

上海市经济和信息化委员会文件

沪经信软〔2021〕543号

上海市经济信息化委关于开展 2021 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：

为推进本市网络安全产业发展，建设网络安全产业创新高地，我委组织编制了“2021 年上海市网络安全产业创新攻关目录”（以下简称目录），现就目录方向公开征集创新成果。有关事项通知如下。

一、征集方向

本次目录征集的创新成果，主要涉及基础技术、应用技术和服务业态创新三个类别，零信任网络访问、隐私计算、新一代数字身份认证、人工智能安全、数据流通安全、智能工控安全、智能汽车安全、金融科技安全、网络安全保险、网络安全监管与合规智能化十个方向。具体内容见附件 1。

二、申报要求

(一) 主体资格。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，具有较好的网络安全技术研发，融合创新能力。

(二) 成果要求。申报成果（技术、产品或服务）应形成于 2019 年及以后，创新性、独占性较好，拥有自主知识产权，整体或核心技术水平领先，并具有较好的市场竞争优势或产业化潜力。申报成果为两个或两个以上单位研发的，由第一完成单位提出申报。

(三) 申报方式。单一申报主体可申报多个目录方向成果，每个需单独填报《上海市 2021 年网络安全产业创新攻关目录成果申报书》（见附件 2），并于 2021 年 8 月 1 日前将申报书一式三份及电子版报市经济信息化委软件和信息服务业处。经形式审查合格后，予以受理。

三、工作流程

(一) 组织评审。市经济信息化委将组织专业机构对有关成果进行必要的技术检测或认定，依托行业专家对申报主体及成果材料进行现场评审和答辩，形成评审意见。市经济信息化委根据意见进行审核排序。

(二) 结果公示。拟纳入目录成果的申报主体及创新成果将在市经济信息化委门户网站、微信、微博等进行公示。

(三) 支持推广。公示无异议的，市经济信息化委将编制目录成果集进行宣传，在开放场景、创新成果应用方面予以重点推广，并通过促进产业高质量发展专项资金等形式对有关项目予以支持。对在本市落地发展的创新申报主体，将在落地、人才、融资等方面加强扶持和服务。

四、联系方式

- (一) 联系人：李宁、吴昊
- (二) 电话：13671522679、18918883983
- (三) 地址：世博村路 300 号 5 号楼 711 室
- (四) 邮箱：amy.li@sicsi.org.cn

- 附件：1. 上海市 2021 年网络安全产业创新攻关目录
2. 上海市 2021 年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
2021 年 7 月 9 日

附件 1

上海市 2021 年网络安全产业创新攻关目录

类别	序号	攻关方向	内容简述
基础 技术 创新	1	零信任网络访问	针对可扩展的混合 IT 环境下平台、业务、用户、终端所呈现的多样化趋势和安全需求，构建零信任网络安全访问架构，包括（但不限于）支持持续认证、细粒度的上下文访问控制、信令分离等防御理念的软件定义边界（SDP）；业务场景动态适配、具备灵活智能策略体系的身份与访问管理系统；云原生微隔离、API 对接微隔离、主机代理微隔离等微隔离技术。实现业务系统动态访问控制和授权，有效实现可持续的零信任安全防护体系。
	2	隐私计算	针对数据资产作为生产要素带来的隐私计算和安全保障需求，构建体系化的隐私计算及安全保障架构，包括（但不限于）隐私计算模型框架、隐私保护场景适应的密码体系应用、隐私控制与抗大数据分析的隐私保护技术、数据敏感性量化、恶意收集数据行为检测和准确溯源、基于信息隐藏的隐私保护技术以及支持高并发的隐私保护服务架构、场景动态适应的隐私动态度量与隐私保护效果评估技术等。有效解决数字化转型下数据安全问题的。
	3	新一代数字身份认证	针对万物智能互联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）器件级硬件指纹技术、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，面向万物智能互联的数字身份安全体系和数字信任体系等。有效应对万物智能互联时代数字身份管理存在的设备数量巨大、智能硬件算力参差不齐、基础计算架构碎片化、身份仿冒和伪造泛滥等安全挑战。
	4	人工智能安全	针对人工智能应用的新型网络攻击检测和防护需求，构建基于人工智能的安全评估与防御技术能力，包括（但不限于）动态可扩展的网络安全大脑、网络攻击的智能检测与效果研判、漏洞智能化挖掘、基于人工智能模型的脆弱性分析。有效应对人工智能时代网络攻击趋于智能化、大规模网络攻击频繁、网络攻击隐蔽性提高等问题。
应用 技术 创新	5	数据流通安全	面向互联网、政务、金融、大数据等重点行业数据流通需求，构建安全合规的数据流通体系，包括（但不限于）安全多方计算、区块链、联邦学习、可信执行环境、开源

			代码供应链安全等技术。实现海量数据在开放流通环境下的安全和隐私，有效支撑数据要素市场的构建。
	6	智能工控安全	针对各类工业企业数字化、网络化和智能化发展需求，构建“5G+AI+工业互联网”下的智能工控安全技术能力，包括（但不限于）工业云平台可信安全环境、安全工业通信协议、工业控制系统漏洞发现与态势感知、CPS 供应链安全体系等。有效保障传统产业数字化转型安全。
	7	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、数据安全的专业化和轻量级的安全技术体系，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、车联网移动 APP 安全防护与检测技术等。全面护航智能网联汽车产业的创新发展。
	8	金融科技安全	针对金融科技发展中的各类安全风险，构建促进金融业务创新发展、满足合规监管需要的安全技术体系，包括（但不限于）区块链安全技术、数字货币安全技术、数字反欺诈技术、数据取证技术、金融创新监管沙箱技术等。
服务业态创新	9	网络安全保险	面向各类组织对冲网络安全残余风险所需的保险工具和服务需求，推动网络安全技术产品的高质量和广覆盖，包括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。
	10	网络安全监管与合规智能化	面向国内外网络安全合规监管需求，以智能化技术平台赋能网络安全领域的监管、合规和治理，推动全行业网络安全能力的提升。包括网络安全和数据安全的检测和评估工具、网络安全等保合规工具/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、网络安全合规情报服务等。

附件 2

上海市 2021 年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	<input type="checkbox"/> 技术知识产权 <input type="checkbox"/> 产品 <input type="checkbox"/> 服务 <input type="checkbox"/> 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	<p>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。</p> <p style="text-align: center;">法定代表人签章: 申报单位公章: 年 月 日</p>

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)
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)

(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有关荣誉、研发能力、收入证明材料; 申报成果所取得的知识产权、获奖情况、技术创新能力、应用情况等证明材料)