Joint technical training with ISOC plan (approve summer 09); first full program conducted fall 2009; two more by 2009) - Conduct exercise planning workshops (initial implementation Oct 2009) - Prototype metrics based on Resiliency Engineering Framework (fall 2009)
Key Stakeholders - ccTLD operators - ccNSO, regional TLD operators - ISOC/NSRC - ICANN staff	**Resources (FY 10)** Human – 1 FTE Financial – $650K for FTE, staff/travel to support; professional services for developing and conducting training programs

DNS Security, Stability & Resiliency Collaboration

(Security)

Objectives	Deliverables (milestones)
- Establish collaborative response mechanisms to DNS abuse - Share key SSR practices - Conduct community-based DNS risks & collaboration symposium - Enhance root server SSR collaboration	- Collaboration construct and on-going responses w/ partners (construct in place summer 2009) - Info Sharing Portal (Dec 09) - Conduct & report on symposium (Feb & Mar 2010) - Co-sponsor joint root community communications exercise (Fall 2009)
Key Stakeholders	**Resources (FY 10)**
- ISOC, DNS-OARC, FIRST - Root Server community - Broader DNS ops community - ICANN staff - RSSAC/SSAC	Human – 1.25 FTE Financial – $590K for FTE, professional services for portal and collaboration support, travel to support activities

Corporate Security Program (Security, IT, others across staff)

Objectives	Deliverables
- Improve and implement IT/Facilities/ Personnel Security Programs - Establish Formal Plans - Institute Security Training - Implement Traveler and Meetings Security & Contingency Plans	- Conduct Security Training Programs (embedded part of ICANN on-boarding by Sep 2009) - Improved IT & Physical Access Control Systems implemented (improved IT authentication on key systems – Fall 09) - Exercise Traveler and Meetings Security (one drill per trimester)
Key Stakeholders	**Resources**
- ICANN Security & Resiliency Team - ICANN IT/IANA/DNS Ops - ICANN Human Resources - ICANN Global Meetings Team - Other ICANN Staff	Human – 2 FTEs (includes IT support for security) Financial – $1.1 M including FTEs, physical & IT access controls, professional services for conducting training and audits

Corporate Continuity Program (Security, IT, others across staff)

Objectives	Deliverables

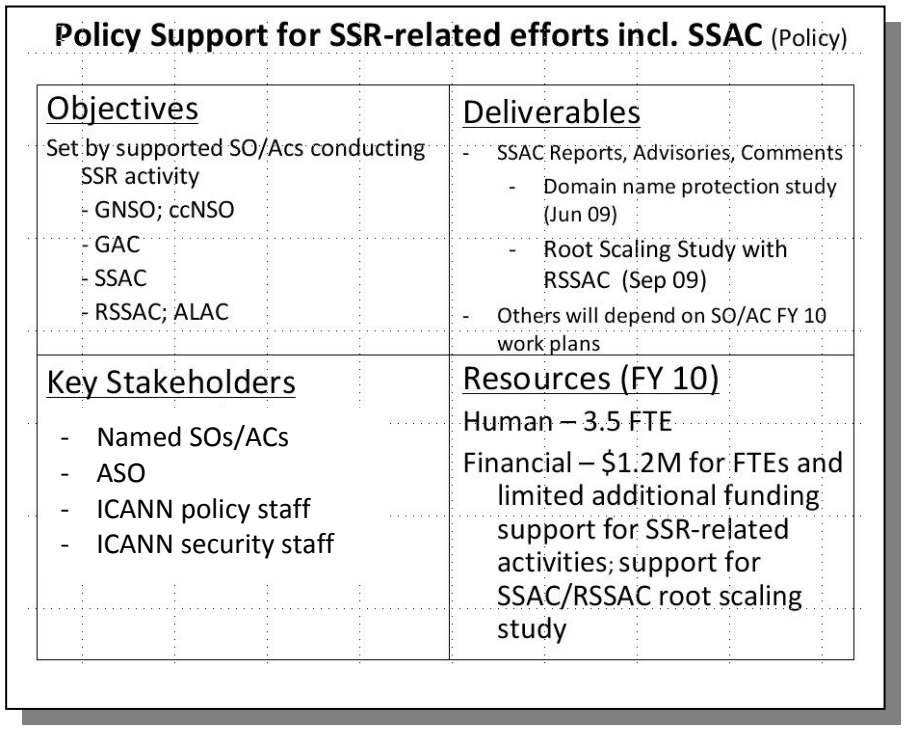
- Improve Business Continuity program
  - Establish formal plan
  - Establish secure data center
  - Establish formal drill/exercise programs
	- Initial ICANN Business Continuity plan (Oct 09)
	  - Improved Crisis Management plan (Aug 09)
	- Establish Secure IT Data Center (Sep 09)
	- Exercise Business Continuity/Crisis Management (Spring 10)

