

上海市政务外网第三方专业服务 采购需求

一、项目概述

项目背景：为充分发挥上海市政务外网的支撑保障作用，持续提升其运行质量与服务能力，通过引入第三方专业服务机构，构建涵盖规划建设、运维支持、安全防护、数据赋能的一体化服务体系。本项目通过提供日常管理、质量管理、安全管理等方面的专业化支撑服务，对政务外网服务商运营活动实施综合监管，推动服务质量持续提升，实现政务外网资源的高效配置、规范运行与长效发展。

服务期限：自合同签订之日起一年

服务地点：上海市寿阳路 99 弄 15 号

预算金额：150 万元

采购金额（最高限价）：150 万元

组织形式：集中采购

采购方式：竞争性磋商

面向企业类型：大中小微

是否接受联合体响应：否

二、服务范围

供应商应协助采购人在服务周期内对政务外网建设、接入、运行和安全管理提供专业化支撑，涵盖网络建设、运维、性能、安全和运营的合规性审核、现场检查及制度执行监督，以及服务质量评估、通信服务费数据稽核、通信服务项目验收等工作。通过专业化技术支撑，提升运营的专业性与规范性，驱动服务质量持续提升。

三、服务需求

供应商应协助采购人，对政务外网服务商和 5G 运营商的服务过程及输出成果进行合规性审核与服务质量评估；针对发现的问题，供

应商需提出整改建议并督促实施；全程追踪整改结果，形成闭环管理。政务外网专业服务内容主要包括：协助完善服务质量体系，优化管理规范、评估指标与评估方案，开展能力培训；对网络建设、运维运营、性能、安全等环节开展过程监管与合规性审核；组织服务质量评估考核与通信服务费稽核；协助完成项目验收与合同履行审核。

具体服务内容如下：

序号	主要模块	子模块
1	服务质量体系完善	(1) 服务管理优化与能力提升
		(2) 服务质量评估指标设计与优化
		(3) 服务质量评估方案设计与优化
2	规范性监管服务	(1) 专业服务方案设计
		(2) 网络建设合规性支撑
		(3) 运维运营合规性支撑
		(4) 网络性能符合性核查
		(5) 网络安全管理支撑
		(6) 闭环式管理服务
3	服务质量评估考核	(1) 服务抽查
		(2) 数据采集
		(3) 数据稽核
		(4) 指标分析
		(5) 质量评估
		(6) 优化建议
		(7) 报告撰写
4	通信服务费稽核	(1) 政务外网通信服务费数据稽核
		(2) 政务外网通信服务费稽核报告撰写
5	验收服务	(1) 协助组织验收，核验材料完整性与合规性
		(2) 开展服务商履约审核

3.1 服务质量体系完善

为充分发挥上海市政务外网的支撑保障效能，建立"标准统一、指标量化、评估闭环、持续改进"的长效管理机制，供应商应根据采购人现行的制度框架和政务外网运营管理实际，提出优化建议，协助采购人完善服务质量体系，为政务外网的稳定运行和服务能力持续提升提供坚实的制度保障。

3.1.1 服务管理优化与能力提升

1. 供应商应基于运营服务支撑中发现的问题，协助采购人按需优化管理规范，持续完善覆盖网络建设、性能保障、运维支持与安全防护等环节的服务管理规范体系，明确各环节的服务标准、操作流程、岗位职责、时限要求与质量要求，并针对日常运营中的高频事项制定专项管理规范。

2. 供应商应提供一年不少于 2 次的政务外网能力培训服务，培训对象为采购人及政务外网服务商，培训内容涵盖管理、技术、安全及运营等核心领域。所有培训费用（含教材费）及其他相关支出，应整体计入总费用中。

3.1.2 服务评估指标设计与优化

1. 供应商应协助采购人依据相关管理规范，设计运营服务的合规性检查清单，明确资源交付效率、故障响应时效、安全合规性、用户满意度等维度的具体评估指标，制定各指标的可量化阈值与数据采集来源，形成完整的服务质量评估指标体系，支撑日常专业化服务质量管理。

