工业和信息化部办公厅

工信厅联网安函〔2022〕2号

关于开展网络安全技术应用试点示范工作的通知

各省、自治区、直辖市及新疆生产建设兵团工业和信息化、电信、网信、水利、卫生健康、应急管理、广电、能源主管部门，中国人民银行各分行、营业管理部、各省会（首府）城市中心支行，各银保监局，各证监局，各地区铁路监管局，民航各地区管理局及其监管局，相关单位：

为深入贯彻落实《中华人民共和国网络安全法》《中华人民共和国数据安全法》《关键信息基础设施安全保护条例》，加强网络安全先进技术应用引导，推动网络安全产业高质量发展，现决定开展网络安全技术应用试点示范工作。有关事项通知如下：

一、试点示范内容

适应数字产业化和产业数字化发展新形势，以新型基础设施安全、数字化应用场景安全、安全基础能力提升为主线，面向公共通信和信息服务、能源、交通、水利、应急管理、金融、医疗、广播电视等重要行业领域网络安全保障需求，从云安全、人工智能安全、大数据安全、车联网安全、物联网安全、智慧城市安全、网络安全共性技术、网络安全创新服务、网络安全“高精

尖”技术创新平台9个重点方向（附件1），遴选一批技术先进、应用成效显著的试点示范项目。

二、申报要求

（一）申报主体。主要由公共通信和信息服务、能源、交通、水利、应急管理、金融、医疗、广播电视等行业和领域的企事业单位，以及为其提供网络安全技术、产品和服务的企事业单位等组成联合体申报（牵头单位1家，联合单位不超过2家）。网络安全“高精尖”技术创新平台方向主要面向技术创新或试点示范区运营、管理机构。申报主体应在中华人民共和国境内注册、具备独立法人资格。

（二）申报项目。主要包括支撑本单位自身网络安全工作或为用户提供安全服务的网络安全技术平台或系统，具备创新性、先进性、实用性、可推广性等特点。网络安全“高精尖”技术创新平台方向主要包括地市级及以上各类技术创新或试点示范区，具备区域优势明显、产业基础良好、政策制度完善、创新要素聚集等特点。

（三）每个申报主体可最多牵头或参与申报2个项目，每个申报项目仅可选择1个试点方向。

（四）已入选国家级或十二个部门有关试点示范项目、已获得国家专项资金支持的项目不可重复申报，未建及在建项目不可

申报。

三、工作流程

（一）申报。申报联合体的牵头单位向项目所在地省级有关部门提交网络安全技术应用试点示范申报书（附件2）。牵头单位为国家行业主管监管部门直接管理的机构，可向行业主管监管部门申报。申报项目不可通过多途径同时申报，否则取消项目资格。

（二）初审和推荐。各省级有关部门组织对本地区本行业本领域网络安全技术应用试点示范申报项目进行初审，并按推荐项目的优先顺序填写推荐项目汇总表（附件3），于2022年2月28日前将推荐项目汇总表（纸质版一式两份和电子版光盘）及企业申报书（纸质版一式三份和电子版光盘）提交国家行业主管监管部门。各主管监管部门汇总本行业本领域推荐项目材料，于2022年3月15日前送工业和信息化部（网络安全管理局）。各省级有关部门推荐的项目总数原则上不超过5个，其中网络安全“高精尖”技术创新平台不超过2个。

（三）遴选。工业和信息化部会同有关部门组织专家对申报项目进行遴选评审，并对符合要求的项目开展试点示范。试点示范期为2年。

（四）推广。建立部门间工作机制，加强对入选项目的支持、指导和监督，综合运用政策、标准、项目配套等资源，促进入选

项目推广应用，扩大示范带动效应。

四、联系方式

联系人：赵泰　010—62305321　赵爽　010—66022774

地　址：北京市海淀区花园北路52号（100191）

附件：1. 网络安全技术应用试点示范重点方向

2. 网络安全技术应用试点示范申报书

3. 推荐项目汇总表

工业和信息化部办公厅　　国家互联网信息办公室秘书局

水利部办公厅　　国家卫生健康委员会办公厅

应急管理部办公厅　　中国人民银行办公厅

国家广播电视总局办公厅　　中国银行保险监督管理委员会办公厅

中国证券监督管理委员会办公厅　　国家能源局综合司

国家铁路局综合司　　中国民用航空局综合司

2022年1月7日

附件 1

网络安全技术应用试点示范重点方向

一、新型信息基础设施安全方向

（一）云计算安全。面向多云、云原生、边缘云、分布式云等新型云计算架构，云环境中云主机、云存储、云网络等基础资源，以及云上业务、应用等服务，采用云身份管理、软件定义边界、云工作负载保护等技术实现云架构安全、多网边界隔离、跨网安全交互、多网一体化防护，保障云上资源安全可靠、云上业务运行稳定的安全解决方案。

