CNCERT 网络安全应急服务支撑单位
申报指南

一、 指导思想

以习近平新时代中国特色社会主义思想特别是习近平总书记关于网络强国的重要思想为指导，按中央网信办有关工作要求，全面贯彻落实《网络安全法》，根据《国家网络空间安全战略》、《国家网络安全事件应急预案》等文件要求，加强网络安全技术支撑体系建设。

二、 工作目的

面向国家网络安全保障需要，按照开放、合作、自愿、共享的发展理念，坚持公平公正、开放竞争，面向全国企事业单位组织开展 CNCERT 网络安全应急服务支撑单位（以下简称“支撑单位”）遴选，凝聚全国技术力量共同维护国家网络安全。

三、 合作意义

随着我国互联网产业和信息化进程加速发展，新技术新应用大规模发展，网络安全威胁和风险融合叠加、快速演变，对网络空间安全治理带来挑战。CNCERT 作为国家级应急中心，按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展互联网网络安全事件的预防、发现、预警和协调处置等工作，运行和管理国家信息安全漏洞共享平台

（CNVD），维护公共互联网安全，保障关键信息基础设施的安全运行。

为发掘网络安全领域优秀技术力量，推动完善我国互联网网络安全应急体系，CNCERT 于 2004 年启动“CNCERT 网络安全应急服务支撑单位”遴选工作，通过组织网络安全企业、科研机构、社会组织，协调骨干网络运营单位、域名服务机构和其它应急组织等，协同国家有关部门共同应对处理各类互联网重大网络安全事件，维护国家网络安全。通过开展这项工作，**一是**拓宽掌握互联网宏观网络安全状况和网络安全事件信息的渠道，增强对互联网上重大突发网络安全事件的应对能力，提高国家网络安全保障能力。**二是**与国内网络安全领域企事业单位加强网络安全领域技术合作，探寻可持续发展的合作机制，共同促进我国网络安全行业发展。

四、 遴选周期及类别

支撑单位每两年一个遴选周期（届满到期后所有单位重新参加新一轮遴选），实行总量控制、开放竞争、考核评估、动态调整。支撑单位类别分为国家级、省级、重点技术领域，其中重点技术领域根据工作需要设置。

国家级支撑单位应是长期从事网络安全领域工作、具有领先技术优势、综合实力强、机构分布广、社会认可度高的企事业单位，拥有国内领先的高水平技术、人员和资源积累。

省级支撑单位应是在网络安全领域具有突出技术优势、

在部分区域认可度较高的企事业单位，或其技术特长为国家网络安全工作急需、或具有重大行业或区域影响。

重点技术领域支撑单位应是在某个特定的网络安全技术方向具有突出技术优势、在特定行业具有突出影响力的企事业单位。

五、 遴选流程

（一）自主申报。网络安全领域企事业单位按照遴选通知要求自主申报。

（二）提名推荐。组织 CNCERT 相关部门对申报单位进行提名推荐，开展形式审查。

（三）专家评审。组织网络安全领域专家进行评审，确定遴选建议名单。

（四）确认发布。确认发布支撑单位名单，根据确认类别分别颁发证书和铜牌。

六、 权利与义务

入选后，支撑单位应接受 CNCERT 的指导与协调，在合作期内，本着“义务服务和市场运作互为补充，权利与义务高度一致”的原则，在充分享有规定之权利的同时，切实履行承诺的义务。

（一） 享有的权利

1、在商务宣传、项目投标时对“CNCERT 网络安全应急服务支撑单位”称号的使用权。

2、优先参与 CNCERT 举办或组织的网络安全国内外交流活动、项目合作或其它专项工作。

3、CNCERT 优先推荐参与相关网络安全服务工作。

4、优先获得 CNCERT 的网络安全报告和信息。

5、获得与 CNCERT 成功合作案例的宣传权。

（二） 应履行义务

1、严格遵守国家保密相关法律法规和 CNCERT 保密工作规定，加强人员背景审查和保密教育培训，采取合理有效措施保守网络安全支撑任务相关秘密和敏感信息，在任何情况下（无论是否在合作期）不得以任何方式扩大其知悉范围，或向不应知悉者透露，严防失泄密等事件发生。

2、严格遵守《中华人民共和国网络安全法》等有关法律法规和国家网络安全相关工作规定，接受 CNCERT 对本单位网络安全工作的指导与协调。

3、在 CNCERT 指导协调下为国家网络安全应急工作提供技术支撑服务，工作内容包括但不限于:

（1）与 CNCERT 建立 7*24 小时工作联系机制，明确工作负责人和联系人。

（2）提供必要的人员、技术和设备支持，以保障相关工作顺利完成，包括远程和驻场支持等方式。

（3）配合开展网络安全动态或事件分析研判、调查取证、处置验证等工作，提供工作所需的数据和技术支持。

（4）发现或掌握重要网络安全信息后，应在面向社会公开发布之前、或在向其它部门报告的同时，向中心报告所掌握的情况，并配合开展后续工作。

（5）积极参与 CNCERT 举办或组织的网络安全国内外交流活动、项目合作或其它专项工作。

（6）定期报告网络安全支撑工作开展情况，包括但不限于：以支撑单位名义开展的投标及商务宣传、市场活动、安全服务情况；对 CNCERT 网络安全工作支撑情况；网络安全应急工作典型案例等。