2. 供应商应基于实际运营数据及问题反馈，协助采购人动态优化评估指标，确保指标的实效性、准确性与管理牵引力。

3.1.3 服务评估方案设计与优化

1. 供应商应以管理规范 and 评估指标体系为基础，结合行业研究和对标成果，设计上海市政务外网及 5G 接入服务质量的专业评估方案，方案需明确评估指标与评分规则、标准化评价流程、责罚条款。

2. 供应商应根据服务质量改进成效与运营变化，按需调优评估方案，确保评估方法的专业性与科学性，将评估结果纳入政务外网服务商绩效考核，驱动服务商专业能力与规范性的持续提升。

3.2 规范性监管服务

3.2.1 专业服务方案设计要求

1. 供应商应结合政务外网及 5G 接入运营特点，设计针对性的运营服务管理支撑方案。方案应明确以下内容：服务合规性审核、现场检查、制度执行监督的具体事项、执行标准与管控要点；季度及月度工作计划的详细安排。

2. 供应商应根据服务实际执行情况、最新政策法规要求及上一阶段检查发现的问题，对管理支撑方案实施动态迭代优化。

3. 供应商应就日常运营服务过程中的专项任务或重点问题，进行专项专业支撑，包括明确工作目标、实施内容、时间计划及交付标准，确保专项工作有序推进、落地见效。

3.2.2 网络建设合规性支撑

1. 供应商应协助采购人对服务商网络建设实施全周期规范性管理。具体包括：技术可行性审核，评估服务商及 5G 运营商提交的建设方案、实施计划、技术文档等材料的技术可实现性；安全合规审查，评估方案及文档符合国家及行业安全标准；计划有效性核验，分析实施计划的节点合理性及资源保障措施。

2. 供应商应协助采购人对建设过程的合规性进行跟踪检查，在完工阶段进行工单复核，确保建设成果符合业务需求、技术规范及相关政策要求。

3.2.3 运维运营合规性支撑

1. 供应商应协助采购人对业务开通、故障处理、资源巡检、割接管理、应急响应、资产管理、系统数据对接等日常运维活动的规范性进行审核，督促服务商按时提交各类运维报告，并对报告的规范性、内容完整性及数据准确性进行核验。

2. 供应商应针对 5G 接入涉及的关键环节，包括号卡开通进度、故障处理时效、网络服务保障、用户投诉处理、应急保障机制等，协助采购人开展专项合规性检查和过程管理支撑，建立问题跟踪台账，闭环跟进问题处理进度与整改结果。

3.2.4 网络性能符合性核查

1. 供应商应协助采购人对政务外网及 5G 接入的关键性能指标（包括网络可用性、丢包率、时延、带宽使用率等）实施符合性核查，督促服务商按要求提交网络性能 ping 测数据并进行统计分析，依据相关考核要求对指标偏离情况进行核查记录，出具网络性能数据报告或分析意见，为网络优化升级提供参考依据。

2. 供应商应对政务外网服务商提交的 ping 测数据在测试节点选取合理性、测试频率合规性及数据有效性验证等方面进行技术审核，必要时开展现场抽查测试，确保数据真实有效。

3. 针对网络优化升级、重要时段保障、5G 接入区性能测试等场景，供应商核验政务外网服务商提交的网络性能测试记录，评估带宽性能是否达标、确认端口性能配置是否满足网络扩容要求。

3.2.5 网络安全管理支撑

1. 供应商协助采购人监督政务外网服务商开展市级政务外网的以下安全保障工作：资产安全、物理环境安全、通信安全、平台系统安全、访问控制安全、业务连续性保障，并按季度对物理环境、设备运行状态及安全防护措施开展合规性抽查。