专栏 1　云计算安全重点方向

公有云安全。面向云、网、应用深度融合场景需求，在公有云用户提供集约化、数据互通、云网一体化，以及集网络安全、主机安全、数据安全、应用安全于一体的安全解决方案。

政务云安全。面向政务网、互联网跨网一体化防护需求，采用云上多网边界隔离、数据分类分级、跨网安全交互、终端集中管控及安全隔离等技术，在多网“一朵云”、“一端多网”安全管控等方面的安全解决方案。

媒体云安全。结合融合媒体智能生产、多渠道播出分发、网络直播点播、视听应用 APP、媒体智能终端、监测监管等需求，在媒体内容安全、播出安全、分发安全、平台安全、应用安全等方面的安全解决方案。

工业云安全。围绕推动工业设备和业务系统上云，构建基于云、网、端的协同联动防护体系，加强双栈流量可视化、微隔离、软件定义边界、云工作负载保护、云上数据保护等安全能力的解决方案。

（二）人工智能安全。面向智慧工厂、智能通信、智慧金融、公共安全等典型应用场景，针对人工智能基础研发平台、核心算法、训练数据、智能应用的安全需求，在机器学习框架漏洞挖掘和修复、算法鲁棒性及公平性评测和增强、数据泄露安全防护、智能应用安全风险监测预警等方面的安全解决方案。

专栏2　人工智能安全重点方向

人工智能基础设施安全。面向高效能计算基础设施，在人工智能公共数据资源库、标准测试数据集、算法与平台安全性测评工具集等方面的安全解决方案。

基础网络安全智能防御。发挥骨干网络和基础资源优势，在提升基础网络安全感知、分析、响应、决策等综合防控能力，实现网络安全威胁快速溯源定位等方面的安全解决方案。

金融交易欺诈和钓鱼欺诈智能防范。针对金融业智能高效的交易反欺诈、跨行业联防联控反钓鱼等安全需求，建立事前防范、事中监控、事后处置三位一体的智能金融反欺诈安全解决方案。

（三）大数据安全。面向优化数据安全治理，推动密码技术、区块链等为数据安全增效，在数据应用安全防护、存证取证、监测预警和应急处置、隐私保护和流向溯源、国产商用密码应用等方面，探索数据确权、流通、共享新业态新模式，实现数据资源可视、可管、可控，促进数据有序流动的安全解决方案。

专栏3　大数据安全重点方向

大数据基础设施安全。在推动构建绿色、集约、安全的大数据中心，促进数据资源安全整合、安全共享，强化大数据安全保障支撑、网络安全信息共享和重大风险识别等方面的安全解决方案。

金融大数据安全。结合金融核心业务和大数据分布特点，基于金融多源情报融合分析技术，构建大规模复杂异构金融服务模拟网络，支持常态化、高频度、多样化攻防实战演练等方面的安全解决方案。

广播电视与网络视听大数据安全。结合广播电视和网络视听媒体内容、网络、用户、运营和系统运行等大数据的安全需求，在提升数据防泄露、防篡改、防窃取等传统数据安全保障能力，优化数据安全管理、分类分级安全防护、深度伪造视频鉴别等方面的安全解决方案。

交通运输旅客信息安全。面向铁路、民航等涉旅客用户个人信息安全需求，在保障铁路和民航信息系统、第三方票务软件安全，防范旅客信息在传输、处理、存储过程中被泄露或篡改等的安全解决方案。

医疗健康数据安全。面向疾病预防控制信息系统、医院信息系统和数据库安全保障支撑，打通卫生健康领域数据壁垒，确保数据访问安全及第三方数据交换中用户隐私、临床、科研和综合管理信息等重要数据安全的解决方案。

商用密码应用。针对商用密码在数据传输加密、数据存储加密、大数据加密、数据接口安全等业务场景应用，在密码设备、加密计算、加密搜索、数据全生命周期管控、接口防护等方面的安全解决方案。

