上海市经济和信息化委员会文件

沪经信软〔2023〕1192 号

上海市经济信息化委关于开展 2023 年重点行业网络安全解决方案揭榜工作的通知

有关单位:

为保障本市重点行业数字化转型过程中的网络安全、数据安全建设需求，加快牵引一批示范应用场景，形成一批行业解决方案，打造一批专业服务厂商，根据《上海市经济信息化委关于开展 2023 年重点行业网络安全建设需求征集的通知》（沪经信软〔2023〕988 号），我委组织开展了场景需求征集，形成了网络安全建设需求清单，现集中开展网络安全解决方案揭榜挂帅（以下简称“揭榜”）工作。有关事项通知如下。

一、揭榜内容

本次揭榜包括上海复星医药（集团）股份有限公司、上海振华重工（集团）股份有限公司、中远海运科技股份有限公司、上

海汽车集团服份有限公司乘用车分公司、上海申通轨道交通检测认证有限公司、上海汽车集团股份有限公司技术中心、上海微创医疗器械（集团）有限公司、上海核工程研究设计院股份有限公司、工业互联网创新中心（上海）有限公司、联创汽车电子有限公司、零束科技有限公司、上海弘卓网络科技有限公司等企业（以下简称“发榜企业”）的十二个应用场景和安全需求，征集相应的网络安全解决方案。具体内容见附件 1。

二、揭榜要求

（一）揭榜主体资格。揭榜单位应在中华人民共和国境内注册、具备独立法人资格，信用良好且具有较好的网络安全融合创新、项目集成建设等能力。鼓励各揭榜单位组建申报联合体，为发榜企业提供理念先进、技术一流、集成度好的整体安全解决方案。

（二）揭榜意向征集。12 月 22 日前，各揭榜单位根据自身优势和市场竞争能力条件确定揭榜意向，填写揭榜意向征集表（附件 2）并反馈至联系邮箱。

（三）解决方案揭榜。12 月 28 日前，市经济信息化委将组织发榜企业开展集中需求解读，为揭榜单位做好解决方案编制的对接服务。2024 年 1 月 12 日前，各揭榜牵头单位将《2023 年重点行业网络安全解决方案揭榜申报书》（附件 3）一式三份及电子版报市经济信息化委。同一揭榜主体最多牵头揭榜两项建设需求。

（四）方案评审。2024 年 1 月底前，市经济信息化委组织发榜单位、相关行业以及网络安全领域专家开展解决方案评审工作，遴选行业优秀解决方案。

（五）方案实施推广。市经济信息化委将加强评估，推动相应方案落地实施。对其中符合本市促进产业高质量发展等专项支持政策的相关工程项目，予以支持；对纳入应用场景解决方案的创新产品，推荐纳入《上海市创新产品推荐目录》；对解决行业共性问题，可复制推广的优秀方案及经验做法，将在征询有关企业及方案提供厂商意见后，加强案例的行业推广和宣传报道，有条件的将推动制定相应技术标准。

三、联系方式

（一）联系人：代淑杰、华宇涵

（二）电话：18521402980、021-23112657

（三）地址：懿德路519号1号楼903室

（四）邮箱：admin@sisa.org.cn

附件：1.2023年重点行业网络安全建设需求清单

2.揭榜意向征集表

3.2023年重点行业网络安全解决方案揭榜申报书

上海市经济和信息化委员会

2023年12月14日

附件 1

2023 年重点行业网络安全建设需求榜单

一、上海复星医药（集团）股份有限公司——医药研发数据分类分级及外溢风险管理

（一）场景应用简介

医药研发数据主要包括先导化合物筛选、临床前、临床试验、药品申报、上市后疗效副作用跟踪、销售额、专利和文献等数据，涉及对个人信息、医疗数据、病历资料、人类遗传资源、健康大数据、临床试验数据等数据处理。

（二）安全需求简介

目前未对全量的研发数据进行统一的盘点、识别及管控，需针对医药研发数据实行数据分类分级，形成切合自身的制度和标准，并对分类分级数据实行相应的保护措施，防止重要研发数据外溢及合规风险。