2. 供应商协助采购人审核政务外网服务商提交的重要时段的安全保障方案，提出修改建议，实施重保前政务外网服务商安全工作的现场抽查，保障重保工作的有效执行。

3. 供应商协助采购人健全市级政务外网总体应急预案，并按需修订，审核政务外网服务商提交的安全应急预案、演练计划及演练记录，督促其按规范开展应急演练并实施全流程监管，确保所有应急演练有效执行。

4. 供应商协助采购人对政务外网服务商的安全自查及等保测评情况进行跟进，并督促其对自查及测评中发现问题的进行整改，审核整改方案及整改报告，并不定期组织专项抽查复核，确保整改措施落实到位。

5. 供应商协助采购人核查政务外网 5G 无线接入区机房的物理安全环境、重要业务系统运行状态、安全边界功能部署情况及安全策略配置的合理性。

3.2.6 闭环式管理服务

1. 供应商协助采购人在业务需求、问题处理等方面建立全流程闭环管理机制。对支撑服务过程中发现的问题进行梳理归类，形成动态更新的问题清单，督促政务外网服务商制定整改方案并限期落实，推动共性问题根治与服务流程优化。

2. 供应商协助采购人按月跟踪并汇总各项工作进展、问题处理进度及运营指标达标情况，编制服务过程管理月报，作为闭环管理核心载体，为采购人管理决策提供持续信息支撑，确保运营监管全程留痕可追溯。

3.3 服务质量评估考核

供应商按以下要求协助采购人开展服务质量评估考核工作：依据政务外网及 5G 接入服务质量评估方案，按期执行评估考核；完整涵盖服务抽查、数据采集、数据稽核、指标分析、质量评估、优化建议及报告编制。具体工作内容包括：

1. 服务抽查

供应商基于政务外网等保测评及安全自查结果，按季度对机房进行现场抽查（每季度不少于 3 个机房），重点复核政务外网服务商安全整改措施的真实性与有效性；同时通过电话抽查测试报障专线，评估服务商 7×24 小时服务响应的及时性与规范性。

2. 数据采集

评估数据主要来源于政务外网运行与安全监测支撑系统以及现场检查测试数据。测试节点采用随机抽样法确定，每季度抽查数量不低于纳入考核范围节点总数的 10%，确保样本覆盖面和统计代表性，为后续分析提供充分的数据基础。

3. 数据稽核

供应商按照标准化的数据处理与稽核流程，对采集数据进行规范化处理和逐项稽核，重点核实数据的准确性与完整性，溯源排查异常数据成因，确保数据分析结论客观反映网络运行实况。

4. 指标分析

基于稽核的有效数据，同步开展服务流程关联分析与时间趋势波动分析：既通过逐项监测指标完成度及变化趋势识别异常波动或持续下滑问题，又结合服务周期对多环节关键指标进行关联分析，定位服务链条中的薄弱环节与关键短板。

5. 质量评估

基于指标分析结果，对网络运维、性能、安全及运营服务开展综合评价。严格依据政务外网服务质量评估方案所制定的评分规则进行量化评分，并将评估结果作为政务外网通信服务费用支付金额的重要参考依据。

6. 优化建议

基于指标分析与质量评估结论，系统梳理政务外网服务质量的薄弱环节，针对短板开展深度分析研判，提出具体、可落地的优化建议，支撑服务质量持续提升。

7. 报告编制

综合指标分析、质量评估结果及优化建议，编制《政务外网服务质量季度/年度评估报告》与《政务外网 5G 接入服务质量年度评估报告》，作为政务外网整体运行评估的标准化依据。

3.4 通信服务费稽核

1. 供应商协助采购人对政务外网通信服务费基础数据进行稽核，重点对带宽、流量数据及计费规则的准确性进行稽核，确保基础数据准确性。

2. 供应商基于稽核确认的数据，对实际服务量进行核算与计量分析，并出具《政务外网网络通信服务费稽核报告》。采购人将报告中稽核确认的实际政务外网通信服务量提交至业务管理单位，该报告作

