

上海市经济和信息化委员会文件

沪经信软〔2026〕481号

上海市经济信息化委关于开展 2026 年网络安全产业创新 攻关目录成果征集工作的通知

有关单位：

为推进网络安全产业创新升级，深度发掘产业优秀成果，我委组织编制 2026 年上海市网络安全产业创新攻关目录，现公开征集各类创新成果。

一、重点支持方向

本次重点支持以下 14 个方向（具体内容见附件 1）：

（一）人工智能技术创新：人工智能赋能安全、AI 与智能体安全防护

（二）基础技术创新：量子密码安全、软件供应链安全、数据流通安全、数字身份安全、智算云安全

（三）应用技术创新：智能汽车安全、低空安全、物联网安全、智能工控安全、网络安全防护有效性验证、安全评测与合规智能化、网络安全保险

二、申报条件

（一）申报主体：在中华人民共和国境内注册、具有独立民事责任能力的单位，具备良好的网络安全技术研发与融合创新能力。

（二）申报成果：2024年1月1日后研发形成的网络安全相关技术、产品或服务，需满足以下要求：

1. 具有自主知识产权，创新性、独占性突出；
2. 整体或核心技术水平处于行业领先地位；
3. 具备市场竞争力或产业化应用潜力；
4. 多单位联合研发成果由第一完成单位申报；
5. 同一申报单位申报2个成果的，每个成果需单独填报。

三、申报程序

（一）材料提交

1. 提交时间：2026年9月24日前
2. 提交方式：申报书电子版（含所有附件）发送至邮箱 zhenbiao.wang@sicsi.org.cn

（二）评审流程

1. 资质审核：对申报材料进行完整性、合规性审查
2. 现场评审：实施产品演示及答辩环节
3. 结果公示：2026年第四季度发布最终目录

四、支持措施

- (一) 支持符合条件的研发项目申请相关软件政策
- (二) 推荐参与本市重点行业场景应用
- (三) 提供企业落地支持、人才引进、融资对接等配套服务

五、联系方式

联系人：周雪静、汪涵

联系电话：17826856604； 021-23117605

(工作日 9:00-18:00)

附件：1. 2026 年上海市网络安全产业创新攻关目录成果方向
2. 2026 年上海市网络安全产业创新攻关目录成果申报书

上海市经济和信息化委员会
2026 年 8 月 10 日

附件 1

2026 年上海市网络安全产业创新攻关目录成果方向

类别	序号	攻关方向	内容简述
人工智能技术创新	1	人工智能赋能安全	基于 AI 技术重构新型网络安全防御能力，包括（但不限于）AI、Agentic AI 驱动的智能漏洞挖掘、自动化攻防、网络攻击智能检测、威胁情报分析、深度伪造治理、安全运营（SOC）等成果，通过网络安全集成 AI、AI 智能涌现构建网络安全体系，有效应对人工智能时代网络攻击智能化、大规模网络攻击频繁、网络攻击隐蔽性提高等风险问题。
	2	AI 与智能体安全防护	面向大模型（大语言模型、多模态大模型、推理大模型等）及智能体全生命周期安全需求，构建内生及护栏式安全防护框架。包括（但不限于）覆盖大模型训练/精调/推理、部署、运营等关键阶段，构建缓释训练数据安全、模型窃取及篡改、对抗样本攻击、投毒攻击、自身脆弱性等风险的大模型安全技术及解决方案；针对智能体、插件、调用工具等实现全方位安全管控。
基础技术创新	3	量子密码安全	针对量子计算技术发展对于现代密码技术带来的安全威胁，构建量子信息技术和信息安全技术融合应用的网络安全量子解决方案，包括（但不限于）应对 HNDL 等网络安全风险的抗量子计算密码（QRC）或后量子密码（PQC）算法，量子密钥分发设备、接收量子密钥并对网络传输信息进行加密的量子安全网关等量子安全应用；以及在“AI+密码”、密码智能生成等方面实现的技术创新。
	4	软件供应链安全	针对第三方开发人员、开源代码库、智能体 Skill 的供应链安全问题，构建供应链的透明、可追溯和安全可控能力，包括（但不限于）利用自动化、智能化、平台化技术，实现安全、开发和运营流程融合，对软件开发、开源软件、源代码、AI 组件、智能体 Skill 等进行全面安全检测及防护的安全技术体系，如 DevSecOps 安全解决方案、软件成分分析、应用安全测试、源代码安全、代码风险平台、AIBOM 等技术、产品和服务；覆盖从供应商、资产测绘到漏洞修复的全生命周期态势感知平台，如 ASPM 解决方案等。
	5	数据流通安全	面向制造业、互联网、政务、金融等重点行业数据流通需求，围绕数据治理自动化、个人信息保护等需求，构建数据流通安全解决方案，包括（但不限于）数据加密、匿名化、差分隐私、隐私计算、联合计算及建模算法、多源数据融合、零信任安全访问、区块链、数据沙箱、API 风险检测等技术。针对语料数据采集与流转环节，建立安全可信平台，包括（但不限于）跨域数据血缘追踪、RAG 安全等技术。实现海量数据在开放流通环境下的安全和隐私保护。