（三）分项需求清单

建设内容	技术参数/能力要求	交付类型
研发数据分类分级，对研发数据进行盘点与识别，制定数据分类分级制度及标准，按照既定制度或标准进行归类、确定等级，并识别在数据全生命周期中的合规风险。	具有医药行业数据分类分级经验案例；主导进行研发数据分类分级工作落地及合规识别。	咨询服务及文档
基于分类分级制度，针对研发数据外溢风险管理，对数据采集、数据传输、数据存储、数据使用、数据共享、数据销毁等进行管控以及识别合规风险。	能够提供一体化数据安全解决方案，不仅限于加密、DLP、备份等技术能力，了解并能够应对外部合规监管风险。	产品及服务

二、上海振华重工（集团）股份有限公司——企业级 IoT 数据安全及网络安全

（一）场景应用简介

振华重工正在推进 IoT 数字化建设，需采集各生产基地的设备、能耗及其他生产数据，建立统一数据源、统一口径的基于数据的生产运营监控与决策支持体系，为 ERP、MOM 平台提供生产数据底层支撑，为建设智能制造管理平台建立基础。

（二）安全需求简介

振华重工 IoT 平台数字化建设项目，部署于公司总部数据中心，各基地现场部署工控相关设备，通过工业防火墙与各基地办公网络逻辑隔离，经安全策略管控后，与总部数据中心连接，各基地以专线方式与总部连接，实时将工控数据传递至平台进行分析处理。在工控数据传输过程中，由于工厂及设备都比较老旧，部分设备加装了 4G 模块，由 4G 通过互联网传输至总部数据中心，很难做到在工厂侧做到统一的数据出口安全。

（三）分项需求清单

建设内容	技术参数/能力要求	交付类型
IoT 数据安全建设: 通过数据分类分级产品，实现智能识别港机装备制造业数据类型，完成数据分类、分级，在此基础上实现数据安全建设。	自动识别数据类型，进行数据分类、分级及数据安全建设。	产品
IoT 网络安全建设: 工控安全产品的运维及管理难度远高于传统网络安全，希望将工业网络安全产品（如工业日志审计类产品、流量分析类产品、工业防火墙类产品等）整合至一套产品中。	工业级硬件，无风扇全封闭设计、冗余电源、满足工业现场恶劣环境应用，支持多种工业协议。	产品

三、中远海运科技股份有限公司——云平台漏洞治理

（一）场景应用简介

作为新型基础设施，云计算对企业的数字化转型至关重要，为此中远海科专项研发建设了云计算平台，并逐步推进“应用上云”。由于存在规模庞大、复杂多样的特点，在云平台建设和“应用上云”过程中也可能存在较大的网络安全风险，需要有针对性的对重点组件形成一套有效的漏洞发现和治理框架，并利用揭榜机制和产学合作模式，形成示范性试点应用，全面提升云计算环境的健壮性。

（二）安全需求简介

中远海运科技近年来正在配合中远海运集团大力推进专有云建设和应用上云等工作，云平台漏洞治理工作需要能够适应“云优先”和“云原生”的应用环境，全面考虑复杂技术组件的安全场景,确保识别云平台漏洞的全面性和准确性,并在 2024 年完成。云平台架构和漏洞数据本身作为技术敏感信息，存在泄露风险，要重点防护，并且需要满足各方面合规要求,包括但不限于《网络安全法》、《数据安全法》、《个人信息保护法》和《密码法》以及等级保护等法律法规、标准要求。

（三）分项需求清单

建设内容	技术参数/能力要求	交付类型
全面考虑云平台技术组件的安全场景，针对重点组件开展风险评估，提出漏洞发现和治理的技术框架，形成示范性试点应用。	1）具有独立法人资格; 2）可在上海本地完成技术服务，具备相关技术研究和服务能力。	外包服务

四、上海汽车集团股份有限公司——智能网联汽车车端数据安全及网络安全合规建设

（一）场景应用简介

聚焦智能网联汽车的两大痛点，开展相关能力建设。第一项为匿名化处理：哨兵模式、远程泊车、极拍等功能场景的实现均涉及个人敏感数据匿名化处理效果是否合规，随着国内数据安全及网络安全标准的落地，功能场景的合规性直接影响到车型产品公告能否通过；第二项为远程控车 app：为了提供更优质的用户体验，远程控车 app 被广泛应用，100%覆盖智能网联汽车，但是由于每款车型的用户群体不够广泛，app 的加固及更新迭代不够及时，比较容易被黑客利用。