为通信服务费支付的依据。

3.5 通信服务项目验收

1. 供应商协助采购人依据验收要求,组织并开展政务外网通信服务项目的验收工作。包括但不限于督促政务外网服务商准备并完整提交验收材料,审核验收材料完整性及其与验收标准的符合度,确保验收基础工作规范、完备。

2. 供应商协助采购人开展政务外网服务商合同履行审核,明确审核内容清单与审核方式,记录审核结果,明确审核结论,确保履约结果有记录、可验证追溯。

四、项目成果

政务外网专业服务方案(1份)

政务外网服务质量评估方案(1份)

政务外网服务过程监管月报(12份)

政务外网服务质量评估季度报告(4份)

政务外网服务质量评估年度报告(1份)

政务外网网络通信服务费稽核报告(1份)

政务外网 5G 接入服务质量评估方案(1份)

政务外网 5G 接入服务质量年度评估报告(1份)

政务外网专项服务报告(按需提供)

五、验收要求

本项目验收采用服务年度验收方式开展,待每年合同约定的服务期满,由采购人组织专家评审会对评估的所有成果文档和过程文档开展验收工作。

1. 验收标准:完成合同内容,提交项目相关成果报告,通过终

期项目汇报。

2. 验收方法：由采购方成立项目评审专家组，通过召开专家评审会，审阅项目验收材料，听取项目经理介绍项目开展基本情况和主要成果汇报，评审专家按照合同要求进行评审，主要从成果的质量、完成进度等方面进行评审。

3. 验收时间和地点：按照采购人要求确定。

六、服务组织和人员要求

供应商按第三方专业服务内容配置不少于 10 名成员（含至少 3 名驻场服务人员）的团队。项目经理具有信息工程或通信工程相关的高级及以上职称证书的，以及具备政务信息化项目经理工作经历的，优先考虑。其他团队成员具有信息系统项目管理师、信息安全专业认证(CISP)证书等证书的优先考虑。服务质量评估拟投入人员具备信息化项目质量评估或绩效评价经验，安全支撑服务人员具备网络安全技术工作相关经验，运维支撑服务人员具备网络运维技术工作相关经验。具体要求如下：

角色	主要职责	人员数量	驻场要求
项目经理	负责项目质量和进度控制	1 人	按需
专业咨询服务	负责服务体系优化、评估方案与管理支撑方案设计优化、管理规范健全、各类报告撰写等工作	至少 2 人	驻场 1 人
安全管理支撑服务	负责网络安全管理支撑工作，包括安全月报审核、安全问题研判以及现场勘测，网络安全检查、网络安全问题整改落实情况跟踪与整改复核等。	至少 2 人	驻场 1 人
运维管理支撑服务	负责网络性能和工程建设进度符合性与合规性检查，包括网络性能分析报告审核、竣工及时性情况跟踪等；负责网络运维合规性检查，包括故障报告审核、故障原因研判、整改意见出具、整改落实情况跟踪与闭环等。	至少 2 人	驻场 1 人

角色	主要职责	人员数量	驻场要求
技术支持服务（含评估考核、服务费稽核与验收服务等）	为团队提供技术支持，解决问题及方案等服务；负责服务质量评估考核、评估报告编制；负责政务外网通信服务费稽核与验收服务等。	至少 3 人	按需

七、服务提供方要求

供应商具有近三年类似项目业绩的优先考虑。

八、安全管理要求

供应商在提供服务过程中，应将安全管控措施与服务实施同步落实，并将安全服务相关管控措施纳入安全保障方案。

1、在提供服务过程中，供应商应在采购人限定的办公区域内、访问或使用采购人限定的信息资产（包括但不限于场地办公设施、计算机、服务器等），并在规定的安全环境中进行数据处理、系统查询等活动。

2、提供服务过程中若涉及开源软件、组件等产品的使用，供应商应在使用前向采购人提供项目涉及产品的完整清单，并附相应产品的漏洞扫描报告、安全评估报告等证明材料，经审核通过后方可使用。