类别	序号	攻关方向	内容简述
应用技术创新	6	数字身份安全	针对智能时代数字身份管理需求,构建新一代数字身份认证技术,包括(但不限于)身份和访问管理(IAM)、去中心化身份(DID)与可验证凭证(VC)、机器身份和访问管理(MIM)、身份威胁检测和响应(ITDR)、低功耗密码技术及应用、多场景适用的物联网安全通信协议、云和边缘计算多维适配的可信身份安全计算环境,以及智能体身份凭证管理、A2A跨智能体身份管控、非人类身份(NHI)访问控制安全等技术。
	7	智算云安全	针对云发展应用趋势,构建云原生安全能力,包括容器安全、微服务安全、微隔离、AI安全网关等有关技术和产品,采用云原生架构、提供新的部署模式的安全服务体系。针对智算云的管理需求,构建智算云平台安全管理服务产品,包括(但不限于)增强应用、平台、算力中心、多云管控等多维度稳定性,提供故障检测、故障自愈、渗透测试的产品及解决方案,以及智算云数据安全治理工具与平台等。
	8	智能汽车安全	针对智能网联汽车发展的安全需求,构建融合终端安全、通讯安全、数据安全的专业化安全技术体系,包括(但不限于)传感器异常数据识别技术、CAN总线认证加密技术、车载IDPS技术、V2X通信安全防护技术、智驾模型对抗攻击防御、车联网移动APP安全防护与检测技术、威胁分析与风险评估(TARA)、车辆安全运营中心(VSOC)、软硬件协同安全隔离技术。全面护航智能网联汽车产业的创新发展。
	9	低空安全	针对低空经济发展的安全需求,围绕低空适飞区、重点基础设施和关键设备,打造空天一体的安全防护体系,包括(但不限于)低空通信网络安全,卫星互联网安全,无人机、飞行器等低空设备安全管控、网络安全和数据传输加密、地面起降基础设施物理与环境安全等,有效应对信号劫持、敏感数据泄露、敏感空域入侵等风险,保障低空物流、应急救援等低空场景的安全和连续性。
应用技术创新	10	物联网安全	面向物联网数据传输安全、个人信息保护以及防范RFID系统威胁等需求,构建物联网安全解决方案,包括(但不限于)数据传输安全与加密通信、身份认证和授权、固件安全、智能终端软件安全执行环境SEE、网络监控与异常行为检测、物理安全措施、漏洞管理、安全韧性等技术。
	11	智能工控安全	面向工业企业数字化、网络化和智能化发展需求,构建以工业互联网安全分类分级管理为核心的综合防护安全方案,通过转变传统以单点防护为核心的防御思路,形成与行业业务流程、网络架构、数据特点、控制工艺等紧密结合的融合防御机制。聚焦智能工厂、工业机器人、远程运维等新型场景,推出面向工业设备、控制系统和机器人终端的安全解决方案。

类别	序号	攻关方向	内容简述
	12	网络安全防护有效性验证	面向网络安全防护有效性验证需求，优化企业防护配置和事件响应流程，提升企业网络安全建设效果，包括（但不限于）通过单点评估、暴露面与后渗透评估、安全靶场等方式开展渗透测试、攻防演练、漏洞扫描、安全检查、安全防护能力持续评估等服务。
	13	安全评测与合规智能化	面向数据流通安全合规监管需求，构建数据合规治理的安全管理架构，包括但不限于数据安全风险检测和评估工具、数据安全合规工具/平台、个人信息保护自评估服务平台、跨境数据审查和合规服务、数据安全合规情报服务等。针对生成式人工智能服务、大模型、智能体安全合规监管要求，提供 AI 安全检测平台、大模型内容安全合规检测工具、AIGC 安全评测服务等。
	14	网络安全保险	面向企业对冲网络安全残余风险所需的保险工具和服务需求，构建事前预防、事中防护、事后补偿的全周期网络安全保险服务保障模式，涵盖针对不同业态的网络安全保险解决方案，以及面向网络安全保险业态的新型网络安全产品服务，包括（但不限于）云网络安全保险、智能网联汽车网络安全保险、人工智能数据安全保险等。

附件 2

2026 年上海市网络安全产业创新攻关目录成果申报书

一、基本信息

(一) 申报主体信息			
主体名称			
机构代码/ 三证合一码		成立时间	
通讯地址		注册资本 (万元)	
联系人姓名		移动电话	
邮箱		单位性质	
上年销售额 (万元)		上年利润额 (万元)	
主体简介	(发展历程、主营业务、经营管理状况, 网络安全方面已开展的 业务及有关工作情况、所获的有关奖项等, 不超过 400 字)		
(二) 申报成果信息			
申报方向序号及 名称			
成果形式	☐ 技术知识产权 ☐ 产品 ☐ 服务 其他_____	成果名称	
已投资金额 (万元)		所获认定 或奖项	
成果概述	(简要阐述成果建设内容、实施情况, 与申报方向有关的技术创 新特点, 不超过 400 字)		

应用情况	(简要阐述成果应用情况、解决的问题及具体成效, 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: 申报单位公章: 年 月 日

二、成果详细介绍

(一) 成果研发建设情况

1. 背景和意义 (开展相关研发攻关的背景、目的、意义、目标等)
2. 研发建设进度 (按时间简要介绍立项、研发、建设等情况)
3. 实施方案及创新点 (主要技术或模式实现路线简介, 围绕攻关目录方向实现的创新点、关键性能指标)
4. 主要团队介绍 (主要牵头人资质及工作经验, 主要参与单位及分工, 主要参与人员情况)

(二) 成果应用及推广价值

1. 成果应用情况 (介绍成果目前已应用点位、范围、用户规模等应用情况)
2. 示范意义及推广价值 (简析成果市场定位及竞争力、示范及推广价值)

3. 申报成果所取得的计算机软件著作权等知识产权，以及近一年度签署的有效合同等证明材料（需含真实销售价格信息）

（三）相关附件

列出文件清单，后附文件复印件。包括但不限于申报主体的有关荣誉、研发能力、收入证明材料；申报成果所获的奖励情况、技术创新能力、应用情况；相关产品市场销售情况证明。

