附件 1

网络安全技术应用试点示范重点方向

一、新型信息基础设施安全方向

（一）云计算安全。面向多云、云原生、边缘云、分布式云等新型云计算架构，云环境中云主机、云存储、云网络等基础资源，以及云上业务、应用等服务，采用云身份管理、软件定义边界、云工作负载保护等技术实现云架构安全、多网边界隔离、跨网安全交互、多网一体化防护，保障云上资源安全可靠、云上业务运行稳定的安全解决方案。

专栏 1　云计算安全重点方向
公有云安全。面向云、网、应用深度融合场景需求，在公有云用户提供集约化、数据互通、云网一体化，以及集网络安全、主机安全、数据安全、应用安全于一体的安全解决方案。 **政务云安全**。面向政务网、互联网跨网一体化防护需求，采用云上多网边界隔离、数据分类分级、跨网安全交互、终端集中管控及安全隔离等技术，在多网“一朵云”、“一端多网”安全管控等方面的安全解决方案。 **媒体云安全。**结合融合媒体智能生产、多渠道播出分发、网络直播点播、视听应用 APP、媒体智能终端、监测监管等需求，在媒体内容安全、播出安全、分发安全、平台安全、应用安全等方面的安全解决方案。 **工业云安全。**围绕推动工业设备和业务系统上云，构建基于云、网、端的协同联动防护体系，加强双栈流量可视化、微隔离、软件定义边界、云工作负载保护、云上数据保护等安全能力的解决方案。

（二）人工智能安全。面向智慧工厂、智能通信、智慧金融、公共安全等典型应用场景，针对人工智能基础研发平台、核心算法、训练数据、智能应用的安全需求，在机器学习框架漏洞挖掘和修复、算法鲁棒性及公平性评测和增强、数据泄露安全防护、智能应用安全风险监测预警等方面的安全解决方案。

专栏 2　人工智能安全重点方向
人工智能基础设施安全。面向高效能计算基础设施，在人工智能公共数据资源库、标准测试数据集、算法与平台安全性测评工具集等方面的安全解决方案。 **基础网络安全智能防御。**发挥骨干网络和基础资源优势，在提升基础网络安全感知、分析、响应、决策等综合防控能力，实现网络安全威胁快速溯源定位等方面的安全解决方案。 **金融交易欺诈和钓鱼欺诈智能防范。**针对金融业智能高效的交易反欺诈、跨行业联防联控反钓鱼等安全需求，建立事前防范、事中监控、事后处置三位一体的智能金融反欺诈安全解决方案。

（三）大数据安全。面向优化数据安全治理，推动密码技术、区块链等为数据安全增效，在数据应用安全防护、存证取证、监测预警和应急处置、隐私保护和流向溯源、国产商用密码应用等方面，探索数据确权、流通、共享新业态新模式，实现数据资源可视、可管、可控，促进数据有序流动的安全解决方案。

专栏 3　大数据安全重点方向
大数据基础设施安全。在推动构建绿色、集约、安全的大数据中心，促进数据资源安全整合、安全共享，强化大数据安全保障支撑、网络安全信息共享和重大风险识别等方面的安全解决方案。

金融大数据安全。结合金融核心业务和大数据分布特点，基于金融多源情报融合分析技术，构建大规模复杂异构金融服务模拟网络，支持常态化、高频度、多样化攻防实战演练等方面的安全解决方案。

广播电视与网络视听大数据安全。结合广播电视和网络视听媒体内容、网络、用户、运营和系统运行等大数据的安全需求，在提升数据防泄露、防篡改、防窃取等传统数据安全保障能力，优化数据安全管理、分类分级安全防护、深度伪造视频鉴别等方面的安全解决方案。

交通运输旅客信息安全。面向铁路、民航等涉旅客用户个人信息安全需求，在保障铁路和民航信息系统、第三方票务软件安全，防范旅客信息在传输、处理、存储过程中被泄露或篡改等的安全解决方案。

医疗健康数据安全。面向疾病预防控制信息系统、医院信息系统和数据库安全保障支撑，打通卫生健康领域数据壁垒，确保数据访问安全及第三方数据交换中用户隐私、临床、科研和综合管理信息等重要数据安全的解决方案。

商用密码应用。针对商用密码在数据传输加密、数据存储加密、大数据加密、数据接口安全等业务场景应用，在密码设备、加密计算、加密搜索、数据全生命周期管控、接口防护等方面的安全解决方案。

二、数字化应用场景安全方向

（四）车联网安全。面向在线升级（OTA）、远程诊断监控、自动驾驶、车路协同、智慧交通等典型场景，针对智能驾驶系统、联网关键设备、网络基础设施、车联网服务平台等网络安全需求，在轻量化防护、安全认证、数据合规、威胁监测、应急处置、检测评估等方面的安全解决方案。

专栏 4　车联网安全重点方向
在线升级（OTA）安全。面向汽车动力/电池系统、底盘系统、车身

系统等 OTA 升级场景网络安全需求，在 OTA 升级服务全过程安全监测和应急响应，以及 OTA 安全检测等方面的解决方案。

车辆远程诊断监控安全。结合车联网远程诊断、远程控制、远程监测等场景安全需求，在安全认证、“云-管-端”一体化协同防护等方面的安全解决方案。

车联网 C-V2X 通信安全。面向车云、车车、车路、车设备通信安全需求，在重点城市、高速公路、园区码头等应用场景下，汽车、联网设施安全认证及通信安全保障等方面的解决方案。

