上海市经济和信息化委员会文件

沪经信软〔2021〕542 号

上海市经济信息化委关于开展 2021 年重点行业数字化转型安全解决方案揭榜工作的通知

有关单位:

为保障本市经济数字化转型，形成本市重点行业转型网络安全、数据安全新供给，我委组织有关企业征集了应用场景和安全需求，现集中开展相关网络安全解决方案揭榜工作（以下简称揭榜）。有关事项通知如下。

一、揭榜内容

本次揭榜包括中远海运科技股份有限公司、中国联合网络通信有限公司上海市分公司、中国电信股份有限公司上海分公司、上海航空工业（集团）有限公司、中国宝武钢铁集团有限公司、上海汽车集团股份有限公司、上海国际港务（集团）股份有限公

司、申能（集团）有限公司、上海城投水务（集团）有限公司、上海华谊能源化工有限公司等企业（以下简称发榜企业）的十个业务应用场景及其安全建设需求,征集相应的网络安全解决方案。具体内容详见附件 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、项目集成建设等相应能力。鼓励各揭榜单位形成申报联合体，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。原则上一个单位只能作为一个需求的揭榜牵头单位。

（二）揭榜意向征集。7 月 20 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（一家单位可报多个需求方向），填妥揭榜意向征集表（见附件 2）并反馈至联系邮箱。

（三）解决方案揭榜。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。8 月 15 日前，各揭榜牵头单位将《上海市 2021 年重点行业数字化转型安全解决方案揭榜申报书》（见附件 3）一式三份及电子版报市经济信息化委软件和信息服务业处。

（四）方案评审。市经济信息化委将组织发榜企业、行业及网络安全领域专家开展解决方案评审工作，形成评审意见，并按照意见编制优秀方案集，反馈到相应发榜企业。

（五）支持推广。对于相应优秀安全解决方案，市经济信息化委将加强建设支持和宣传推广。对符合本市促进产业高质量发展等相关专项资金支持政策，并在上述优秀方案中形成的工程项

目，将予以优先支持；对解决行业共性问题，可复制推广的优秀方案及经验做法，将在征询各企业及相关方案提供厂商意见后，加强案例宣传报道、行业推广，有条件的组织开展相应技术标准的研究制定工作。

三、联系方式

（一）联系人：代淑杰、吴昊

（二）电话：18521402980、18918883983

（三）地址：世博村路 300 号 5 号楼 711 室

（四）邮箱：admin@sisa.org.cn

附件：1.上海市 2021 年重点行业网络安全建设需求榜单

2.揭榜意向征集表

3.上海市 2021 年重点行业数字化转型安全解决方案揭榜申报书

上海市经济和信息化委员会

2021 年 7 月 9 日

附件 1

上海市 2021 年重点行业网络安全建设需求榜单

一、中远海运科技股份有限公司——船舶卫星通信网络安全与态势感知

（一）场景应用简介

船舶海上航行依赖卫星的微波通信技术以及宽带通信技术来实现各类信息的传输。随着船舶数字化、智能化、网络化的发展智能化水平的提升，越来越多的控制系统、通讯导航系统、信息管理系统及设备不断接入船舶网络，实现对外信息交互，使其遭受网络威胁的隐患不断加剧，在这样的背景下，船舶的网络安全显得尤为重要。但目前尚没有一套成熟解决方案对船舶网络安全进行全面防护，因此希望能够针对该应用场景进行安全防护和态势感知。

（二）安全需求简介

中远海运科技建设了上海、北京两地数据中心的态势感知平台，希望能以该平台为依托，采集船舶卫星通信流量，进行综合处理和关联分析，识别通信中的威胁与异常行为，提前进行预警，利用现有功能模块进行全面管控。依据国家通信及网络安全相关要求，建设安全可控的远海船舶通信网络，确保通信安全、网络安全和信息安全，建立健全船舶网络安全管理体系。

（三）分项需求清单

建设内容	技术参数/能力要求	交付类型
船舶卫星通信网络安全态势感知系统	以态势感知平台为依托，采集船舶卫星通信流量，进行综合处理和关联分析，识别通信中的威胁与异常，提前预警，实现全面管控。	外包服务（全局规划）
	在船舶上部署采集网络流量的设备，包括船员上网及系统流量。如有可能采集智能船舶设备的工控设备流量。	产品（专用设备）

