中央网络安全和信息化委员会办公室

中网办发函〔2025〕286号

关于发布国家重点研发计划“网络空间安全治理”重点专项2025年度项目申报指南的通知

各省、自治区、直辖市、计划单列市党委网信办、科技厅（委、局），新疆生产建设兵团党委网信办、科技局，各有关单位：

根据《国家重点研发计划管理暂行办法》相关要求，现将中央网络安全和信息化委员会办公室作为主责单位的国家重点研发计划“网络空间安全治理”重点专项2025年度项目申报指南予以公布，请按照指南要求组织项目申报工作。有关事项通知如下。

一、申报条件

申报单位应根据指南方向的研究内容以项目形式组织申报，项目可下设课题。项目应整体申报，并覆盖相应指南方向的全部考核指标。项目设1名负责人，每个课题设1名负责人，项目负责人可担任其中1个课题的负责人。其中，青年科学家项目不下设课题。

项目（课题）负责人应聚焦指南任务，坚持应用目标导向，强化基础研究、共性关键技术研发和典型应用示范各项任务间的统筹衔接，整合优势创新团队，并积极吸纳优秀青

年和女性科研人员参与项目研发。鼓励有能力的优秀青年和女性科研人员作为项目（课题）负责人承担任务。

（一）申报单位

1.申报本次重点专项的项目（课题）牵头单位和参与单位应为中国大陆境内注册的科研院所、高等学校和企业等，具有独立法人资格，注册时间为2024年6月30日前。

2.牵头单位和参与单位应具有较强的科技研发能力和条件，运行管理规范。

3.中央和地方各级国家机关不得作为牵头单位或参与单位。

4.牵头单位和参与单位无在惩戒执行期内的科研严重失信行为记录和相关社会领域信用“黑名单”记录。

（二）项目（课题）负责人和参与者

1.项目（课题）负责人应具有高级职称或博士学位，每年用于项目的工作时间不得少于6个月。

2.项目（课题）负责人应为60周岁以下（1965年1月1日以后出生）。

3.青年科学家项目负责人应为40周岁以下（1985年1月1日以后出生）。原则上团队其他参与人员年龄要求同上。

4.项目（课题）负责人应为该项目（课题）主体研究思路的提出者和实际主持研究的科研人员。

5.中央和地方各级国家机关的公务人员（包括行使科技计划管理职能的其他人员）不得牵头或参与申报项目（课

题）。

6.参与重点专项实施方案或本年度项目指南编制的专家，原则上不得牵头或参与申报该重点专项项目（课题）。

7.项目（课题）负责人和参与者无在惩戒执行期内的科研严重失信行为记录和相关社会领域信用“黑名单”记录。

8.申报项目受理后，原则上不能更改申报单位和负责人。

二、申报书

1.申报单位、项目（课题）负责人和参与者应认真阅读本指南、申报书填报说明等，按照相关要求填报申报书。

2.项目申报书应包括相关协议和承诺等，具体要求如下。

（1）项目的牵头单位应与所有参与单位签署联合申报协议，明确各单位任务分工、考核指标、经费分配、知识产权归属等；项目负责人、课题负责人应在联合申报协议上签字，协议签署时间应明确体现。

（2）项目（课题）牵头单位、项目（课题）负责人应签署诚信承诺书，并严格遵守承诺。

（3）项目（课题）负责人为受聘于内地单位的外籍人员或港澳台居民的，聘用期应覆盖所申报项目（课题）的执行期，并应提供相应聘用材料。其中，全职受聘人员应由内地聘用单位提供全职聘用的有效材料，非全职受聘人员应由所有受聘单位同时提供聘用的有效材料。

（4）牵头单位为企业的，应提供企业营业执照等相关资质证明材料。

（5）对于明确配套经费的项目，应提供自筹经费来源证明，明确配套金额。

3.项目（课题）牵头单位应按照《国务院办公厅关于改革完善中央财政科研经费管理的若干意见》《国家重点研发计划资金管理办法》等相关文件的具体要求，遵循“目标相关性、政策相符性、经济合理性”的基本原则，结合项目（课题）牵头单位及参与单位现有基础及支撑条件，根据项目（课题）任务目标的实际需要，科学合理、实事求是地编制项目（课题）预算。

