附件 1

国家网络空间安全国家科技重大专项
第三批项目申报指南
（公开类）

3.1 网络安全极端场景下的抗毁重构与快速恢复技术

研究目标：面向高强度国家级网络对抗等风险，针对电力、公安等重要领域信息系统韧性网络的抗毁重构和快速恢复需求，构建抗毁重构网络安全理论体系，突破高强度网络攻击抗毁生存、业务损失控制快速恢复、瘫毁性破坏重构适应技术，实现极端情况下的安全机制向“解裂愈合、弹性恢复”模式转移。面向重要行业单位典型场景开展示范验证，提升关键信息基础设施的网络、系统、数据抗毁生存及韧性恢复能力。

研究内容：研究可定义、可重构、智能感知和主动变迁的抗毁重构架构，设计零信任、移动目标防御、多态替身网络、智能调度等新型网络安全架构部署模式；研究多源信息融合的复杂攻击行为理解技术，研究网络攻击路径折叠和危险态阻断方法，研究深度融合业务的多态混合替身智能体及跨域协同策略；研究天地一体化的灾难备份技术，研究业务级联失效动态隔离控损技术，研究韧性层次化快速恢复技术；研究面向多维度损害的分级解裂愈合方法，研究基于微服务的异构资源重构技术，研究基于

拓扑动力学的动态安全防线重塑技术；针对不少于 2 个重要行业信息系统开展抗毁重构与快速恢复示范验证。

考核指标：结构安全机制不少于 4 种；构建抗毁机制的量化评估模型，抗毁能力与功能安全度量指标不少于 6 种；攻击行为语义推理识别准确率不低于 95%，支持不少于 120 个仿真节点多态替身网络；10TB 以上数据恢复时间小于等于 30 分钟，控损隔离动态自愈成功率不低于 85%；池化安全能力不少于 15 种，支持秒级按需伸缩，安全防线重塑能力种类不少于 6 种，重构后攻击链断裂比不低于 90%；依托内生安全机制实现极端破坏下的降级生存，确保核心业务保障率不低于 95%；在不少于 5 个重要场景开展示范验证。按照网安重大专项构建可持续演进的国家网络空间安全技术体系的总体要求，适应关键信息基础设施和重要信息系统防护等关键技术的快速发展，应动态优化调整项目研究内容和技术指标。

实施期限：3 年

项目密级：公开

联合管理部门：公安部

立项要求：支持 1 个项目，采用公开竞争方式。

中央财政资金支持方式：事前立项事前补助。配套资金与中央财政资金不低于 4:1 匹配。

3.2 关基安全保护系列化检测评估技术

研究目标: 针对关基测评对象自动化识别难、实景检测受限、高阶智能化攻击模拟手段缺失、保护能力评价未成体系等问题，以“基线-实战化-极限生存”三阶检测评估为导向，通过构筑框架体系、创立技术范式、研制工具平台、开展应用验证，支持国家关基安全能力图谱构建，开展针对性风险消控行动，提升大规模网络对抗能力。

研究内容: 研究检测评估技术体系框架，设计多行业关基安全能力量化指标体系和检测评估范式；研究关基对象全息关联识别、实战化攻击对抗效能评估技术，研制关基抗智能化、持久化、立体化攻击能力的测评手段，研究监测型入侵痕迹检测与追踪技术，形成未知威胁发现评估能力；研究含利用 0-Day 漏洞的一般、连锁、级联、整体失能等多级极限故障场景构设和极限条件影响演化分析技术，实现“生存-失能-恢复”全周期效能度量；研究深层次风险溯源分析与趋势预测技术，研制跨域智能分析平台，实现国家层面的关基安全掌控能力；构建关基虚实同构仿真验证环境，在不少于 3 个行业的重要关基场景开展应用验证。

考核指标: 构建关基安全量化评估体系，包含不少于 5 种场景动态检测评估的模型，国家标准立项不少于 3 项；研制基线检测评估工具集，关基测评对象底图生成准确率不低于 90%，支持不少于 8 类异常策略发现；研制智能无损攻击模拟系统，内置技战法不少于 200 种（不少于 5 种 APT 攻击），支持不少于 3 类专

