国家网络威胁信息汇聚共享技术平台（CNTISP）技术支撑单位计划指南

版本： V2.0

中国信息安全测评中心

目录

一、计划介绍

国家网络威胁信息汇聚共享技术平台（China National Threat Information Sharing Platform，以下简称“CNTISP）是中国信息安全测评中心（以下简称“测评中心”）为切实履行威胁监测职能，负责建设运维的国家级威胁信息共享平台，旨在促进威胁信息共享和国家整体威胁防护能力提升，为我国网络威胁信息发现提供技术支持服务。

CNTISP技术支撑单位计划主要面向具有威胁发现能力的国内信息安全厂商、软硬件厂商与互联网公司等，以平等自愿、互利共赢的原则，通过签约合作的方式开展合作。本计划将通过整合业内资源，联合技术支撑单位，共同开展网络威胁信息共享与交流反馈，进一步提升信息网络威胁发现的效率和质量，定期对技术支撑单位开展评级奖励，从而提高我国网络威胁发现的整体水平和预警能力。

CNTISP不对技术支撑单位收取申请、评审等相关服务费用。合作过程中所产生的费用由各单位自行承担。

二、计划内容

（一）技术支撑单位组成及等级

本计划主要面向国内信息安全厂商、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网络威胁信息分析能力，具有一定规模的网络威胁信息发现阵地，了解并