二、数字化应用场景安全方向

（四）车联网安全。面向在线升级（OTA）、远程诊断监控、自动驾驶、车路协同、智慧交通等典型场景，针对智能驾驶系统、联网关键设备、网络基础设施、车联网服务平台等网络安全需求，在轻量化防护、安全认证、数据合规、威胁监测、应急处置、检测评估等方面的安全解决方案。

专栏4　车联网安全重点方向
在线升级（OTA）安全。面向汽车动力/电池系统、底盘系统、车身

系统等 OTA 升级场景网络安全需求，在 OTA 升级服务全过程安全监测和应急响应，以及 OTA 安全检测等方面的解决方案。

车辆远程诊断监控安全。结合车联网远程诊断、远程控制、远程监测等场景安全需求，在安全认证、“云-管-端”一体化协同防护等方面的安全解决方案。

车联网 C-V2X 通信安全。面向车云、车车、车路、车设备通信安全需求，在重点城市、高速公路、园区码头等应用场景下，汽车、联网设施安全认证及通信安全保障等方面的解决方案。

（五）物联网安全。面向智能家居、智能抄表、零售服务、智能安防、智能穿戴设备等典型场景应用，在物联网终端设备及固件安全威胁监测、固移融合物联网安全接入、异构物联网端到端安全防护、物联网平台安全防护等方面的安全解决方案。

专栏 5　物联网安全重点方向

智慧家居安全。面向智能家电、智能照明、智能安防监控、新型穿戴设备、服务机器人等场景网络安全需求，在媒体框架安全防护、远程控制、测试验证、设备资源共享协同等方面的安全解决方案。

水利感知网安全。结合智慧水利感知网等安全需求，在传感器芯片、嵌入式加密、物联网网关、物联网平台安全保障，强化网络攻击监测等方面的安全解决方案。

智慧应急物联网安全。围绕安全生产监管、城市安全管理、自然灾害监测预警及应急处置等过程中接入的物联网设备暴露面大、认证方式单一、联网协议复杂、技术标准不统一等现状，在物联网终端认证、安全传输、信息利用、威胁综合监测等方面的网络安全解决方案。

（六）智慧城市安全。适配智慧城市政务、交通、能源、制造、教育、医疗等业务场景，构建网络安全防御能力集群、智慧

城市安全大脑，实现网络安全感知、分析、响应、决策能力提升，大规模临时组网安全能力快速部署，以及城市安全运行保障等的安全解决方案。

专栏6　智慧城市安全重点方向

智慧政务安全。面向电子证照、电子合同、电子签章、电子发票、电子档案等政务服务一网通办场景安全需求，在促进政府资源优化配置和数据流动等方面的安全解决方案。

智慧社区安全。面向车辆管理、物业管理、社区服务、应急救援救护、智慧养老等场景网络安全需求，在促进政务服务平台、社区感知设施和家庭终端联动，提升社区管理数字化方面的安全解决方案。

智网融合安全。围绕“5G+”智慧交通、智慧医疗、应急通信等融合应用场景，在服务城市网络基础设施安全保障，提升实时感知、精准研判、快速处置水平等方面的安全解决方案。

城市应急通信。面向城市大震大灾等灾害场景，在紧急构建集无线通信、卫星通信、边缘计算等融合通信网络，建设一体化安全防护设备和边缘安全分析系统，实现应急组网的网络安全解决方案。

三、基础安全能力提升方向

（七）网络安全共性技术。以促进公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域网络安全能力为目标，面向关键软硬件安全，在基础技术、工具、协议等方面的创新攻关成果，面向传统防护类、检测类、分析类网络安全产品，在能力集约化、智能化、精益化等方面的优化升级，以及面向网络开放互联、边界模糊、暴露面扩大等共性问题，在强化网络安全架构内生、自适应发展等方面的安全解决方案。

（八）网络安全创新服务。提供安全防护一体化，安全托管、安全咨询、安全运营等安全服务专业化，安全能力自动化、流程化、工具化，威胁情报精准化、智能化的公共服务平台。提供网络安全基础知识库、底层引擎、网络仿真环境、安全孪生试验床等的共性基础支撑平台。为重要行业领域提供网络资产测绘、漏洞挖掘、监测预警、检测评估、应急处置、态势感知、信息共享、攻击溯源等的专业服务平台。

专栏7　网络安全服务创新重点方向

电信网络安全。面向基础通信网络、大型互联网平台网络安全需求，基于网络侧木马病毒、移动恶意程序和高级持续性威胁等监测处置技术，实现网络资产测绘、监测预警、应急处置等的安全解决方案。