网的网络控制逻辑及不少于 3 类工控系统业务逻辑的脆弱性评估；研制未知威胁智能发现及追踪系统，支持异常模型不少于 25 类；构建包括物理设备级、网络级、应用数据级等不少于 3 个技术层级、4 类演变等级的极限故障场景；研制跨域智能分析平台，支持不少于 6 种维度的能力画像与风险预测预警；构建虚实融合关基仿真环境，在不少于 5 个关基场景应用验证。按照网安重大专项构建可持续演进的国家网络空间安全技术体系的总体要求，适应关键信息基础设施和重要信息系统防护等关键技术的快速发展，应动态优化调整项目研究内容和技术指标。

实施期限：3 年

项目密级：公开

联合管理部门：公安部

立项要求：支持 1 个项目，采用公开竞争方式。

中央财政资金支持方式：事前立项事前补助。配套资金与中央财政资金不低于 4:1 匹配。

3.3 关基供应链安全风险识别技术

研究目标：面向关基安全，针对关基系统规模庞大、成分复杂，导致漏洞风险难以精确识别的瓶颈问题，构建支持漏洞精确检测的代码血缘图谱和检测规则生产体系，突破供应链组件库规模化采集、多语言代码融合分析、大规模漏洞情报发现能力的制约，形成具有自主知识产权的代码成分分析工具和静态代码安全

扫描工具，推动关基安全领域的技术升级与产业变革。建立体系化的供应链安全风险识别技术和平台，为保障我国关键信息基础设施供应链安全提供坚实的技术支撑。

研究内容：研究多语言供应链组件库统一标识及智能表征，支持海量规模的组件特征库高效采集；研究公开漏洞多源汇聚和未公开漏洞高效捕获技术，建立高时效的大规模漏洞情报获取能力；研究多粒度代码相似性分析及海量代码高效关联，支持构建代码血缘图谱和精确识别供应链组件漏洞；研究大模型赋能的多语言代码融合分析和漏洞检测规则自动化生成，支持跨语言、跨文件的代码语义深度分析和大模型驱动的检测规则自动优化和演化；研制供应链安全风险识别平台，有效缓解重点关基行业面临的供应链安全风险。

考核指标：研制 1 套多语言供应链组件库采集技术体系框架，构建供应链组件特征库规模不少于 1 亿条，覆盖不少于 6 种软件语言、不少于 2 种硬件描述语言；研制 1 套供应链漏洞情报捕获技术体系框架，构建漏洞数据库规模不少于 100 万条，自动化生成漏洞检测规则数量不少于 1000 万条；针对开源组件，支持百万行级大型系统代码血缘图谱的构建，组件识别准确率不低于 95%，供应链组件漏洞检测准确率不低于 90%；支持不少于 6 种语言的跨文件融合分析，漏洞检测准确率不低于 80%；在至少 2 个关基重点行业及国家安全部开展应用示范，有效缓解重要系统的供应链安全风险。按照网安重大专项构建可持续演进的国家

网络空间安全技术体系的总体要求，适应关键信息基础设施和重要信息系统防护等关键技术的快速发展，应动态优化调整项目研究内容和技术指标。

实施期限：3 年

项目密级：公开

立项要求：支持 1 个项目，采用公开竞争方式。

中央财政资金支持方式：事前立项事前补助。配套资金与中央财政资金不低于 4:1 匹配。

3.4 下一代互联网安全域间路由协议关键技术

研究目标：针对当前互联网域间路由协议在策略灵活性、安全保障与自动化协同等方面的短板问题，围绕未来可信、安全、智能互联的重大需求，构建具备多目标优化能力与治理意图驱动的自动化策略引擎。面向路由系统面临的劫持、泄漏、起源伪造等安全威胁，探索逐跳转发特性下的信任建立与传递机制，增强部分部署环境下的安全可验证能力。引入安全偏好驱动的路由关系重构机制，实现基于地缘合作等级和组织安全策略的差异化路径选择能力。构建高可扩展、策略自治、安全可信的新型域间路由技术体系，为支撑复杂现实场景下的网络策略表达、动态配置和自动化协同提供理论依据与技术方案。

