项目编号：**310107000260803126749-07372939**

智联普陀光纤专网安全加固政务信息化购买服务项目（2026 年度）

公开招标文件

采购单位：上海市普陀区城市运行管理中心（上海市普陀区城市网格化综合管理中心、上海市普陀区政务服务中心、上海市普陀区大数据中心）

2026年10月21日

集中采购机构：上海市普陀区政府采购中心

2026年10月21日

目　　录

第一章　招标公告

第二章　投标人须知

第三章　政府采购政策功能

第四章　招标需求

第五章　评标办法及评分标准

第六章　政府采购合同主要条款指引

第七章　投标文件格式附件

第一章　招标公告

项目概况

智联普陀光纤专网安全加固政务信息化购买服务项目（2026 年度）招标项目的潜在供应商应在上海市政府采购网获取招标文件，并于 2026-11-13 10:00:00 前递交投标文件。

一、项目基本情况

1.1 项目编号：31010700026080312674 9-07372939

1.2 项目名称：智联普陀光纤专网安全加固政务信息化购买服务项目（2026 年度）

1.3 预算编号：0726-00006784、0726-K00007664

1.4 预算金额（元）：4766200.00 元（国库资金：4766200.00 元；自筹资金：0 元）

1.5 最高限价（元）：包 1-4766200.00 元

1.6 采购需求：

1）包名称：智联普陀光纤专网安全加固政务信息化购买服务项目（2026 年度）

2）数量：1

3）预算金额：4766200.00 元

4）简要规格描述或项目基本概况介绍、用途：购买智联普陀光纤专网安全加固政务信息化购买服务项目（2026 年度），具体详见招标需求。

1.7 合同履约期限：本项目服务周期为合同签订后一年。

1.8 本项目（不允许）联合体投标。

二、申请人的资格要求

1、符合《中华人民共和国政府采购法》第二十二条的规定

2、未被“信用中国”（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单

3.本项目的特定资格要求：

1 根据《上海市政府采购供应商登记及诚信管理办法》已登记入库的供应商；

2 根据财库[2016]125 号文，未被列入“信用中国”网站（www.creditchina.gov.cn）失信被执行人名单、重大税收违法案件当事人名单和中国政府采购网（www.ccgp.gov.cn）政府采购严重违法失信行为记录名单的供应商；

3 本项目不允许转包与分包。

三、获取招标文件

1. 合格的供应商可于 2026-10-23 至 2026-11-01，上午 00:00:00~12:00:00；下午 12:00:00~23:59:59（北京时间，法定节假日除外）

2.地址：上海政府采购网

3.方式：网上获取

4、售价（元）：0

四、提交投标文件截止时间、开标时间和地点

1、提交投标文件截止时间：2026-11-13 10:00:00

2、投标地点：上海电子投标客户端上传加密标书（纸质文件递交：**上海电子投标客户端上传加密标书（纸质文件递交：上海市大渡河路 1668 号 5 号楼 A418 室。）**

3、开标时间：2026-11-13 10:00:00（北京时间）

4、开标地点：**上海市大渡河路 1668 号 5 号楼 A418 室**

5、开标所需携带其他材料：届时请投标供应商的法定代表人（负责人）或法定代表人（负责人）授权委托人持法定代表人（负责人）证明书或法定代表人（负责人）授权委托书及相应身份证明、对招标文件的无疑问函（加盖公章）、所使用的数字证书（CA 证书）和可以无线上网的笔记本电脑出席开标仪式。投标单位需在网上填报并上传全套投标文件（加盖公章后扫描上传），并在项目开标时递交响应文件书面文本：正本一份，副本四份。

五、公告期限

自本公告发布之日起 5 个工作日。

六、其他补充事项

1、根据上海市财政局的规定，本项目招投标工作必须在上海市政府采购云平台上进行。本项目潜在投标人在投标前应当自行了解政府采购云平台的基本规则、要求、流程，具备网上投标的能力和条件，知晓并愿意承担电子招投标可能产生的风险；

2、投标人须保证报名及获得招标文件时提交的资料和所填写内容真实、完整、有效、一致，如因投标人递交虚假材料或填写信息错误而造成的任何损失由投标人承担；

3、集中采购机构将会在开标前一个工作日起对投标文件进行统一网上签收，投标人若需撤回已签收的投标文件，应以传真或其它书面形式（须签字并盖章）及时告知集中采购机构；

4、投标签收回执不作为判断投标文件数据是否完整、有效的依据。如果投标人发现投标文件存在数据丢失、缺漏、乱码等情况，或在投标过程中遭遇因系统、网络故障等技术原因产生的问题，请及时联系政府采购云平台 95763； 政采云平台由上海市财政局建设并管理，政采云有限公司提供技术支持，若投标人因平台系统的故障或缺陷而产生纠纷或造成损失，请与平台管理方上海市财政局及政采云有限公司联系。采购人及集中采购机构仅作为平台使用方，不因此承担任何法律责任。

5、本项目不接受进口产品。

七、联系方式

采购人信息

名 称：上海市普陀区城市运行管理中心

地 址：上海市普陀区同普路 602 号 4 号楼 B 区 2、3 楼

联系方式：021-52564588

集中采购机构：上海市普陀区政府采购中心

地址：上海市大渡河路 1668 号 5 号楼 A413 室

邮编： 200333

联系人：沈老师

电话： 021-52564588*8491

第二章　投标人须知

序号	内　容	要　　求
1.	项目名称及数量	详见《招标公告》
2.	服务内容	详见《招标公告》
3.	投标最高限价	最高限价为：4766200.00 元（超出预算作无效标处理）
4.	采购方式	公开招标
5.	合同履约期限	本项目服务周期为合同签订后一年。
6.	付款方式	签订服务合同支付合同金额 20%费用，服务期满半年后支付合同金额 50%费用，服务期满后支付合同金额 30%尾款。
7.	信用记录	根据财库[2016]125 号文件，通过“信用中国”网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn），以开标当日网页查询记录为准。对列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单的供应商，其投标将作无效标处理。
8.	政府采购节能环保产品	投标产品若属于节能环保产品的，请提供财政部、环境保护部发布有效期内环境标志产品政府采购清单以及财政部、发改委联合发布有效期内节能产品政府采购清单。 招标需求中要求提供的产品属于节能清单中政府强制采购节能产品品目的，投标人须提供该清单内产品，否则其投标将作为无效标处理。
9.	中小企业有关政策	1、本项目**整体预留。包 1 面向中小企业预留。** 中小企业应当按照规定提供《中小企业声明函》。 2、根据财库[2017]141 号的相关规定，在政府采购活动中，残疾人福利性单位视同小型、微型企业，享受评审中价格扣除政策。属于享受政府采购支持政策的残疾人福利性单位，应满足财库[2017]141 号文件第一条的规定，并在磋商响应文件中提供《残疾人福利性单位声明函》（见附件）。 3、根据财库[2014]68 号的相关规定，在政府采购活动中，监狱企业视同小型、微型企业，享受评审中价格扣除政策，并在磋商响应文件中提供由省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件（格式自拟）。”(注：未提供以上材料的，均不给予价格扣除）。
10.	答疑与澄清	投标单位对招标文件有疑问的以书面形式(加盖投标人公章)向上海市普陀区政府采购中心提出，电话告知：021-52564588*8491。
11.	是否允许采购进口产品：	不允许进口产品具体要求详见第四章招标需求各标项的对应内容。
12.	是否允许转包与分包	转包：否 分包：否
13.	是否接受联合体投标	不允许
14.	是否现场踏勘	不组织现场踏勘
15.	是否提供演示	不进行演示

16.	是否提供样品	不要求提供样品
17.	备选投标方案和报价	不接受备选投标方案和多个报价
18.	签字盖章	投标人必须按照招标文件的规定和要求签字、盖章（法定代表人（负责人）或授权代表的签字可以具有法定效力的签章替代）
19.	投标文件组成	电子投标文件：1 份（供应商应在投标截止时间前通过投标客户端软件完成投标文件编制、加密、上传提交）。纸制投标文件：正本 1 份、副本 4 份。
20.	投标文件的装订	每份正本或副本均需装订成册
21.	投标文件封面的标注	每份投标文件封面上均应标明招标项目名称、招标编号、标包号（如有的话）、投标日期、投标人名称等内容，并在右上角标明“正本”或“副本”字样。投标人名称处需加盖单位印章。
22.	投标文件外层密封袋（箱）的标注	招标项目名称、招标编号、标包号（如有的话）、投标人名称、投标截止时间等，名称处加盖单位印章。
23.	中标结果公告	中标供应商确定之日起 2 个工作日内，将在上海市政府采购网(http://www.zfcg.sh.gov.cn/)发布中标公告，公告期限为 1 个工作日。
24.	投标保证金	无
25.	合同签订时间	中标通知书发出后 30 日内。
26.	履约保证金	无
27.	投标文件有效期	90 天
28.	投标文件的接收	招标方于投标截止时间前半小时内接收投标文件，投标文件送达回执、政府采购活动现场确认声明书（格式详见附件）应单独提供，如投标人递交投标文件时未提供回执，视同不需要回执。 投标人递交投标文件时，如出现下列情况之一的，投标文件将被拒收： 1、未按规定密封或标记的投标文件； 2、由于包装不妥，在送交途中严重破损或失散的投标文件； 3、仅以非纸制文本形式的投标文件； 4、未成功办理投标人报名手续的； 5、超过投标截止时间送达的投标文件。 投标人在投标截止时间前，可以书面通知（加盖公章）招标方，对所递交的投标文件进行补充、修改或者撤回。补充、修改的内容应当按照招标文件要求签署、盖章、密封后，作为投标文件的组成部分。
29.	解释权	本招标文件的解释权属于上海市普陀区政府采购中心。