	通过本地初步识别或者流量压缩，筛选有风险的流量通过卫星上传到数据中心的态势感知系统中，统一进行风险管控和预警。	系统建设

二、中国联合网络通信有限公司上海市分公司——数据资产地图与数据溯源

（一）场景应用简介

工业和信息化部下发《电信和互联网企业网络数据安全合规性评估要点》（2020 年版）明确要求运营商建设数据资产管理能力，针对数据生命周期评估要点要求，将针对数据对外开放共享实施审核，确认没有超出需求和授权范围，采取必要措施提升共享场景下的数据溯源能力。

（二）安全需求简介

基于数据资产地图与数据溯源，通过构建数据资产体系化、结构化的管控视图，根据角色区分对应功能，控制权限，帮助用户构建企业级数据信息知识库，展示用户数据资产的分布、存储和流动情况。以数字水印作为核心技术，通过建立数据的唯一标识，实现数据的权属证明和泄漏者溯源，为大数据流通共享和安全交易提供技术支撑。

（三）分项需求清单

建设内容	技术参数/能力要求	交付类型
数据资产地图与数据溯源系统	敏感数据识别：采用字典匹配和人工识别相结合的方式对敏感数据进行识别，精确分析出敏感数据，确保权限允许情况下才可脱敏访问。识别算法应设计为立体多维度，降低因不合理的单一维度识别命中率而导致的偏差情况的发生。 数据流向可视化：基于分布式集群架构，每一应用服务器上配置有应用子模块；基于日志文件，获取应用子模块的输入参数和输出参数应用数据流向，监控敏感数据分布出口，不需要安装客户端软件，不依赖平台和系统，数据可自由流转。 溯源能力强：基于多种算法能力基座，在文件被破坏，残留 20%内容的基础上也能溯源成功。不依赖数据的载体形式和文件结构，防文件转换和内容复制。	系统建设

	全视角资产管理：提供全视角数据资产管理能力，满足资产创建者、管理者、消费者等管理和使用需求，结合资产应用环境，构建资产概览，从而有效帮助管理者总览数据资产全局。 支持多种数据类型：支持结构化和非结构化格式文件，如 Word、Excel 等文件，也支持文本、数据库导出文件或图片、声音及视频等数据。 系统架构：应采用并行处理的计算机制，基于 hadoop 分布式存储框架搭建，支持文件+实时流多种方式和 spark+flink 组件模式提升数据模型输出的时效性。 系统安全性：系统采用统一认证和授权，代码增加拦截过滤功能，防止恶意访问和远程攻击。 系统时效性：系统登录时间不超过 3 秒；结构化数据文件异常操作行为预警 3 秒内输出，基于非结构化文件异常行为 3 分钟内响应，支撑短信及页面可视化提醒。	

三、中国电信股份有限公司上海分公司——基于攻防背景下的安全态势感知体系

（一）场景应用简介

随着网络安全攻防态势的不断升级，网络安全攻击的自动化程度越来越高，大力提升实战攻防能力，确保基础电信运营商网络的安全可控，已经成为十分紧急的生产需求。通过建设安全态势感知体系，提升企业安全监测防护自动化水平，及时感知发现安全事件。

（二）安全需求简介

随着网络安全攻防态势的不断升级，网络安全攻击的自动化程度越来越高，每天都会产生百万量级的告警，范围覆盖各个业务系统和部门，单纯依靠人工来抵御攻击的时代已经过去，传统的监测处置体系，因为人工干预多，人员能力参差不齐，实际攻击处理中耗费时间长，并且处置质量不可控。亟需建立网络安全纵深防御体系和自动化处置手段，以自动化的监测防护体系来应对自动化的攻击。