3、供应商需提供自身的网络与数据安全管理制度及保密管理制度，上述制度如有变动或更新，供应商应及时向采购人提交相关材料。

4、供应商成交后与采购人签订保密协议，同时供应商应对项目相关人员开展安全培训，并与该项目人员的签订保密协议，且保证用于项目实施工作的相关终端安装正版杀毒软件及防火墙。

5、提供服务过程中，供应商需要对收集到的所有信息严格管理，严禁在网络上传播、散布和出售，牟取商业利益；供应商人员不得以任何方式泄露、公开或传播项目涉及的内容及成果；不得非法篡改数据、非法入侵政务外网，不得影响数据的完整性及可用性；不得留存

任何安全风险隐患；参与项目的服务人员，不得私自拷贝和留存上述信息副本。

6、指定专人负责项目实施过程中的安全工作，协助采购人开展安全检查等工作。

7、供应商通过项目获取到的政务外网数据禁止超过合同限定范围使用，以及违规转发第三方。

8、供应商应按规定申请数据服务接口，加强认证和鉴权防护，保护中心敏感数据不被泄露；禁止将管理后台暴露在互联网上；

9、加强对项目人员的安全管理。进入项目前，供应商应提供项目人员的无犯罪记录证明，与采购人签订保密协议。入场前，项目人员应填写入场申请，按需申请系统账号、云桌面账号和工位。入场后，项目人员应在规定的安全环境中进行数据处理、运营监管等活动，遵守环境安全监控的要求，禁止共用账号、拍照等。禁止个人私自搭服务端和共享网络、终端跨互联网和政务外网。禁止在互联网传输敏感文件。非驻场人员，按需提出入网申请，并安装终端管理工具。禁止将政务外网数据在个人电脑上留存使用，因需求调研或设计获取数据的，禁止将敏感数据外发，或存储在共有云上，数据使用后应进行销毁。

10、供应商应按照采购人场地及人员管理制度，加强人员管理，并配合采购人落实人员背调、入离场、终端管理、网络限制、数据权限最小化等管控措施。

九、安全处罚措施

如供应商在服务周期内发生网络和数据安全工作违约，导致安全事件或对政务外网系统造成重大安全影响的，采购人将根据事件严重

程度，由安全管理部门确定采取以下一项或多项处罚措施：

- (1) 出具书面整改通知，限期整改；
- (2) 约谈供应商负责人；
- (3) 按次扣除项目服务合同金额的 1%-3%作为违约金；
- (4) 上报主管部门，必要时终止项目合同并追究相关刑事责任。

事件类型与等级及与之相应的处罚措施详见附表《安全事件处罚措施》。

十、项目的变更、解除和终止

如果服务提供方丧失履约能力、发生资不抵债或进入破产程序，采购人可在任何时候以书面形式通知服务提供方终止本项目的执行而不给予服务提供方补偿。该终止本项目将不损害或影响采购人已经采取或将要采取任何行动或补救措施的权利。

如遇国家、行业管理部门等机构的有关标准和规定调整的，导致本项目内容需做相应调整时，双方应按照公平、合理的原则共同协商修改本项目对应的合同的相关条款。

十一、保密责任

1. 成交供应商因履行本项目而知悉的所有数据、信息和资料(包括但不限于账号信息、图表、文字、计算过程、任何形式的文件、访谈记录、现场实测数据、采购人相关工作程序等)以及因履行本项目而形成的数据、信息和任何形式的工作成果，均是采购人要求保密的信息。未经采购人书面同意，成交供应商不得对外泄露采购人要求保密的信息，不得用于其他用途，否则成交供应商需承担由此引起的法律责任和经济责任，包括但不限于直接损失、间接损失、律师费、诉讼费/仲裁费、调查费、公证费等。

2. 成交供应商应采取必要的有效措施保证其参与本项目的人员（包括成交供应商聘用的人员、借调的人员、实习的人员）无论是在职或离职后，以及成交供应商的合作方无论是合作中或合作终止后，都能够履行本项目约定的保密义务。若成交供应商人员或成交供应商合作方违反保密规定，成交供应商应承担连带责任。