一、总则

1.概述

根据《中华人民共和国政府采购法》、《上海市政府采购管理办法》等有关法律、法规和规章的规定，本项目已具备采购条件，现对本项目进行国内公开招标。

2.定义

2.1“招标人”系指本项目公告中所述招标人。

2.2“集中采购机构”系指上海市普陀区政府采购中心。

2.3“投标人”系指响应招标公告，向集中采购机构提交投标文件的投标人。

2.4“服务”系指招标文件规定投标人承担的各类专业服务，包含但不限于产品设计开发、产品交付、安装调试、质量检测、技术指导、售后服务、专业劳务服务和其他类似的义务。

2.5“货物”系指投标人按招标文件规定，须向招标人提供的各种形态和种类的物品，包括一切设备、产品、机械、仪器仪表、备品备件、工具、手册等有关技术资料和原材料等，以及其所提供货物相关的运输、就位、安装、调试、技术协助、校准、培训、技术指导以及其他类似的义务。

2.6“甲方”系指在合同的买方项下签字的法人单位。

2.7“乙方”系指提供合同服务的供应商。

3.合格的投标人

3.1 符合《招标公告》和《投标人须知》前附表中规定的合格投标人所必须具备的资质条件和特定条件。

3.2 招标公告中规定接受联合体的，还应遵守以下规定：

3.2.1 参加联合体的供应商均应当符合招标文件规定的合格供应商的条件，并应当向招标人提交联合体协议书，载明联合体各方承担的工作和义务。联合体各方必须指定牵头人，授权其代表所有联合体成员负责投标和合同实施阶段的主办、协调工作，并使用牵头人数字证书（CA 证书）参加投标报价。

3.2.2 联合体中有同类资质的供应商按照联合体分工承担相同工作的，应当按照资质等级较低的供应商确定资质等级。

3.2.3 以联合体形式参加政府采购活动的，联合体各方不得再单独参加或者与其他供应商另外组成联合体参加同一合同项下的政府采购活动，否则，相关投标文件均无效。

3.2.4 招标文件要求提交投标保证金的，可以由联合体中的一方或者多方共同交纳，其交纳的投标

保证金对联合体各方均具有约束力。

3.2.5 联合体中标的，联合体牵头人与招标人在云采交易平台签订采购合同，联合体各方就采购合同约定的事项对招标人承担连带责任。

3.2.6 根据《财政部关于在政府采购活动中查询及使用信用记录有关问题的通知》（财库〔2016〕125 号）的规定，应当对所有联合体成员进行信用记录查询，联合体成员存在不良信用记录的，视同联合体存在不良信用记录，将拒绝其参与政府采购活动。

3.2.7 联合体中标的项目，在中标公告中联合体各方的相关信息均应一并公告。

3.3 投标人所使用的资格、信誉、业绩及企业认证必须为本法人所拥有。被省级或省级以上政府采购监管部门处分，禁止参加政府采购活动且尚在禁止期内的供应商不得参加本项目的投标。

4.合格的服务

4.1 投标人所提供的服务应当没有侵犯任何第三方的知识产权、技术秘密等合法权利。

4.2 投标人提供的服务应当符合招标文件的要求，并且其质量完全符合国家标准、行业标准或地方标准，均有标准的以高（严格）者为准。没有国家标准、行业标准和企业标准的，按照通常标准或者符合采购目的的特定标准确定。

5.投标费用

不论投标的结果如何，投标人均应自行承担所有与投标有关的全部费用，招标人在任何情况下均无义务和责任承担这些费用。

6.信息发布

本采购项目需要公开的有关信息，包括招标公告、招标文件澄清或修改公告、中标公告以及延长投标截止时间等与招标活动有关的通知，招标人均将通过“上海政府采购云平台”（http://www.zfcg.sh.gov.cn）公开发布。投标人在参与本采购项目招投标活动期间，请及时关注以上媒体上的相关信息，投标人因没有及时关注而未能如期获取相关信息，及因此所产生的一切后果和责任，由投标人自行承担，招标人在任何情况下均不对此承担任何责任。

二、招标文件

7.招标文件的组成

7.1 招标文件是阐明招标的项目范围、投标文件的编写、递交、招标投标程序、评标原则、中标条件和相关的协议条款的文件。招标文件由下述部分组成：

第一章 招标公告；

第二章 投标人须知；

第三章 政府采购政策功能；

第四章 招标需求；

第五章 评标办法及评分标准；

第六章 政府采购合同主要条款指引；

第七章 投标文件格式附件。

7.2 招标文件用汉语编印。

7.3 除非有特殊要求,招标文件不单独提供具体服务项目的相关情况，投标人被视为熟悉上述与履行协议有关的一切情况。

7.4 投标人应详细阅读招标文件的全部内容，如果投标人没有按照招标文件要求提交全部资料或者没有对招标文件在各方面的要求都做出实质性响应，可能导致其投标被拒绝。

8. 招标文件的澄清和修改

8.1 招标人可以对已发出的招标文件主动进行澄清或修改。澄清和修改的内容可能影响投标文件编制的，招标人应当在投标截止时间至少 15 日前，以书面形式通知所有获取招标文件的潜在投标人；不足 15 日的，招标人应当顺延提交投标文件的截止时间。

8.2 招标文件的修改将在上海政府采购网上发布公告，并对投标供应商具有约束力。投标供应商应主动上网查询。

8.3 补充文件将构成招标文件的一部分，对投标人有约束力。

8.4 当后发的补充文件与原招标文件或此前发出的补充文件之间存在不一致时，以后发的补充文件为准。

9. 对招标文件的疑问和处理

9.1 投标方对招标文件如有疑问，可要求澄清，应按《投标人须知》前附表规定的时间前按投标邀请中载明的地址以书面形式（盖单位公章）（并提供 E_mail）通知到集中采购机构。由采购单位负责统一解答。如有需要，将安排召开答疑会，并通过“上海政府采购网”以澄清或修改公告形式发布。投标人未在规定时间内提出疑问的，则视为对招标文件无异议。

9.2 标前会集中采购机构将根据投标人的澄清要求决定是否召开标前会，标前会召开的具体时间和地址将另行通知。如召开标前会，投标人应在标前会召开前一天内将问题以书面形式提交给集中采

购机构。在标前会上，招标方、最终用户和集中采购机构只答复与招标文件内容有关的问题,并有权对于任何与招标文件无关的问题不作解答。

三、投标文件

10.电子招投标系统的使用须知

10.1 投标单位应确保 CA 证书在本项目进行过程自始至终处于有效状态，中途不得对证书进行任何更换及更新，并严格按照网上招标系统的要求及步骤进行报名投标，任何由于投标单位自身 CA 证书及网上招标系统信息录入错误等导致的项目挂起均由投标单位承担相关责任。

10.2 投标单位须在投标截止前详细了解网上招标系统中与其相关的所有操作（包括投标文件的编制、上传、开标、解密等）若因投标单位自身原因导致无法正常进行投标活动的，其责任由投标单位自行承担。

10.3 投标文件的组成及相关要求(以下各项复印件须加盖单位公章)，顺序投标单位自定。

10.4 商务部分内容：

（1）投标函；

（2）法定代表人（负责人）证明书、法定代表人（负责人）授权委托书（投标时需另附一份并单独提交）；

（3）报价一览表（开标一览表）；

（4）报价分类表；

（5）资格条件响应表、符合性要求响应表；

（6）3 年内经营活动中没有重大违法记录的书面声明；

（7）近三年完成同类业绩一览表；

（8）中小企业声明函；

（9）财务状况及税收、社会保障资金缴纳情况声明函；

（10）残疾人福利性单位声明函；

（11）营业执照；质量管理和质量保证体系等方面的认证证书（如有，复印件加盖公章）投标单位企业情况介绍及相关资信证明材料（复印件加盖单位公章）；

（12）未被“信用中国”（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）列

入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单，提供信用截屏：“信用中国”网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）；