（7）根据有关网络安全应急响应值守工作规范，按照应急响应不同级别，配备相应的值守力量。

七、 申报基本条件

申报单位需符合以下公共条件和相应类别的具体要求。

（一） 公共条件

1、在中华人民共和国境内成立，为独立实体，具有独立法人资格，具有相关部门颁发的合法经营资格，在中华人民共和国境内从事网络安全服务。

2、遵守中华人民共和国现行法律和法规，无违法犯罪记录，社会责任感强，信誉良好，在国家企业信用信息公示系统中无不良记录。

3、申报单位的子公司或分支机构不得同时提交申报。

（二） 申报国家级

1、符合上述“公共条件”要求。

2、机构注册资金在 1000 万元人民币以上，人员规模在 300 人以上，至少在全国 10 个省（直辖市、自治区）内设有固定办事机构，在网络安全领域从业 5 年以上，组织管理结构和监管体系清晰明确，经营状况良好。

3、具有稳定网络安全技术和服务团队，从事网络安全技术工作的人员不少于 50 人，至少 25 人具备相应的信息安全服务或应急处理等相关资质，至少 25 人具有三年以上大型网络安全服务项目经验，近三年完成至少 5 个金额不低于 100 万元人民币的网络安全服务项目，具备 7*24 小时网络安全应急保障支撑能力，具备实施网络安全服务必要的工作环境、研究环境、设备工具以及其它必要的保障措施。

4、在以下网络安全领域具有领先技术优势的单位优先，包括但不限于：监测分析（态势感知、威胁情报、漏洞挖掘、APT 监测分析、取证溯源、流量分析、拒绝服务攻击监测分析、网络空间资产测绘等）、安全服务（应急处理、渗透测试、应急演练、攻防竞赛、风险评估、安全运维、安全集成等）、应用安全（Web 安全、代码审计、域名安全等）、移动 APP 安全、云安全（云抗 D、云 WAP、云基础架构安全等）、物联网安全等。

5、承担过第 3 项所列领域的国家网络安全项目或课题的单位获先，承担过第 3 项所列领域的网络安全项目或课题

并获省部级以上科技奖励的单位优先。

（三） 申报省级

1、符合上述“公共条件”要求。

2、机构注册资金在 200 万元人民币以上，人员规模在 50 人以上，至少在国内 1 个省（直辖市、自治区）内设有固定办事机构，在网络安全领域从业 2 年以上，组织管理结构和监管体系清晰明确，经营状况良好。

3、具有稳定网络安全技术和服务团队，从事网络安全技术工作的人员不少于 20 人，至少 10 人具备相应的信息安全服务或应急处理等相关资质，至少 10 人具有两年以上中大型网络安全服务项目经验。近三年完成至少 3 个金额不低于 30 万元人民币的网络安全服务项目，具备 7*24 小时网络安全应急保障支撑能力，具备实施网络安全服务必要的工作环境、研究环境、设备工具以及其它必要的保障措施。

4、在以下网络安全领域具有突出技术优势的单位优先，包括但不限于：监测分析（态势感知、威胁情报、漏洞挖掘、APT 监测分析、取证溯源、流量分析、拒绝服务攻击监测分析、网络空间资产测绘等）、安全服务（应急处理、渗透测试、应急演练、攻防竞赛、风险评估、安全运维、安全集成等）、应用安全（Web 安全、代码审计、域名安全等）、移动 APP 安全、云安全（云抗 D、云 WAP、云基础架构安全等）、物联网安全等。

5、承担过第 3 项所列领域的国家或省内网络安全项目或课题的单位获先，承担过第 3 项所列领域的网络安全项目或课题并获省级科技奖励的单位优先。

（四） 申报反网络诈骗类别（重点技术领域）

1、符合上述“公共条件”要求。

2、机构注册资金在 1000 万元人民币以上，人员规模在 100 人以上，至少在国内 1 个省（直辖市、自治区）内设有固定办事机构，组织管理结构和监管体系清晰明确，具备反网络诈骗领域应急服务经验。

3、具有稳定反网络诈骗技术和服务团队，从事相关服务的人员不少于 20 人，其中本科以上学历不低于 70%，至少有 4 人具备行业认可的计算机、网络安全等相关领域技术资质。具备 7*24 小时应急响应能力，具备实施反网络诈骗服务必须的工作环境、研究环境及相应设备和工具。

4、近三年来至少有 1 项反网络诈骗类产品在相关业务部门应用并取得实际效果，佐证实际效果需要 1 家以上业务单位的应用证明。

（五） 申报 APT 监测分析类别（重点技术领域）

1、符合上述“公共条件”要求。

2、机构注册资金在 200 万元人民币以上，人员规模在 20 人以上，至少在国内 1 个省（直辖市、自治区）内设有固定办事机构，组织管理结构和监管体系清晰明确，在 APT

监测分析领域有 3 年以上从业时间，具备 APT 跟踪监测工作经验。

3、具有稳定和经验丰富的 APT 监测分析技术团队，从事 APT 监测分析工作的人员不少于 10 人，其中本科以上学历不低于 60%，具备 7*24 小时应急响应能力，具备 APT 监测分析必须的工作环境、研究环境及相应设备和工具。

4、近三年至少承担 3 项 APT 领域相关项目或服务，至少对外披露或报送 6 份 APT 领域深度分析报告。

CNCERT/CC