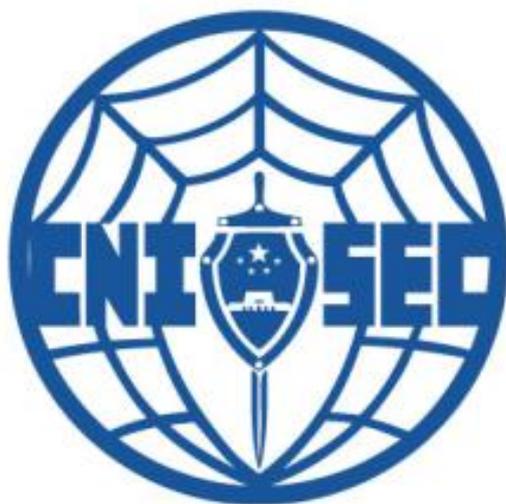


国家信息安全漏洞库（CNNVD）

技术支撑单位计划指南



版本：V4.1

中国信息安全测评中心

目录

一、	计划介绍	1
二、	计划内容	1
三、	申请流程	3
四、	证书维持与年度评价	4
附件 1:	技术支撑单位考察评估阶段贡献指标	6
附件 2:	技术支撑单位年度支撑指标	7

一、 计划介绍

国家信息安全漏洞库 (China National Vulnerability Database of Information Security, 以下简称“CNNVD”) , 是中国信息安全测评中心 (以下简称“测评中心”) 为切实履行漏洞分析和风险评估职能, 负责建设运维的国家级信息安全漏洞数据管理平台, 旨在为我国信息安全保障提供服务。经过几年的建设与运营, CNNVD 在信息安全漏洞搜集、重大漏洞信息通报、高危漏洞安全消控等方面发挥了重大作用, 为我国重要行业和关键信息基础设施安全保障工作提供了重要的技术支撑和数据支持。

CNNVD 技术支撑单位计划主要面向信息安全厂商、软硬件厂商与互联网公司等, 以平等自愿的原则, 通过签约合作的方式与这些单位开展合作。本计划通过整合业内资源, 联合技术支撑单位, 提高重大漏洞的发现、分析、处置能力, 进一步助力信息安全漏洞研究、事件解读, 形成漏洞的收集、分析、处置、披露的良性机制, 从而提高我国信息安全漏洞的研究水平和预警能力。

CNNVD 不对技术支撑单位收取申请、评审等相关服务费用。CNNVD 与技术支撑单位合作过程所产生的费用由各自自行承担。

二、 计划内容

本计划主要面向信息安全厂商、软硬件厂商与互联网公司等, 通过共享资源和服务, 逐步形成优势互补、协同发展的技术支撑单位合作体系。

技术支撑单位需要具有专业的信息安全研发团队和较强的漏洞分析能力，了解并认同 CNNVD 的业务和职能，致力于和 CNNVD 保持积极向上的技术业务合作关系。

CNNVD 技术支撑单位共设置三种级别,分别是一级、二级和三级（一级为最高级别），依据技术支撑单位的公司规模、技术研究能力、贡献程度等，以确定其支撑级别及其对应的年度贡献指标。同时，伴随技术支撑单位贡献程度的变化，相应的级别等方面也会有相应的调整。CNNVD 技术支撑单位的年度贡献包括如下几方面（具体要求见附件一）：