（二）安全需求简介

当前对于数据安全及网络安全已有 GDPR、《智能网联汽车数据通用要求》、UN ECE R155、《汽车整车信息安全技术要求》等合规要求，企业产品在开发及公告过程中应充分考虑合规风险，基于已有的数据安全、网络安全开发框架，形成重点功能场景的合规性检测能力，提供合规检测服务。

（三）分项需求清单

建设内容	技术参数/能力要求	交付类型
出车数据匿名化效果合规性评价，支撑功能场景开发迭代。	供应商应具有正向开发经验，向用户提供过数据匿名化产品。	系统平台
控车 app 合规检测，对 app 漏洞挖掘，识别 app 应用风险。	具备 app 逆向、加壳、脱壳、代码混淆等分析能力。	测试工具及测试能力
作为第三方试验室提供数据安全及网络安全合规检测服务。	具备数据安全合规检测能力、网络安全合规检测能力，并具备第三方试验室资质及服务体系。	外包服务

五、上海申通轨道交通检测认证有限公司——城市轨道交通网络安全关键产品检验检测平台建设

（一）场景应用简介

为了满足城市轨道交通产业发展，对网络安全产品的选用及管理进行统一规范，形成轨道交通企业网络安全产品检测合格目录，同时对质量及效果进行验证监督，透明化网络安全产品的安全性、可靠性和可用性，推动适配轨交行业网络安全产品的开发及发展，现设计建设一套适用于城市轨道交通网络安全关键产品的检验检测平台实现以测促改。

（二）安全需求简介

平台基于标准化、流程化、规范化及自动化测试平台技术，研究城市轨交业务场景安全产品各方面需求，对接国内外网络安全产品重要参数要求，定义各类检测工具要求，构建轨交行业网络安全产品测试评价标准体系，形成集检测、培训、标准为一体的城市轨交创新安全检测服务体系。执行期限为一年。

（三）分项需求清单

建设内容	技术参数/能力要求	交付类型
研制一套软硬件结合的城市轨道交通网络安全关键产品检验检测平台，打造城市轨道交通检测实验室，针对主流网络安全产品，内置国内外测试技术要求、测试用例、测试方法、测试工具、评价体系等支持网络安全产品自动化引导式检验检测，结合轨道交通安全应用场景需求，输出评价报告，有效验证网络安全产品有效性及适配性。	支持工控防火墙、工控入侵检测、网络准入、日志审计等不少于 4 种主流安全产品体系化测试流程; 支持功能测试、稳定性和可靠性测试、一致性和互连互通性测试、安全性测试以及性能测试 7 类测试内容。	检验检测平台的建设方案及软硬件产品
构建城市轨道交通网络安全产品测试标准体系，基于国内外测试技术要求及安全应用场景需求研究轨道交通主流网络安全产品的重要安全参数及评价指标，建设一套满足轨道交通行业特点、业务安全要求的测试评价标准。	形成一套网络安全产品测试评价标准。	企业标准

六、上海汽车集团服份有限公司乘用车分公司——安心驾：上汽网联车综合安全智能管理助手（一期）

（一）场景应用简介

网联车目前正面临着多样且严峻的安全风险（如网络安全风险、数据安全风险、功能安全风险等），严重威胁消费者的人身安全/财产安全以及公共的交通安全。鉴于此，上汽致力于打造创新的用户侧综合安全智能管理助手，通过移动端 APP 与座舱大屏等多种用户触达方式，为消费者提供可靠实用且个性化的安全服务，提升网联车驾驶体验。

（二）安全需求简介

上汽安心驾的“一期”规划（执行期限 2 年）旨在建立“云+端”的功能框架，面向典型车联网安全威胁实现示范性的检测与处置能力。该智能助手须具备“安全感知、通报预警、智能响应”能力，实现安全态势的“可见、可管、可控、可信”。具体而言，依托于合规采集的车辆数据与车主数据，该助手须针对多类网联车安全风险建立智能威胁模型，实现安全威胁的实时检测与治理；同时，该助手须依托于云端大数据与 A1 大模型等先进技术，面向不同的用户群体构建安全画像，并针对满足不同特征的被画像群体采取个性化的安全防治方案（如主动安全告警，安全应急策略咨询和自动化安全应急策略部署）。

