国科发资〔2017〕294 号附件 10

“网络空间安全”重点专项
2018 年度项目申报指南

为落实《国家中长期科学和技术发展规划纲要（2006-2020 年）》提出的任务，国家重点研发计划启动实施“网络空间安全”重点专项。根据本重点专项实施方案的部署，现发布 2018 年度项目申报指南。

本重点专项总体目标是：聚焦网络安全紧迫技术需求和重大科学问题，坚持开放发展，着力突破网络空间安全基础理论和关键技术，研发一批关键技术装备和系统，逐步推动建立起与国际同步，适应我国网络空间发展的、自主网络空间安全保护技术体系、网络空间安全治理技术体系和网络空间测评分析技术体系。

本重点专项按照网络与系统安全防护技术研究、开放融合环境下的数据安全保护理论与关键技术研究、大规模异构网络空间中的可信管理关键技术研究、网络空间数字资产保护创新方法与关键技术研究、网络空间测评分析技术研究等 5 个创新链（技术方向），共部署 49 个重点研究任务。专项实施周期为 5 年（2016-2020 年）。

2016 年，本重点专项在 5 个技术方向已启动 8 个研究任务的

8 个项目。2017 年，在 5 个技术方向已启动 14 个研究任务的 14 个项目。2018 年在 3 个技术方向启动 6 个重点研究任务，拟支持 6-12 个项目，拟安排国拨经费 1.53 亿元。凡企业牵头的项目须自筹配套经费，配套经费总额与国拨经费总额比例不低于 1：1。

项目申报统一按指南二级标题（如 1.1）的研究任务进行。除特殊说明外，每项研究任务拟支持项目数均为 1-2 项。项目实施周期不超过 4 年。申报项目的研究内容须涵盖该二级标题下指南所列的全部考核指标。项目下设课题数原则上不超过 5 个，每个课题参研单位原则上不超过 5 个。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。

指南中“拟支持项目数为 1-2 项”是指：在同一研究方向下，当出现申报项目评审结果前两位评价相近、技术路线明显不同的情况时，可同时支持这 2 个项目。2 个项目将采取分两个阶段支持的方式。第一阶段完成后将对 2 个项目执行情况进行评估，根据评估结果确定后续支持方式。

1. 网络与系统安全防护技术研究方向

1.1 物联网与智慧城市安全保障关键技术研究（共性关键技术类）

面向物联网节点计算资源、体积、功耗受限和网络规模、复杂度提升带来的安全挑战，研究物联网安全体系架构；研究在大连接、异构数据、时延复杂的条件下，能够与物联网节点融合的一体化安全机制；研究基于标识技术的安全物联网互联互通架构；

研究大规模信任服务机理及关键技术，包括安全协商、数据完整性与机密性、跨域设备身份与认证服务等；研究大规模设备监控技术，实现在无安全代理条件下设备自动发现、识别及状态、行为智能感知；研究智慧城市安全保障总体技术架构；研究支持智慧城市统一管理且支持隐私保护的智慧小区或智慧家庭适用的安全技术架构及其相关原型系统。

考核指标：

1．提出适应智慧城市与物联网安全目标的模型和体系框架，指导智慧城市与物联网安全实践；

2．研制安全物联网原型平台，支持大规模物联网对象的分级分层管理与安全解析，物联网设备发现、识别和监控以及身份认证、密钥管理服务均支持 10 亿规模；

3．设计完成采用国家标准密码算法的物联网管理域的强逻辑隔离安全机制，安全隔离方案应通过国家主管部门的安全审查；

4．设计完成多物联网管理域之间的受控互联互通机制与协议，支持基于身份和基于角色的授权策略映射，支持时间、环境以及安全上下文敏感的授权管理，其中时间粒度应不大于 1 分钟，支持的环境鉴别应包括物理位置、网络接入途径、操作系统安全配置等因素；

5．开发完成支持智慧城市统一管理的适用于智慧小区或智慧家庭适用的安全控制中心、安全网关、智能防火墙等原型系统，

具有隐私保护能力、深度感知与检测能力，相关原型系统应通过权威部门测评，并得到试点应用；

6．申请发明专利不小于 10 项。

1.2 工业控制系统安全保护技术应用示范（应用示范类）

研究工业控制系统（ICS）主动防御技术体系，抵御跨越信息物理空间的未知威胁；研发主动防御安全网关、安全管理系统、未知威胁主动发现与跟踪溯源系统、控制运行系统与编程编译系统等相关组件、工具与控制装备，改进提高相关组件、工具与控制装备的行业工程适应性；研究开发典型行业主动防护的设备驱动组件集与工程应用模板；研究 ICS 综合安全评估认证技术，建立综合安全定量评估体系；从基础设备安全、实时控制行为安全、业务流程作业安全等维度，构建结合功能安全、信息安全、操作安全，覆盖 ICS 管理层、监控层、控制层、器件（部件）层，贯穿控制工程的设计、运行、服务等全生命周期的自主可控深度安全主动防护体系；突破功能安全与信息安全深度融合场景下的工控安全防护难题，保障 ICS 全生命周期的安全性、可用性、可靠性与稳定性；在电力、冶金、石化等重点行业关键场景进行规模化应用示范，形成相关行业示范的安全测评报告与深度安全的主动防护解决方案。

