国家标准《信息安全技术 网络安全众测服务要求》（征求意见稿）编制说明

一、工作简况

1、任务来源

根据国家标准化管理委员会2022年下达的国家标准制修订计划:《信息安全技术　网络安全众测服务要求》，国标计划号：20220608-T-469，标准由国家计算机网络应急技术处理协调中心主办，由全国信息安全标准化技术委员会（SAC/TC 260）归口管理。

2、主要起草单位和工作组成员

《信息安全技术　网络安全众测服务要求》由国家计算机网络应急技术处理协调中心牵头研制，起草单位为：国家计算机网络应急技术处理协调中心、中国电子技术标准化研究院、中国信息安全测评中心、国家信息技术安全研究中心、阿里云计算有限公司、网神信息技术（北京）股份有限公司、北京中金安服科技有限公司、中国移动通信集团有限公司、中国科学院软件研究所、上海斗象信息科技有限公司、北京天融信网络安全技术有限公司、中通服咨询设计研究院有限公司、上海文鳐信息科技有限公司、浙江蚂蚁小微金融服务集团股份有限公司、杭州安恒信息技术股份有限公司、北京信息安全测评中心、北京东方通网信科技有限公司、北京众安天下科技有限公司、北京奇虎科技有限公司、中国电子科技网络信息安全有限公司、北京北信源软件股份有限公司、启明星辰信息技术集团股份有限公司、工业和信息化部计算机与微电子发展研究中心（中国软件评测中心）、北京数字观星科技有限公司、上海计算机软件技术开发中心。

本标准主要起草人：云晓春、舒敏、严寒冰、王文磊、刘贤刚、王惠莅、张大江、杨晨、高继明、秦磊、王宏、孙彦、何能强、王江波、董航、邓萍萍、俞斌、崔婷婷、李媛、胡鸣、王俊杰、郭亮、闫宏石、王龑、邱勤、左敏、凌墨缘、张奇、杨蔚。

3、主要工作过程

（1）草案阶段：

2019年9月25日，起草组组织召开了标准研制启动会，各参编单位讨论后确定了标准大纲，并进行了任务分工，编制形成了草案（第1稿）。

2019 年 10 月 17 日，起草组组织召开了专家评审会，征集到专家意见 14 条，处理结果均为采纳。起草组根据专家意见对标准草案进行了修改，修改形成了草案（第 2 稿）。

2019 年 10 月 28 日，起草组在 TC260 重庆会议周 WG7 会上进行汇报，征集到专家意见 14 条，处理结果为采纳 13 条，未采纳 1 条。

2019 年 12 月 4 日，起草组召开编制讨论会，会上根据重庆会议周的意见处理修改形成了草案（第 3 稿）。

2020 年 3 月 31 日，起草组内部对标准内容提出多轮修改意见，对起草组内部意见处理后修改形成了草案（第 4 稿）。

2020 年 5 月 12 日，在 TC260 线上会议周汇报，成功推进形成征求意见稿。

（2）征求意见稿阶段：

2020 年 5 月 13 日至 6 月 4 日，起草组对线上会议周征集到的 12 条工作组专家意见进行处理，处理意见为采纳 8 条，部分采纳 4 条。

2020 年 6 月 17 日，参加 TC260 秘书处组织的线上专家评审会，会上收集到专家意见 11 条，均采纳。6 月 24 日，秘书处责任编辑对征求意见稿进行了审查，根据责任编辑意见进行了相应修改，处理意见为采纳 6 条。

2020 年 7 月 17 日，受信安标委秘书处委托，国家计算机网络应急技术处理协调中心组织 12 家众测相关单位召开标准试点验证启动会，项目牵头单位汇报了试点验证方案和计划，3 位外部专家对试点验证方案进行了审核，并按计划于 2020 年 8 月 15 日完成了标准试点验证工作。

2020 年 9 月 25 日至 2020 年 11 月 24 日，信安标委秘书处向工业和信息化部科技司、公安部十一局、国家保密局、国家密码管理局、国家认证认可监督管理委员会、中国信息安全测评中心、中央网信办网络安全协调局等上级主管部门发函征求意见，并在信安标委官网公开征求意见，征求意见范围具有广泛性和代表性。共收到意见 6 条，意见处理结果为采纳 5 条、未采纳 0 条、部分采纳 1 条。