认同CNTISP的业务和职能，致力于和CNTISP保持积极向上的技术业务合作关系。

CNTISP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。

（二）技术支撑单位年度贡献

CNTISP技术支撑单位的年度贡献包括如下几方面：

1、原创网络威胁信息支撑

按照CNTISP要求向平台共享自主发现的网络威胁信息。

2、网络威胁信息验证反馈支撑

技术支撑单位对平台共享的网络威胁信息进行核查，并主动向CNTISP反馈核查结果（包含但不限于威胁信息威胁影响范围、影响规模等）。

3、其他支撑

与CNTISP开展网络威胁信息验证研判、技术研讨、数据分析等合作。

三、申请流程

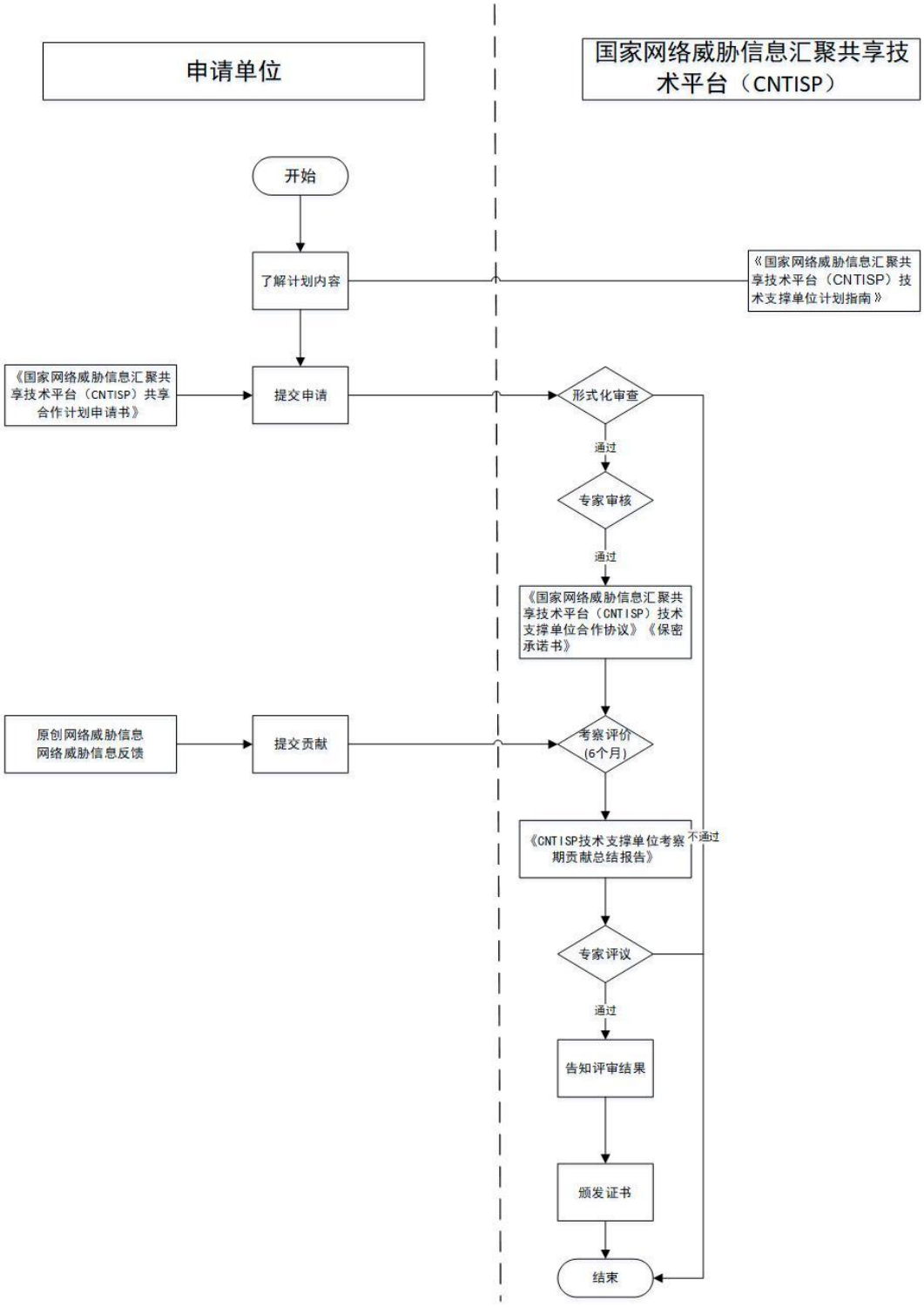

图 1 技术支撑单位申请流程

(1) 申请阶段：申请单位仔细阅读《国家网络威胁信息汇聚共享技术平台（CNTISP）技术支撑单位计划指南》，编写并提交《国家网络威胁信息汇聚共享技术平台（CNTISP）共享合作计划申请书》（附件4），由CNTISP对其进行形式化审查和专家审核。初审通过后，申请单位签订《国家网络威胁信息汇聚共享技术平台（CNTISP）技术支撑单位合作协议》（附件3），参与人员签署《保密承诺书》，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，申请单位在此期间向CNTISP提交原创网络威胁信息、参与网络威胁信息验证反馈等，CNTISP依据考察评估阶段贡献指标（附件1）对申请单位进行考察评估。

(3) 专家评审阶段：CNTISP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、考察期贡献内容以及CNTISP沟通配合情况等进行综合评估和级别判定。

(4) 证书颁发阶段：CNTISP向技术支撑单位颁发证书。

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。CNTISP在证书有效期结束之前20个工作日内对其进行年度贡献审核，依据技术支撑单位年度支撑指标（附件2）核实其证书有效期内贡献情况，如满足该级别续期要求则办理证书续期。

证书续期办法如下：

1、如果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，如果年度支撑贡献达到更高级对应的要求（例如，本年度是二级支撑单位，通过年度评价确定其贡献满足一级支撑单位要求），可申请升级一个或两个级别，经审批通过后办理升级。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、如果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”降级后将取消资格）。