电力系统安全。适配电网侧调度控制系统、配电监控系统、电源侧各类型电厂监控系统及虚拟电厂、新型储能、用电侧负荷聚合平台业务发展，在网络安全防护体系结构、典型场景防护策略、安全支撑系统平台等方面的安全解决方案。

水利系统安全。面向水利设施和控制系统，在计算设备、网络隔离、基线管理、威胁监测、漏洞防护、应急处置，以及网络空间拓扑绘制、资产智能测绘、网络安全影响建模等方面的安全解决方案。

广播电视专网安全。面向广播电视专网系统，在网络流量分析、网络攻击监测发现、资产和漏洞发现管理、威胁预警管理等方面的安全解决方案。

金融网络安全。围绕金融核心业务，面向银行、证券、保险等金融信息系统，建立应对数字化转型的网络安全运营体系，在网络安全靶场、威胁情报关联分析、资产测绘及漏洞处置机制等方面的安全解决方案。

（九）网络安全“高精尖”技术创新平台。结合前沿性、创新性、先导性的重大网络安全技术理念，汇聚产学研用等创新资源，加快实现网络安全“高精尖”技术创新融合，打造具备核心技术攻关、产业化应用推广等关键环节协同创新环境和载体的网络安全技术创新或试点示范区，打造产融合作的网络安全产业生态优化解决方案。

附件 2

网络安全技术应用试点示范申报书

网络安全技术应用试点示范申报书

项 目 名 称：_____

申 报 类 别：_____

申 报 方 向：_____

牵头申报单位：_____（ 加盖单位公章 ）_____

推 荐 单 位：_____

申 报 日 期：_____年_____月_____日

工业和信息化部编制

填 报 说 明

1.申报材料应客观、真实，不得弄虚作假，不涉及国家秘密，申报主体对所提交申报材料的真实性负责。

2.本申报书除表格外，其他各项填报要求：A4 幅面编辑,正文应采用仿宋_GB2312 四号字，1.5 倍行间距，两端对齐，一级标题三号黑体，二级标题为四号楷体_GB2312 加粗。

3.有关项目页面不够时，可在电子版中扩充，用 A4 纸打印。

4.将申报书同附件材料按顺序打印/复印，装订成册，并按要求签字、加盖单位公章及骑缝章。

5.多家单位联合申报的项目,每个申报单位均需提供单独的责任声明及信用信息报告。

一、申报单位和项目基本信息

<table>
<tr><td colspan="4">（一）申报单位基本信息</td></tr>
<tr><td>牵头申报单位</td><td colspan="3">（全称）</td></tr>
<tr><td>组织机构代码/
三证合一码</td><td></td><td>成立时间</td><td></td></tr>
<tr><td>通讯地址</td><td></td><td>注册资本
（万元）</td><td></td></tr>
<tr><td>联系人</td><td></td><td>联系电话</td><td></td></tr>
<tr><td>传真</td><td></td><td>邮箱</td><td></td></tr>
<tr><td>上年销售额
（万元）</td><td></td><td>上年利润额
（万元）</td><td></td></tr>
<tr><td>单位性质</td><td colspan="3">☐事业单位 ☐国有企业 ☐民营企业 ☐合资企业 ☐国有控股企业
☐国有参股企业 ☐其他（请注明）：_____</td></tr>
<tr><td rowspan="3">联合申报单位</td><td>单位名称</td><td>单位性质</td><td>组织机构代码/
三证合一码</td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td>申报单位
简介</td><td colspan="3">（发展历程、经营管理状况、主营业务、研发创新情况、资源整合共享能力、技术成果转化能力等方面情况，不超过400字）</td></tr>
</table>

（二）项目基本信息			
项目名称			
项目所在地			
网址	（已建网站的填写）		
项目负责人		职务/职称	
项目投资金额（万元）	（综合性项目仅限网络安全相关部分）		
项目应用行业	目前已应用行业： □公共通信和信息服务 □水利 □医疗 □应急 □金融 □广电 □能源 □交通 □航空航天 □其他_____		
	将来可应用推广行业： □公共通信和信息服务 □水利 □医疗 □应急 □金融 □广电 □能源 □交通 □航空航天 □其他_____		
平台已注册用户总数		平台用户类型	
项目概述	（简要阐述项目建设目标、主要内容、投资概况、研发和推广应用等有关情况，不超过400字）		

