国家网络威胁信息汇聚共享技术平台（CNTISP）企业参与章程

第一章 总则

第 1 条 平台名称

国家网络威胁信息汇聚共享技术平台，英文全称 China National Threat Information Sharing Platform，简称 CNTISP。

第 2 条 平台性质

国家网络威胁信息汇聚共享技术平台（以下简称“平台”）是由中国信息安全测评中心发起，邀请国内信息安全企业共同参与的网络威胁信息汇聚与共享的技术交流平台。

第 3 条 目的与宗旨

本章程旨在规范国家网络威胁信息汇聚共享技术平台的运营与管理，明确技术支撑单位的权利与义务，促进威胁信息的有效、安全与合法共享，推动企业间合作与创新发展，同时保障各参与方的合法权益。

平台本着人人为我，我为人人的宗旨，呼吁国内信息安全企业协同合作，及时共享各自发现的可疑行为，携手排查网络威胁在各自网络阵地的活动线索，促进国家网络空间人民防线的构建。

第 4 条 平台运行管理

平台由中国信息安全测评中心负责运行管理，并制定一系列的运行管理机制以及自律公约，接受技术支撑单位的广泛监督。

第 5 条 平台工作组

平台设立工作组负责日常运行管理事务，包括维护平台的正常运转，组织安全企业的遴选、审核和管理，组织评价激励等。

工作组设在中国信息安全测评中心。

第 6 条 适用范围

本章程适用于所有申请加入并经审核同意参与平台的单位。

第二章 工作范围

第 7 条 工作原则

坚持以业务需求为导向。紧密围绕国家安全急迫需求，通过平台形成威胁信息高效共享机制，倡导群策群力协作精神，引导安全企业有效发现 APT 攻击线索，充分发挥合力优势，确保威胁情报能够在第一时间被收集、分析并传播给有关方。

坚持以实战效益为重点。重视共享威胁数据在实际应用中的表现，将效益贯穿在安全实战、科技建设和技术合作中。在评价数据时，将发挥的实战效益作为评价数据的重要依据之一，高价值线索甚至可一锤定音。

坚持系统性协作理念。平台作为需求单位与技术单位沟通的桥梁，不仅要促进双方的无缝对接，还要确保信息流通的高效与安全。通过构建一个开放共享、互动频繁的生态系统，需求单位能够准确表达业务所需，技术支撑单位则能提供多元化的专业见解与技术资源，扩大威胁发现数据视野，双方共建良好的系统性协作模式。

第 8 条 工作内容

（一）共享威胁信息指标。共享独立研判和发现的威胁情报指标，并保障信息的真实性、完整性和有效性。

（二）反馈活动统计结果。利用共享的威胁情报指标进行核查，统计威胁信息指标在各自网络阵地的活动情况，并尽快反馈至平台。

（三）参与事件研判与讨论。参与平台对于重要事件、重大线索、争议事件的研判讨论；参与平台运营机制、评价体系修订与讨论，促进平台向好发展。

（四）其它。参与平台宣传推广、评价奖励等活动。

第三章 参与方式

第 9 条 资格要求

凡是中国大陆境内具有独立法人资格、从事网络威胁发现的企业、事业单位及相关机构，同时承认本章程的，均可向平台提出申请。经批准后成为参与单位（即技术支撑单位），分发平台账号，参与数据共享活动。

第 10 条 申请程序

申请应办理如下手续：

（一）向工作组提交书面申请材料，包括《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》及相应附件。

（二）工作组收到申请材料后对相关内容进行审核。

（三）审核通过后签署《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》及《保密承诺书》。

第 11 条 考察与认定

对已提交《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》及《保密承诺书》的技术支撑单位进行为期六个月的考察，考察期的贡献度由 CNTISP 工作组考察认定，满足技术支撑单位考察评估阶段贡献指标要求的企业，可申请评级认定。

CNTISP 工作组对技术支撑单位贡献情况进行核查确认，确认无误的定期分批授予技术支撑单位称号，颁发技术支撑单位证书（有效期为一年）。

第 13 条 续期、降级与淘汰

（一）工作组在证书有效期结束之前 20 个工作日对其进行年度贡献审核，证书有效期内贡献度满足当前技术支撑单位等级要求的，根据证书续期规则办理证书续期。

（二）工作组在证书有效期结束之前 20 个工作日对其进行年度贡献审核，证书有效期内贡献度未满足当前技术支撑单位等级要求的，启动降级评估流程，开展为期 3 个月的能力考察，对仍不能满足要求的目标支撑单位采取降级处理，直至取消资格。