（三）分项需求清单

建设内容	技术参数/能力要求	交付类型
网络流量分析检测	通过对网络流量采集和深度解析，分析潜在威胁的能力，主要包括（特征检测、文件沙箱动态行为检测、机器学习检测、威胁情报检测）等。	产品
威胁诱捕	基于网络欺骗技术，在企业网络中创建高交互蜜网，智能部署诱捕节点，即时发现 APT(HHD)攻击、蠕虫勒索和挖矿等新型威胁，将攻击转移到蜜网中隔离，保护企业核心资产。	产品
机器学习	是以安全大数据为基础,从全局视角提升对安全威胁的发现识别、理解分析、响应处置能力的一种方式，支持机器学习的离线分析能力，结合历史事件对进行周期分析，发现未知威胁事件。	产品
安全告警实时分析	是以安全大数据为基础,从全局视角提升对安全威胁的发现识别、理解分析、响应处置能力的一种方式，提供多种场景配置模版,将契合用户环境的安全场景通过规则配置落地，通过实时分析匹配标准化处理后的日志数据，产出相关的安全事件。	产品
实时网站监测	提供网站实时在线安全监测及性能监测,发现问题时可及时通过邮件等方式进行告警。	产品
威胁情报	基于证据的知识，用于识别和检测威胁的失陷标识，如文件 HASH，IP，域名，程序运行路径，注册表项等，以及相关的归属标签,可用于资产相关主体对威胁或危害的响应或处理决策提供信息支持。	产品
自动化应急处置	以安全事件为导向，以应急处置为核心，通过内置的技术标准和实践，将应急响应流程整体细化、分解，并对整个应急响应进展进行监控，实现处置流程平台化，应急响应自动化，并结合现状，快速进行安全事件应急处置能力，形成闭环。	产品
产品运营	以业务的最终安全为目的，实现人、技术、流程、管理与业务有机结合，验证其效果持续迭代优化过程的统筹管理，通过运营过程的统筹管理，满足安全的动态性、持续性和整体性需求。	外包服务

四、上海航空工业（集团）有限公司——分层防御下的应用发布与数据交换系统

（一）场景应用简介

针对企业内部不同安全区应用交换数据需求，为不同区域的用户提供系统服务，以及提供集中管控、统一安全标准的信息数据交换解决方案。

（二）安全需求简介

目前企业内部网络已顺序形成多个区域，不可跨区域访问。当前各区域间系统通过非统一的数据交互方式联通，部分使用代理服务器进行区域穿越、部分使用前置主机，在工作中，发现代理服务器无法有效的解决区域间安全的数据交换，无法提供统一的安全管控，本需求是为了解决该问题而提出。

（三）分项需求清单

建设内容	技术参数/能力要求	交付类型
交换系统建设	以软件或硬件交付，提供系统间双向数据数据交互，为不同应用、不同模块提供标准化的数据交换、API 接口交互、文件交换等，解决中国商飞复杂业务、多种业务、多地域、多云间协同和数据融合。拓展网络边界，提供供应商、合作伙伴数据、系统、文件交互的便捷性、敏感数据加密等。	系统建设
实现身份验证功能	向注册程序验证对 API、数据传输、文件交换的调用，跟踪请求方，跟踪上述的使用，对访问速率或超限功能进行控制，作为实现不同级别应用权限控制的基础功能，包括但不限于以下认证授权方式: 1.支持 API 预制密钥，支持公钥体系的密钥分发使用; 2.支持Basic Auth，传输过程中应支持HTTPS 封装和发送; 3.支持 HMAC 基于哈希的消息授权代码,将唯一密钥密码编码，并通过安全哈希算法（SHA）传递; 4.支持 OAuth2.0。	系统建设
隔离典型网络攻击	支持 IPV4、IPV6 攻击的检测和隔离能力，能够记录攻击方向、时间、源 IP 地址、目的 IP 地址、源端口、目的端口;攻击规则库能够自动或手动升级，能够有效抵御 DDOS 攻击，吞吐率≥10Gbps; 结合基础防护手段，免疫典型的网络攻击，如端口扫描、ICMP 攻击、HTTP 漏洞、FTP 漏洞、POP3 漏洞、SSH 漏洞，SQL 注入、跨站、页面盗链等，能有效防御暴力破解，识别并记录攻击来源，识别和禁止木马通信，保护内部系统，防止非授权数据传输。	系统建设
对传输的非结构化数据的恶意代码检测	系统应具备自动或手动病毒库升级能力。在分析能力方面应同时进行静态分析和动态分析,支持病毒沙箱分析功能，提供接口，能够与第三方沙箱联动，提高恶意代码的检出率。包括但不限于以下反病毒技术: 1.基于特征的文件扫描，根据病毒库进行比对，发现恶意代码程序; 2.文件格式识别，禁止非允许的文件格式传输;	系统建设

	3.根据二进制文件的反汇编结构,发现和禁止恶意代码; 4.加壳识别和代码脱壳识别; 5.根据恶意代码对文件系统、运行进程列表、注册表、本地网络栈等方面的行为动作,进行实时监视、记录和显示,发现和禁止恶意代码。	
支持实时数据交互应用	系统延迟≤20ms,小文件传输≥5000个每秒,支持≥2GB的大文件数据传输; 满足从飞机设计、生产、客户服务、公司运营等各环节的数据交换需求、系统交互需求,向外部合作伙伴、供应商、监管机构提供中国商飞的定制应用与安全数据交换标准。	系统建设