考核指标：

1．针对电力、冶金、石化等重点行业关键场景，考虑高可

用性、强实时性、大规模化、广域全局协同等工业控制系统的典型工程特征，完成3类关键行业领域的3至5套控制系统安全脆弱性测试；

2．针对工业控制系统核心控制设备（控制器、变送器、执行机构、工作站、网络设备等）以及关键控制数据交互的安全需求，构建识别、保护、检测、响应一体化的主动防护安全技术示范体系，覆盖控制系统基础设备安全、实时控制行为安全、业务流程作业安全的主动防护安全技术示范体系，覆盖控制系统管理层、监控层、控制层与部件层的各层次，实现总体功能覆盖率不少于90%，形成示范验证报告；

3．分析评估深度安全保护技术对工控系统功能流程及性能指标需求的影响，以及工业控制系统脆弱性与威胁事件间的关联关系；实现工业控制系统深度安全对系统功能业务流程无影响，深度安全主动防护功能对运行态实时性能影响<10%，对编程态性能影响<25%；提出工业控制系统综合安全评估认证技术方案，建立典型工业控制系统应用现场的安全性定量评估体系；

4．应用试点工业控制主动防御示范场景不小于 3 个，包括电力、冶金、石化等，其中至少1个高可用性与强实时性的局域万点级示范场景，该场景的工业数据不少于10000点，工业控制节点不少于 30 个，各类控制终端不少于 100 个，典型控制周期50-100ms，快速控制周期5-20ms；至少1个大规模化与广域全局

协同的万点级示范场景，该场景工业数据不少于30000点，信息域不少于5个，控制节点不少于100个，各类控制终端不少于300个，典型控制周期50-500ms，跨域数据同步0.5-10s。

2. 开放融合环境下的数据安全保护理论与关键技术研究

2.1 移动互联网数据防护技术试点示范（应用示范类）

面向移动互联网应用，基于国产密码算法，从云、管、端三个层面布局移动互联网数据防护保障技术，完成试点示范。研究智能移动终端的数据防护技术和基于终端的高安全鉴别技术，完成基于国产密码算法的智能移动终端数据安全存储、数据安全计算、数据安全擦除、数据访问控制与安全鉴别方案，防范各种软件攻击和终端丢失情况下的关键数据泄露；研究智能移动终端的用户个人隐私数据保护技术方案，保护用户的身份和属性隐私、位置隐私、交易隐私；选择有代表性的移动互联网云服务应用，研究移动业务的全生命周期安全技术，包括移动设备管理技术、应用软件管理技术、文档内容管理技术，支持多级安全策略管理，实现国产密码技术在移动业务安全系统中的深度融合；研究移动高速视频服务中的数据加解密技术，实现透明化的、无缝接入的数据加解密服务；针对移动设备管控、移动高速视频服务等应用完成试点示范系统。

考核指标：

1．完成移动终端数据与隐私保护技术方案设计开发。技术

方案全面支持国产密码算法，能够抵御操作系统内核攻击，安全原理简洁易证,并在至少 2 款商用移动终端系统中得到应用部署，实现万台规模的试点应用；

2．示范应用中移动智能终端的数据签名速度不大于 50ms，关键数据的加解密速度不少于 10Mbps；

3．在移动管控领域开展试点应用。移动设备管控的应用部署不小于 2 家应用单位，支持 30 款以上主流移动终端；

4．在大型的移动高速视频云服务系统中得到部署，终端加解密时延不大于 8ms，示范终端数量不少 800；

5．申请发明专利 20 项。

3. 网络空间数字资产保护创新方法与关键技术研究

3.1 互联网+环境中基于国产密码的多媒体版权保护与监管技术（共性关键技术类）

面向互联网+环境中媒体融合及 4K 超高清视频播控以及虚拟现实（VR）对多媒体版权保护与监管的新需求，研究互联网+环境中基于国产密码算法的多媒体版权保护方案；研究支持国产密码算法的多媒体版权保护技术，重点研究新一代视频加密授权技术、基于硬件安全的智能终端版权保护技术、融合媒体智能终端安全认证技术、融合媒体版权监管技术及测试评估方法等共性关键支撑技术；研究 VR 和超高清视频版权保护技术要求与测试规范，研发支持国产密码的超高清视频内容版权保护系统关键装