（13）投标人认为可以证明其能力、信誉和信用的其他商务资料。

10.5 技术部分内容：

(1) 针对本项目的总体要求理解；

(2) 针对本项目的具体实施方案；

(3) 针对本项目的规章制度与应急预案；

(4) 针对本项目的服务质量保障措施及人员培训计划；

(5) 投标人的组织构架、内部管理规章制度等；

(6) 拟投入本项目人员安排（人员配置一览表）及项目经理及主要管理人员一览表；

(7) 承担同类项目情况及业主好评证明（以提供的中标通知书或合同复印件等证明材料为准）；

(8) 针对本项目提供的其他技术性资料、资格资料以及需要说明的其他事项。

注：投标单位应将投标文件装订成册、编写目录，并填写“投标文件目录”。

11.电子投标文件制作注意事项

11.1 网上报名成功且领取了招标文件的潜在投标人应认真阅读招标文件的所有内容，按照招标文件的要求编制完整的投标文件。投标单位完成电子投标文件后应制作相应纸质投标文件正本 1 份，副本 4 份。

11.2 招标文件对投标文件格式有要求的应按格式逐项填写内容，不准有空项；无相应内容可填的项应填写“无”、 “没有相应指标”等明确的回答文字。投标文件中格式文件留有空项的，将被视为不完整响应的投标文件，其投标有可能被拒绝。

11.3 投标人必须保证投标文件所提供的全部资料真实可靠，并接受招标单位及集中采购机构对其中任何资料进一步审查的要求。

11.4 开标一览表为在开标仪式上唱标的内容，要求按格式统一填写，不得自行增减内容。

11.5 投标文件须对招标文件中的内容做出实质性和完整的响应，否则其投标将被拒绝。如果投标文件填报的内容资料不详，或没有提供招标文件中所要求的全部资料及数据，包括但不限于第 10 条（投标文件的组成及相关要求）规定的内容，将导致投标被拒绝。

12.纸质投标文件的编制及编目

12.1 投标人技术文件规格幅面（A4）应与正文一致，按照招标文件规定的顺序，统一编目编码装订。

12.2 投标人编制的技术文件应能够证明投标人提供的货物及服务是符合招标文件规定的合格的服务。技术文件应包括但不限于第 10 条（投标文件的组成及相关要求）中的技术方案。

12.3 投标人提交的以及投标人与招标单位就有关投标的所有电子文件及来往函电均应使用中文简化字。

投标人所提供的技术文件和资料，包括图纸中的说明，应使用中文简化字。所使用的计量单位，应使用国家法定计量单位。

13.投标报价

13.1 报价依据：本招标文件所要求的服务内容、服务期限、工作范围和要求。

13.2 投标人应当按照国家和上海市有关行业管理服务收费的相关规定，结合自身服务水平和承受能力进行报价，投标报价应是履行合同的最终价格，除《项目需求》中另有说明外，投标报价应当是投标人为提供本项目所要求的全部服务所生的一切成本，税费和利润，包括人工（含工资、社会统筹保险金、加班工资、工作餐、相关福利、关于人员聘用费）等一切费用。

13.3 投标人提供的服务应当满足合同约定的服务内容和质量等要求。投标人不得违反标准规范规定或合同约定，通过降低服务质量、减少服务内容等手段进行恶性竞争，扰乱正常市场秩序。

13.4 评审时，最低投标报价不作为中标的唯一保证。

13.5 除《项目需求》中说明并允许外，投标的每一种单项服务报价以及采购项目的投标总价均只允许有一个报价，投标文件中不允许有任何选择的报价，招标人对于其投标均将予以拒绝，视作无效投标。

13.6 投标报价应是固定不变的，不得以任何理由予以变更。任何可变的或者附有条件的投标报价，招标人均予以拒绝，视作无效投标。

13.7 投标人应按照招标文件中第七章提供的格式完整地填写各类报价分类明细表，说明其拟提供服务的内容、数量、价格、时间构成等。

13.8 投标应以人民币报价。

14.投标货币

投标文件的报价一律用人民币报价。

15.投标保证金

不收取。

16. 投标有效期

投标文件从开标日起有效期为 90 天（日历日）。如果投标文件有效期不足 90 天，将导致投标无效。特殊情况下，集中采购机构可于投标有效期满之前要求投标人同意延长有效期，要求与答复均应为书面形式。投标人可以拒绝上述要求而其投标保证金予以退还。对于同意该要求的投标人，既不要求也不允许其修改投标文件，但将要求其相应延长投标保证金的有效期。有关退还和不予退还投标保证金的规定在投标有效期的延长期内继续有效。

17.投标文件的制作及签署

17.1 按照《上海市电子政府采购暂行管理办法》规定执行。

17.2 投标文件书写应清楚工整，除投标人对错处作必要修改外，投标文件中不得有加行、涂抹或改写。若有修改须法定代表人（负责人）或其授权代表签名/印章。

四、投标文件的递交

18.电子文件的录入和上传

18.1 投标人在投标文件制作完成后须使用上海市电子签名认证证书（CA 证书）登录“云采交易平台投标客户端”，按照系统设置和招标文件要求填写基本信息并勾选本次参与投标的包件号。

18.2 填写完成后，导入线下编制的投标文件，并对各检查项、打分项进行标记匹配响应。匹配完成后，系统会对供应商的“基本信息”、“导入投标文件”和“标书匹配”等操作进行完整度检查。

18.3 待检查进度变为 100%后，点击“生成电子加密标书”输入 CA 密码生成电子加密标书，点击“上传电子加密标书”将加密标书上传至云采交易平台,供应商须自行对上传情况进行确认。

18.4 投标文件加密上传后，投标人须及时联系集中采购机构进行投标签收（投标截止时间之后，集中采购机构业务员将无法投标签收）。投标人应及时查看签收情况，并打印签收回执。未签收的投标文件视为投标未完成，投标失败。

19.投标截止时间

19.1 所有电子投标文件必须按招标文件规定的投标截止时间上传、解密。

19.2 网上投标截止时间前，投标人应充分考虑到网上投标可能发生的故障和风险。对发生的任何

故障和风险造成投标人投标内容不一致或利益受损或投标失败的，招标人、集中采购机构不承担任何责任。

19.3 出现本须知第 8 条的情形，因招标文件的修改而推迟投标截止日期时，投标人应按集中采购机构发布的修改通知中规定的时间递交。

20.迟交的投标文件

20.1 按照《上海市电子政府采购暂行管理办法》规定执行。

20.2 集中采购机构将拒绝接收在投标截止时间后上传的投标文件。

21. 投标文件的修改、撤回和撤销

21.1 按照《上海市电子政府采购暂行管理办法》规定执行。

21.2 投标人在提交投标文件后可对其投标文件进行修改或撤回，但必须在投标截止时间前对已完成上传投标的项目进行撤销或重新修改。（注：投标人可在政采云投标客户端大厅中的“进行中的项目”标签页下找到需要撤回的项目，点击“撤回”即可。如集中采购机构已签收投标文件，则投标人需先联系集中采购机构项目业务员撤销签收，再进行撤回修改。）

21.3 投标截止后，投标人不得修改投标文件。

21.4 投标人不得在开标时间起至投标文件有效期期满前撤销投标文件。

五、开标及评标

22.开标

22.1 集中采购机构将在招标文件中规定的日期、时间和地点组织开标。投标人的法定代表人（负责人）或其授权代表须携带纸质投标文件及设备（笔记本电脑、无线上网卡、电子签名认证证书、纸质投标文件）出席开标会议。投标人未参加现场开标的，视为认同开标结果。

22.2 投标人须在电子平台规定的时间登录上海政府采购网云采交易平台，并按电子平台操作流程完成签到、唱标、结果确认签章等开标流程。

22.3 投标截止时，网上上传的电子投标文件少于 3 家的，不得开标；招标人将重新招标。

22.4 投标人对开标有异议的，应当场提出，招标人应当场做出答复，并制作记录。

22.5 开标后，招标人或集中采购机构将拒绝投标人主动提交的任何澄清与补正。

22.6 所有在开标会上被接受的投标文件都将作为档案保存,不论中标与否，招标人或集中采购机构

均不退回投标文件。

23.资格审查

23.1 开标结束后，招标人或者集中采购机构依法对投标人的资格进行审查。

23.2 资格审查的内容，详见资格条件响应表。

23.3 资格审查小组须依据招标文件第五章评标办法与程序中规定的资格审查标准和方法，对投标人提供的资格证明文件逐一进行审查，并在资格审查表上详细记录审查情况；未通过资格审查的，还应注明未通过资格审查的原因或理由。

23.4 未通过资格审查的投标人的投标文件，不得进入符合性审查。

23.5 通过资格审查的合格投标人不足 3 家的，不得评标。招标人将重新组织招标或依法变更采购方式。

24.符合性审查

24.1 评标委员会由招标人或其委托的集中采购机构依法组建。

24.2 评标委员会将对通过资格审查的投标人的投标文件进行符合性审查，以确定其是否满足招标文件的实质性要求，具体详见招标文件第五章评标办法与程序中规定的符合性审查标准和方法。

