山东省教育厅网络安全和信息化领导小组办公室

鲁教网信办函〔2026〕6号

山东省教育厅网络安全和信息化领导小组办公室关于转发《省委网信办 省大数据局关于开展2026年山东省“人工智能+网络安全”揭榜挂帅工作的通知》的通知

各高等学校:

现将《省委网信办 省大数据局关于开展2026年山东省“人工智能+网络安全”揭榜挂帅工作的通知》(以下简称《通知》)转发给你们，请有意申报的高校按照文件要求，结合实际认真编制《2026年山东省“人工智能+网络安全”揭榜挂帅项目申报书》(《通知》附件2)，于4月24日下班前通过教育通用工作平台(https://gzpt.sdei.edu.cn//sjbsrw/?465307)报送盖章扫描件和电子版。相关材料电子版也可在此平台下载。

联系人：王琛、徐长棣，0531-51793975、51793718。

山东省教育厅

网络安全和信息化领导小组办公室

2026年4月7日

中共山东省委网络安全和信息化委员会办公室
山　东　省　大　数　据　局

鲁网办通字〔2026〕12号

关于开展2026年山东省“人工智能＋网络安全”揭榜挂帅工作的通知

各市党委网信办、市大数据局，省有关部门（单位）：

根据《关于加快人工智能赋能重点领域高质量发展的推进方案》（鲁政办字〔2025〕48号），为深化我省人工智能与网络安全融合赋能，统筹推进新型网络安全保障体系建设，省委网信办、省大数据局现组织开展2026年山东省“人工智能＋网络安全”揭榜挂帅工作。有关事项如下：

一、工作目标

聚焦网络安全保障体系以及相关前沿技术应用等重点方向，着力推进安全资产管理、威胁监测、漏洞治理、智能安全运营、供应链安全与人工智能技术的融合创新。围绕人工

智能网络安全融合赋能，通过揭榜挂帅机制，遴选一批具备技术能力、实践成果与发展潜力的单位及团队，形成一批可复制、可推广、可示范的应用成果，构建一批在智能感知、主动防御、精准研判与协同响应方面具有代表性的先进示范案例。

二、榜单内容

榜单项目分为理论研究类与实践探索类（详见附件1）。理论研究类重点围绕以下方向开展，**一是**网络安全基础要素智能管理方向，如多元异构环境下安全资产智能管理、敏感数据动态识别与智能管理等；**二是**网络安全威胁监测与主动防御方向，如多源威胁数据的监测与响应、漏洞治理与恶意软件主动防御等；**三是**人工智能安全与隐私保护方向，如人工智能隐私保护计算的密码技术、人工智能技术应用中的安全风险与治理等。要求系统开展理论研究与路径设计，形成兼具理论深度与实践指导价值的研究报告，为政策制定与产业发展提供支撑。实践探索类重点围绕以下方向开展，**一是**保障能力建设方向，如安全资产智能管理、数据智能安全监管、数据安全与可信共享等；**二是**威胁监测分析预警与主动防御方向，如网络安全智能态势感知、边界主动防御、智能渗透测试、全域智能安全运营与内生防护等；**三是**供应链安全风险管理方向，如供应链安全风险管理等；**四是**人工智能网络安全治理方向，如工业互联网安全、网络安全保险等。

要求推动技术创新、场景应用与模式探索，形成成效显著、具备示范意义的实践案例。

三、申报条件

揭榜单位须满足以下基本条件：

（一）为具备独立法人资格的企事业单位，并在数据领域具有较强的研究创新能力。鼓励揭榜单位联合省内外具备相应能力的单位组成联合体申报。联合体成员总数不超过3家，且各方应具备良好的前期合作基础。同一单位最多牵头或参与揭榜项目原则上不超过2个。

（二）具备稳定的研究团队，能够为项目实施提供必需的场地、人员、经费及技术保障。近三年内无重大违法违规记录，未被列入失信被执行人名单或经营异常名录，发生较大或有影响的网络安全事件的不予参评。无不良行为记录，未被列入经营异常名录。

（三）申报材料应内容真实、重点突出、表述准确，相关内容应拥有自主知识产权。为保障可推广性，要求申报材料应进行脱敏。围绕所申报榜单项目提出明确的任务举措、实施路径与预期成果。其中，理论研究类须至少完成1份研究报告，实践探索类须至少形成1个应用场景或实践案例。