五、中国宝武钢铁集团有限公司——工业互联网平台安全防护

（一）场景应用简介

中国宝武工业互联网平台是基于智慧制造应用场景的 iPlat 和智慧服务应用场景的 ePlat 两部分构成，以数据为中心构建，服务于智能制造的企业信息化互联网+时代的工业互联网平台基础环境。同时，也是一个提供跨企业应用和共享服务平台的多元化产业链生态圈。

（二）安全需求简介

从安全合规和内生安全两个维度，通过评估 ePlat/iPlat 平台及接入应用的安全风险，形成标准防御配置与举措，建立常态监测、防护、应急处置的闭环机制。合规性标准包括《网络安全等级保护基本要求》（GBT22239-2019）、《工业互联网平台安全防护要求》（AII/004-2014）、《工业互联网平台企业安全防护规范（草案）》;《工业互联网企业数据安全防护规范（草案）》。安全防护需求主要有数据接入安全、应用接入安全、平台安全、访问安全。其中，平台安全防护内容进一步可划分为设备接入层、边缘计算层（iPlat）、宝之云工业 IaaS 层、工业 PaaS 层（ePlat）、应用接入层。

（三）分项需求清单

建设内容	技术参数/能力要求	交付类型
数据接入安全，包括平台数据分类分级、防止数据泄露、被侦听或篡改，保障数据在源头和传输过程中安全等。	1.定制开发具备 CMMI3 资质; 2.安全产品为国内厂商，且支持国密算法。	产品
平台安全，包括工业互联网平台的代码安全、应用安全、微服务架构安全、共享服务与应用接口调用安全、容器安全、DevOps 系统安全等。	1.定制开发具备 CMMI3 资质; 2.SDL 工具与产品的厂商为国内厂商且具备自主知识产权。	产品
访问安全，包括通过建议统一的访问机制，限制用户的访问权限和所能使用的计算资源和网络资源对工业互联网平台重要资源的访问控制和管理，防止非法访问。	安全产品为国内厂商，且支持国密算法。	产品

六、上海汽车集团股份有限公司——智能网联车数字化工厂多层级内生安全防护体系

（一）场景应用简介

上海汽车集团有限公司乘用车公司临港基地数字化工厂于 2008 年 9 月建成投产，包含了整车和发动机制造，是国内率先达到传统技术和新能源技术全覆盖的高柔性化制造基地。临港工厂聚焦制造全业务链数字化运作，构建了完善的数字化平台，建设了“智工艺、智生产、智物流、智品质、智运营”应用生态圈。数字化工厂是汽车产业智能化的重要部分，其安全防护体系也应全面考虑及多层级规划建设。

（二）安全需求简介

临港工厂需要满足关键信息基础设施保护，网络安全等级保护及工业互联网等监管要求，还需要通过网络安全管理系统建设与落地实施来提升网络安全管理能力，构建业务系统及数据安全全生命周期管理机制，提升 IT 及 OT 系统的网络安全保障能力。结合相关法规、国标与白皮书，网联车数字化工厂安全治理与防护框架充分考虑信息安全、功能安全和物理安全，聚焦数字化工厂安全治理与防护所需具备的主要特征，综合汇聚为设备、边缘、