24.3 通过符合性审查的实质性响应的投标文件，应该是与招标文件要求的全部条款、条件相符，没有重大偏离或保留的投标。所谓重大偏离或保留，是指投标文件通过的服务及相关货物的范围、质量和性能与招标文件的实质性要求不一致，限制了招标人的权利或减轻了投标人的义务。

24.4 评标委员会只根据投标文件的内容判定投标文件的响应性，而无义务寻求其他外部证据。如投标文件没有实质性响应招标文件要求的，评标委员会将判定其投标无效，投标人不得通过修正或撤销不符合要求的偏离或保留，而使其投标成为实质上响应的投标。

25.投标文件的澄清

25.1 投标文件中含义不明确、同类问题表述不一致或者有明显文字和计算错误的内容，评标委员会应当以书面形式要求投标人作出必要的澄清、说明或者补正。投标人的澄清、说明或者补正应当采用书面形式，并加盖公章，或者由法定代表人（负责人）或其授权代表签字。投标人的澄清、说明或者补正不得超出投标文件的范围或者改变投标文件的实质性内容。

25.2 投标文件未响应招标文件实质性要求和条件的，不得通过修正或撤销其不符合要求的差异或保留，使之成为具有响应性的投标。

25.3 投标人的澄清、说明和补正材料作为其投标文件的补充文件，和之前递交的投标文件共同构成投标文件的组成部分，对投标人具有约束力。

25.4 投标文件中如有其他错误（明显的文字和计算错误除外），对于错误的内容，除招标文件另有规定外，评标时将按照对投标人不利的情形进行评分；如该投标人中标，签订合同时按照对投标人不利、对招标人有利的原则签约。

25.5 财政部令第 87 号《政府采购货物和服务招标投标管理办法》第三十一条规定：使用综合评分法的采购项目，提供相同品牌产品且通过资格审查、符合性审查的不同投标人参加同一合同项下投标的，按一家投标人计算，评审后得分最高的同品牌投标人获得中标人推荐资格；评审得分相同的，由采购人或者采购人委托评标委员会按照招标文件规定的方式确定一个投标人获得中标人推荐资格，招标文件未规定的采取随机抽取方式确定，其他同品牌投标人不作为中标候选人。

非单一产品采购项目，采购人应当根据采购项目技术构成、产品价格比重等合理确定核心产品，并在招标文件中载明。多家投标人提供的核心产品品牌相同的，按前款规定处理。

26.商务技术评审

26.1 评标委员会应当按照招标文件中规定的评标方法和标准，对通过符合性审查的投标文件进行商务、技术评估，对投标文件进行比较和评价，并择优推荐中标候选人。

26.2 评标时除考虑投标价以外，还应考虑的各项因素详见第五章评标办法。

27.中标候选人的推荐

详见第五章评标办法及评分标准。

28.保密

28.1 在评标过程中及评标结束后，评标委员会的研究情况和所有投标人的商业秘密都属于保密内容。

28.2 有关投标文件的审查、澄清、评估和比较，以及有关授予合同的意向等一切情况，都不得透露给任一投标人或与上述评标工作无关的人员。

28.3 投标人不得干扰评标委员会的评标活动，否则其投标将被认定为无效。

六、定标

29.定标准则

29.1 集中采购机构应当在评标结束后 2 个工作日内将评标报告送交招标人。

29.2 招标人应当自收到评标报告之日起 5 个工作日内，在评标报告确定的中标候选人名单中按顺序确定中标人。中标候选人并列的，由招标人或者招标人委托评标委员会按照招标文件规定的方式确定中标人；招标文件未规定的，采取随机抽取的方式确定。

29.3 招标人在收到评标报告 5 个工作日内未按评标报告推荐的中标候选人顺序确定中标人，又不能说明合法理由的，视为按评标报告推荐的顺序确定排名第一的中标候选人为中标人。

29.4 如供应商对采购过程、中标结果提出质疑，质疑成立且影响或可能影响中标结果的，当合格供应商符合法定数量，可以从合格中标候选人中另行确定中标供应商的，应当依法另行确定中标供应商；否则，应当重新开展采购活动。

29.5 中标供应商拒绝签订合同的，招标人可以按照评审报告推荐的中标候选人名单排序，确定下一候选人为中标供应商，也可以重新开展政府采购活动。

30.终止招标活动

除因重大变故采购任务取消情况外，不得擅自终止招标活动。

31.中标通知

31.1 招标人或者集中采购机构应当自中标人确定之日起 2 个工作日内，在省级以上财政部门指定的媒介上公告中标结果。

31.2 在公告中标结果的同时，招标人或者集中采购机构应当向中标人发出中标通知书。中标通知书对招标人和中标供应商具有同等法律效力。

31.3 中标通知书发出后，招标人改变中标结果，或者中标供应商放弃中标，应当承担相应的法律责任。

32. 询问与质疑

32.1 投标人对招标活动事项有疑问的，可以向招标人提出询问。询问可以采取电话、电子邮件、当面或书面等形式。对投标人的询问，招标人将依法及时作出答复，但答复的内容不涉及商业秘密或者依法应当保密的内容。

32.2 投标人认为招标文件、招标过程或中标结果使自己的合法权益受到损害的，可以在知道或者应知其权益受到损害之日起七个工作日内，以书面形式向招标人提出质疑。其中，对招标文件的质疑，应当在其下载招标文件之日（以电子采购平台显示的报名时间为准）起七个工作日内提出；对招标过程的质疑，应当在各招标程序环节结束之日起七个工作日内提出；对中标结果的质疑，应当在中标公告期限届满之日起七个工作日内提出。

投标人应当在法定质疑期内一次性提出针对同一采购程序环节的质疑，超过次数的质疑将不予受理。以联合体形式参加政府采购活动的，其质疑应当由组成联合体的所有供应商共同提出。

32.3 投标人可以委托代理人进行质疑。代理人提出质疑应当提交投标人签署的授权委托书，并提供相应的身份证明。授权委托书应当载明代理人的姓名或者名称、代理事项、具体权限、期限和相关事项。投标人为自然人的，应当由本人签字；投标人为法人或者其他组织的，应当由法定代表人（负责人）签字或者盖章，并加盖公章。

32.4 投标人提出质疑应当提交质疑函和必要的证明材料。质疑函应当包括下列内容：

（1）供应商的姓名或者名称、地址、邮编、联系人及联系电话

（2）质疑项目的名称、编号

（3）具体、明确的质疑事项和与质疑事项相关的请求

（4）事实依据

（5）必要的法律依据

（6）提出质疑的日期

投标人为自然人的，应当由本人签字；投标人为法人或者其他组织的，应当由法定代表人（负责人），或者其授权代表签字或者盖章，并加盖公章。质疑函应当按照财政部制定的范本填写，范本格式可通过中国政府采购网（http://www.ccgp.gov.cn）右侧的“下载专区”下载。

32.5 投标人提起询问和质疑，应当按照《政府采购质疑和投诉办法》（财政部令第 94 号）的规定办理。质疑函或授权委托书的内容不符合《投标人须知》第 32.3 条和第 32.4 条规定的，招标人将当场一次性告知投标人需要补正的事项，投标人超过法定质疑期未按要求补正并新提交的，视为放弃质疑。

质疑函的递交应当采取当面递交形式，质疑联系：上海市普陀区政府采购中心，联系电话：021-52564588*8491。地址：上海市普陀区大渡河路 1668 号 5 号楼 A413 室。

32.6 招标人将在收到投标人的书面质疑后七个工作日内作出答复，并以书面形式通知提出质疑的投标人和其他有关投标人，但答复的内容不涉及商业秘密或者依法应当保密的内容。

32.7 对投标人询问或质疑的答复将导致招标文件变更或者影响招标活动继续进行的，招标人将通知提出询问或质疑的投标人，并在原招标公告发布媒体上发布变更公告。

33.签订合同

33.1 招标人应当自中标通知书发出之日起 30 日内，按照招标文件和中标人投标文件的规定，与中标人签订书面合同。所签订的合同不得对招标文件确定的事项和中标人投标文件作实质性修改。

33.2 招标人不得向中标人提出任何不合理的要求作为签订合同的附加条件。

33.3 政府采购合同履行中，招标人需追加与合同标的相同的货物、工程或者服务的，在不改变合同其他条款的前提下，可以与供应商协商签订补充合同，但所有补充合同的采购金额不得超过原合同采购金额的 10%。

34.履约保证金：无

七、其它

35.投标注意事项

投标人应自行办理云采交易平台所须的相关手续、证书或设备等，并自行完成系统操作的学习（详见上海政府采购网“操作须知”），投标人须自行承担因系统操作、网络设备情况导致的任何问题或风险，包括造成的利益损失、投标失败等，招标人及集中采购机构不承担任何责任。