Key Stakeholders - ICANN Security & Resiliency Team - ICANN IT/IANA/DNS Ops - ICANN Human Resources - ICANN Global Meetings Team - ICANN Staff	**Resources** Human – 5 FTEs (includes planning and IT for data center) Financial – $3.0M including FTEs, capital support for data center, professional services for conducting training and audits

Global Security, Stability and Security Engagement

(Global Partnerships & Security)

Objectives	Deliverables
- Sustain partnerships with key organizations (ISOC; IISI; IMPACT; EC/ENISA; CSIS; Atlantic Council) - Continue participation in IGO sponsored cyber security dialogues OECD, IGF, others) - Collaborate with others on global cyber security response	- Conduct joint activities with partner organizations (One per trimester) - Engagement in forums across all major regions (On-going) - Engage with Forum of Incident Response and Security Teams regarding ICANN role in response (initial findings Jan 2010)
Key Stakeholders - Global/international organizations - ISOC; IETF; ITU; IGF - Cyber security forums - Governments/Commercial Stakeholders - ICANN Global Partnerships Team & Security Staff	**Resources (FY 10)** Human – 1.5 FTE Financial – $530K for FTEs; staff/travel support; support to ICANN-led or supported forums; professional services support for metrics development


Policy Support for SSR-related efforts incl. SSAC (Policy)
Objectives
Set by supported SO/Acs conducting SSR activity
- GNSO; ccNSO
- GAC
- SSAC
- RSSAC; ALAC
Deliverables
- SSAC Reports, Advisories, Comments
- Domain name protection study (Jun 09)
- Root Scaling Study with RSSAC (Sep 09)
- Others will depend on SO/AC FY 10 work plans
Key Stakeholders
- Named SOs/ACs
- ASO
- ICANN policy staff
- ICANN security staff
Resources (FY 10)
Human – 3.5 FTE
Financial – $1.2M for FTEs and limited additional funding support for SSR-related activities; support for SSAC/RSSAC root scaling study

附录 B — SSR 计划中的术语和缩略词

ACRP — 攻击事件及应急响应计划

延长宽限期 — 注册 ICANN 监管的二级域名开始阶段的五天选择期。域名注册人可在这五天内选择取消注册，此时域名注册管理机构必须全额退还注册费。

APWG — 反网络钓鱼工作组

ASN — 自治系统号码：在互联网内部，自治系统 (AS) 是一组相连的 IP 路由前缀，代表了接入互联网的定义明确的通用路由策略。互联网服务提供商 (ISP) 必须拥有一个已在 IANA 正式注册的自治系统号码 (ASN)。

ccNSO — ICANN 的国家或地区代码域名支持组织，负责在 ICANN 机构内部就限定范围内的全球国家或地区代码顶级域名问题制定相关政策。

ccTLD — 国家或地区顶级域名

CENTR — 欧洲国家顶级域名注册管理机构委员会，是由欧洲各地的互联网国家或地区代码顶级域名（如英国的 .uk 和西班牙的 .es）注册管理机构组成的协会。运营国家或地区代码顶级域名注册管理机构的组织、机构实体或个人都可以成为正式会员。

CSIS — 国际战略研究中心，为政府、国际机构、私营企业和民间协会的决策人提供战略远见和政策解决方案。

FIRST — 应急响应与安全小组论坛

gTLD — 通用顶级域名

IANA — 互联网号码分配当局

IDN — 国际化域名

IETF — 互联网工程任务组

IP — 互联网协议，规定了数据包格式和编址方案。大多数网络将 IP 与一个名为传输控制协议 (TCP) 的更高级别协议相结合，该协议在目的地与来源之间建立虚拟连接。IP 本身就像是一个邮政系统。 它允许您注明数据包的地址并使用该系统进行发送，但您的数据包与接受者之间并无直接联系。TCP/IP 在两台主机之间建立起连接，因而可以互相发送信息。