4.申报书中不得出现任何违反法律法规或含有涉密信息、敏感信息的内容。

5.项目（课题）的牵头单位及所有参与单位要落实《关于进一步加强科研诚信建设的若干意见》《关于进一步弘扬科学家精神加强作风和学风建设的意见》等要求，加强对申报材料的审核把关，杜绝夸大不实，严禁弄虚作假。

三、限项申报要求

1.项目（课题）负责人限牵头申报1个项目（课题）；国家重点研发计划、国家科技重大专项的在研项目负责人不得牵头或参与申报项目（课题），课题负责人可参与申报项目（课题）。

2.作为项目（课题）负责人、项目骨干申报的项目（课题）和国家重点研发计划、国家科技重大专项在研项目（课题）总数不得超过2项。中央财政专项资金预算不超过400

万元的“政府间国际科技创新合作”重点专项项目、中央财政专项资金预算不超过400万元的“战略性科技创新合作”重点专项港澳台项目，不计入上述2项总数的限项范围；但其他重点专项项目的在研项目负责人不得参与申报此类不计入总数限项范围的项目。

3.国家重点研发计划、国家科技重大专项的在研项目（课题）负责人和项目骨干不得因申报新项目而退出在研项目；退出项目研发团队后，在原项目执行期内原则上不得牵头或参与申报新的国家重点研发计划项目。

4.国家重点研发计划项目（不含青年科学家项目、科技型中小企业项目、国际合作类项目，限项目负责人和课题负责人）、国家科技重大专项（不含青年科学家项目，限项目负责人和课题负责人），与国家自然科学基金重大项目（限项目负责人和课题负责人）、基础科学中心项目（限学术带头人和骨干成员）、国家重大科研仪器研制项目（限部门推荐项目的项目负责人和具有高级职称的主要参与者）实施联合限项，科研人员同期申报和在研的项目（课题）总数原则上不得超过2项。

5.执行期（包括延期后执行期）结束时间早于2025年12月31日的项目（课题），不计入总数限项范围。

四、申报程序

本专项项目采用一轮申报的程序，具体工作要求如下。

1.网上填报。项目牵头单位根据指南相关申报要求，通

过国家科技管理信息系统公共服务平台（http://service.most.gov.cn，以下简称“国科管系统”）填写并提交项目申报书，申报书中所需附件材料全部以电子扫描件上传。网上填报的申报书将作为后续形式审查和项目评审工作的依据。

各申报单位在正式提交项目申报书前，可利用国科管系统查询相关科研人员承担国家重点研发计划重点专项、国家科技重大专项、国家自然科学基金重大项目、国家自然科学基金基础科学中心项目和国家重大科研仪器研制项目等在研项目情况，避免因不符合限项申报要求导致形式审查无法通过。

项目牵头单位网上填报申报书的受理时间为2025年8月1日8:00至9月23日16:00。

2.组织推荐。申报书须经相关单位推荐（组织申报的推荐单位见附件）。各推荐单位应加强对所推荐的项目申报材料的审核把关，于2025年9月26日16:00前通过国科管系统逐项确认推荐项目，并将加盖推荐单位公章的推荐函以电子扫描件上传。