第三章　政府采购政策功能

根据政府采购法，政府采购应当有助于实现国家的经济和社会发展政策目标，包括保护环境，扶持不发达地区和少数民族地区，促进中小企业发展等。

一、推行节能产品、环境标志产品政府采购政策

列入财政部、发展改革委发布的《节能产品政府采购品目清单》中强制采购类别的产品，按照规定实行强制采购；列入财政部、发展改革委、生态环境部发布的《节能产品政府采购品目清单》和《环境标志产品政府采购品目清单》中优先采购类别的产品，按规定实行优先采购。

二、促进中小企业发展政策

中小企业按照《政府采购促进中小企业发展管理办法》享受中小企业扶持政策，对预留份额项目专门面向中小企业采购，对非预留份额采购项目按照规定享受价格扣除优惠政策。中小企业应提供《中小企业声明函》，如为联合投标的，联合体各方需分别填写《中小企业声明函》。享受扶持政策获得政府采购合同的，小微企业不得将合同分包给大中型企业，中型企业不得将合同分包给大型企业。

三、促进监狱企业、残疾人福利性单位发展政策

在政府采购活动中，监狱企业和残疾人福利性单位视同小微企业，监狱企业应当提供由省级以上监狱管理局、戒毒管理局(含新疆生产建设兵团)出具的属于监狱企业的证明文件，残疾人福利性单位应当提供《残疾人福利性单位声明函》。

如果有国家或者上海市规定政府采购应当强制采购或优先采购的其他产品和服务，按照其规定实行强制采购或优先采购。

若供应商未按要求提供相关证明文件的，评标时不予认可。

第四章　招标需求

一、项目概况

1.1 项目名称：智联普陀光纤专网安全加固政务信息化购买服务项目（2026 年度）

1.2 预算金额（元）：476.62 万元

1.3 服务地址：采购人指定地址

二、服务目标

通过本项目购买服务，落实智联普陀光纤专网链路安全加固，提升网络通信链路信息系统的安全及区域边界安全传输能力，增加链路安全性及系统管理人员的安全意识，提升智联普陀光纤专网在信息系统安全管理、维护的层次，保证信息系统的安全稳定运行，满足智联普陀光纤专网核心网络等保三级要求。

在服务目标上，确立自身信息安全等级保护策略及安全管理基线，通过实现对安全访问的控制及操作行为的记录审计；建立起信息安全体系，提高智联普陀光纤专网链路信息系统整体安全防护的水平，预防安全事件发生，最大限度降低安全问题所带来的损失，降低信息安全管理成本。具体技术方面目标如下：

2.1 政策与标准合规性保障

信息系统安全保障体系的建设过程及其成果完全依据核心业务信息系统特点；确保建设完毕后符合建设要求。

2.2 构建适度安全保障体系

确保信息系统在存储、传输和使用过程中安全，确保核心业务系统持续、稳定地运行，确保重要业务操作行为可审计，抵御恶意攻击、恶意代码、病毒等对信息系统攻击与破坏，防止对信息系统资源的非法、非授权访问。

2.3 提升安全风险的控制和评价能力

提升链路安全加固能力，有效控制安全链路传输风险及区域边界风险，保障业务传输的安全性与连续性。

2.4 建立整体安全管理体系，丰富应急响应预案，形成安全管理的长效机制解决现网智联普陀光纤专网核心网络相关安全问题，同时满足三级等保要求。

三、服务内容

对智联普陀光纤专网通信网络及区域边界进行安全加固，主要包括以下三块服务内容：

3.1 智联普陀光纤专网核心网络区政府核心机房至各委办局上行边界光纤专网链路安全加固。

3.2 智联普陀光纤专网核心网络区政府核心机房至各街道汇聚机房光纤下行边界专网安全加固。

3.3 满足智联普陀光纤专网核心网络等保三级评测要求。

四、服务依据

4.1《公安部第三研究所评估报告》；

4.2《中华人民共和国网络安全法》；

4.3《关键信息基础设施安全保护条例》；

4.4 公安机关互联网安全监督检查规定（公安部令第 151 号）；

4.5《加快推进落实〈政务信息系统整合共享实施方案〉工作方案》（发改高技〔2017〕1529 号）。

五、具体需求

（一）服务内容要求

1.资产管理服务

区光纤专网核心接入区资产发现服务、入库资产管理服务、待入库资产管理服务、资产画像服务、资产主机资产画像服务、异常资产分析服务、环境要素识别服务

服务时间：现场服务：工作日 5×8 小时；远程服务：全年 7×24 小时监控。资产盘点每季度开展 1 次，日常资产变更实时更新。

交付成果和标准：交付成果：《资产清单》（每季度更新）。交付标准：资产清单应包含资产 IP 地址、MAC 地址、设备类型、所属区域、责任人等关键字段；报告格式符合采购人要求，内容基于实际数据编制，经采购人确认后归档。

2.漏洞脆弱性管理服务

区光纤专网核心接入区脆弱性配置服务、扫描任务管理服务、漏洞处置工单生成服务、漏洞利用热度展示服务

服务时间：现场服务：工作日 5×8 小时；远程服务：全年 7×24 小时监控。漏洞扫描每季度开展 1 次，高危漏洞应急响应按需启动

交付成果和标准：交付成果：《季度漏洞扫描报告》《漏洞处置工单台账》《高危漏洞应急处置报告》（按需）。交付标准：漏洞报告应包含漏洞名称、CVE 编号、风险等级、影响资产、漏洞描述、修复建议等内容；工单台账应记录漏洞发现时间、处置状态、责任人、闭环时间等信息。

3.安全威胁分析服务

区光纤专网核心接入区威胁事件研判服务、威胁事件研判配置服务、威胁攻击者画像服务、风险行为分析服务

服务时间：远程服务：全年 7×24 小时监控与分析；现场服务：工作日 5×8 小时，重大威胁事件按需到场。威胁分析报告每月出具 1 次。

交付成果和标准：交付成果：《月度安全威胁分析报告》《重大威胁事件专项分析报告》（按需）。交付标准：月度报告应包含本月威胁态势总览、重点威胁事件分析、攻击者画像、风险行为分析、趋势预测与防护建议等内容。

4.安全事件溯源分析服务

区光纤专网核心接入区溯源流量取证服务、溯源日志搜索服务、威胁狩猎服务

服务时间：远程服务：全年 7×24 小时响应；现场服务：工作日 5×8 小时，重大安全事件按需到场。溯源分析在事件发生后按需启动。

交付成果和标准：交付成果：《安全事件溯源分析报告》（按需）、《威胁狩猎报告》（按需）。交付标准：溯源报告应包含事件概述、攻击时间线、攻击路径还原、攻击手法分析、影响范围评估、处置建议与改进措施等内容。

5. 安全威胁监控服务

区光纤专网核心接入区攻击者监控服务、防护资产监控服务、攻击行为监控服务、自动化响应监控服务、监控配置服务、重点事件监控服务、目标 IP 跟踪服务

服务时间：远程服务：全年 7×24 小时实时监控；现场服务：工作日 5×8 小时。监控告警实时推送，重大告警立即通知。

交付成果和标准：交付成果：《月度安全威胁分析报告》《重大告警事件处置记录》（按需）。交付标准：月度报告应包含本月监控告警统计、告警级别分布、重点事件处置情况、监控策略优化建议等内容。

6. 安全态势感知服务

区光纤专网核心接入区综合态势可视化服务、环境感知服务、威胁态势呈现服务、运维响应态势展示服务、脆弱性态势感知服务、日志审计态势展现服务

服务时间：远程服务：全年 7×24 小时态势监测；现场服务：工作日 5×8 小时。态势分析报告每月出具 1 次。

交付成果和标准：交付成果：《月度安全态势分析报告》。交付标准：月度报告应包含本月安全态势总览、各维度态势分析、重点风险提示、态势趋势预测与改进建议等内容。

7. 安全威胁规则库运营服务

区光纤专网核心接入区预判规则服务、攻击识别规则配置服务、攻击识别实例配置服务、攻击识别规则管理服务、攻击识别规则调试服务、攻击识别防护策略配置服务、攻击识别全局配置服务、攻击识别简易模式自定义规则服务、攻击识别策略配置服务、规则升级服务

服务时间：远程服务：全年 7×24 小时规则运行监控；现场服务：工作日 5×8 小时。规则库更新按需推送，每月至少更新 1 次。

交付成果和标准：交付成果：《规则库运营台账》《规则升级台账》。交付标准：台账应记录规则变更时间、变更内容、变更原因、效果评估等信息。

8. 漏洞库运营服务

区光纤专网核心接入区漏洞模板管理服务、漏洞分类服务、配置模板管理服务、密码字典管理服务、漏洞库升级服务

服务时间：远程服务：全年 7×24 小时漏洞库运行监控；现场服务：工作日 5×8 小时。漏洞库更新按需推送，每月至少更新 1 次。

交付成果和标准：交付成果：《规则升级台账》

9. 流量采集服务

区光纤专网核心接入区及街道接入区 IPV4/IPV6 流量解析服务、 VXLAN 、MPLS 、GRE 、VLAN 流量解析服务、常见协议的深度解析服务、工控协议的深度解析服务、物联网协议的深度解析服务、数据库协议的解析服务、应用识别服务；