研究内容：研究拓扑-策略解耦的新型域间路由架构，重点突破网络连接关系与逻辑路由意图的解耦机制，构建面向安全治

理与业务需求的多层级意图语义描述模型；通过形式化方法定义支持带宽、时延、地缘合规与信任关系等的路由策略原语；研究具备在线学习与自演进能力的自动化策略认知引擎、自动化策略代理与多目标优化决策方法，解决安全合规、传输性能与商业成本等多维目标下的策略优化问题；研究路由意图承诺与执行一致性验证技术；面向重点区域，实现特定流量差异化路由策略的支持能力；突破传统基于外部威胁检测的思维，聚焦于自动化引擎下发的策略意图与实际转发行为之间的可信绑定与验证技术，研究设计融合安全风险感知的路由权重动态评估框架，实现基于地缘关系、组织策略的差异化路径选择；研究路由协议系统化实现中的安全主动防御机制，搭建跨域协同的分布式信任基础设施及高效安全的域间路由原型系统，支撑安全域间路由关键技术的能力验证与工程化部署实践；针对新一代安全架构与存量 BGP 网络长期共存的必然趋势，研究支持域间路由技术体系过渡的激励机制与部署验证，支撑新型互联网域间路由技术体系的平滑过渡。

考核指标：实现策略与路径计算解耦的功能验证；支持与现有 BGP 协议互操作，路由策略更替延迟小于 100 毫秒；意图语言原型支持不少于 8 类涵盖性能、合规与信任维度的策略原语组合表达，策略语义转换准确率不小于 98%；支持与现有 BGP 协议双向互操作，自动化策略更替导致的硬件转发表平均收敛延迟不超过 500 毫秒；构建自动化策略引擎，支持不少于 5 个目标的

策略优化，模拟环境中策略响应时间低于 1 秒；策略引擎系统具备策略冲突检测准确率不低于 95%；路径执行一致性审计机制在不超过 30%的部分部署场景下，对策略执行偏差（含路径篡改与泄漏）的检测覆盖率不低于 85%，误报率不超过 2%；搭建不少于 100 个共识参与节点的分布式信任基础设施，验证延迟为秒级；研制自动化域间路由原型设备，并在国家级试验设施完成跨不少于 3 个运营商的真实设备组网验证；在不少于 80 个 AS 的混合网络拓扑中完成新旧协议协同仿真验证，并在国家有关机构开展试点部署与应用示范；在自动化策略迁移过程中，确保关键业务流平均不中断率高于 99%；新旧协议共存期间的全网路由收敛延迟，相比传统网络增幅控制在 5%以内；提交 IETF 草案不少于 3 项。按照网安重大专项构建可持续演进的国家网络空间安全技术体系的总体要求，适应下一代互联网路由安全关键技术的快速发展，应动态优化调整项目研究内容和技术指标。

实施期限：3 年

项目密级：公开

立项要求：支持 1 个项目，采用公开竞争方式。

中央财政资金支持方式：事前立项事前补助。配套资金与中央财政资金不低于 2.4:1 匹配。

3.5 新型处理器安全架构研究

研究目标：面向当前主流处理器普遍缺乏内生安全机制的核

心问题，以安全指令集扩展驱动的新型处理器安全架构设计为核心，构建覆盖处理器微结构、系统软件与上层应用的全栈安全能力体系。通过统一的安全指令集扩展体系，形成面向芯片级、系统软件级、应用级的立体化安全支撑能力。在国产 28nm 工艺上研制原型验证芯片，构建基于新型安全架构的服务器原型机并适配新型安全架构操作系统，为我国构建可持续演进、自主可控的新一代安全计算体系提供关键技术基础。

研究内容：以新型处理器安全架构为核心，针对处理器自身微架构漏洞，研究 SoC 平台安全指令扩展及安全架构，包括度量认证指令、侧信道防护指令等，实现后量子密码支持的固件完整性保护、缓存侧信道防护等处理器自身安全能力增强，并构建支持后量子密码的内生硬件可信根；针对操作系统内生结构存在的内存访问漏洞和安全隔离问题，研究内存访问安全和可信执行环境系统安全指令扩展及安全架构，包括安全内存标记和跳转指令、特权等级切换指令等，实现同地址空间内细粒度访存安全防护、安全中断和 IO 物理内存保护的可信执行环境等系统安全能力的增强；针对应用层敏感数据的保护问题，研究数据密态计算指令扩展及安全架构，包括密文多项式计算指令、密态计算访存指令等，支持内生的高性能密态计算硬件加速，并构建密态计算系统软件，包括密态计算算子库、可扩展密态计算环境等，实现对应用敏感数据的安全保护能力增强；在全国产 28nm 工艺下研制原理性验证芯片，研究支持安全指令集扩展的编译器，构建基