每个项目只能通过单个推荐单位申报，不得多头申报和重复申报。

3.形式审查。专业机构将对申报书进行形式审查，形式审查要点见附件。

五、项目管理改革举措

1.坚持服务国家需求，聚焦国家和行业网络安全重大风

险，解决国家网络安全重大技术问题，项目以应用为导向设置考核指标，原则上不设置论文指标。

2.建立责任部门机制，每个项目确定一个责任部门，一般为项目需求部门。责任部门负责指导项目实施，参与中期检查、实施成效评估等工作。

六、咨询方式

1.国科管系统技术咨询电话及邮箱：

010-58882999（中继线），program@istic.ac.cn。

2.业务咨询电话：

010-68207726、68207794

附件：1.“网络空间安全治理”重点专项2025年度项目申报指南

2.组织申报的推荐单位

3.申报指南形式审查条件要求

中央网络安全和信息化委员会办公室

2025年8月1日

附件 1

“网络空间安全治理”重点专项
2025年度项目申报指南

为落实“十四五”期间国家科技创新有关部署安排，组织实施好“网络空间安全治理”重点专项，根据本重点专项实施方案部署，现发布 2025 年度项目申报指南。

项目坚持服务国家需求，坚持应用目标导向，聚焦国家和行业网络安全重大风险，解决国家网络安全重大技术问题。建立责任部门机制，每个项目确定一个责任部门，一般为项目需求部门。

申报项目的研究内容必须涵盖指南所列的全部研究内容和考核指标，项目以应用为导向设置考核指标，原则上不设置论文指标。除特殊说明外，每个指南支持项目数为 1 项，实施周期不超过 3 年。

一般项目配套经费与国拨经费比例不低于 1:1，项目下设课题数不超过 5 个，项目参与单位总数不超过 5 家，项目设 1 名项目负责人，项目中每个课题设 1 名课题负责人。

青年科学家项目不再下设课题，项目参与单位总数不超过 2 家，项目骨干人数不超过 5 人。青年科学家项目负责人应为 1985 年 1 月 1 日以后出生，原则上团队其他参与人员

年龄要求同上。

具体项目申报指南如下:

1.气象卫星星地一体化网络安全综合防御体系研究

研究内容: 研究星地一体化测控业务中网络安全防御及数据安全管理的需求，研究指令可信生成、安全高效加密、多路径高可信传输等业务测控安全关键技术，提出适应卫星业务测控流程的可信验证模型和方案框架，构建星地一体化网络安全防御体系；研究气象卫星应用的细粒度动态访问控制、跨域访问实体身份可信认证与角色自适应授权、权限冲突检测与消解、安全策略引擎等智能微边界防护关键技术；研究气象卫星数据分类分级标识与访问策略、授权共享、责权界定、风险识别等数据治理技术，研发气象卫星数据安全管理与风险分析平台，支持数据全流程安全防护与精准管控，全面监测气象卫星数据流转过程安全状态；研制气象卫星星地一体化网络安全综合防御系统，满足气象卫星网络海量吞吐需求；研究成果在国家卫星气象中心网络得到试点应用。

考核指标: 研制可信计算安全软硬组件，支持星地一体化业务测控网络的安全防护；支持星地和星间安全加密通信，具备多路径优先级控制、业务指令的带权识别与分发调度、密钥管理能力，支持 SM2/SM3/SM4 等不少于 3 种国家商用密码算法，星地星间加解密速率不低于 10Mbps；研制

基于动态信任评估的气象卫星应用访问控制机制，支持多元实体跨域可信认证与协同动态授权，支持对网络位置、接入途径、操作系统配置等不少于3种因素的实体鉴权和权限冲突消解；研发数据安全管理与风险分析平台，支持气象卫星数据规模≥100PB，支持符合国家气象数据管理要求的气象卫星数据完整分级分类，具备数据可信标识与治理能力，支持数据治理操作不低于5万TPS（次每秒）。支持数据风险种类识别不少于15类、异常行为识别不少于15种，识别准确率均不低于95%（检测样本数量不低于1万个）。支持基于国家商用密码算法的数据全周期全域流转安全管控，形成全局数据风险视图，统一管理数据安全策略，防范违规、越权、滥用数据行为；研制气象卫星星地一体化网络安全综合防御系统，支持智能网络安全策略管理与防御能力调度，支持安全域灵活动态扩展，涵盖静止和极轨2个系列气象卫星、5个卫星地面站，支持气象信息安全服务用户数≥200万；在国家卫星气象中心网络进行试点应用。