2021 年 3 月 10 日，参加 TC260 WG7 组织的专家评审会，共收到意见 21 条，意见处理结果为采纳 16 条、未采纳 0 条、部分采纳 5 条。

2021 年 5 月 10 日至 5 月 13 日，参加信安标委武汉会议周 WG7 工作组会议并在 WG7 工作组武汉会议上汇报，成功推进形成送审稿。

（3）送审稿阶段：

2021 年 5 月 14 日至 7 月 20 日，起草组对武汉会议周征集到的 6 条工作组专家意见进行处理，处理意见为采纳 5 条，部分采纳 1 条。因 2020 年公开征求意见，2022 年才获得国标计划号，拟再次公开征求意见。

2022 年 9 月 16 日，参加信安标委秘书处组织的专家评审会，共收到意见 11 条，意见处理结果为采纳 11 条，部分采纳和未采纳 0 条。会后形成新版标准文稿，拟以征求意见稿形式再次公开征求意见。

二、标准编制原则和确定主要内容的论据及解决的主要问题

1、编制原则

本标准在研制过程中遵循的原则包括：

（1）实用性原则

研制过程中，紧密围绕众测服务产业发展实践和需求，力求标准能够为规范众测服务提供有效指导。

（2）合规性原则

遵循国家以及各行业的相关规定，对众测组织方、授权测试方等行为进行规范，确保众测服务合规、合法。

2、主要内容

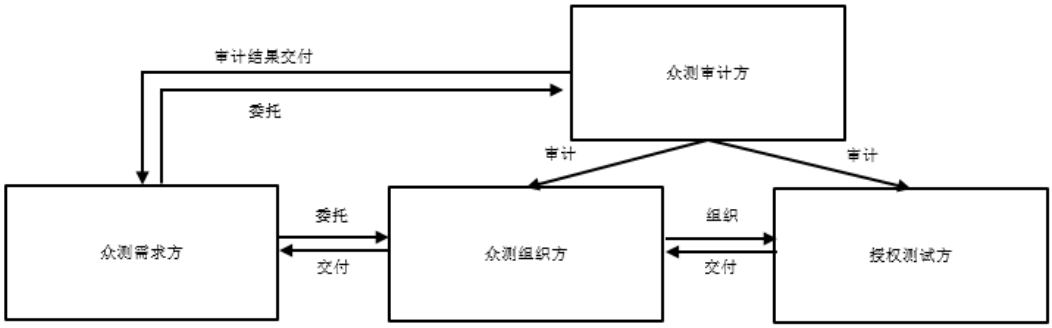
本标准确立了网络安全众测服务的角色及其职责，描述了服务流程，规定了服务要求。

本标准适用于众测需求方、众测组织方、授权测试方和众测审计方在开展网络安全众测服务时使用。

3、主要章节内容

（1）定义：网络安全众测服务是以自由自愿的方式组织非特定的自然人或组织，在审计及监督下，开展安全测试的过程。并给出了网络安全众测服务平台、众测需求方、众测组织方、授权测试方、众测审计方的定义。

（2）角色及职责：网络安全众测服务涉及的角色包括众测需求方、众测组织方、授权测试方、众测审计方。本标准界定了各角色的职责。各角色的交互关系如图1所示。



（3）流程：网络安全众测服务流程包括准备阶段、实施阶段、后处理阶段。具体活动包括：

——准备阶段：众测需求方和众测组织方相互协商，明确双方权利义务；众测需求方向众测组织方明确授权并授权众测组织方组织符合要求的授权测试方实施众测；众测组织方按照众测需求方的要求发布众测项目，依托网络安全众测服务平台在获得众测需求方授权的前提下组织授权测试方；授权测试方做好测试准备；众测审计方做好审计准备。

——实施阶段授权测试方通过获得授权的安全接入方式执行测试，按要求提交漏洞；众测组织方对漏洞进行初步审核后交付给众测需求方；众测需求方（也可委托众测组织方）对漏洞进行审核确认；众测需求方及时修复漏洞；众测审计方对众测过程进行审计和监督。