（五）物联网安全。面向智能家居、智能抄表、零售服务、智能安防、智能穿戴设备等典型场景应用，在物联网终端设备及固件安全威胁监测、固移融合物联网安全接入、异构物联网端到端安全防护、物联网平台安全防护等方面的安全解决方案。

专栏 5　物联网安全重点方向

智慧家居安全。面向智能家电、智能照明、智能安防监控、新型穿戴设备、服务机器人等场景网络安全需求，在媒体框架安全防护、远程控制、测试验证、设备资源共享协同等方面的安全解决方案。

水利感知网安全。结合智慧水利感知网等安全需求，在传感器芯片、嵌入式加密、物联网网关、物联网平台安全保障，强化网络攻击监测等方面的安全解决方案。

智慧应急物联网安全。围绕安全生产监管、城市安全管理、自然灾害监测预警及应急处置等过程中接入的物联网设备暴露面大、认证方式单一、联网协议复杂、技术标准不统一等现状，在物联网终端认证、安全传输、信息利用、威胁综合监测等方面的网络安全解决方案。

（六）智慧城市安全。适配智慧城市政务、交通、能源、制造、教育、医疗等业务场景，构建网络安全防御能力集群、智慧

城市安全大脑，实现网络安全感知、分析、响应、决策能力提升，大规模临时组网安全能力快速部署，以及城市安全运行保障等的安全解决方案。

专栏 6　智慧城市安全重点方向

智慧政务安全。面向电子证照、电子合同、电子签章、电子发票、电子档案等政务服务一网通办场景安全需求，在促进政府资源优化配置和数据流动等方面的安全解决方案。

智慧社区安全。面向车辆管理、物业管理、社区服务、应急救援救护、智慧养老等场景网络安全需求，在促进政务服务平台、社区感知设施和家庭终端联动，提升社区管理数字化方面的安全解决方案。

智网融合安全。围绕“5G+”智慧交通、智慧医疗、应急通信等融合应用场景，在服务城市网络基础设施安全保障，提升实时感知、精准研判、快速处置水平等方面的安全解决方案。

城市应急通信。面向城市大震大灾等灾害场景，在紧急构建集无线通信、卫星通信、边缘计算等融合通信网络，建设一体化安全防护设备和边缘安全分析系统，实现应急组网的网络安全解决方案。

三、基础安全能力提升方向

（七）网络安全共性技术。以促进公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域网络安全能力为目标，面向关键软硬件安全，在基础技术、工具、协议等方面的创新攻关成果，面向传统防护类、检测类、分析类网络安全产品，在能力集约化、智能化、精益化等方面的优化升级，以及面向网络开放互联、边界模糊、暴露面扩大等共性问题，在强化网络安全架构内生、自适应发展等方面的安全解决方案。

（八）网络安全创新服务。提供安全防护一体化，安全托管、安全咨询、安全运营等安全服务专业化，安全能力自动化、流程化、工具化，威胁情报精准化、智能化的公共服务平台。提供网络安全基础知识库、底层引擎、网络仿真环境、安全孪生试验床等的共性基础支撑平台。为重要行业领域提供网络资产测绘、漏洞挖掘、监测预警、检测评估、应急处置、态势感知、信息共享、攻击溯源等的专业服务平台。

专栏 7　网络安全服务创新重点方向

电信网络安全。面向基础通信网络、大型互联网平台网络安全需求，基于网络侧木马病毒、移动恶意程序和高级持续性威胁等监测处置技术，实现网络资产测绘、监测预警、应急处置等的安全解决方案。

电力系统安全。适配电网侧调度控制系统、配电监控系统、电源侧各类型电厂监控系统及虚拟电厂、新型储能、用电侧负荷聚合平台业务发展，在网络安全防护体系结构、典型场景防护策略、安全支撑系统平台等方面的安全解决方案。

水利系统安全。面向水利设施和控制系统，在计算设备、网络隔离、基线管理、威胁监测、漏洞防护、应急处置，以及网络空间拓扑绘制、资产智能测绘、网络安全影响建模等方面的安全解决方案。

广播电视专网安全。面向广播电视专网系统，在网络流量分析、网络攻击监测发现、资产和漏洞发现管理、威胁预警管理等方面的安全解决方案。

金融网络安全。围绕金融核心业务，面向银行、证券、保险等金融信息系统，建立应对数字化转型的网络安全运营体系，在网络安全靶场、威胁情报关联分析、资产测绘及漏洞处置机制等方面的安全解决方案。

（九）网络安全“高精尖”技术创新平台。结合前沿性、创新性、先导性的重大网络安全技术理念，汇聚产学研用等创新资源，加快实现网络安全“高精尖”技术创新融合，打造具备核心技术攻关、产业化应用推广等关键环节协同创新环境和载体的网络安全技术创新或试点示范区，打造产融合作的网络安全产业生态优化解决方案。