IPv4 — 第 4 版互联网协议，是互联网协议 (IP) 发展中的第四个版本，也是首个被广泛部署的协议版本。和 IPv6 一样，它也是互联网的基于标准的网络方式的核心，并且至今仍是部署最为广泛的互联网层协议。

IPv6 — 第 6 版互联网协议，是分组交换网络和互联网的下一代互联网层协议。1998 年 12 月，互联网工程任务组 (IETF) 发布了标准通道说明书 (RFC 2460)，在其中指定 IPv6 为第 4 版 IP 的下一版本。

ISOC — 互联网协会

IT — 信息技术

僵尸网络 — 入侵者通常先欺骗普通用户在计算机上打开附件，看似未做任何异常操作，实际上已在用户的计算机上安装了供日后攻击之用的隐藏软件，以此建立僵尸网络。此时被入侵的计算机（或称“僵尸”）连成了网络，入侵者能对它们任意控制，最常见的便是进行恶意攻击。

缓存投毒 — 利用 DNS 软件的缺陷使其接受错误信息，使服务器存储虚假信息，从而将之后所有的服务器请求发送至虚假验证的新域名。

拒绝服务 (DoS) 攻击 — 通过恶意代码发送大量信息，强迫目标系统关闭，从而无法向合法用户提供服务。

分布式拒绝服务 (DDoS) 攻击 — 一种类型的拒绝服务攻击，攻击者利用安装在多个系统中的恶意代码对单一目标实施攻击。这种方式比仅用单一攻击机器对目标造成的破坏更大。在互联网中，分布式拒绝服务攻击是利用大量被入侵的系统攻击单一目标，从而造成目标系统无法向用户提供服务。大量涌入的信息最终迫使目标系统关闭，从而无法向合法用户提供服务。通过大量开放递归式服务器实施的 DDoS 攻击最具破坏力：分布式攻击增加了流量，分散了对攻击来源的注意力。这种攻击对于被滥用的开放递归式服务器的影响一般较小，但对目标却有很大影响。放大系数估计约为 1:73。基于这种方式的攻击速度已超过 7 千兆 / 秒。

DNS — 域名系统，将域名（字母）转化为 IP 地址（数字）。由字母构成的域名更易记。但是，互联网是以数字 IP 地址（如 198.123.456.0）为基础的。使用域名（如 www.examplir.gratis.com）时，DNS 服务将字母名称转化为相应的数字 IP 地址。

DNSSEC — 域名系统安全扩展，提供了一种通过软件来验证域名系统 (DNS) 数据在互联网传输过程中未被更改的方式。这是通过将公/私签名密钥组融入 DNS 层级结构，形成一条源于根区域的信任链来实现的。重要的一点是，DNSSEC 不是一种加密形式。它能向后兼容现有的 DNS，保留记录的未加密状态。DNSSEC 通过使用能证明自身真实性的数字签名来确保记录的完整性。

DNSSEC 的核心是信任链概念。ICANN 有关使用 DNSSEC 对根区域文件进行签名的提案（2008 年 10 月）以这一概念和相关安全建议为基础，提出以下建议：负责修改、添加和删除根区域文件并确认这些修改是否有效的机构应创建相应的根区域更新文件，并对其进行数字签名；然后将签名后的文件传送给其他机构（目前为 VeriSign 公司）进行分发。也就是说，在最终产品分发之前，负责

构建信任基础（与顶级域名运营商共同验证根区域的修改之处）的组织还应证明该产品的有效性。

抢先注册域名 — 一些域名注册服务商利用内幕消息提前注册某些域名，目的是将其高价卖给那些使用该域名理论上必然会受益的注册人，目前这种行为尚存在争议。

域名体验 — 域名注册人利用注册 ICANN 监管的二级域名开始阶段的五天延长宽限期来测试域名的市场反应。在这段时间内，注册人将根据该域名网站上的广告收入潜力，进行成本收益分析。

域名体验不应与**域名重复注册**相混淆，后者指的是在五天延长宽限期内删除域名并立即重新注册以便再次获得五天延长宽限期的行为。这种方法通过无数次的重复注册，最终实现了免费域名注册。