厂区、产业（集团）各个层级，分层次分类分级分域治理构建内生安全防御；同时建设对应的态势感知平台、数据安全治理专项等智能化防护。

（三）分项需求清单

建设内容	技术参数/能力要求	交付类型
多层级数字化工厂安全治理与防护体系	整个安全治理与防护体系，包括但不局限于可靠性、保密性、完整性、可用性、隐私、合规和数据保护。 可靠性：数字化工厂制造业务在一定时间内、一定条件下无故障地执行指定功能的能力或可能性。一是设备硬件可靠性，二是软件功能可靠性，三是数据分析结论可靠性，四是人身安全可靠性。 保密性：数字化工厂业务中的信息按给定要求不泄漏给非授权的个人或企业加以利用的特性，即杜绝有用数据或信息泄漏给非授权个人或实体。一是通信保密性，二是信息保密性。 完整性：数字化工厂内用户、进程或者硬件组件具有能验证所发送的信息的准确性，并且进程或硬件组件不会被以任何方式改变的特性。一是通信完整性，二是信息完整性，三是系统完整性。 可用性：数字化工厂业务在指定时间区间内能够正常运行的概率或时间占有率期望值，主要用来衡量数字化工厂业务在投入使用后实际使用的效能。一是通信可用性，二是信息可用性，三是系统可用性。 隐私、合规与数据保护：数字化工厂用户个人隐私数据或企业拥有的敏感数据等提供保护的能力，且符合相应国家或区域相关法律法规的规定与要求。一是用户隐私保护，二是企业敏感数据保护，三是安全合规治理。	外包服务（全局规划） 系统建设（综合治理与管理平台）
数字化工厂边缘安全防护系统	数字化工厂边缘安全防护系统同时涵盖设备层和边缘层。设备层对应工业设备、产品的运行和维护功能，关注设备底层的监控优化、故障诊断等应用。边缘层对应车间或产线的运行维护功能，关注工艺配置、物料调度、能效管理、质量管控等应用。两个层级都是属于同一个数字化工厂内部业务直接治理范围，需合并治理与防护。 边缘安全防护系统致力于面向实体实施分层分域安全策略，构建多技术融合安全防护体系，从而实现边缘安全防护。部署的关键在于确保数字化工厂边缘侧的设备安全、控制安全、网络安全。 边缘安全防护系统实施需要边缘层和设备层的各	外包服务（全局规划） 系统建设（多层级数字化工厂边缘安全防护系统，以及关联支撑子系统、子应用）

	项功能包括，首先，保障设备安全，通过采取设备身份鉴别与访问控制、固件安全增强、漏洞修复等安全策略，确保工厂内生产设备、单点智能装备器件与产品，以及成套智能终端等智能设备的安全。其次，保障控制安全，通过采取控制协议安全机制、控制软件安全加固、指令安全审计、故障保护等安全策略，确保控制软件安全和控制协议安全。最后，保障边缘侧网络安全，通过采取通信和传输保护、边界隔离（工业防火墙）、接入认证授权等安全策略，确保工厂内网安全、标识解析安全等。可进一步划分为设备安全、控制安全与网络安全三个次生层级。	
数字化工厂厂区层安全防护系统	数字化工厂厂区层安全防护系统从防护技术策略角度出发，提升企业安全防护水平，降低安全攻击风险。部署的关键在于确保数字化工厂企业侧的网络安全、应用安全、数据安全。厂区层对应企业平台、网络等关键能力，关注订单计划、绩效优化等应用。 厂区安全防护系统实施需要边缘层和设备层的各项功能。首先，保障企业侧网络安全，通过采取通信和传输保护、边界隔离（防火墙）、网络攻击防护等安全策略，确保工厂外网安全、标识解析安全等。其次，保障应用安全，通过采取用户授权和管理、虚拟化安全、代码安全等安全策略，确保平台安全、本地应用安全、云化应用安全、移动端应用安全等。	外包服务（全局规划） 系统建设（多层级数字化工厂厂区层安全防护系统，以及关联支撑子系统、子应用）
数字化工厂产业（集团）层安全防护系统	数字化工厂产业（集团）层安全防护系统从防护管理策略角度出发，以安全风险可知、可视、可控作为安全防护体系建设的主要目标，强化集团企业综合安全管理能力。产业（集团）层对应跨工厂/企业平台、网络和安全系统，关注供应链协同、资源配置等应用。部署的关键在于对企业网络口及企业内安全风险进行监测，在平台网络出口建设流量探针，实现对企业的安全信息采集、资产识别管理、安全审计、安全告警、安全处置跟踪以及数据治理等功能，并与供应链、省/行业级安全平台甚或国家级安全平台的对接。 企业安全综合管理平台需要涵盖的防护管理包括：安全信息采集、资产识别管理、安全审计、安全告警、安全处置跟踪等关联支撑子系统、子应用。	外包服务（全局规划） 系统建设（多层级数字化工厂产业集团层安全防护系统，以及关联支撑子系统、子应用）
数字化工厂数据安全治理专项	在汽车生产环节，智慧化自动化工厂通过引入 AI 等新兴技术，进一步提升生产效率降低运营成本，累积了大量的数据。这些数字化数据资产具有极高的价值，在布局数字化创意数字化工厂、电子架构、ICV 基础软件团队、数据架构与网络安全业务方向，全面建设“软	外包服务（全局规划） 系统建设（多层级数字化工厂数据安全治理