（三）分项需求清单

建设内容	技术参数/能力要求	交付类型
网联车数据采集：采集基本的车主信息和车型信息，并采集车辆	数据的采集过程须符合《汽车数据安全管理若干规定(试行)》，保护消费者的	系统建设

的地理位置信息、车辆功能状态信息(电池和零部件等)、车载网络状态信息(CAN和以太网等)等。	隐私安全;数据的采集不能影响正常的车辆驾驶功能。	
安全态势感知:具备典型网络安全威胁的检测能力,主要包括近场攻击、远程攻击(含来自云端)、车内攻击及对云端的攻击等网络安全威胁;面向代表性的车辆功能安全威胁(如车辆自燃和电池异常等)以及驾驶安全威胁(如疲劳驾驶和分心驾驶等)构建示范性检测方案。	实现对信息娱乐系统(IVI)、车载网联通讯终端(T-BOX),车载网关(Gateway)、车载诊断(OBD)、车载信息服务(TSP)等攻击行为检测,常见的攻击行为覆盖率≥90%。 提供至少 2 个功能安全或驾驶安全示范性检测方案。 其中,网络安全风险的检测与治理须参照《R155》法规以及国内强标《汽车整车信息安全技术要求》。	系统建设 原型技术方案
安全威胁治理:面向用户群体构建安全画像,以便实现安全事件的联合响应和主动治理;面向不同被画像群体实现个性化的安全应对方案,如安全告警和自动部署应急安全策略等;基于 AI 大模型和语音问答等前沿技术,为用户提供智能化的安全应急策略咨询服务。	基于可靠的策略划分用户群体,构建用户画像;通过车载大屏/短信提醒/APP/人工联系等方式实现安全告警服务,触达率≥90%;基于 OTA/IDPS/TSP 等基础设施实现安全策略的自动部署或响应,中低危安全事件应急响应时间≤24 小时,高危安全事件应急响应时间≤1 小时;实现安全应急策略咨询服务的技术原型方案,构建 10 类以上的安全应急知识策略。	系统建设 原型技术方案
安全态势中台:实现安全事件的“可见与可溯源”,为车企、车联网平台以及监管部门提供安全决策数据和依据。	可查看上汽用户群体安全事件的总体概览;可进行基本的数据统计以分析安全态势的走向(地域/时间/车型等);可用于配置基本的安全检测与治理策略。	系统建设

七、上海微创医疗器械（集团）有限公司——云上/当地数据库敏感数据加密及脱敏

（一）场景应用简介

针对个别含有重要的敏感数据和个人隐私信息的应用系统，要求能对数据进行识别，其中包括重要数据进行加密和个人隐私信息的脱敏。

（二）安全需求简介

数据安全治理：针对含有员工个人信息或业务重要数据等敏感信息的系统数据库，需要从底层进行动态脱敏/加密处理，达到公司安全风控和相关法律合规要求，避免重要数据和隐私数据泄露或被不当利用的风险。

目标期限：在 9 个月内达到预期效果。

（三）分项需求清单

建设内容	技术参数/能力要求	交付类型
数据安全治理	能识别特定数据类型并进行各场景（法律条例要求/医疗健康数据管理要求/医疗研发生产环节相匹配的规则），对其进行加标签或关键字过滤，进而底层数据加密或者脱敏处理，同时具备数据复原可逆功能。	系统建设

八、上海核工程研究设计院股份有限公司——基于内生安全的核能工业控制系统一体化保障平台

（一）场景应用简介

核安全局在2020年发布《核动力厂网络安全技术政策》，要求识别关键数字资产并在遭受网络攻击时对关键数字资产提供充分保护。2021年，国务院发布《关键信息基础设施安全保护条例》，核能行业控制系统作为关键信息基础设施，需要从分析识别、安全防护、检测评估、监测预警、主动防御、事件处置等方面进行网络安全建设。因此，需要在上海核工程研究设计院股份有限公司设计的非能动三代核电工业控制系统中，基于内生安全建设一体化保障平台，保障核能的本质安全。