——后处理阶段：在约定的测试时间结束后，众测组织方向众测需求方提供众测服务报告；众测需求方进行分析总结并进行复检，众测组织方及时删除众测需求方相关材料、漏洞等敏感信息；众测审计方提交审计报告。

（4）服务要求：给出了准备阶段、实施阶段、后处理阶段中众测需求方、众测组织方、授权测试方、众测审计方的服务要求。

4、解决的主要问题

（1）如何界定众测服务各参与角色的职责和义务；

（2）如何规范众测服务的服务流程；

（3）如何强化对众测服务参与人员的管理，规范测试人员行为不可控的风险；

（4）如何构建网络安全众测服务平台并做好众测平台的安全保障，规范由于众测服务可能带来的信息泄露等风险；

（5）如何规范众测服务事后可能存在的残余风险。

三、主要试验[或验证]情况分析

编制组在编制过程中，广泛听取众测服务提供商、测评机构、研究机构等的意见，也征求行业专家的意见，形成现行版本。

《信息安全技术　网络安全众测服务要求》标准编制组于2020年7月-8月组织开展了标准征求意见稿试点工作，组织12家众测相关单位进行了标准试点验证，对标准条款进行试点验证。

本次验证活动，各参与单位结合自身在网络安全众测服务中的角色（主要为众测组织方和众测审计方），对照《信息安全技术 网络安全众测服务要求》（征求意见稿）的条款内容进行验证，按照标准条款的要求，检查自身的授权测试方规范管理、漏洞管理能力、审计能力、众测服务平台安全保障能力等是否能达到标准要求，或标准要求本身是否需要改进完善。

经过本次试点验证，从众测组织方的角度来看，《信息安全技术 网络安全众测服务要求》国标征求意见稿的大部分条款要求适用于业界现状，但也存在部分条款要求存在要求偏高或不适用情况。从众测审计方的角度来看，该标准具备可行的管理要求，能够适用于实际的网络安全众测项目，可进行推广实施。

四、知识产权情况说明

本标准不涉及专利。

五、产业化情况、推广应用论证和预期达到的经济效果

国内主要的网络安全众测服务提供商、网络安全众测服务第三方审计机构均深度参与标准研制进程，标准研制过程中充分征集并尽量反映了业界需求以及监管需求，当前标准内容适用于国内产业实践和发展需求。

本标准的制定将为后续有意提供网络安全众测服务的企业、机构等提供参考，有助于推动网络安全众测服务的产业化。目前美国HackerOne、Synack、BugCrowd等平台为美国国防部等客户组织开展了大量网络安全众测活动，国内由中央网信办指导建设的国家网络安全人才与创新基地网络安全众测平台以及由相关企业

运营的网络安全众测服务平台均已组织开展大量众测项目，为众多政府机构及企事业单位提供安全服务。

六、采用国际标准和国外先进标准情况

本标准为自主制定，暂无网络安全众测服务相关的国际标准和国外先进标准。

七、与现行相关法律、法规、规章及相关标准的协调性

《中华人民共和国网络安全法》第二十七条规定“任何个人和组织不得从事非法侵入他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动；不得提供专门用于从事侵入网络、干扰网络正常功能及防护措施、窃取网络数据等危害网络安全活动的程序、工具……”。本标准将众测组织方获得众测需求方明确授权作为网络安全众测服务启动的必要前置条件，可规范网络安全众测服务相关方的活动，以确保符合《网络安全法》等相关法律法规的要求。

针对网络安全众测服务，通信、金融等领域制定发布了行业标准：YD/T 3744-2020《网络安全众测平台技术要求》，YD/T 3745-2020《网络安全众测服务管理要求》，JR/T 0214-2021 《金融网络安全 网络安全众测实施指南》。

本标准符合现有法律法规的要求，并与现有相关标准协调一致。

八、重大分歧意见的处理经过和依据

无

九、标准性质的建议

建议本标准作为推荐性国家标准发布实施。

十、贯彻标准的要求和措施建议

在正式执行本标准之前，对标准中的条款进行宣贯，以在利益相关方之间达成标准条款理解上的一致性。

十一、替代或废止现行相关标准的建议

无

十二、其它应予说明的事项

无。

《信息安全技术 网络安全众测服务要求》

标准编制工作组

2022 年 9 月 27 日