	件定义汽车”数字体系过程中，把数据安全作为专项工作独立关注与开展有着现实必要性。主要对象涉及：智能生产管理系统(PMS)、智能能源管理系统(EMS)、智能设备管理系统(TPMS)、中央监控系统(SCADA)相关的数字化工厂数据的全生命周期防护。 专项主要目的在于通过保障数据安全进而确保数据资产的防护，通过采取数据防泄漏、数据加密、数据备份恢复等安全策略，确保包括数据收集安全、数据传输安全、数据存储安全、数据处理安全、数据销毁安全、数据备份恢复安全在内的数据全生命周期各环节的安全。可部署构建敏感数据发现、数据分类分级治理、数据防泄漏、数据加密、数据备份恢复等关联支撑子系统、子应用。	与防护系统，以及关联支撑子系统、子应用）
数字化工厂新基建安全专项	数字化工厂安全规划、建设与运营过程中，应充分、全面、妥善考虑我国在关键信息基础设施保护、新基建等相关领域的规定与要求，故此需作为专项工作独立关注与开展。 数字化工厂新基建相关系统与应用可包括如下内容，每一个对应领域都需要建设与运营相应的专项安全：新基建数字化工厂自主可控大数据中心、国产芯片、国产操作系统、国产数据库、国密算法、北斗与关联应用；5G 以及数字化工厂专用基站/小基站、配套终端与网联组件；数字化工厂新能源与碳中和，包括充电桩/充电站、业务平台。	外包服务（全局规划） 系统建设（数字化工厂新基建相关系统与应用）
建立数字化工厂网络安全管理体系，规范网络安全管理活动，保障生产运营安全	融合《网络安全法》、关键信息基础设施保护、网络安全等级保护、工业互联网安全、车联网安全，Auto CSMS（智能网联车辆网络安全管理体系）等相关政策及标准要求。 具有 OT 网络的安全策略、安全组织、物理环境安全、网络安全、业务系统安全、设备及控制系统安全、数据安全等的管理制度和流程，并落地执行项目经验。 具有安全体系审核员资质。	外包服务

七、上海国际港务（集团）股份有限公司——现代化超大型港口的数据安全避风港

（一）场景应用简介

上港集团是国际航运重要枢纽企业，以建设领先的国际航运中心为目标，在由信息技术支撑的现代化数字港口中，信息安全将成为保障安全生产的中坚力量。上港集团需要建设一个可靠的

数据安全避风港，以确保与运营相关的关键信息数据安全。港口生产作业主要围绕集装箱的装卸运输等开展，上海港已实现了所有业务数字化，网络安全以及安全管理团队都是确保生产运维的重中之重。围绕落实《网络安全法》、《数据安全法》合规要求在港口行业的落实，也是本项目的实施重点之一。同时，希望将此次安全避风港的数据安全建设形成新模式，在全国信息化港口中做应用推广。

（二）安全需求简介

上港集团与外部航运公司数据互通，需保证数据收集、存储、使用、加工、传输、提供、公开过程中的安全，及时发现网络攻击行为，降低损失和恶劣影响。按照等级保护规范要求、数据安全法要求，结合区块链、网络安全态势感知、网络安全动态编排等领先安全技术，率先开展数字航运背景下的数据安全避风港安全防护与保障系统建设，通过专业的持续的安全服务，开展全面的安全建设和服务保障工作。同时，发挥龙头示范作用，与行业科研院所、知名网络安全公司共同研究、编制行业标准。

（三）分项需求清单

建设内容	技术参数/能力要求	交付类型
数字避风港合规建设	1.物理环境安全要求：支持物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、湿温度控制、电力供应、电磁防护、完善物理环境异常的灾备问题。 2.通信安全要求：支持业务系统用户信息安全、操作日志和操作审计、系统高可用设计、通信过程加密、关键线路和设备冗余。采用密码技术保证通信的完整性和保密性。 3.边界安全要求：完善访问控制、支持入侵防御、恶意代码防范、应用过滤、工业协议数据过滤等功能。 4.业务安全要求：支持对系统敏感数据识别、对敏感信息的脱敏、对关键信息存储的加密、授权、灾备、异常恢复问题。对应用系统、数据库和主机提供相应的防护，并提供相应的安全配置，提供数据的备份和快速恢复能力。 5.安全管理要求：支持安全风险管理、终端接入管控、	系统建设