证书续期办法参见《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》。

第 12 条 退出与除名

（一）技术支撑单位退出应提前十个工作日书面通知工作组；

（二）技术支撑单位如有严重违反本章程的行为，将予以除名；

（三）技术支撑单位退出与除名以正式通知为准。

第 14 条 技术支撑单位权利

（一）通过平台获知更多的高质量 IOC 指标，共用其他技术支撑单位的工作成果，丰富自己的数据来源；

（二）通过威胁信息共享，获得更大的数据视野，从而提升自身威胁情报数据的质量；

（三）通过共享和反馈，积累在平台中的贡献度，体现其在网络威胁情报行业中的先进性。

第 15 条 技术支撑单位义务

（一）严格遵守本章程；

（二）配合工作组的工作，包括：共享独立研判和发现的境外网络威胁信息；利用共享的境外网络威胁信息进行扩线，形成更准确、更有效的研判结果；对被共享的境外网络威胁信息在各自数据视野中进行验证，形成对威胁数据的正向反馈；

（三）满足《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》能力要求；

（四）向工作组反映工作机制的情况，提供有关信息；

（五）自觉执行平台全体成员达成的其他决议。

第 16 条 评价与奖励

工作组每年度将根据技术支撑单位对平台的贡献程度进行评价，对表现突出的单位给与表彰，对表现特别突出的单位颁发证书和奖励。

评价维度包括贡献积极程度、数据质量、数据数量、数据丰富度、

反馈积极、共享度等多个方面。具体评价方式详见附件 1《网络威胁信息积分评价指南》（草稿）。

第四章 平台运行

第 17 条 联系人

技术支撑单位须指定一名网络安全专业背景的人员作为单位的运行联系人。该联系人将代表单位参与运行活动，参加 CNTISP 平台组织的技术交流和定期反馈。

第 18 条 账号安全

每个技术支撑单位都会获得一个专属的账号，联系人应妥善保管并避免泄露。如因账号问题导致信息丢失或误操作，由所在单位自行承担责任。

第 19 条 共享数据

使用平台账号共享与反馈数据，不得对平台提交与威胁信息汇聚与共享无关的网络活动，一经发现取消平台访问权限，并追究法律责任。

第五章 章程文本

第 20 条 章程建立

章程文本由工作组起草，经征询现有技术支撑单位意见，超过三分之二单位通过后生效。

第 21 条 章程修改

章程后续的修改和更新均需工作组征询超过三分之二技术支撑单位意见，无异议后报中国信息安全测评中心审批通过后生效。

第六章：附则

一、任何在平台内或由平台讨论的内容，包括平台大会、工作组会议议题、会议内容等，仅在成员内部公开。任何成员都应该遵守平台的保密制度。

二、平台所从事的所有活动均严格遵从所有现行的法律法规。平台成员应知悉其各公司按一定的商业规则互相竞争，他们的行为不能违反任何现行的反垄断法律和法规。每位平台成员应积极地鼓励和促进威胁情报生态的竞争环境。成员应确认他们不会竞争者之间谈论有关产品成本、产品定价、销售渠道、市场分区或客户配售等问题。因此，每位成员有责任为其参加平台活动的代表就限制在正式会议或非正式聚会等场合谈论关于平台目标宗旨的重要问题上提供相应法律的建议和忠告。每个成员还应知悉在符合平台章程规定的范围内，开发竞争性的技术和标准以及将该成员的专利权许可给第三方以使竞争技术和标准进行运作的行为是自由的。

三、知识产权：任何成员不得因参加平台而明示或默示地授予或被视为授予该平台或其他成员关于专利、版权、商标、商业秘密或该成员拥有或控制的其他知识产权的任何权利或许可，除非本章程另有规定。未经其他成员的明示书面许可，任何成员不得以任何公开方式

使用其他成员的名称，但是任何成员均可以披露和公开其在平台的成员身份，并且平台也可以披露和公开任何成员的成员身份，除非该成员以书面形式明示请求平台不披露或公开其在平台的成员身份。

四、此章程不是为了（也不应该被理解为）在成员之间建立一个公司、合伙企业、合资企业、代理关系等实体。任何成员在没有得到其他成员或平台的书面授权时，都没有权利代表其他成员或平台签订协议或承担义务。成员不应承担由其他成员或平台的未授权行为带来的责任、损失或损害。

五、本章程自平台大会表决通过后生效。

六、本平台的官方语言为中文。本章程即使被翻译为其他语言，仍以中文版本为准。

七、本章程的解释权属于中国信息安全测评中心。

八、平台使用反馈：如果您在使用平台过程中有任何疑问、建议或者遇到问题，可以通过以下两种方式联系我们：

1）直接与我们的平台人员联系，他们会尽快为您提供帮助；

2）发送电子邮件至 liangzy@itsec.gov.cn，工作组会在收到邮件后的第一时间回复您。

CNTISP 工作组

2025 年 5 月 13 日