四、组织实施

（一）**申报程序**。各市党委网信办、市大数据局共同负责组织开展本市揭榜挂帅工作。省直单位、省属企业、中央

驻鲁单位等负责本单位和归口管理单位的征集、审核、汇总、推荐、申报工作。每家揭榜单位须结合实际编制《2026年山东省“人工智能＋网络安全”揭榜挂帅项目申报书》（附件2）。各市、各单位汇总材料并进行审核，于2026年4月28日前将汇总材料（盖章文件扫描版和电子版光盘）报送至山东省网络安全和信息化技术中心（以下简称“技术中心”）（地址：经十路20637号文博写字楼二楼；联系方式：李宁宁 任传旭 053151778552，18853192103）。技术中心负责对申报材料完整性、申报内容等进行初审，通过初审的申报项目作为综合评审的备选对象。请各申报单位认真填写申报书，并将电子版发送至邮箱（sdwxjszx@shandong.cn）。

（二）评审与发布。省委网信办、省大数据局将组织专家对通过初审的申报项目开展综合评审，采用现场答辩的方式进行。申报单位项目团队现场介绍项目背景目的、总体目标、主要做法、特色亮点、预期成果和应用成效等内容，时长不超过规定时限；专家围绕项目技术创新性、落地可行性、推广价值、风险应对措施等维度提问，项目团队现场作答。评审专家结合需求代表性、技术创新性、推广价值等维度对申报项目进行综合评定，择优确定揭榜单位名单，并按规定程序予以公布。

五、其他事项

省委网信办、省大数据局将定期督导“揭榜挂帅”项目

进展，并于2026年12月底前组织验收评估，遴选一批优秀创新成果进行宣传推广。对具备复制推广条件的成熟经验，将逐步纳入制度规范，并在全省范围内实施推广。

联系人：省委网信办 韩旭东 张文静 0531—59622118

省大数据局 何同乐 0531—51785063

中共山东省委网络安全和信息化委员会办公室

山东省大数据局

2026年3月25日

附件 1

2026 年山东省“人工智能+网络安全”揭榜挂帅榜单目录

序号	类别	项目名称	拟解决问题	成果形式
1	理论研究类	多元异构环境下安全资产智能管理关键技术研究	研究多元异构数据融合与安全资产自动发现关键技术，分析复杂网络环境下资产动态识别与画像构建机理，构建智能管理关键技术模型，提高安全资产精准识别与动态管理能力。	研究报告
2	理论研究类	多源威胁情报智能分析处置关键技术研究	围绕多源威胁情报分析中的关键问题，研究人工智能在威胁信息融合、异常行为与威胁事件识别、告警关联压缩、攻击实体关系挖掘、攻击路径推演及响应优先级评估中的作用机理，提升威胁发现、风险研判与响应决策能力。	研究报告
3	理论研究类	漏洞与恶意软件主动防御关键技术研究	围绕漏洞与恶意软件威胁防御中的关键问题，研究人工智能在风险精准评估、未知漏洞与异常行为识别、利用及攻击路径分析、告警与处置优先级排序、误报甄别与自动阻断中的作用机理，实现智能化漏洞治理与恶意软件主动防御能力。	研究报告
4	理论研究类	敏感数据智能识别管理关键技术研究	研究多源敏感数据动态识别与分类分级的关键技术机理，分析数据流转实时监控、异常行为研判及智能管理的核心问题，明确全流程防护与智能预警机制的实现路径。	研究报告
5	理论研究类	面向人工智能隐私保护计算的密码技术	研究面向人工智能隐私保护计算的同态加密与安全多方计算关键技术，剖析现有密码技术在人工智能任务中的关键瓶颈及其成因，构造适配卷积神经网络及大语言模型推理的安全计算方案，提升人工智能应用的安全性与计算效率。	研究报告

序号	类别	项目名称	拟解决问题	成果形式
6	理论研究类	人工智能应用安全风险治理机制研究	围绕人工智能应用中的安全风险与治理需求，系统研究算法偏差、数据污染、模型攻击、隐私泄露等风险类型及其形成机理，分析相关风险对社会治理、行业应用和网络安全的影响，探索风险识别、监测预警、分级治理、协同监管与防护机制，为政策制定、标准规范和安全治理体系建设提供支撑。	研究报告
7	实践探索类	安全资产高质量管理体系建设及应用路径探索	围绕安全资产全生命周期管理需求，梳理资产发现、业务关系与风险量化的核心问题，探索高质量管理体系建设的关键环节及智能化应用实施路径，提升安全资产管理的整体化与持续运行能力。	实践案例
8	实践探索类	人工智能驱动的网络安全态势感知关键技术研究	面向网络安全实战应用需求，研究人工智能在网络威胁信息分析、APT 攻击早期发现和态势感知中的应用方法，提升多源安全数据汇聚分析、异常行为识别、风险预警研判和运营支撑能力，探索可推广的应用模式、建设路径与协同机制，为网络安全防护能力提升提供实践支撑。	实践案例
9	实践探索类	人工智能驱动自动化渗透测试应用推广机制与行业适配策略研究	围绕自动化渗透测试实践需求，梳理人工智能在渗透流程化管控、漏洞自动化探测发现中的应用经验，探索主动防御能力建设与人工智能赋能自动化渗透测试的应用推广机制，明确针对各行业的具体适配策略。	实践案例
10	实践探索类	AI 赋能的边界自动防护体系应用示范与推广	围绕互联网边界防护漏防多的痛点需求，解决安全系统恶意访问检出率低，自动处置时效性差，安全防护不能多点联动等问题，探索边界防护的多系统情报 AI 分析共享，数据流实时阻断及多点联动防护的应用示范模式，提升边界防护能力，形成一个 AI 赋能的跨区域，自动防护系统。	实践案例