服务时间：远程服务：全年 7×24 小时不间断流量采集；现场服务：工作日 5×8 小时。采集策略优化每月开展 1 次。

交付成果和标准：交付成果：《月度流量采集分析报告》《流量采集策略配置文档》。交付标准：月度报告应包含本月流量总量、协议分布、应用分布、流量趋势、采集完整性评估等内容。

10. 流量还原服务

区光纤专网核心接入区及街道接入区常规协议元数据还原服务、流量中出现的文件进行发现和还原服务

服务时间：远程服务：全年 7×24 小时；现场服务：工作日 5×8 小时。还原任务按需执行。

交付成果和标准：交付成果：《流量还原分析报告》（按需）、《还原文件清单》（按需）。交付标准：报告应包含还原任务概述、还原文件统计、可疑文件分析、安全建议等内容。

11. 流量威胁检测服务

区光纤专网核心接入区及街道接入区 webshell 检测服务、加密代理识别服务、webshell 加密通信识别服务、钓鱼邮件检测服务、隐蔽隧道检测服务、dga 域名检测服务。

服务时间：远程服务：全年 7×24 小时实时检测；现场服务：工作日 5×8 小时。检测规则优化每月开展 1 次。

交付成果和标准：交付成果：《月度流量威胁检测分析报告》。交付标准：月度报告应包含本月检测到的威胁类型统计、重点威胁事件分析、威胁趋势、检测规则优化建议等内容。

12. 流量风险行为分析服务

区光纤专网核心接入区及街道接入区暴力破解行为检测服务、弱口令行为检测服务、侦查探测行为检测服务、翻墙行为检测服务、主机外联行为检测服务、违规网站行为检测服务、异地登录行为检测服务。

服务时间：远程服务：全年 7×24 小时行为监测；现场服务：工作日 5×8 小时。行为分析报告每月出具 1 次。

交付成果和标准：交付成果：《月度流量风险行为分析报告》。交付标准：月度报告应包含本月风险行为类型统计、重点风险事件分析、行为基线变化、白名单管理情况、改进建议等内容。

13. 流量留存服务

区光纤专网核心接入区及街道接入区元数据存储服务、原始 pcap 包存储服务、威胁包存储服务、恶意文件存储服务

服务时间：远程服务：全年 7×24 小时不间断留存；现场服务：工作日 5×8 小时。留存策略每季度评估 1 次。

交付成果和标准：交付成果：《季度流量留存策略评估报告》。交付标准：报告应包含当前留存策略、存储使用率、留存数据完整性评估、存储扩容建议等内容。

14. 流量检索服务

区光纤专网核心接入区及街道接入区流量日志查询服务、流量全局检索服务

服务时间：远程服务：全年 7×24 小时检索服务可用；现场服务：工作日 5×8 小时。检索任务按需执行。

交付成果和标准：交付成果：《流量检索结果报告》（按需）。交付标准：报告应包含检索条件、检索时间范围、命中结果统计、重点结果分析等内容。

15. 设备日志接入服务

区光纤专网核心接入区设备海量日志数据采集服务、保存原始日志数据服务、异构日志格式进行统一化处理服务、保存统一化处理后的日志数据服务、界面配置未识别日志接入服务

服务时间：远程服务：全年 7×24 小时日志采集；现场服务：工作日 5×8 小时。新设备日志接入按需配置。

交付成果和标准：交付成果：《设备接入清单》、《月度日志接入情况报告》。交付标准：应包含已接入设备清单、日志类型、采集方式、等内容；月度报告应包含日志接入总量、设备覆盖率、日志格式处理情况、未接入设备清单及建议等内容。

16. 设备日志备份恢复服务

区光纤专网核心接入区设备手动或自动备份日志服务、设置日志存储备份策略服务、备份日志导入查询服务日志备份至远程服务器服务

服务时间：远程服务：全年 7×24 小时备份任务运行；现场服务：工作日 5×8 小时。备份策略每季度评估 1 次。

交付成果和标准：交付成果：《日志备份策略文档》《季度备份恢复测试报告》（按需）、《备份任务执行台账》。交付标准：测试报告应包含备份任务执行成功率、恢复测试结果、存储使用率、策略优化建议等内容。

17. 设备日志检索服务

区光纤专网核心接入区设备实时日志查询服务、历史日志查询服务、原始日志范式化日志查询服务、自定义查询规则服务、全文检索模糊检索正则检索日志服务

服务时间：远程服务：全年 7×24 小时检索服务可用；现场服务：工作日 5×8 小时。检索任务按需执行。

交付成果和标准：交付成果：《日志检索结果报告》（按需）。交付标准：报告应包含检索条件、检索范围、命中结果统计、重点日志分析等内容。

18. 设备日志表分析服务

区光纤专网核心接入区多种维度统计日志信息服务、统计分析报表与多种文件格式导出服务

服务时间：远程服务：全年 7×24 小时；现场服务：工作日 5×8 小时。分析报表每月出具 1 次。

交付成果和标准：交付成果:《月度日志分析报告》。交付标准：月度报表应包含日志总量统计、设备日志分布、事件类型分布、严重级别分布、趋势分析、异常事件提示等内容。

19. 设备日志事件告警服务

区光纤专网核心接入区多源事件关联分析服务、查询实时事件服务、告警抑制服务

服务时间：远程服务：全年 7×24 小时实时告警；现场服务：工作日 5×8 小时。告警规则优化每月开展 1 次。

交付成果和标准：交付成果:《月度日志告警分析报告》。交付标准：月度报告应包含本月告警总量、告警级别分布、告警类型分布、误报率、重点告警事件处置情况、规则优化建议等内容。

20. 设备主机漏洞扫描服务

区光纤专网核心接入区设备主机操作系统、数据库、中间件等进行漏洞扫描服务

服务时间：现场服务：工作日 5×8 小时；远程服务：全年 7×24 小时监控。漏洞扫描每季度开展 1 次，在采购人指定维护窗口内执行。

交付成果和标准：交付成果:《季度漏洞扫描报告》。交付标准：报告应包含扫描范围、扫描时间、漏洞统计（按风险等级、按资产、按类型）、漏洞详情（漏洞名称、CVE 编号、风险等级、影响资产、漏洞描述、修复建议）、整体安全评估与改进建议等内容。

21. 设备弱口令漏洞扫描服务

区光纤专网核心接入区设备系统进行弱口令扫描服务

服务时间：现场服务：工作日 5×8 小时；远程服务：全年 7×24 小时监控。漏洞扫描每季度开展 1 次，在采购人指定维护窗口内执行。

交付成果和标准：交付成果:《季度漏洞扫描报告》。交付标准：报告应包含扫描范围、扫描时间、漏洞统计（按风险等级、按资产、按类型）、漏洞详情（漏洞名称、CVE 编号、风险等级、影响资产、漏洞描述、修复建议）、整体安全评估与改进建议等内容。

22. 设备漏洞扫描任务管理服务

区光纤专网核心接入区设备已下发任务的列表展示，任务暂停、断点续扫等管理服务、任务参数展示，任务综述信息汇总分析展示，主机信息列表展示服务

服务时间：现场服务：工作日 5×8 小时；远程服务：全年 7×24 小时任务监控。任务管理贯穿服务全过程。

交付成果和标准：交付成果:《漏洞扫描任务执行台账》。交付标准：台账应记录任务名称、创建时间、计划执行时间、实际执行时间、执行状态、扫描目标数、发现漏洞数等信息。

23. 设备漏洞报表分析服务

区光纤专网核心接入区设备漏洞报表报表任务下发服务、报表类型选择服务、报表内容设置服务、对比分析服务、任务信息对比服务、漏洞对比服务，脆弱性账号对比服务

服务时间：现场服务：工作日 5×8 小时；远程服务：全年 7×24 小时。报表分析每月开展 1 次，对比分析每季度开展 1 次。

交付成果和标准：交付成果：《季度漏洞分析报表》《季度漏洞对比分析报告》。交付标准：月度报表应包含漏洞统计、漏洞分布、重点漏洞提示、修复进度跟踪等内容；季度对比报告应包含漏洞趋势、修复效果评估、安全状况变化分析等内容。