	安全运营管理、智能响应处置功能；支持设备漏洞库、指纹库、威胁情报库等知识库功能；支持攻击链分析、潜在威胁分析等功能；支持动态监测、安全联动等功能。	
数字避风港安全保障服务	1.保障服务包括安全规划与安全建设咨询服务、漏洞扫描与脆弱性分析服务、安全检查服务、代码审计服务、渗透测试服务、安全运维服务、安全评估服务、应急响应服务、安全培训教育服务等内容。 2.具备相应的安全风险评估和安全运维服务资质的单位。	外包服务
数据安全避风港规划	1.编制《港务系统数据安全技术要求》、《港务系统数据安全交换要求》等行业标准。 2.完成各系统网络规划（带宽、延时等）设计，保护数据增值服务。 3.根据港务系统现状完成各系统数据分级分类及相应KPI指标（RTO/RPO）规划。 4.具备国家、行业标准编制经验、工业互联网数据分级分类经验；具备安全运维服务资质、安全应急服务资质、安全集成服务资质。	外包服务

八、申能（集团）有限公司——天然气主干网全场景业务传输安全分析和赋能平台

（一）场景应用简介

上海天然气管网有限公司负责统一投资、建设和管理上海天然气主干输气管网系统，“西气东输”天然气及其他各种气源的统一接收工作。上海天然气主干网输配调度系统是集生产实时监测、控制、调度管理为一体的工控系统，实现对主干网长输管线、各类站点远程管理、集中控制、工艺数据实时采集、事故报警、参数调整等管理功能，应用有多种通讯方式。在申能集团“智慧能源”的战略部署下，应用5G、物联网、云计算等先进技术，开展了无人机智能巡检等探索。随着《网络安全法》、《数据安全法》等陆续出台，需面向智能气网相关应用场景需要明确新威胁和系统脆弱点，构建全场景下的业务数据传输安全防护解决方案。

（二）安全需求简介

上海天然气管网公司上海天然气主干网输配调度SCADA系

统、主干网 5G 无人机智能巡检系统、主干网设备远程诊断系统目前均存在数据传输模式、软硬件、应急演练、安全监测四个方面的短板问题。本项目涉及到老站点传输改造、5G 边缘数据传输、工控设备诊断数据传输等全场景业务传输安全问题，以及天然气监测点、系统指标数据、远程控制数据等多类型数据，需要对数据安全传输进行相关防护，建设全场景下的统一业务传输安全感知平台，并对不同的系统制定相关的应急演练方案。

（三）分项需求清单

建设内容	技术参数/能力要求	交付类型
私有云场景下重要业务数据安全传输建设	边界安全要求：支持主流工业协议深度解析、通信过程加密、访问控制、入侵防御、恶意代码防范。部署简单，无需改变原有网络架构。 管理安全要求：数据需要传输到上层的安全分析平台。支持工业/物联网网络信息安全态势评估与决策支撑技术，包含但不限于攻击链溯源技术、潜在威胁行为分析技术。 相关厂家在工业防护产品研发方面有多年的研发经验并已在其他 ICS 或 DCS 系统中已有实际的使用场景，具有国家的相关资质。	系统建设
公有云场景下物联网数据和工业诊断数据远传安全传输建设	边界安全要求：支持运营商专网等环境下的主流工业协议深度解析、通信过程加密、访问控制、入侵防御、恶意代码防范。部署简单，无需改变原有网络架构。 管理安全要求：数据需要传输到上层的安全分析平台。支持工业/物联网网络信息安全态势评估与决策支撑技术，包含但不限于攻击链溯源技术、潜在威胁行为分析技术。 相关厂家已在其他 ICS、DCS 系统、公有云安全应用方面中已有实际的使用场景，具有国家的相关资质。	系统建设
应急演练规划需求	重新编写 SCADA 系统安全事件应急预案并进行应急演练，符合 GB/T 38645-2020《信息安全技术 网络安全事件应急演练指南》规定，相关厂家在工业自动化领域具有多年安全服务经验和应急规划能力，安全服务方面具有国家认可的相关网络安全服务资质、例如安全集成、安全运维、应急响应、风险评估等。	外包服务

九、上海城投水务（集团）有限公司——水务数字化转型升级云边端协同安全防护体系

（一）场景应用简介

城投水务集团面向生产控制智能化、管理决策智能化、数据业务共享化、数据服务精准化的数字化转型升级能力建设。在推进落实水务数字化转型升级过程中，初步明确了 IT 和 OT 技术融合的工业互联网能力建设思路，形成了水务系统云、边、端一体化协同联动的新型应用场景。随着《网络安全法》、《数据安全法》等数据合规相关的立法和标准趋于完善，城投水务集团面向云边端协同场景安全需要，明确新型复杂应用场景下面临的安全威胁和系统脆弱点，构建具备混合云架构数据安全防护、边缘数据传输安全防护、工控数据传输安全防护等立体化云边端协同安全防护解决方案。