真实性承诺	我单位申报的所有材料，均真实、完整，如有不实，愿承担相应的责任。 法定代表人签章： 牵头申报单位公章： 年　月　日 法定代表人签章： 联合申报单位公章： 年　月　日 法定代表人签章： 联合申报单位公章： 年　月　日
推荐单位及意见	（如有推荐单位，推荐单位填写意见） 推荐单位盖章： 年　月　日

二、申报项目详细介绍

（一）项目建设情况

1.项目建设背景和意义

（联合申报的项目需说明联合申报的理由。）

2.项目建设目标和主要任务

3.项目建设内容

（包括项目主要功能、主要技术指标、技术路线、难点和创新点以及出台的配套管理机制等。重点说明项目采用的关键技术方案，包括项目功能架构图、项目采取的技术方案或实施流程，以及后续技术升级和动态更新方案。）

4.项目负责人及项目团队实力

（项目负责人资质及工作经验、项目主要参与单位及其分工、项目主要参加人员情况和项目经验等情况。）

（二）项目运行情况

1.项目运行状态

（项目运行的详细情况，如应对网络安全威胁的相关经历，服务用户规模、行业、区域等。）

2.项目已产生的效益

（包括社会效益、经济效益等。）

3.项目的可推广性

（示范意义及推广的价值、可行性和范围，已开展应用推广情况。）

（三）相关附件

（应先列出文件清单，后附文件复印件，文件电子版与纸质版应保持一致。）

1.申报单位相关证明材料及清单

（申报单位相关荣誉证明材料，如高新技术企业、重点实验室、工程实验室、科技类奖励等；研发能力证明材料，如获得专利、标准、知识产权等；主营业务最近一年的收入证明材料，如财务审计报告、纳税证明等；申报单位入驻（拟入驻）国家网络安全产业园区的情况。）

2.申报项目相关证明材料及清单

（项目的系统架构、关键技术等获得的知识产权证明，如专利、标准、软件著作权；政府扶持及项目获奖情况；核心技术创新能力证明，如自主技术应用、自主基础软硬件环境等；推广效果应用证明，如经应用单位盖章的使用证明；社会影响力证明，如为重点行业部门和地方政府提供管理支撑、疫情防控、重大活动保障相关证明；服务能力证明，如服务资质证明、合作资源相关情况等。）

3.申报主体责任声明及信用信息报告

（申报单位责任声明，模板附后；申报单位信用信息报告，获取方式：在“信用中国”官方网站首页右上方“信用信息”搜索框中，输入申报单位名称或统一社会信用代码。多家单位联合申报的项目,每个申报单位均需提供单独的责任声明及信用信息报告。）

申报主体责任声明

根据《关于开展网络安全技术应用试点示范工作的通知》要求，我单位提交了网络安全技术应用试点示范申报书。

现就有关情况声明如下：

1.我单位对申报材料的真实性负责。

2.我单位在申报过程中所涉及的内容和程序皆符合国家有关法律法规及相关产业政策要求。

3.我单位对所提交的内容负有保密责任，按照国家相关保密规定，所提交的项目内容未涉及国家秘密、个人信息和其他敏感信息。

4.我单位申报所填写的相关文字和图片已经审核，确认无误。

我单位对违反上述声明导致的后果承担全部法律责任。

法定代表人：

单位（盖章）

年　　月　　日

网络安全技术应用试点示范申报书

（网络安全“高精尖”技术创新平台方向）

申 报 地 区：_____

牵头申报单位：_____（ 加盖单位公章 ）_____

推 荐 单 位：_____

申 报 日 期：_____年_____月_____日

工业和信息化部编制

填 报 说 明

1.申报材料应客观、真实，不得弄虚作假，不涉及国家秘密，申报主体对所提交申报材料的真实性负责。

2.本申报书除表格外，其他各项填报要求：A4 幅面编辑,正文应采用仿宋_GB2312 四号字，1.5 倍行间距，两端对齐，一级标题三号黑体，二级标题为四号楷体_GB2312 加粗。