24. 设备漏洞验证服务

区光纤专网核心接入区设备对漏洞对取证性质的验证服务、支持漏洞库中标记可验证漏洞服务、漏洞验证漏洞利用原始结果服务

服务时间：现场服务：工作日 5×8 小时；远程服务：全年 7×24 小时。漏洞验证按需执行，在采购人指定维护窗口内进行。

交付成果和标准：交付成果：《漏洞验证报告》（按需）。交付标准：报告应包含验证目标、验证时间、验证漏洞清单、验证方法、验证结果（可利用/不可利用/无法验证）、验证证据、风险评估与处置建议等内容。

25. 设备漏洞资产管理服务

区光纤专网核心接入区设备资产树对象的资产风险统计分析服务，展示整体资产范围的风险等级、风险评分服务

服务时间：现场服务：工作日 5×8 小时；远程服务：全年 7×24 小时。资产风险统计每月更新 1 次。

交付成果和标准：交付成果：《资产风险统计报告》（季度）、《高风险资产清单》（季度更新）。交付标准：报告应包含资产风险等级分布、风险评分排名、高风险资产详情、风险变化趋势、处置优先级建议等内容。

26. 设备运维权限托管服务

区光纤专网核心接入区高价值设备登录运维和高危命令操作指定级金库授权服务、运维工单管理服务

服务时间：现场服务：工作日 5×8 小时；远程服务：全年 7×24 小时权限管理平台运行。权限审批在工作时段内处理。

交付成果和标准：交付成果：《月度运维权限审计分析报告》。交付标准：月度报告应包含本月运维数量、类型分布、高危操作统计、违规操作提示等内容。

27. 设备字符运维审计服务

区光纤专网核心接入区设备 Telnet、SSH、Rlogin 等字符运维管理协议服务、密钥和密码方式 SSH 运维登录目标设备服务、对监控到的非法操作实时手工切断服务

服务时间：远程服务：全年 7×24 小时审计监控；现场服务：工作日 5×8 小时。审计记录实时生成，每月开展 1 次。

交付成果和标准：交付成果：《月度审计分析报告》。交付标准：月度报告应包含本月字符运维会话数量、操作时长统计、高危命令统计、违规操作提示、审计完整性评估等内容。

28. 设备文件运维审计服务

区光纤专网核心接入区设备 FTP、SFTP、Samba、SCP 等文件运维协议运维管理服务、web 文件插件方式运维目标服务器服务、 WEB 界面直接调用 WinSCP 、xsftp 等三方工具运维目标设备服务

服务时间：远程服务：全年 7×24 小时审计监控；现场服务：工作日 5×8 小时。审计分析，每月开展 1 次。

交付成果和标准：交付成果：《月度审计分析报告》。交付标准：月度报告应包含本月文件运维会话数量、文件传输量统计、操作类型分布、违规操作提示、审计完整性评估等内容。

29. 设备图形运维审计服务

区光纤专网核心接入区设备 RDP 、VNC 、X11 等图形运维协议运维管理服务、web 图形插件方式运维目标服务器服务、RDP、 VNC 客户端软件直接登录堡垒机 MSTSC、Vnc Viewer 等客户端服务

服务时间：远程服务：全年 7×24 小时审计监控；现场服务：工作日 5×8 小时。审计分析每月开展 1 次。

交付成果和标准：交付成果：《月度审计分析报告》。交付标准：月度报告应包含本月图形运维会话数量、会话时长统计、操作类型分布、违规操作提示、录像存储使用率、审计完整性评估等内容。

30. 设备数据库运维审计服务

区光纤专网核心接入区设备 Oracle、MS SQL Server、IBM DB2、 Sybase、IBM Informix Dynamic Server、MySQL 等数据库类型运维管理服务、数据库图形方式操作审计与字符方式（数据库操作命令级）操作审计服务、数据库操作命令审计定位数据库图形审计服务

服务时间：远程服务：全年 7×24 小时审计监控；现场服务：工作日 5×8 小时。审计分析每月开展 1 次。

交付成果和标准：交付成果：《月度审计分析报告》。交付标准：月度报告应包含本月数据库运维会话数量、SQL 操作统计、高危操作（如 DROP、DELETE、UPDATE 无 WHERE 等）统计、违规操作提示、审计完整性评估等内容。

31. 入侵检测防护服务

区光纤专网核心接入区入侵规则分类防护服务，制定分类防护策略。包含勒索、挖矿、 SQL 注入、XSS 注入、webshell、命令代码执行、内存破坏、类型混淆、反序列化、信息泄露、目录遍历、文件操作漏洞、注入攻击、重定向漏洞、 CSRF、僵木蠕、拒绝服务、弱口令、欺骗劫持、扫描类攻击等防护服务、SQL 注入、XSS 注入、webshell 等多种常见的应用层安全威胁抵御服务

服务时间：远程服务：全年 7×24 小时实时检测与防护；现场服务：工作日 5×8 小时。防护策略优化每月开展 1 次。

交付成果和标准：交付成果：《月度入侵检测防护分析报告》《防护策略配置台账》《入侵事件处置记录》（按需）。交付标准：月度报告应包含本月检测到的攻击类型统计、攻击源分析、重点攻击事件处置、防护策略命中情况、策略优化建议等内容。

32. DDOS 攻击检测防护服务

区光纤专网核心接入区 DoS/DDoS 攻击防护服务，支持 PING/UDP/SYN/ACK/DNS Reply/DNS Req Flood，支持 TCP Port Scan/UDP Port Scan, 支持 PING Sweep，支持 ARP Spoof 以及 HTTP GET/HTTP POST FLood 等常见的 DoS/DDoS 的攻击抵御服务

服务时间：远程服务：全年 7×24 小时实时检测与防护；现场服务：工作日 5×8 小时。防护策略每季度评估 1 次。

交付成果和标准：交付成果：《月度入侵检测防护分析报告》《DDoS 防护策略配置文档》《重大 DDoS 攻击事件处置报告》（按需）。交付标准：月度报告应包含本月检测到的 DDoS 攻击次数、攻击类型、攻击流量峰值、攻击源、防护效果、策略优化建议等内容。

33. 服务器外联防护服务

区光纤专网核心接入区服务器外联异常告警功能，可以手动添加或自学习服务器外联行为，并以此为基线检测服务器非法外联行为并告警服务

服务时间：远程服务：全年 7×24 小时监控；现场服务：工作日 5×8 小时。外联基线每季度更新 1 次。

交付成果和标准：交付成果：《月度入侵检测防护分析报告》。交付标准：月度报告应包含本月外联告警统计、异常外联事件分析、外联基线变化、白名单管理情况、改进建议等内容。

34. 应用管理服务

区光纤专网核心接入区主流的应用程序识别服务，识别不少于 6000 个应用、多种抗逃避或欺骗检测技术识别服务，能检测出的躲避行为包括但不限于：IP 数据包乱序分片、TCP 报文乱序分段、RPC 分片分段、SMB 分片分段、FTP 无效命令混淆、HTTP 响应消息异常、 HTML 文件内容多种字符编码混淆、数据流分隔、 协议端口重定位、URL 混淆、shell 代码变形等。

服务时间：远程服务：全年 7×24 小时应用识别与监控；现场服务：工作日 5×8 小时。应用

识别库更新按需推送。

交付成果和标准：交付成果：《月度入侵检测防护分析报告》。交付标准：月度报告应包含本月应用流量分布、Top 应用排行、异常应用行为、应用识别率、策略优化建议等内容。

35. 数据泄露防护

敏感数据保护服务，能够识别、阻断、告警超过阈值的敏感数据信息，其中敏感数据包括身份证号、银行卡、电话号码等，且支持自定义敏感数据、关键文件保护服务，能够识别、阻断通过自身的关键文件，以防止非法外传行为。

服务时间：远程服务：全年 7×24 小时监控；现场服务：工作日 5×8 小时。敏感数据规则每季度评估 1 次。

交付成果和标准：交付成果：《月度入侵检测防护分析报告》。交付标准：月度报告应包含本月敏感数据传输统计、告警事件分析、阻断事件统计、规则优化建议等内容。

36. 安全策略管理服务

区光纤专网核心接入区一体化入侵防护策略管理服务、超过 1000 条访问控制策略服务，可基于 IP 地址、端口（单个、多个和范围）、协议、动作（阻断、允许） 进行访问策略配置，并可支持是否生成访问控制策略的会话日志生成；

服务时间：现场服务：工作日 5×8 小时；远程服务：全年 7×24 小时策略运行监控。策略变更按需执行，策略审计每季度开展 1 次。

交付成果和标准：交付成果：《安全策略台账》、《策略变更记录》、。交付标准：台账应包含策略编号、策略名称、源/目的地址、端口、协议、动作、启用状态、创建时间、变更记录等信息。