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

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

（二）年度评价

CNTISP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CNTISP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、网络威胁信息团队能力	1、单位主营领域包含网络安全相关业务，具备一定的网络威胁信息研究分析能力、安全应急响应能力； 2、网络威胁信息团队要求： 一级：人数不少于50人，能够提供团队人员基本信息、组织架构、团队技术能力情况等资料，且人员分工明确； 二级：人数不少于30人,能够提供团队人员基本信息、组织架构、团队技术能力情况等资料，且人员分工明确； 三级：人数不少于15人,团队研究方向与获得成绩符合要求。
数据基础与技术能力	能够提供威胁信息研判的数据基础（包含但不限于数据类型、数据来源、覆盖行业、海外部署情况等），具备在信息安全领域的科研、工程和服务能力。
原创网络威胁信息支撑	考察期间向CNTISP提交原创网络威胁信息： 一级：网络威胁信息不少于20组，其中有效支撑网络威胁信息不少于5组； 二级：网络威胁信息不少于10组，其中有效支撑网络威胁信息不少于3组； 三级：网络威胁信息不少于5组，其中有效支撑网络威胁信息不少于1组。
网络威胁信息验证反馈支撑	考察期间向 CNTISP 提交网络威胁信息验证反馈： 一级：能够对共享信息提供有效验证结果不少于20组； 二级：能够对共享信息提供有效验证结果不少于10组； 三级：能够对共享信息提供有效验证结果不少于5组。

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	《CNTISP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CNTISP沟通配合顺畅，态度积极，未出现接口人失联（超过3个工作日无法取得联系）或通知邮件回复不及时的情况。
原创网络威胁信息支撑	年度内向CNTISP提交原创网络威胁信息。 一级：网络威胁信息不少于30组，其中有效支撑网络威胁信息不少于10组； 二级：网络威胁信息不少于20组，其中有效支撑网络威胁信息不少于5组； 三级：网络威胁信息不少于10组，其中有效支撑网络威胁信息不少于1组。
网络威胁信息验证反馈支撑	年度内向CNTISP提交网络威胁信息验证反馈报告。 一级：能够提供对于共享信息的提供有效验证结果不少于30组； 二级：能够对共享信息提供有效验证结果不少于20组； 三级：能够对共享信息提供有效验证结果不少于10组。
其他支撑	根据CNTISP的需求，积极响应由CNTISP发起的关于网络威胁信息技术的验证研判、技术研讨、数据分析专项支撑、事件型网络威胁信息专项支撑等。

附件 3：国家网络威胁信息汇聚共享技术平台（CNTISP）技术支撑单位合作协议

甲方：中国信息安全测评中心

乙方：_____

甲乙双方本着平等合作、优势互补、共同发展、诚实信用、公平自愿的原则，针对合作内容，经友好协商，现签署本合作协议书，以便双方共同遵守。

一、 合作内容

1.网络威胁信息共享

2.网络威胁信息联合研判及反馈

3.网络威胁信息分配和使用

4.网络威胁信息同步披露、更新

二、 甲乙双方权利与义务

1.甲乙双方按照《中华人民共和国民法典》签订本协议，自签订之日起，双方将享有以下的权利，并承担相应的义务。

2.甲方有权对乙方提供的《国家网络威胁信息汇聚共享技术平台(CNTISP)共享合作计划申请书》中威胁信息的真实性进行确认。

3.甲方有权对网络威胁信息汇聚与共享平台的信息系统、系统账户及其数据进行管理。

4.甲方有权定期组织乙方开展管理办法修订、数据研判、评审、数据应用研讨等相关工作。

5.甲方有权对乙方的贡献进行评价，给与奖励，并向社会公开。

6.甲方有权授予乙方“威胁信息共享合作厂商”称号。

7.甲方有权根据乙方的参与程度和表现，授予、调整、收回称号。

8.乙方享有使用自身提交信息和通过平台共享得到数据的权利。

9.乙方享有获得“威胁信息共享合作厂商”称号的权利，并可在本单位宣传推广时使用该称号。

10.乙方有义务配合甲方如实提供《国家网络威胁信息汇聚共享技术平台（CNTISP）共享合作计划申请书》中要求的信息，在协议有效期内，如果乙方相关信息（申请书中涉及的信息）发生变更，有义务第一时间通知甲方进行同步更新。