（二）安全需求简介

水务数字化转型升级建设通过将物理世界内的传感器、智能水泵、智能阀门等各项设备数据采集起来，利用物联网技术和云计算，将物理世界的生产运营情况转换成数字世界的实时数据和可视化图形展示，为数字化举措的全感知、在线化、智能化、数据化和全渠道提供基础数据和基础设计。本项目涉及到混合云架构、边缘数据传输、工控数据传输等云边端典型场景下的敏感数据保护问题。

（三）分项需求清单

建设内容	技术参数/能力要求	交付类型
混合云架构数据安全防护系统	1. 物理环境安全要求：支持系统漏洞发现、防止病毒入侵、完善云资源的访问控制、物理环境异常的灾备等问题。 2. 业务系统安全要求：支持业务系统用户信息安全、操作日志和操作审计、系统高可用设计、会话安全管理、通信过程加密。 3. 业务数据安全要求：支持系统敏感数据识别、对敏感信息的脱敏、对关键信息存储的加密、授权、灾备、异常恢复问题。 4、网络安全要求：支持阿里公有云租户网络和互联网之间的网络隔离、防止外网攻击、配置访问控制、保证数据传输过程中的安全性。	外包服务（全局规划）系统建设

边缘数据传输安全防护系统	支持可信中心管控、安全风险管理、终端可信接入管控、安全运营管理、智能响应处置等功能；支持身份可信认证、持续度量、动态授权等功能；具备最小权限访问、可信加密传输、动态监测、安全联动等功能。	系统建设
工控数据传输安全防护系统	部署适用工控环境的加密或数字证书产品，兼具统一管理界面及可视化数据传输监控等功能；支持国密算法，可识别主流工控协议，统一的管控平台界面展示，数据异常报警等。	系统建设

十、上海华谊能源化工有限公司——绿色化工工厂工业网络安全建设

（一）场景应用简介

上海华谊能源化工有限公司是对煤炭资源进行综合利用的国有大型化工企业。能化公司吴泾基地目前有各类控制系统 58 套，数据通过 OPC 服务器发送到数据采集设备，数据采集设备将数据提供给 PI 系统，PI 系统将重要生产安全数据远传到市政专用平台，多处边界区域网络安全措施缺失，迫切需要进行相关加固工作。

（二）安全需求简介

网络边界安全的需求有以下三个方面，一是各个装置与 PI 服务器的网络边界，技术应用上要考虑轻量化、无扰动、业务数据的采集与安全数据采集之间的关联;二是 PI 服务器和市政专用平台的网络边界，技术应用上要求具备入侵防御、抗 DDos 攻击、工业协议深度过滤、数据加密传输等功能；三是工业控制系统网络安全运维服务，要求提供策略优化、风险评估、应急响应、安全运维等服务。

（三）分项需求清单

建设内容	技术参数/能力要求	交付类型
装置边界安全加固防御系统	1.功能上支持主流工业协议深度解析、访问控制、入侵防御、恶意代码防范。部署简单，无需改变原有网络架构。 2.相关厂家在工业防护产品研发方面有多年的研发经验并已在其他 ICS 或 DCS 系统中已有实际的使用场景，具有国家的相关资质。	系统建设

远传边界安全加固防御系统	1.功能上支持安全认证、访问控制、加密通信、入侵防御、工业协议深度过滤等功能。 2.相关厂家在工业防护产品研发方面有多年的研发经验并已在其他 ICS 或 DCS 系统中已有实际的使用场景，具有国家的相关资质。	系统建设
工业控制系统网络安全运维服务	1.提供策略优化、风险评估、应急响应、安全运维等安全服务。 2.相关厂家在工业自动化领域具有多年安全服务经验和应急规划能力，安全服务方面具有国家认可的相关网络安全服务资质，例如安全集成、安全运维、应急响应、风险评估等。	外包服务

附件 2

揭榜意向征集表

企业名称	
联系人	
移动电话	
意向申报需求序号及名称（可多选）	如“九、上海城投水务（集团）有限公司——水务数字化转型升级云边端协同安全防护体系”

附件 3

上海市 2021 年重点行业数字化转型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 法定代表人签章: 申报单位公章: 年 月 日 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　　2021年7月12日印发