有关说明：项目责任部门为中国气象局。项目承担单位遴选方式为公开竞争。

2.电子产品信息清除关键技术与效果验证研究

研究内容：针对电子产品现有信息清除功能清除不彻底、技术标准不统一导致数据泄露等问题，研究典型电子产品、不同存储介质的信息存储和清除技术，研制强制性国家

标准配套技术文件；研究电子产品存储功能组件快速识别、指令清理多系统融合调用、高可靠数据覆写算法等技术，开发混合多种技术方案的国产化信息清除软件；研究信息清除效果验证的形式化方法，开发涵盖“存储器寻址验证、专业恢复软件测试、清除日志审计”三级验证机制的信息清除效果验证公共服务平台；研究电子产品信息清除标识追溯技术与认证机制，在国内主流电子产品厂商、二手交易平台、资源回收企业内开展技术试点与应用推广。

考核指标：信息清除软件具备存储功能组件快速识别、用户数据定向清除、数据覆写定制化设置等不少于3项功能，适配安卓、鸿蒙、Windows、Linux等不少于4类主流操作系统；数据覆写技术适配95%以上的主流存储介质，与全0/全1覆写方式相比覆写效率提升不少于20%，残留数据恢复概率<0.001%；清除效果验证平台万次重复测试误报率<0.01%，支持接入不少于手机、平板、笔记本电脑、办公设备、服务器、智能穿戴等6类主流电子产品；建立电子产品二手流通信息清除标识追溯与检测认证案例库，案例不少于1万项且覆盖不少于30家主流厂商。

有关说明：项目责任部门为中央网信办。项目承担单位遴选方式为公开竞争。

3.网络安全高质量数据集高效构建关键技术（青年科学家项目）

研究内容：针对当前网络安全领域高质量数据集规模严重不足、数据人工标注效率低、缺乏多模态数据编码理论的问题，研究网络安全领域多模态数据采集技术，包括策略配置、恶意样本、漏洞特征方面的文本、日志、流量等多种模态网络安全数据；研究网络安全数据细粒度高效标注技术，降低人工标注依赖，实现大规模数据自动标注；研究网络安全数据集动态迭代机制，实现新数据样本自动化清洗、去重与融合；研究网络安全多模态数据集质量评估技术；研究网络安全多模态数据编码技术，突破网络安全领域异构数据共性表征理论，为大模型训练与评测提供数据基准支撑。

考核指标：建立策略配置、恶意样本、漏洞特征的高质量多模态网络安全数据集，每种类型数据集规模达到 TB 级，支持网络安全运维、漏洞挖掘等领域；建立网络安全多模态数据细粒度标注工具链，细粒度标签准确率≥85%；构建网络安全多模态数据集质量评估和数据编码理论体系，设计网络安全数据集质量评估方法≥3 个，网络安全数据编码方法≥3 个，网络安全数据编码质量指标≥3 个，立项行业以上相关标准≥2 项，在不少于 3 个典型大模型进行应用验证。

有关说明：项目责任部门为中央网信办。项目面向在中央网信办 2024 年、2025 年组织的人工智能技术赋能网络安全应用测试活动相关场景测试中排名前三的单位遴选牵头承担单位。项目成果、技术、代码按照主责单位要求在国内

相关高校、科研机构、企业等一定范围内开源。

4.网络安全运维垂直大模型构建关键技术（青年科学家项目）

研究内容：针对当前安全威胁检测与异常事件响应高度依赖经验丰富的运维人员、安全运维技术智能化程度弱的问题，研究面向安全威胁感知与响应的安全运维垂直大模型构建与安全运维知识注入技术，设计面向安全运维大模型的高效训练机制，提高对于动态化、隐蔽化新型攻击的应对能力；研究基于自学习的安全运维大模型参数训练技术，持续学习新兴威胁特征，实现对威胁态势的实时感知与智能响应处置生成；研究安全运维应用智能体安全治理技术，对实时威胁监测和自动化安全响应流程中的应用智能体行为进行监控和风险评估；研发面向安全威胁感知与响应的安全运维垂直大模型与应用智能体协同系统，并开展应用示范。