Double flux — ICANN 十分关注的一个问题，是 fast flux 的一个变种，攻击者不仅会更改指向非法网站的地址，还会更改其在网络钓鱼电子邮件中嵌入的“简单易用”域名的 DNS 域名服务器的地址。这两种情况下的更改都非常迅速，只需大约 3 分钟的时间，调查人员几乎没有时间做出反应。ICANN 的 SSAC 正与品牌保护人员、执法部门和注册管理机构及注册服务商密切合作，共同寻找对策，特别是能使 DNS 避开 fast flux 程式的方案。

Fast flux — 网络钓鱼者、身份窃贼及其他电子罪犯采用的一种逃避技术，用于扰乱应急响应工作组和执法部门追踪和记录非法网站的工作。Fast flux 技术与三张牌赌博游戏极为类似，“庄家”将三张折叠过的牌放在桌上，并引诱受害人对其能否找到“红桃 Q”下赌注（英国人将此骗局称为“寻找皇后”）。庄家以极快的速度移动三张牌，同时通过闲聊、说俏皮话和熟练的手法分散受害人的注意力。然而，Fast flux 是一种高赌注骗局，并已成为一种非常棘手而又无处不在的攻击手段。在 fast flux hosting 中，“庄家”会迅速更改指向非法网站的地址。

Malware（恶意软件） — 英文单词“malicious”（恶意的）和“software”（软件）的合称，常用于统称计算机病毒、蠕虫病毒、木马、rootkit、间谍软件、广告软件、犯罪软件及其他经过或未经用户许可而在计算机上安装的多余软件。判断恶意软件的根据是创造者的可知意图，而非软件的特定功能。

NOC — 网络运营中心，是管理、监控和监管普通大型网络的物理地点。NOC 还让从该物理地点以外接入网络的用户能够访问网络。

NOG — 网络运营组织

NRO — 号码资源组织

补丁 — 用于修复软件缺陷的程序，通常会自动安装，以减轻终端用户的工作量，提高易用性。

网络钓鱼 — 网络诈骗的一种形式，通过创建与合法组织网站类似的网站，然后将电子邮件链接至该欺诈性网站，以获取个人信

息，如信用卡号、社会保险号码、用户名和密码等，达到经济或政治利益。

RAA — 注册服务商委任协议

注册管理机构 — 对顶级互联网域名注册进行管理的机构

注册服务商 — 被授权注册互联网域名的公司

RIR — 地区互联网注册管理机构

rPKI — 资源公共密钥基础架构

RSEP — 注册管理机构服务评估流程

RSTEP — 注册管理机构服务技术评估小组

垃圾邮件 — 未征得同意而发送的电子邮件。垃圾邮件通常被视为代价高昂的骚扰行为，而现在经常含有恶意软件。恶意软件是一种蓄意破坏软件（如病毒、蠕虫病毒、木马和间谍软件），用于感染电脑和系统、窃取重要信息、删除应用程序、驱动程序和文件，或将计算机转变为外部人员或攻击者的操控对象。

欺诈 — 某人或某个程序通过篡改数据伪装成他人或其他程序进行攻击：而正在尝试连接合法系统或程序的个人系统将信任这些篡改数据的有效性。

TLD — 顶级域名

木马 — 恶意软件的一种，表面看来执行的是所需的功能，实际执行的却是隐秘的恶意功能，让木马操控者在未经授权的情况下访问主机，将其文件保存到不知情用户的计算机上，甚至能观看用户的屏幕并控制其计算机。

病毒 — 在用户不知情的情况下载入计算机并运行恶意软件的一种程序或一串代码。即使是很简单的病毒也能进行自我复制，能迅速占用被感染计算机系统上的所有可用内存，因而破坏性更强。

蠕虫病毒 — 蠕虫病毒在设计上与病毒类似，被认为是病毒的变种，但由于其能在网络间自我传输，因此危险性更高。蠕虫病毒在电脑之间传播，但与病毒相比，它还能在没有任何人为操作（有意或无意）的情况下传播。蠕虫病毒利用了文件或信息在计算机系统上的传输功能，因而能进行独立传播。例如，蠕虫病毒能利用不知情用户的电子邮件地址簿发送自身的拷贝：然后它将在新感染的计算机上进行复制，并通过被入侵系统的电子邮件地址簿再次传播，如此反复进行，直至消耗大量的内存和带宽，导致整个网络中断。