（二）安全需求简介

目前核能行业网络安全防御主要采用传统安全防御手段，对于供应链预先安插的后门和未知的外部攻击没有有效的防御手段。所以，需要围绕核能工业控制系统内生安全、重要数字资产识别和网络安全预警等方面开展安全建设，形成基于内生安全的核能工业控制系统一体化保障平台，满足监管要求和合规要求，保护关键数字资产，进行监测预警和主动防御。建议执行周期2024年-2026年。

（三）分项需求清单

建设内容	技术参数/能力要求	交付类型
基于内生安全的核能工业控制系统一体化保障平台	1）实现内生安全架构在核能工业控制系统具体场景下的构造，实现要地部署，应对未知威胁; 2）实现资产识别、风险评估、网络预警等产品创新升级和应用，结合三代非能动核电厂工艺场景，实现网络攻击对功能安全和电厂运行的实际影响的分析，并利用人工智能和大数据分析技术对关键工艺参数进行学习与分析，通过人工智能模型和优选裁决模块，形成网络安全事件预警机制。开发资产管理、风险评估和安全预警一体化的核能网络安全运维支持平台，提升核设施的网络安全运维水平。	产品 系统建设

九、工业互联网创新中心（上海）有限公司——基于网络API流量的数据防泄漏

（一）场景应用简介

通过与业务应用的API流量集成对接，实现应用外发场景中文件内容的识别，达到敏感数据外发的有效审计/阻断管控。

（二）安全需求简介

根据企业内部数据安全建设制度及管理要求，内部部署文件外发平台、应用DLP应用平台，通过restful API集成对接；使用范围覆盖使用文档外发平台、外发文档的内部终端用户。

具体实现场景：在用户向文件外发平台上传资料时或定期对文件进行扫描，将扫描结果反馈给应用DLP平台，文件外发平台根据DLP的反馈结果选择允许或者阻断，从而保证文件上传的安全；当用户从外部下载数据时，文件外发平台会将下载的内容发给DLP检测是否含有敏感信息，并将结果反馈给外发平台，文件外发平台选择放行、阻断、脱敏后外发，从而保障文件外发的安全。

（三）分项需求清单

建设内容	技术参数/能力要求	交付类型
统一内容管理平台	统一管理DLP相关功能及报告。	软/硬件
应用DLP平台	通过API 与应用系统对接，实现DLP检测赋能。	软/硬件

十、联创汽车电子有限公司——核心研发数据的安全保护

（一）场景应用简介

为保护公司商业秘密，对核心研发数据进行全方位的安全保护，确保其可用性、完整性、保密性。

（二）安全需求简介

核心研发数据的安全保护措施应符合国家关于商业秘密保护及数据安全保护的有关法律法规，应符合上汽集团以及联创汽车对于网络及数据安全的相关规章制度，应充分考量联创关于数据保护的实际应用场景，适配联创的网络架构，兼容联创已有的网络及数据安全框架，能够与联创已有的网络安全系统适度联动，形成整体的数据安全防御态势，确保联创的核心研发数据安全。

（三）分项需求清单

建设内容	技术参数/能力要求	交付类型
实现对核心研发数据分类、分级及数据外发管理	应具有上汽集团内数据防泄漏系统的实施经验。 对核心研发数据进行全方位保护，对数据分布、分类、分级进行自动统计，对所有外发管道进行管控，对数据外发、拷贝、截屏、打印、聊天、上网等行为进行审计、按需阻断。	本地部署现场实施
实现核心研发数据不落地及数据安全管理等功能	应具有上汽集团内虚拟桌面系统的实施经验。 核心研发数据不落地，集中存储于云端，定期备份；向用户提供云端的虚拟桌面功能，用户可随时安全接入，兼容主流操作系统及办公、研发类软件；具有资产管理、安全审计、文件导出审计、录屏、屏幕水印、防截屏等安全功能。	本地部署现场实施
实现对终端计算机安全管控	应具有上汽集团内桌面管理系统的实施经验。 实现对终端计算机的资产管理、安全基线管理、软件标准化管理，以及远程协助控制、端口外设控制、移动存储介质控制等安全功能。	本地部署现场实施
实现有限及无线网络的准入管控	供应商应具有上汽集团内网络准入系统的实施经验。 对有限及无线网络的准入管控，入网设备的资产管理，识别入网设备的安全基线，建立准许入网设备的名单；对于异常的网络接入行为进行阻断并告警。	本地部署现场实施
实现工业网络中设备的安全防护	应具有上汽集团内工控安全系统的实施经验。 能够识别工业网络中的各类威胁,适配工业设备的网络协议;能够与防火墙等设备联动。	本地部署现场实施