序号	类别	项目名称	拟解决问题	成果形式
11	实践探索类	人工智能驱动的数据安全治理与可信共享应用研究	面向数据开发利用及安全共享需求，研究人工智能在数据识别分类、流转监测、风险预警和安全管控中的应用方法，提升数据治理精细化水平和可信共享能力，探索跨场景应用模式、协同管理机制和实施路径，形成可复制可推广的实践方案，为数据安全治理与价值释放提供支撑。	实践案例
12	实践探索类	基于人工智能的全域安全运营防护体系研究及应用	围绕组织机构安全运营与全域网络防护需求，解决安全运营自动化水平低、态势感知滞后、决策辅助不足等问题，构建基于人工智能的全域智能安全网络体系，探索人机协同安全运营模式，突破多智能体协同与内生安全防护关键技术，全面提升安全处置效率与网络全域防御能力。	实践案例
13	实践探索类	供应链安全风险管理体系建设与应用探索	围绕供应链安全管理需求，梳理多维度风险评估、组件漏洞监控、事件溯源及风险预警的实践经验，探索基于人工智能的供应链安全管控体系建设及落地应用路径。	实践案例
14	实践探索类	人工智能全生命周期安全治理体系建设及应用研究	面向人工智能安全治理实践需求，研究覆盖数据、模型、应用等环节的安全治理方法，提升风险识别、监测预警、协同处置和综合管控能力，探索全生命周期安全治理的应用模式、实施路径和运行机制，形成可复制可推广的实践方案，为人工智能安全应用和规范发展提供支撑。	实践案例
15	实践探索类	人工智能赋能的工业互联网安全公共服务体系建设与应用	围绕工业互联网安全公共服务实践需求，梳理中小工业企业安全团队缺失、防护资源碎片化、告警误报率高、威胁研判依赖人工经验等突出问题，探索基于大模型与安全智能体的告警精准降噪、企业安全画像自动生成、攻击溯源智能研判、安全知识智能问答与自动化响应处置的应用路径，构建工业互联网安全公共服务体系，形成面向中小企业的轻量化安全服务模式，提升工业领域整体安全防护水平与政企协同治理效能。	实践案例

序号	类别	项目名称	拟解决问题	成果形式
16	实践探索类	互联网多模态敏感数据智能安全监管体系建设与应用探索	围绕互联网文本、图像、音视频等多模态复杂敏感数据识别监管需求，分析当前敏感数据识别、分析与处置关键环节实践基础，探索基于人工智能的互联网多模态敏感数据精准识别、流转监测与威胁研判等智能安全监管体系建设与应用示范，提升互联网数据安全治理智能化服务效能。	实践案例
17	实践探索类	人工智能系统网络安全保险服务模式创新与实践	针对人工智能系统在开发、训练、部署、运行各阶段面临的模型投毒、数据泄露、算法偏见、对抗攻击等新型网络安全风险，传统保险产品难以精准承保与定价。研发 AI 系统动态风险评估模型，设计与之匹配的网络安全保险产品及“技术加固+保险保障”服务套餐，并在数字政府、工业大模型等重点行业开展试点，形成可推广的 AI 系统安全风险金融对冲方案。	实践案例

附件 2

2026 年山东省“人工智能+网络安全”揭榜挂帅项目申报书

揭榜单位：_____（加盖单位公章）_____

联合单位：_____（加盖单位公章）_____

申报日期：_____年_____月_____日

山东省委网信办　山东省大数据局

填 表 说 明

一、申报书内各项内容应填写完整、实事求是、表述明确。表格内容字体为小四号仿宋，行距22磅。

二、申报书统一用A4纸双面打印、左侧装订。一式一份加盖公章。

三、行政职务：厅级、处级、科级、其他。专业职务：正高职称、副高职称、中级职称、初级职称、其他。最后学历：研究生、大学本科、大学专科、其他。最后学位：博士、硕士、学士。