3. 成交供应商(含成交供应商参与本项目的人员以及其合作方)未经采购人书面许可，不得以任何形式自行使用或以任何方式向第三方披露、转让、授权、出售与本项目有关的技术成果、计算机软件、源代码、策划文档、技术诀窍、秘密信息、技术资料和其他文件。

4. 以上内容的保密期限自成交供应商知悉保密信息起始至保密信息被合法公开之日止。

5. 成交供应商对采购人提供的临时使用账号要保密，不得公开，对组件开发的账号密码需进行加密，避免信息安全的泄露。未经采购人的同意不得利用采购人的网络及平台进行短信、彩信、微信、邮件等发送,造成的一切后果由成交供应商负责。

服务过程成交供应商如出现失、窃密事情，参照附表《安全事件处罚措施》同等处置，具体处罚措施由中心保密管理部门确定。

十二、违约责任

1. 除因不可抗力或供应商取得采购人允许延期的书面通知外，供应商未能按时提交评估报告的，每迟延一个工作日，扣除本项目总金额千分之二的款项。

2. 供应商未使用双方约定的方法开展评估，或已按双方约定的方法开展评估但因自身原因造成评估结果明显不准确的，采购人有权要求供应商在指定的时间内完成整改，逾期未整改完成的，供应商应

将本项目相应评估工作模块报价的全部价款退还给采购人，并扣除本项目总金额 5%的款项。

3. 供应商提供的服务不符合本合同的约定，采购人有权要求供应商在指定的时间内完成整改，逾期未整改完成的，供应商应将本项目相应工作模块报价的全部价款退还采购人，并扣除本项目总金额 5%的款项。

4. 供应商违反本项目的安全要求、知识产权要求、保密要求、转包分包规定的，供应商应当退还采购人已支付的款项，并按照本项目总金额的 5%支付违约金。

5. 供应商有其他违反本项目合同约定的行为，采购人有权要求供应商在指定的时间内完成整改，逾期未整改完成的，扣除本项目总金额 5%的款项。

6. 供应商违反以上条款的，如果供应商支付的违约金不足以弥补给采购人造成的损失，除要求供应商支付违约金外，采购人还有权要求供应商支付违约金与所受损失的差额。

十三、关于转让和分包的规定

本项目不得转包和分包。

附表：安全事件处罚措施

序号	类型	负面行为分级情况	处罚措施
1	安全事件	1、发生网络安全事件或数据泄露事件，每发生一起，按不同级别进行追究。	见下
2		(1)发生重大(Ⅱ级)及以上网络和数据安全事件的；	1、限期整改； 2、约谈供应商负责人； 3、扣除项目服务合同金额的 3%； 4、上报主管部门，必要时终止项目合同并追究相关刑事责任。
3		(2)发生较大网络安全和数据事件(Ⅲ级)的；	1、限期整改； 2、约谈供应商负责人； 3、扣除项目服务合同金额的 2%。
4		(3)发生一般网络和数据安全事件(Ⅳ级)的。	1、限期整改； 2、约谈供应商负责人； 3、扣除项目服务合同金额的 1%。
5		2、被主管部门通报安全事件，每发生一起，按不同级别进行追究。	见下
6		(1)被中央有关部门通报，并核实的。	1、限期整改； 2、约谈供应商负责人； 3、扣除项目服务合同金额的 3%。
7		(2)被本市有关部门通报，并核实的。	1、限期整改； 2、约谈供应商负责人； 3、扣除项目服务合同金额的 2%。
8		(3)被中心通报，对业务造成影响。	1、限期整改； 2、约谈供应商负责人； 3、一个服务周期内累计发生 3 次及以上的，扣除项目服务合同金额的 1%。
9		3、未经批准，擅自在各种媒体发表与中心有关的评论或言论。	1、限期整改； 2、约谈供应商负责人； 3、扣除项目服务合同金额的 2%