十一、零束科技有限公司——车载系统研发型企业核心数据资产安全体系构建

（一）场景应用简介

零束科技有限公司将创新型研发数据以及车辆数据视为企业发展至关重要的核心数据资产，需要在保障研发工作进度的情况下，提高研发数据的安全性。同时，车载系统开发完成投入使用后，需要以大量的数据采集为基础，不断优化产品，进行迭代升级。此外，在汽车运行过程中也会收集大量数据。因此，亟需建立一套切实有效的管理机制，保证数据采集合规。

（二）安全需求简介

针对研发类代码数据安全，经过分析研判，识别出主要的安全风险集中在内部泄露、数据中心、外部入侵等。而对汽车数据而言，主要有两方面核心监管要求：个人信息保护、重要数据安全。建立汽车数据安全合规采集管理能力刻不容缓。

（三）分项需求清单

建设内容	技术参数/能力要求	交付类型
数据分区安全管理方案	制定并明确基于项目生命周期的数据安全管理方案，并实现基于物理环境、网络和数据中心的分区分级管控模式。	系统建设
数据共享系统建设	形成数据、代码交互等核心资产文件区域间的交互管控平台，包括数据文件交互和数据接口交互的安全体系合规。	系统建设
数据全生命周期安全评价与认证	通过引入第三方专业机构，对现有的核心数据及云端数据安全成熟度进行评价并获证。	外包服务
汽车数据采集需求管理平台建设	以研发流程为框架，搭建线上的汽车数据采集需求管理平台，将各车型的数据采集需求从分散、线下，转移到集中、线上管理，提升管理效率和管理质量，便于需求追溯管理，并可为后续汽车数据治理奠定基础。	系统建设
汽车数据安全合规测试	面向GB/T 41871《信息安全技术 汽车数据处理安全要求》、GB/T《汽车数据安全通用要求》的测试服务。	外包服务
云端数据安全防护方案	制定并建立云端数据安全整体防护方案，包括数据存储加密、数据传输加密、访问控制、安全审计、漏洞扫描。	系统建设
云端数据安全服务平台	为云端业务系统数据安全提供全方位的安全服务能力，建设数据安全服务平台，满足容器安全、主机安全、WEB 应用安全等各项安全能力。	系统建设

十二、上海弘卓网络科技有限公司——下一代漏洞管理和安全运营整体解决方案

（一）场景应用简介

针对个人信息面临的安全问题，对移动应用中个人信息控制者在收集、存储、使用、共享、转让、公开披露等信息处理环节中的相关行为，检测应用是否存在个人信息非法收集、滥用、泄漏等问题。

（二）安全需求简介

具体包括应用的隐私政策、产品功能的整体设置、用户账户的注销管理、用户权利的响应机制、处理个人信息所使用的技术模块(如 SDK、API、Cookie 等)与重要系统权限(如摄像头、存储读写、麦克风、位置、系统日志等)的调用是否合规等问题的深度检测，及时发现应用存在的潜在风险与不合规之处，帮助用户、企业对 App 隐私、过度收集、滥用等行为进行检测，有效、低成本的做 App 合规自查。合规要求:依据国家相关法律法规及条例，独立自主研发。执行期限为 4 个月。