一、揭榜单位基本信息

<table>
<tr><td>揭榜单位名称</td><td colspan="6"></td></tr>
<tr><td>揭榜单位性质</td><td colspan="6">□企业 □高等学校 □科研机构 □事业单位 □其他</td></tr>
<tr><td>联合单位名称</td><td colspan="6">（如无联合申报单位，请填写“无”）</td></tr>
<tr><td>联合单位性质</td><td colspan="6">□企业 □高等学校 □科研机构 □事业单位 □其他</td></tr>
<tr><td>单位地址</td><td colspan="6"></td></tr>
<tr><td rowspan="3">联系人</td><td>姓　名</td><td colspan="2"></td><td>联系电话</td><td colspan="2"></td></tr>
<tr><td>职　务</td><td colspan="2"></td><td>邮　箱</td><td colspan="2"></td></tr>
<tr><td>通讯地址</td><td colspan="5"></td></tr>
<tr><td rowspan="6">负责人信息</td><td>姓　名</td><td colspan="2"></td><td>性　别</td><td colspan="2"></td></tr>
<tr><td>出生日期</td><td colspan="2"></td><td>联系电话</td><td colspan="2"></td></tr>
<tr><td>行政职务</td><td colspan="2"></td><td>专业职务</td><td colspan="2"></td></tr>
<tr><td>学　历</td><td colspan="2"></td><td>学　位</td><td colspan="2"></td></tr>
<tr><td>邮　箱</td><td colspan="2"></td><td>工作单位</td><td colspan="2"></td></tr>
<tr><td>研究专长</td><td colspan="5"></td></tr>
<tr><td rowspan="4">项目组成员</td><td>姓名</td><td>性别</td><td>职务/职称</td><td>学历/学位</td><td>研究特长</td><td>工作单位</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

情况介绍	1. 简述揭榜单位及联合单位基本情况。 2. 在组织架构、人员构成、工作保障等方面基本情况。 3. 近五年来在人工智能、网络安全、大数据等领域承担过的项目及已取得的研究成果（省级及以上，不超过 5 项）。 4. 近五年来获得相关领域荣誉（省级及以上，不超过 3 项）。 5. 近五年来发表相关论文及著作（发表刊物、出版机构名称及时间，不超过 3 项）。

二、揭榜项目基本信息

榜单项目	理论研究类
	□1. 多元异构环境下安全资产智能管理关键技术研究 □2. 多源威胁情报智能分析处置关键技术研究 □3. 漏洞与恶意软件主动防御关键技术研究 □4. 敏感数据智能识别管理关键技术研究 □5. 面向人工智能隐私保护计算的密码技术 □6. 人工智能应用安全风险治理机制研究
	实践探索类
	□7. 安全资产高质量管理体系建设及应用路径探索 □8. 人工智能驱动的网络安全态势感知关键技术研究 □9. 人工智能驱动自动化渗透测试应用推广机制与行业适配策略研究 □10. AI 赋能的边界自动防护体系应用示范与推广 □11. 人工智能驱动的数据安全治理与可信共享应用研究 □12. 基于人工智能的全域安全运营防护体系研究及应用 □13. 供应链安全风险管理体系建设与应用探索 □14. 人工智能全生命周期安全治理体系建设及应用研究 □15. 人工智能赋能的工业互联网安全公共服务体系建设与应用 □16. 互联网多模态敏感数据智能安全监管体系建设与应用探索 □17. 人工智能系统网络安全保险服务模式创新与实践
解决痛点问题	
思路举措	简要描述基本思路、技术路线、研究方法、工作举措等

总体目标及预期成果		
阶段性目标及阶段性成果	时间节点	阶段性成果

三、揭榜单位资质条件

在网络安全、人工智能、大数据等领域具有研究创新能力。	□是 □否
具有稳定的研究团队。	□是 □否
能够提供必要的场地、人员、经费、技术等支持。	□是 □否
揭榜单位和联合单位近三年内无重大违法经营行为，信用状况良好。	□是 □否

四、其他

承诺	我单位所有申报材料，均真实、完整、准确，不存在知识产权争议。我单位申报材料内容所涉及的活动均符合国家相关法律法规要求。我单位对所提交的材料负有保密责任，按照国家相关保密规定，所提交的材料未涉及国家秘密、个人信息和其他敏感信息。前述声明与实际情况如有不符，我单位愿承担相应的法律责任。 揭榜单位（公章）： 年　月　日

抄送：省委网信委成员单位

中共山东省委网络安全和信息化委员会办公室综合处　2026 年 3 月 26 日印发