于原理性验证芯片的服务器原型机，适配新型安全架构操作系统，制定新型处理器安全指令集标准。

考核指标: 完成具有新型安全架构的处理器芯片设计和流片验证：原理性验证芯片采用 28nm 工艺，构建基于 FPGA 的芯片原型验证平台；可信执行环境支持安全中断和 IO 物理内存隔离；内存安全实现用户态和内核态字节粒度的动态划分，支持权限的时效控制；内存安全技术开启后，性能下降不超过 10%；硬件可信根支持抗量子攻击密码算法；密态计算的安全等级不低于 128bit，在 28nm 工艺下性能相比 Intel 同期服务器处理器提升一个数量级，构建支持不少于 3 种算法的密态计算算子库，支持数据处理全流程加密；基于原理性验证芯片构建服务器原型机，支持新型安全架构操作系统；原理性验证芯片的安全能力通过国家级安全认证机构的认证；面向重要行业或应用场景进行应用验证。

实施期限：3 年

项目密级：公开

立项要求：支持 1 个项目，采用公开竞争方式。

中央财政资金支持方式：事前立项事前补助。配套资金与中央财政资金不低于 2:1 匹配。

3.6 新型基础系统软件安全架构研究

研究目标: 针对国家信息基础设施中基础系统软件缺乏内生

安全架构的问题，研究基于分层隔离与阻断技术的操作系统内核安全架构，突破内存安全的操作系统内核构造方法、操作系统内核组件级安全隔离机制、容器的新型安全机制、系统软件安全风险检测等关键技术，形成具备原生内存安全特性与攻击阻断能力的新型操作系统内核。应用高安全基础软件可信保障技术，构建基于新型安全架构内核的操作系统，适配新型安全架构处理器。为保护我国信息基础设施安全和形成新一代安全计算体系提供关键技术支撑。

研究内容：研究内存安全的操作系统内核构造方法，基于内存安全语言重构操作系统内核主要核心功能；研究跨语言的驱动复用方法，支持 Linux 驱动的复用；研究操作系统内核组件级安全隔离机制，硬件辅助的内存隔离机制具备多样化的内存隔离方式和访问隔离能力；研究操作系统内核的核内分隔方法，支持内存不安全组件的隔离和敏感数据结构的保护；研究容器的新型安全机制，基于容器的细粒度权限访问机制构建以轻量级虚拟机为基础的安全容器，有效防御现有容器安全漏洞；研究系统软件安全风险检测技术，研制基于领域专用语言的系统软件安全风险建模与检测工具；应用高安全基础软件可信保障技术对关键组件进行验证，构建基于新型安全架构内核的操作系统，适配新型安全架构的处理器，面向云计算场景开展应用验证。

考核指标：研制完成具有新型安全架构的操作系统内核：内核的核心功能中超过 95%使用内存安全语言重构，支持不少于 5

类 30 个 Linux 驱动的复用；提供数据只读隔离、读写隔离和代码执行隔离 3 种核内隔离能力，支持 Linux 驱动间的安全隔离和内核特权数据与指令的增强防护；安全容器可防范内存安全与隔离机制缺陷等至少 7 类以上已知容器安全漏洞；可建模的内核安全风险模式不少于 100 种，检测成功率大于 80%；基于新型安全架构内核的操作系统支持 RISC-V 和 X86 等指令集，可运行 Redis、Nginx 等典型云计算应用，相比 Linux 的平均性能开销增量不超过 15%；面向重要行业或应用场景进行应用验证。

实施期限：3 年

项目密级：公开

立项要求：支持 1 个项目，采用公开竞争方式。

中央财政资金支持方式：事前立项事前补助。配套资金与中央财政资金不低于 1.4:1 匹配。

3.7 新型云计算安全技术体系研究

研究目标：针对当前云计算技术在应对数据深度利用、人工智能等新型服务模式时存在安全性与隐私性保护不足、主动防御能力不强的问题，探索新型云计算安全技术体系，建立软硬件协同的数据安全利用和验证技术框架，提出新型云计算人工智能服务的数据隐私保护方法，构建云计算内生安全与主动防御技术体系，为大数据和人工智能时代的云计算安全与隐私保护提供有力的技术支撑，促进国家对大数据、云计算、人工智能等数字技术