(1)原创漏洞支撑

按照 CNNVD 漏洞提交规范向 CNNVD 提交原创漏洞信息，信息需要具备真实性、有效性等特点。

(2)漏洞预警支撑

对重大信息安全漏洞做出及时响应，积极主动向 CNNVD 提供相关信息并协助 CNNVD 完成预警工作。

(3)其他支撑

与 CNNVD 开展与与漏洞技术相关的验证研判、技术研讨、事件性漏洞报送、数据分析等合作。

三、 申请流程

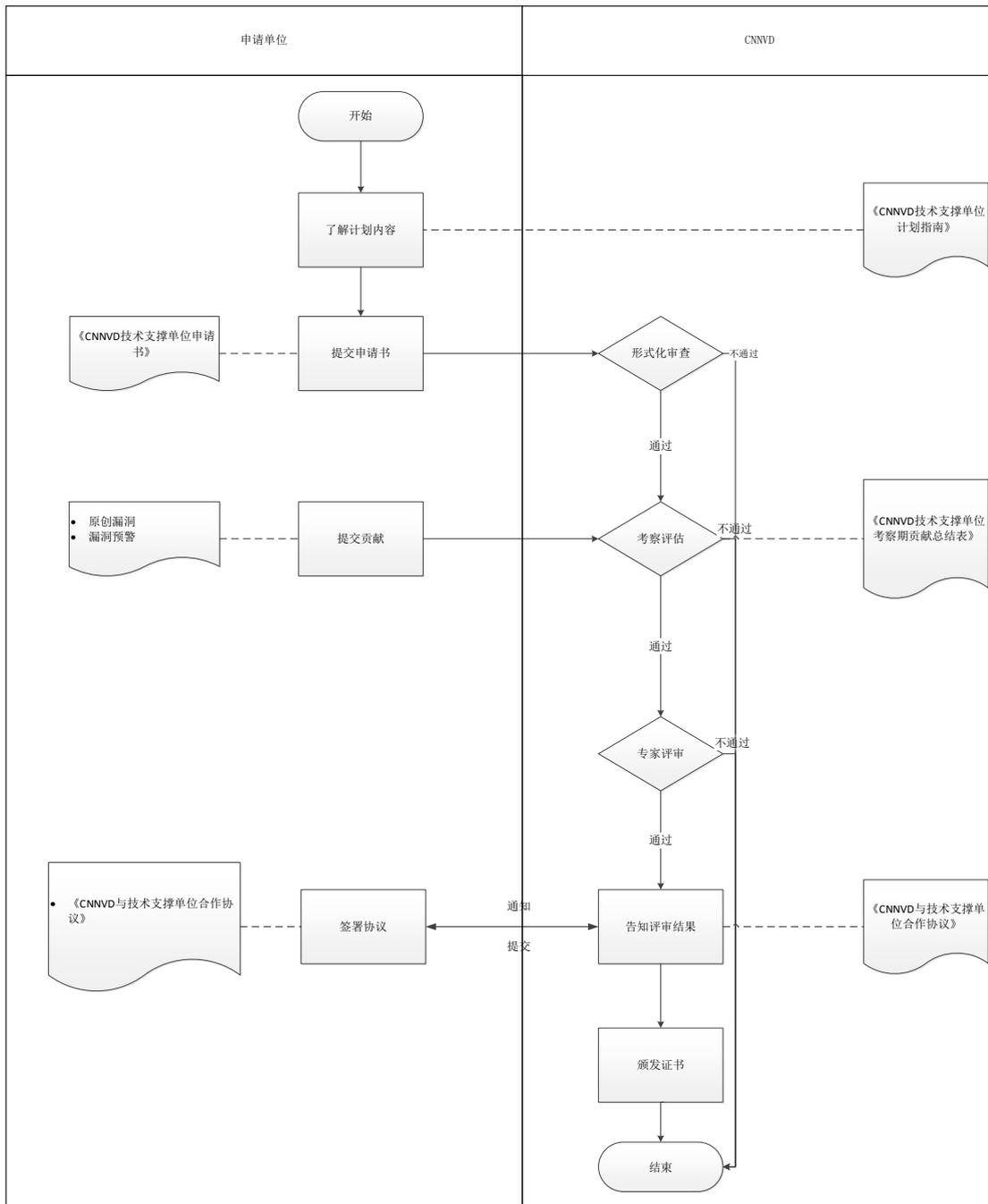


图 1 技术支撑单位申请流程

(1) 申请阶段：申请单位阅读《国家信息安全漏洞库（CNNVD）技术支撑单位计划指南》，提交《国家信息安全漏洞库（CNNVD）技术支撑单位申请书》，由 CNNVD 对其进行