考核指标：建立大规模安全运维多模态数据集，其中警报数据样本不少于 10 万，包含网络流量日志、安全事件日志、策略配置等；构建安全运维多模态大模型，大模型参数不少于 100 亿，可快速处理文本、日志、流量等多模态数据，警报误报率≤5%，警报漏报率≤5%；发现面向 Web 安全、C2 通信等隐蔽攻击类型不低于 5 种；针对不少于 3 种典型网络安全应急响应场景，支持面向 DDoS、C2 通信、后门进程、漏洞探测等攻击方式自动生成网络安全响应策略；支持警报

误报消除准确率不低于90%；支持应用智能体自动生成风险处置策略不低于10种。

有关说明：项目责任部门为中央网信办。项目面向在中央网信办2024年、2025年组织的人工智能技术赋能网络安全应用测试活动相关场景测试中排名前三的单位遴选牵头承担单位。项目成果、技术、代码按照主责单位要求在国内相关高校、科研机构、企业等一定范围内开源。

5.网络安全态势感知大模型构建关键技术（青年科学家项目）

研究内容：针对网络流量规模爆炸式增长及网络攻击行为愈发隐蔽的难题，研究构建网络态势感知大模型，具备原始网络流量检测和分析理解能力，并能够同时完成多项网络态势感知子任务；研究面向网络安全态势感知的高效蒸馏技术，能够大幅提高模型的检测及分析效率；研究网络态势感知大小模型协调推理技术，能够提升多项网络安全态势感知子任务的综合处理能力；研究网络态势感知大模型的上下文关联分析方法，能够监测并识别跨部门长时间周期内隐蔽存在的APT攻击；研究网络态势感知大模型的网络攻击行为预测技术，精准预测网络流量未来发展趋势及潜在攻击手段；研制网络态势感知大模型平台，在典型业务场景下应用示范。

考核指标：构建网络态势感知大模型，大模型的参数量

不低于100亿，覆盖网络态势感知子任务不低于10项，包括恶意软件流量检测、匿名网络行为识别、僵尸网络检测、VPN行为检测等；在至少跨2个部门3个月时间以上周期的真实网络数据集中，APT攻击识别率不低于80%；网络态势感知大模型对潜在网络攻击行为的发现准确率不低于80%；实现面向流量检测等子任务的蒸馏小模型，小模型的参数量不高于15亿，子任务的识别准确率不低于90%；在交通、能源等不少于2种关键信息基础设施场景下对网络态势感知大模型应用示范。

有关说明：项目责任部门为中央网信办。项目面向在中央网信办2024年、2025年组织的人工智能技术赋能网络安全应用测试活动相关场景测试中排名前三的单位遴选牵头承担单位。项目成果、技术、代码按照主责单位要求在国内相关高校、科研机构、企业等一定范围内开源。

6.面向人工智能模型安全的密码分析与防护关键技术（青年科学家项目）

研究内容：针对目前人工智能模型安全存在的依赖经验性防御，缺乏数学可解释性和可验证性问题，探索密码技术在人工智能安全领域的应用，基于密码分析技术评估人工智能模型在机密性、鲁棒性、溯源性等方面的安全性风险，并提出针对性的防护技术；研究基于新型密码分析的模型参数高精度恢复攻击技术，提出模型参数恢复攻击新型防御机

制；研究基于密码分析理论的高效黑盒对抗攻击样本生成方法，提出对抗攻击新型防御机制；研究可认证高稳定性大模型生成内容水印技术，提出可证明安全密码学原语；研发基于密码分析的人工智能模型机密性、鲁棒性与溯源性安全评估与防护工具。