3.有关项目页面不够时，可在电子版中扩充，用 A4 纸打印。

4.将申报书同附件材料按顺序打印/复印，装订成册，并按要求签字、加盖单位公章及骑缝章。

5.多家单位联合申报的项目,每个申报单位均需提供单独的责任声明及信用信息报告。

一、申报创新区基本信息

<table>
<tr><td colspan="5">（一）申报城市基本信息</td></tr>
<tr><td>申报城市及
所在省</td><td colspan="4"></td></tr>
<tr><td>申报主体</td><td colspan="4"></td></tr>
<tr><td>负责人</td><td colspan="2"></td><td>职务</td><td></td></tr>
<tr><td>联系人</td><td colspan="2"></td><td>联系电话</td><td></td></tr>
<tr><td>传真</td><td colspan="2"></td><td>邮箱</td><td></td></tr>
<tr><td>通讯地址</td><td colspan="4"></td></tr>
<tr><td rowspan="3">联合申报单位</td><td colspan="2">单位名称</td><td>单位性质</td><td>组织机构代码/
三证合一码</td></tr>
<tr><td colspan="2"></td><td></td><td></td></tr>
<tr><td colspan="2"></td><td></td><td></td></tr>
<tr><td>申报城市
基本情况</td><td colspan="4">（主要包括城市区位、辖区、人口等基本情况，网络安全技术、产业发展水平情况等。重点包括上一年度统计数据，不超过400字）</td></tr>
</table>

（二）创新区概况	
名　称	
所在地	
技术方向	
入驻单位	□网络安全企业____家，其中，主板/创业板____家；科创板____家；新三板____家 □科研机构____家 □高校____家，其中，设立网络安全学院____家；设置网络安全专业____家 □用户单位____家 □投资机构____家 □其他单位____家，单位类型_____
业务规模	□占地规模_____平方米 □收入规模_____万元 □人员规模_____人，其中科研/技术人员_____人
现有基础条件及优势分析	（简述网络安全“高精尖”技术创新区有关情况，包括网络安全技术产业发展相关政策情况；网络安全企业、科研机构等发展情况；相关高校网络安全学科学院建设和网络安全人才培养情况；创新区运营载体情况等。不超过400字）

真实性承诺	我单位申报的所有材料，均真实、完整，如有不实，愿承担相应的责任。 法定代表人签章： 牵头申报单位公章： 年　月　日 法定代表人签章： 联合申报单位公章： 年　月　日 法定代表人签章： 联合申报单位公章： 年　月　日
推荐单位及意见	（如有推荐单位，推荐单位填写意见） 推荐单位盖章： 年　月　日

二、申报创新区详细介绍

（一）创新区建设情况

1.建设背景和意义

2.建设目标、主要任务和建设内容

（二）运行情况

1.运行状态

2.产生效益

3.示范意义

（三）相关附件

（应先列出文件清单，后附文件复印件，文件电子版与纸质版应保持一致。）

1.创新区相关证明材料及清单

（包括创新区有关政策材料，如促进“高精尖”网络安全技术创新的奖励措施；针对相关单位的财政、税收优惠措施；已发布的促进网络安全产业发展规划等。）

2.入驻企业相关证明材料及清单

（申报创新区相关荣誉证明材料，如入驻单位高新技术企业、重点实验室、工程实验室、科技类奖励等；入驻单位研发能力证明材料，如获得专利、标准、知识产权等；入驻单位主营业务最近一年的收入证明材料，如财务审计报告、纳税证明等。）

3.申报主体责任声明及信用信息报告

（申报单位责任声明，模板附后；申报单位信用信息报告，获取方式：在“信用中国”官方网站首页右上方“信用信息”搜索框中，输入申报单位名称或统一社会信用代码。多家单位联合申报的项目,每个申报单位均需提供单独的责任声明及信用信息报告。）

申报主体责任声明

根据《关于开展网络安全技术应用试点示范工作的通知》要求，我单位提交了网络安全技术应用试点示范申报书。

现就有关情况声明如下：

1.我单位对申报材料的真实性负责。

2.我单位在申报过程中所涉及的内容和程序皆符合国家有关法律法规及相关产业政策要求。

3.我单位对所提交的内容负有保密责任，按照国家相关保密规定，所提交的项目内容未涉及国家秘密、个人信息和其他敏感信息。

4.我单位申报所填写的相关文字和图片已经审核，确认无误。

我单位对违反上述声明导致的后果承担全部法律责任。

法定代表人：

单位（盖章）

年　　月　　日

附件 3

推荐项目汇总表

填表单位（盖章）：　　填表人：　　联系方式：

序号	申报方向	项目名称	申报单位 （牵头单位排首位）	联系人	联系方式 （手机与邮箱）
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					

注：各申报主体项目数量不得超过规定的上限。