审核，初审通过后，申请单位进入考察评估阶段。

- (2) 考察评估阶段：该阶段设定 6 个月的贡献考察期，申请单位可在此期间向 CNNVD 提交原创漏洞、漏洞预警等，由 CNNVD 对申请单位进行综合评估。
- (3) 专家评审阶段：CNNVD 召开技术支撑单位申请专家评审会，通过对申请单位提交的申请材料、考察期贡献内容、与 CNNVD 沟通配合情况等内容进行综合评估和级别判定。
- (4) 协议签订阶段：CNNVD 将评审结果通知申请单位，与通过评审的申请单位签订《国家信息安全漏洞库（CNNVD）与技术支撑单位合作协议》。
- (5) 证书颁发阶段：CNNVD 向技术支撑单位颁发证书，有效期一年。

四、 证书维持与年度评价

（一）证书维持

技术支撑单位证书有效期为一年。CNNVD 在支撑单位有效期结束之前 20 个工作日对其进行年度贡献审核，根据其证书有效期内贡献情况，如满足各级别续期要求则办理证书续期。

证书续期规则如下：

- 1、 若年度支撑贡献满足该级别的要求，等级维持不变。
- 2、 “二级”或“三级”支撑单位，若年度支撑贡献达到上一级对应的要求，可申请升级一个级别，经审批通过后可办理升级。对于贡献

特别突出的单位，经批准可酌情提前予以升级一个级别。

3、 年度支撑贡献不满足该级别的要求，则降低一个支撑等级直至取消资格（如：“一级”降为“二级”，“三级”取消资格）。

4、 如支撑单位在证书有效期内，有违反国家法律法规及双方协议的情况，CNNVD 将有权取消技术支撑单位资格并撤回证书。

技术支撑单位的单位名称及注册地址发生变化时，可向 CNNVD 提交《技术支撑单位信息变更申请表》，经 CNNVD 审核通过实施证书信息变更。证书信息变更内容不包含统一社会信用代码。

(二) 年度评价

CNNVD 每年度根据技术支撑单位贡献情况进行综合评价，对贡献突出的支撑单位给予荣誉奖励。各技术支撑单位应积极配合 CNNVD 贡献统计及年度评价工作。

注：本指南自发布之日起实施，最终解释权归中国信息安全测评中心所有。

附件 1：技术支撑单位考察评估阶段贡献指标

考察项目	考察指标
基本信息	技术支撑单位申请材料内容填写完整、真实准确。
负责安全业务、漏洞团队能力	1) 单位主营业务为信息安全行业，相关安全业务与漏洞分析挖掘密切相关，具备一定安全漏洞研究能力、安全应急响应能力； 2) 漏洞团队要求： 一级：人数达到 20 人以上,团队研究方向与获得成绩非常突出； 二级：人数达到 10 人以上,团队研究方向与获得成绩比较突出； 三级：人数达到 5 人以上,团队研究方向与获得成绩符合要求。
技术能力	具备在信息安全领域的科研、工程和服务能力。
原创漏洞支撑	向 CNNVD 提交原创漏洞： 一级：通用型漏洞不少于 20 个，其中高危及以上漏洞不少于 3 个； 二级：通用型漏洞不少于 15 个，其中高危及以上漏洞不少于 1 个； 三级：通用型漏洞不少于 3 个。
漏洞预警支撑	向 CNNVD 提交漏洞预警报告： 一级：重要预警数量不少于 5 份； 二级：一般及以上预警数量不少于 5 份； 三级：一般及以上预警数量不少于 3 份。

附件 2： 技术支撑单位年度支撑指标

评价项目	评价指标
资料合规性	《CNNVD 技术支撑单位年度工作总结》内容填写真实完整，符合要求。
业务配合度	与 CNNVD 沟通配合顺畅，态度积极，从未出现接口人联系不上或通知邮件回复不及时的情况。
原创漏洞支撑	向 CNNVD 提交原创漏洞： 一级：通用型漏洞不少于 35 个，其中高危漏洞不少于 5 个； 二级：通用型漏洞不少于 25 个，其中高危漏洞不少于 1 个； 三级：通用型漏洞不少于 5 个。
漏洞预警支撑	向 CNNVD 提交漏洞预警报告： 一级：重要预警不少于 10 份； 二级：一般及以上预警数量不少于 10 份； 三级：一般及以上预警数量不少于 5 份。
其他支撑	根据 CNNVD 的需求，积极响应由 CNNVD 发起的关于漏洞技术的验证研判、技术研讨、数据分析专项支撑、事件型漏洞专项支撑等。