11.乙方有义务核实向甲方所共享信息的真实性和有效性，有义务在规定期限内按格式要求对平台所共享数据进行反馈、研判。

12.乙方有义务遵守《国家网络威胁信息汇聚共享技术平台（CNTISP）共享合作计划申请书》中关于平台使用、账户保管、数据反馈等规定。

13.乙方有权参与平台运营期间开展的管理办法修订、数据研判、评审、数据应用等研讨会议，并对平台的管理和运营提出建议。

14.乙方应对在平台上所发布信息的真实性和合法性负责，不得弄虚作假，不得违反国家有关法律法规。

15.甲乙双方共享的威胁信息须在双方协商一致后进行披露，协商内容包括披露时间、内容等。

16.在协议有效期内，任一方如发现对方有违反本协议条款之行为，有权随时终止本合作协议。

三、 保密条款

1.甲乙双方应对本协议内容、共享合作机制、《国家网络威胁信息汇聚共享技术平台（CNTISP）共享合作计划申请书》内容及双方知识产权、商业秘密及一切具有商业价值的信息承担保密义务，甲乙双方应确保其雇员或者其他临时人员对保密信息承担保密义务。本条款不受本协议终止影响，长期有效。如有违反，视为违约，守约方有权依据法律法

规要求追究违约方相应法律责任，同时违约方须承担由此给守约方造成的一切损失。

四、 其他

1.本协议之签署、效力、解释、履行及争议解决均适用中华人民共和国法律。本协议的变更及未尽事宜，由双方另行友好协商解决。

2.双方之间的信任与相互合作是本协议得以履行的重要基础。因本协议而产生或与之相关的任何争议，均应由双方友好协商解决。

3.本协议自双方签署之日起生效，有效期为叁年。

4.本协议正本一式陆份，双方各执叁份，具有同等法律效力。

甲方：

中国信息安全测评中心（盖章）：_____

法定代表人（签字）：_____

_____年____月____日

乙方：

签署单位（盖章）：_____

法定代表人（签字）：_____

_____年____月____日

附件 4：国家网络威胁信息汇聚共享技术平台（CNTISP）共享合作计划申请书

申请信息	组织类别	○厂商 ○联盟
申请机构信息	机构全称 （加盖公章）	中文：_____ 英文：_____
	机构所在地	国家：_____ 地区：_____
	统一社会信用代码	
	主营项目	
	主营产品	
	企业职工总数	
	企业技术人员总数	
	资质证书	
共享合作接口信息	联系人	
	联系电话	
	邮箱	
网络威胁信息共享	威胁数据来源 （包含但不限于数据类型、数据来源、覆盖行业、涉及单位数量等）	
	已部署的威胁检测分析相关设备类型及数量	

	威胁信息共享形式（可填写人工提交、自动反馈等）	
	威胁信息提交联系电话（如有需填写网址，如没有填“无”）	
网络威胁信息反馈	威胁信息核查反馈范围（如有填写大概范围：行业、内部等）	
	威胁信息核查反馈形式（可填写人工反馈、自动反馈等）	
相关附件	（1）经年检的企业法人及营业执照副本复印件 □有 □无	
	（2）财务报表 □有 □无	
	（3）企业资质材料 □有 □无	
	（4）企业相关案例 □有 □无	
	（5）安全业务负责人、网络威胁团队能力及骨干人员情况 □有 □无	
	（6）威胁情报共享方案 □有 □无	

申请日期：　　年　月　日

注：申请书及其附件是考察申请机构是否具备相应能力的重要参考依据，请务必详实准确填写。

申请须知

1. CNTISP 提供支撑网络威胁信息汇聚与共享的信息系统，负责平台运营，对接入系统的用户和单位进行管理，维护系统的正常运行和数据的安全可靠。
2. CNTISP 为支撑单位提供账户、口令，以及通过互联网访问系统软件条件。
3. 技术支撑单位应对平台分发的账号、数据进行有效保管，不得向第三方透露数据来源以及平台运营状况。
4. 技术支撑单位应对在平台上发布的信息的真实性和合法性，不得弄虚作假，违反国家有关法律法规。
5. 技术支撑单位负责对己方参与数据共享、平台使用的人员进行背景审查，优先选择政治信仰坚定、诚实可靠的人员参与合作，并定期开展保密培训。
6. 未经 CNTISP 许可，技术支撑单位不得向第三方机构透露平台的运行机制、共享范围、评价机制等信息。