发展战略的实施。

研究内容：研究云计算环境的可信数据空间构建与验证方法，针对多类型算力平台数据泄露风险，建立软硬件协同的数据安全利用框架，支持多元算力安全协同调度，提供可追溯、可验证的数据隔离计算环境；研究云数据的高效密态检索与计算框架，基于可信执行环境、全同态加密、安全多方计算等技术，实现敏感数据检索、计算与训练；研究智能云服务的隐私风险识别与保护机制，具有智能模型训练与推理、知识库查询等场景隐私泄露风险检测能力；研究新型云计算内生安全与主动防御技术，构建多层次、自适应、抗量子的高性能云平台安全防护体系，设计可扩展、一体化智算云安全服务框架，支持可信隔离、密态计算、隐私保护、内生安全服务的集成与协同工作。

考核指标：新型云计算平台覆盖 CPU、GPU、NPU、DPU 等 4 类通算和智算芯片，其中至少包含 3 种支持 TEE 的国产芯片，至少包含 1 种具有抗量子密码模块的芯片；具备密钥窃取、模型类型与参数窃取等侧信道分析和检测能力；实现基于硬件信任根的数据检索与计算、模型训练与推理行为访问控制和审计；支持半诚实模型、恶意模型假设下的全流程模型密态训练与推理，其中恶意模型假设下的模型精度损失不超过 1%，与半诚实模型相比，推理时延小于 5 倍；具备对密态模型训练和推理场景的数据泄露风险检测与防护能力；支持大模型异常行为识别与阻断，准确率大于 90%；研制 1 套新型云计算安全工具集，在国家

级云平台进行集成，面向重要行业或应用场景进行应用验证。

实施期限：3 年

项目密级：公开

立项要求：支持 2 个项目，采用公开竞争方式。

中央财政资金支持方式：事前立项事前补助。配套资金与中央财政资金不低于 1.12:1 匹配。

3.8 高安全基础软件可信保障技术研究

研究目标：针对国家关键领域高安全基础软件可信保障能力不足、漏洞与安全隐患频发的问题，探索一套覆盖“开发-验证-认证”全过程的软件可信保障技术体系，具体包括：提出融合规约与自动证明能力的开发-验证一体化开发环境；研制大语言模型增强的多层级高效协同形式化验证平台；提出基于证据链的软件安全认证过程管理机制与工具；在国产新型安全架构操作系统等基础软件中开展应用验证。大幅提高基础软件的形式化验证效率和可验证代码规模，为推动高等级认证技术应用、提升国家信息基础设施系统可信度提供关键技术支撑。

研究内容：研究融合多维度规约的一体化开发-验证方法，突破函数契约、精化关系和超性质三个维度的语言增强技术，实现开发与验证深度融合的开发环境；研究大语言模型增强的形式化验证生成技术，构建有不同人工参与度的形式化验证技术的高效协同机制，覆盖轻量级的静态分析、中量级的类型系统与自动

定理证明、重量级的交互式定理证明，实现基础软件的形式化验证平台；研究基于证据链的认证过程管理机制，构建覆盖软件认证全流程的证据可追溯、可复用的支撑工具；针对新型安全架构操作系统的关键组件，进行形式化验证；针对用于网络设备与工控设备的国产嵌入式操作系统，进行安全认证。

考核指标：完成开发-验证一体化的形式化验证平台和认证支撑工具及相关实践验证：验证增强编程语言覆盖 C99 标准中不少于 90%的语法与语义要素，覆盖范围不低于主流编译器 Clang；针对实际软件项目验证过程中产生的定理，大语言模型增强的自动定理证明功能可自动证明的数量不低于 30%；针对链表、树等常用数据结构实现，与主流验证平台 Rocq 相比，验证效率提升 50%以上；手动编写的验证代码降至所验证的程序代码行数的 10 倍以下；针对新型安全架构操作系统等基础软件的关键组件，完成形式化验证，通过验证的代码总规模超过 5 万行；应用认证支撑工具支撑 1 款国产嵌入式操作系统通过 CC EAL6 认证，具备通过 CC EAL7 认证的能力。

实施期限：3 年

项目密级：公开

立项要求：支持 1 个项目，采用公开竞争方式。

中央财政资金支持方式：事前立项事前补助。配套资金与中央财政资金不低于 1:1 匹配。

3.9 新一代机密计算技术体系研究

研究目标：针对当前机密计算技术软硬件协同能力不强、大规模并发效率低的问题，构建软硬件协同信任的新一代机密计算框架，提出多信任根机密计算模型并完成形式化安全分析，支持大规模机密计算节点并发，基于国产信创硬件和可信安全芯片构建全栈可控的新一代机密计算技术体系。