备及版权保护服务平台，研发智能电视终端芯片；选择至少3个具有互联网电视集成播控平台资质的机构开展基于国产密码算法的超高清视频内容版权保护技术试点示范，全面提升我国融合媒体版权保护支撑保障能力。

考核指标：

1．完成基于国产密码算法的超高清视频内容版权保护系统关键装备研发，包括支持基于国密算法的超高清视频内容实时转码加密系统、基于容器的版权保护授权系统等，获得主管部门颁发的产品证书；

2．完成支持国产密码算法的智能电视终端芯片与超高清电视一体机等原型设备研制，支持基于国产密码算法的智能终端硬件信任根、基于硬件安全的安全启动与安全升级，以及视频内容解密、解码、缓存、播放、显示、输出全流程的硬件级别安全保护；

3．完成基于国产密码算法的互联网电视数字版权保护服务平台研发，支持4K超高清视频及VR内容的实时转码加密、智能终端分布式实时授权等版权授权服务，支持版权追踪溯源与实时版权监测服务，其中版权授权服务响应时间小于5秒；

4．制定超高清视频版权保护总体要求、信任与安全体系、终端安全性要求、接口协议、测试方法等方面行业标准规范5项，并获得行业标准主管部门立项或批准，集成研发支持国产密码的

融合媒体版权保护产品与系统测试评估平台，支持对应用国产密码算法的超高清视频内容版权保护系统、智能终端及芯片等的安全评估与测试；

5．选择至少 3 个具有互联网电视集成播控平台资质的机构开展不少于 50 万用户的基于国产密码算法的超高清视频内容版权保护技术试点示范，验证系统有效性；

6．申请发明专利 20 项以上，软件著作权 20 项以上。

3.2 数字电视条件接收系统国产密码应用的关键技术（共性关键技术类）

面向卫星直播及互联网广播环境下，数字电视系统盗播、插播严重，追究困难的问题，研究安全、高效的条件接收系统，研究盗播、插播监管与追踪关键技术；研究支持国产密码算法的数字条件接收层级密钥管理技术；开发支持国产密码算法的条件接收系统前端设备、终端安全芯片和终端设备；建设支持国产密码算法的密钥管理平台，包括密钥保护技术、密钥传输技术和芯片序列化技术等；面向下一代广播电视网（NGB），开展支持国产密码算法的新一代条件接收系统规模应用示范，解决产业化的瓶颈问题；研究基于国产密码算法的数字电视条件接收设备的检测技术。

考核指标：

1．完成一套支持国产密码算法的，适应卫星及互联网环境

的数字电视条件接收系统研制，具备可证明的防盗播、防插播技术特性，具备支持4亿以上用户的能力，终端开机密钥初始化时间不大于30秒；

2．完成支持国产密码算法的新一代条件接收系统前端系统，终端安全芯片和终端系统研制，相关系统及芯片获得主管部门的产品证书；

3．密钥管理支持密钥保护、密钥传输和芯片序列化等；

4．在至少 2 个省级广电网络中开展新一代数字电视条件接收系统应用示范；

5．申请发明专利 4 项，完成至少 8 项软件著作权，提交至少两项行业标准草案，并获得行业标准主管部门立项或批准。

3.3 支持全程电子化的电子发票及服务系统试点示范(应用示范类)

面向“互联网+”应用环境，开展全程电子化的安全电子发票及服务系统的应用示范；研究安全电子发票服务运行机制，搭建规模化的电子发票服务与监管系统，并开展示范应用；针对税务类电子发票，研究基于通用平台的电子发票承载、验证和传递设备；搭建面向公众服务的电子发票第三方可信验证平台，完成企业电子发票报销、财务管理及供应链管理等应用的试点示范。

考核指标：

1．完成至少 5 个电子发票服务系统的建设与试点应用，电

子发票开具量达到 1 亿张/年，实际环境中，单张发票开具时间不多于 10s，可离线验证的单张发票数据量不大于 5K Bytes；

2．完善基于通用平台的电子发票承载、验证和传递系统，在不少于 10 家应用单位进行部署；

3．研制完成电子发票第三方验证系统，并发访问数为 5000 时，单张凭据验证请求的响应时间小于 2 秒；

4．电子发票开具服务覆盖至少 20 个省或直辖市；

5．除电子发票开具应用外，电子发票电子化接收应用试点单位数达到 300 个；

6．完成国家或行业标准草案不少于 3 项，并获得国家或行业标准主管部门立项或批准。