研究指标：提出基于密码分析的新型人工智能模型安全评估与防护理论体系：针对不少于5种典型人工智能模型，提出基于密码分析的模型参数高精度恢复攻击方法，要求参数最大恢复误差≤0.001（不依赖侧信道信号），并提出针对性的防御方法；提出不少于3种基于密码分析的对抗样本攻击方法，相比已有黑盒对抗样本攻击方法成功率相对提高不低于50%，并提出针对性的防御方法，相比已有黑盒对抗样本防御方法成功率相对提高不低于20%，并在不少于5种典型人工智能模型上进行验证；提出不少于3种基于新型密码原语设计可证明安全的模型参数水印以及生成内容溯源方法，在图像压缩、噪声扰动、图像编辑等典型攻击场景下比特恢复率不低于98%，并在不少于5种典型人工智能模型上进行验证。开发基于密码技术的人工智能模型安全评估与防护平台，支持不少于3种常用开发框架。

有关说明：项目责任部门为国家密码管理局。项目承担单位遴选方式为公开竞争。项目成果、技术、代码按照主责单位要求在国内相关高校、科研机构、企业等一定范围内开源。

附件 2

组织申报的推荐单位

1.中央和国家机关有关部门科技、网络安全主管司局；

2.各省、自治区、直辖市党委网信办、计划单列市党委网信办，新疆生产建设兵团党委网信办；

3.各省、自治区、直辖市、计划单列市科技厅（委、局），新疆生产建设兵团科技局。

各推荐单位应根据指南的具体要求，在本单位职能和业务范围内推荐，并对所推荐项目的真实性等负责。对于有主管部门的项目申报单位，推荐单位应为其主管部门；对于没有主管部门或主管部门不明确的项目申报单位，推荐单位可为属地网信、科技部门。

附件 3

申报指南形式审查条件要求

申报项目须符合以下形式审查条件要求。

1.推荐程序和填写要求

（1）由指南规定的推荐单位在规定时间内出具推荐函。

（2）申报单位同一项目须通过单个推荐单位申报，不得多头申报和重复申报。

（3）项目申报书内容与申报的指南方向相符。

（4）项目申报书及附件按格式要求填写完整。

2.申报单位应具备的资格条件

（1）申报本次重点专项的项目（课题）牵头单位和参与单位应为中国大陆境内登记注册的科研院所、高等学校和企业等，具有独立法人资格，注册时间为 2024 年 6 月 30 日前。

（2）牵头单位和参与单位应具有较强的科技研发能力和条件，运行管理规范。

（3）中央和地方各级国家机关不得作为牵头单位或参与单位。

（4）牵头单位和参与单位无在惩戒执行期内的科研严重失信行为记录和相关社会领域信用“黑名单”记录。

3.项目（课题）负责人和参与者应具备的资格条件

（1）项目（课题）负责人应具有高级职称或博士学位，每年用于项目的工作时间不得少于6个月。

（2）一般项目（课题）负责人应为60周岁以下（1965年1月1日以后出生）。

（3）青年科学家项目负责人应为40周岁以下（1985年1月1日以后出生）。原则上团队其他参与人员年龄要求同上。

（4）项目（课题）负责人应为该项目（课题）主体研究思路的提出者和实际主持研究的科研人员。

（5）中央和地方各级国家机关的公务人员（包括行使科技计划管理职能的其他人员）不得牵头或参与申报项目（课题）。

（6）参与重点专项实施方案或本年度项目指南编制的专家，原则上不得牵头或参与申报该重点专项项目（课题）。

（7）项目（课题）负责人和参与者无在惩戒执行期内的科研严重失信行为记录和相关社会领域信用“黑名单”记录。

（8）项目（课题）负责人和参与者满足限项申报要求。

4.本重点专项指南规定的其他形式审查条件要求

（1）除特殊说明外，项目实施周期不超过3年。一般项目配套经费与国拨经费比例不低于1:1，项目下设课题数

不超过5个，项目参与单位总数不超过5家。

（2）青年科学家项目不再下设课题，项目参与单位总数不超过2家，项目骨干人数不超过5人。

本专项形式审查责任人：张炜