研究内容：研究软硬件协同信任的机密计算框架，研究融合多信任根的软硬件协同机密计算模型，通过形式化方法验证机密计算架构的安全性；研究基于国产信创硬件的可信执行环境和国产安全芯片的通用远程证明与可信安全机制，设计机密计算抗量子 TLS 新型远程证明协议并证明其安全性；研究基于开放环境的机密虚拟机及机密容器设计技术；研究面向人工智能大模型密态微调和推理的隐私保护框架，保障大模型数据安全利用与隐私增强；研制跨平台、跨架构的通用机密计算标准，研究硬件异构 TEE 平台测评技术。

考核指标：提出多信任根软硬件协同机密计算模型，支持大规模机密计算节点的并发证明，1000 个以上异构节点的并发证明时间小于 1.5 秒；支持鲲鹏、海光等国产 TEE 处理器，基于 SM2/SM3/SM4 国密算法 TEE 数据加解密吞吐量 200MB/s 以上，TEE 远程证明签名性能至少 1 万次/秒；实现机密虚拟机/容器/TPM 的多信任根协同信任和安全恢复，支持 5 种以上节点类型；设计基于国产处理器的机密计算安全操作系统内核；实现对机密

计算系统核心安全属性的分析验证；研制异构 TEE 机密大模型推理系统，支持不少于 2 种国产 xPU、不小于 7B 的大模型机密推理；建立全密态数据空间基础设施，基于国产 TEE 完成至少 3 个重要行业应用验证；制定机密计算标准草案，具备硬件异构 TEE 平台测评能力。

实施期限：3 年

项目密级：公开

立项要求：支持 1 个项目，采用公开竞争方式。

中央财政资金支持方式：事前立项事前补助。配套资金与中央财政资金不低于 1.2:1 匹配。

3.10 深空网络安全基础研究

研究目标：针对深空网络在非受控环境下面临的物理威胁和网络空间威胁，构建“真实可信、智能协同、动态防御、高效监管”的新一代深空网络安全防御体系。重点突破深空网络新型安全协议体系关键技术、深空网络新型安全防御机制，形成以互联网协议体系为核心的深空网络安全标准与技术规范，从体系结构层面整体提升我国深空网络在复杂对抗环境下的生存性、可用性、安全性。

研究内容：研究深空网络新型安全路由技术，包括动态时变网络环境下的可信编址与寻址技术、智能化安全路由策略；研究深空网络新型传送安全技术，包括分段式数据完整性校验机制、

高安全深空传送体系、多元信息感知与智能流控决策的新型安全传送机制；研究深空网络新型算力服务安全技术，包括星载人工智能安全防御新机制、能耗感知驱动的星载资源管控；研究网络安全新型监管体系，包括监管权限分配与执行机制、灵巧信息安全管控技术；研究深空网络动态拓扑实时异常检测方法，包括基于深空网络攻防领域大模型的攻击溯源方法、未知攻击大小模型协同安全推理方法；研究地基信息风险动态评估方法和未知信息主动感知与预判方法。

考核指标：提出动态时变网络环境下可信编址、寻址技术及其安全协议体系，具备路由防篡改、巨型星座安全智能驾驶等功能，完成国际/国内标准草案 2 项；提出深空网络新型传送安全技术，支持在强干扰、高丢包、连接间歇性中断以及节点损毁等极端条件下的智能化主动修复与安全传送；提出面向星载人工智能的在轨训练方法，具备应对训练推理能耗攻击等新型安全威胁的能力；建立全路径多环节监管评估体系，支持 2 种以上评估模型；建立天地一体化网络信息安全管控模型，支持不少于 5 类信息和 3 个安全等级；深空网络攻击检测准确率大于 85%、攻击溯源准确率大于 80%；检测未知攻击的可信模型能免疫错误注入、参数窃取、成员推理等强力攻击；构建地基重点区域的精准控制模型与方法，支持不少于 2 类重点区域；支持对特定关键信息的快速识别控制和对大规模流数据的持续识别过滤，识别准确率大于 80%；面向重要行业或应用场景进行应用验证。

实施期限：3 年

项目密级：公开

立项要求：支持 2 个项目，采用公开竞争方式。

中央财政资金支持方式：事前立项事前补助。配套资金与中央财政资金不低于 1.1:1 匹配。