（三）分项需求清单

建设内容	技术参数/能力要求	交付类型
一站式移动应用个人信息合规检测平台	1）需具备CCRC信息安全服务资质认证证书，信息安全风险评估服务资质符合CCRC-ISV-C01:2021《信息安全服务规范》三级服务资质要求; 2）需具备CCRC能力验证合格证书; 3）具备三级数字广告企业-数字媒体服务类证书。	产品 系统建设
	平台适配移动应用范围: 检测对象支持Android、iOS、小程序、TV应用、车机应用。	
	平台检测维度: 权限检测、通讯检测、隐私政策检测、行为检测、第三方SDK检测、应用页面全遍历、个人信息非法收集、个人信息滥用、个人信息泄漏等。	
	平台报告可定制: 支持自定义报告水印、封面、页眉、页脚、单位名称、联系方式、文字排版、布局分布等。	
	平台检测设备: 支持真机、手机主板机、云真机接入。	
	手机系统: 包括但不限于支持Android6.0 Android13 版本、iOS13 iOS16。	
	手机品牌: 包括但不限于支持Google、华为、小米、三星。	
	检测结果颗粒度: 具备文字描述与代码堆栈以及图片描述。	

附件 2

揭榜意向征集表

企业名称	
联系人	
移动电话	
邮箱	
意向申报需求序号及名称（可多选）	如“一、　上海复星医药（集团）股份有限公司——医药研发数据分类分级及外溢风险管理”

附件 3

2023 年重点行业网络安全解决方案揭榜申报书

一、基本信息

<table>
<tr><td colspan="4">（一）申报单位信息</td></tr>
<tr><td>牵头单位名称</td><td colspan="3"></td></tr>
<tr><td>机构代码/
三证合一码</td><td></td><td>成立时间</td><td></td></tr>
<tr><td>通讯地址</td><td></td><td>注册资本
（万元）</td><td></td></tr>
<tr><td>联系人姓名</td><td></td><td>移动电话</td><td></td></tr>
<tr><td>邮箱</td><td></td><td>单位性质</td><td></td></tr>
<tr><td>上年销售额
（万元）</td><td></td><td>上年利润额
（万元）</td><td></td></tr>
<tr><td rowspan="3">联合申报
单位
（可添加）</td><td>单位名称</td><td>单位性质</td><td>机构代码/三证合一码</td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td>联合体简介</td><td colspan="3">（申报牵头单位发展历程、主营业务、经营管理状况，网络安全方面已开展的业务及有关工作情况、所获的有关奖项等，以及联合体分工情况，不超过 400 字）</td></tr>
<tr><td colspan="4">（二）申报项目信息</td></tr>
<tr><td>申报方向
序号及名称</td><td colspan="3"></td></tr>
<tr><td>项目负责人</td><td></td><td>职务/职称</td><td></td></tr>
<tr><td>移动电话</td><td></td><td>项目实施
周期（年）</td><td></td></tr>
<tr><td rowspan="6">项目计划
投资金额
（万元）</td><td colspan="2">分项建设内容</td><td>金额</td></tr>
<tr><td colspan="2"></td><td></td></tr>
<tr><td colspan="2"></td><td></td></tr>
<tr><td colspan="2"></td><td></td></tr>
<tr><td colspan="2"></td><td></td></tr>
<tr><td colspan="2">合　计</td><td></td></tr>
</table>

项目建设 方案概述	（简要阐述项目建设目标、主要内容，与申报需求方向有关的创新特点，不超过400字）
真实性承诺 （根据联合申报单位数量调整）	我单位申报的所有材料，均真实、完整，如有不实，愿承担相应的责任。 法定代表人签章: 申报单位公章: 年　月　日

二、申报解决方案详细介绍

（一）项目建设情况

1.项目建设目标（包括对需求方向认识，解决方案总体考虑、目标意义等）

2.项目建设方案（包括项目主要功能、技术路线、技术标准、难点和创新点等，重点说明揭榜需求总体设计、分项需求的相应关键技术方案，包括架构图、技术原理、符合标准等）

3.项目投资概算（按照建设方案，综合测算并按用途列明主要费用概算）

4.项目负责人及项目团队（项目负责人资质及工作经验、项目主要参与单位及其分工、项目参加人员情况等）

5.项目进度及预期效果（项目计划实施周期及安排，项目建成后为发榜单位解决的问题、实现的价值、应用及示范意义等）

（二）相关附件（列出文件清单，后附文件复印件）

1.申报单位相关证明材料（相关资质、荣誉，研发能力，经营管理能力证明材料）

2.申报项目相关证明材料（与申报方案有关的技术、产品和服务相关证明材料）

上海市经济和信息化委员会办公室　　2023年12月15日印发