37. 流量管理服务

区光纤专网核心接入区带宽管理服务，可以根据用户、应用、时间及带宽等因素，实现基于应用、面向对象的流量保护策略；全面的流量分析服务，可察看流量完整性分布情况

服务时间：远程服务：全年 7×24 小时流量监控；现场服务：工作日 5×8 小时。流量管理策略每季度评估 1 次。

交付成果和标准：交付成果：《月度流量管理分析报告》、《流量管理策略配置台账》。交付标准：月度报告应包含本月流量总量、应用流量分布、带宽使用率、流量管理策略命中情况、异常流量提示、策略优化建议等内容。

38. 入侵检测防护服务

区光纤专网街道接入区入侵规则分类防护服务，制定分类防护策略。包含勒索、挖矿、 SQL 注入、XSS 注入、webshell、命令代码执行、内存破坏、类型混淆、反序列化、信息泄露、目录遍历、文件操作漏洞、注入攻击、重定向漏洞、 CSRF、僵木蠕、拒绝服务、弱口令、欺骗劫持、扫描类攻击等防护服务、SQL 注入、XSS 注入、webshell 等多种常见的应用层安全威胁抵御服务

服务时间：远程服务：全年 7×24 小时实时检测与防护；现场服务：工作日 5×8 小时。防护策略优化每月开展 1 次。

交付成果和标准：交付成果：《月度入侵检测防护分析报告》、《防护策略配置台账》、《入侵事件处置记录》（按需）。交付标准：月度报告应包含本月检测到的攻击类型统计、攻击源分析、重点攻击事件处置、防护策略命中情况、策略优化建议等内容。

39. DDOS 攻击检测防护服务

区光纤专网街道接入区 DoS/DDoS 攻击防护服务，支持 PING/UDP/SYN/ACK/DNS Reply/DNS Req Flood，支持 TCP Port Scan/UDP Port Scan, 支持 PING Sweep，支持 ARP Spoof 以及 HTTP GET/HTTP POST FLood 等常见的 DoS/DDoS 的攻击抵御服务

服务时间：远程服务：全年 7×24 小时实时检测与防护；现场服务：工作日 5×8 小时。防护策略每季度评估 1 次。

交付成果和标准：交付成果：《月度入侵检测防护分析报告》、《DDoS 防护策略配置文档》、《重大 DDoS 攻击事件处置报告》（按需）。交付标准：月度报告应包含本月检测到的 DDoS 攻击次数、攻击类型、攻击流量峰值、攻击源、防护效果、策略优化建议等内容。

40. 服务器外联防护服务

区光纤专网街道接入区服务器外联异常告警功能，可以手动添加或自学习服务器外联行为，并以此为基线检测服务器非法外联行为并告警服务

服务时间：远程服务：全年 7×24 小时监控；现场服务：工作日 5×8 小时。外联基线每季度更新 1 次。

交付成果和标准：交付成果：《月度入侵检测防护分析报告》。交付标准：月度报告应包含本月外联告警统计、异常外联事件分析、外联基线变化、白名单管理情况、改进建议等内容。

41. 应用管理服务

区光纤专网街道接入区主流的应用程序识别服务，识别不少于 6000 个应用、多种抗逃避或欺骗检测技术识别服务，能检测出的躲避行为包括但不限于：IP 数据包乱序分片、TCP 报文乱序分段、RPC 分片分段、SMB 分片分段、FTP 无效命令混淆、HTTP 响应消息异常、 HTML 文件内容多种字符编码混淆、数据流分隔、 协议端口重定位、URL 混淆、shell 代码变形等。

服务时间：远程服务：全年 7×24 小时应用识别与监控；现场服务：工作日 5×8 小时。应用识别库更新按需推送。

交付成果和标准：交付成果：《月度入侵检测防护分析报告》。交付标准：月度报告应包含本月应用流量分布、Top 应用排行、异常应用行为、应用识别率、策略优化建议等内容。

42. 数据泄露防护

区光纤专网街道接入区敏感数据保护服务，能够识别、阻断、告警超过阈值的敏感数据信息，

其中敏感数据包括身份证号、银行卡、电话号码等，且支持自定义敏感数据、关键文件保护服务，能够识别、阻断通过自身的关键文件，以防止非法外传行为。

服务时间：远程服务：全年 7×24 小时监控；现场服务：工作日 5×8 小时。敏感数据规则每季度评估 1 次。

交付成果和标准：交付成果：《月度入侵检测防护分析报告》。交付标准：月度报告应包含本月敏感数据传输统计、告警事件分析、阻断事件统计、规则优化建议等内容。

43. 安全策略管理服务

区光纤专网街道接入区一体化入侵防护策略管理服务、超过 1000 条访问控制策略服务，可基于 IP 地址、端口（单个、多个和范围）、协议、动作（阻断、允许） 进行访问策略配置，并可支持是否生成访问控制策略的会话日志生成。

服务时间：现场服务：工作日 5×8 小时；远程服务：全年 7×24 小时策略运行监控。策略变更按需执行，策略审计每季度开展 1 次。

交付成果和标准：交付成果：《安全策略台账》《策略变更记录》、交付标准：台账应包含策略编号、策略名称、源/目的地址、端口、协议、动作、启用状态、创建时间、变更记录等信息。

44. 流量管理服务

区光纤专网街道接入区带宽管理服务，可以根据用户、应用、时间及带宽等因素，实现基于应用、面向对象的流量保护策略；全面的流量分析服务，可查看流量完整性分布情况

服务时间：远程服务：全年 7×24 小时流量监控；现场服务：工作日 5×8 小时。流量管理策略每季度评估 1 次。

交付成果和标准：交付成果：《月度流量管理分析报告》《流量管理策略配置台账》。交付标准：月度报告应包含本月流量总量、应用流量分布、带宽使用率、流量管理策略命中情况、异常流量提示、策略优化建议等内容。

45. 访问控制服务

区光纤专网核心接入区二层协议进行访问控制服务，针对 PPP、 QinQ、MPLS 等协议进行屏蔽，对非 IP 协议进行访问控制服务、基于源安全区、目的安全区、源地址、目的地址、源端口、目的端口、协议等，模拟运行直接获得策略的命中信息，并可对命中的策略信息进行编辑服务

服务时间：现场服务：工作日 5×8 小时；远程服务：全年 7×24 小时策略运行监控。策略变更按需执行，策略审计每季度开展 1 次。

交付成果和标准：交付成果：《访问控制策略台账》《策略变更记录》。交付标准：台账应包含策略编号、源/目的安全区、源/目的地址、端口、协议、动作、启用状态等信息。

46. 应用识别服务

区光纤专网核心接入区应用特征识别库服务，对应用进行识别和控制，应用属性不少于类别、

风险等级、标签、详细信息、实现技术等的服务

服务时间：远程服务：全年 7×24 小时应用识别；现场服务：工作日 5×8 小时。应用特征库更新按需推送。

交付成果和标准：交付成果:《安全分析报告》《应用控制策略台账》。交付标准：月度报告应包含本月应用识别覆盖率、应用类别分布、高风险应用提示、识别库更新情况、策略优化建议等内容。

47. URL 过滤服务

区光纤专网核心接入区提供云端 URL 分类库，提供 64+种精细分类（广告及弹出窗口、烟酒、匿名网站、艺术、聊天、盗用网站、犯罪活动等）

服务时间：远程服务：全年 7×24 小时 URL 过滤；现场服务：工作日 5×8 小时。URL 分类库更新按需推送。

交付成果和标准：交付成果:《安全分析报告》。交付标准：月度报告应包含本月 URL 访问统计、分类分布、阻断/告警统计、误报情况、白名单管理、策略优化建议等内容。

48. DNS 过滤服务

区光纤专网核心接入区针对 DNS 的 URL 过滤和分类识别服务

服务时间：远程服务：全年 7×24 小时 DNS 过滤；现场服务：工作日 5×8 小时。DNS 过滤规则每季度评估 1 次。

交付成果和标准：交付成果:《安全分析报告》。交付标准：月度报告应包含本月 DNS 请求统计、过滤分类分布、阻断/告警统计、异常 DNS 请求提示、策略优化建议等内容。

49. 内容过滤服务

区光纤专网核心接入区网页浏览、论坛发帖、电子邮件、即时通讯、文件传输、服务器操作等信息关键字的实时检测和过滤服务

服务时间：远程服务：全年 7×24 小时内容过滤；现场服务：工作日 5×8 小时。过滤关键字每季度评估 1 次。

交付成果和标准：交付成果:《安全分析报告》。交付标准：月度报告应包含本月内容过滤事件统计、过滤类型分布、关键字命中情况、误报分析、策略优化建议等内容。

50. 敏感数据发现服务

区光纤专网核心接入区敏感信息过滤服务，对用户的个人隐私信息（手机号、身份证号码、社保号等）泄露进行检测或阻断服务

服务时间：现场服务：工作日 5×8 小时；远程服务：全年 7×24 小时监控。敏感数据扫描每季度开展 1 次。

交付成果和标准：交付成果:《安全分析报告》。交付标准：报告应包含、敏感数据类型统计、

敏感数据分布、风险等级、整改建议等内容。

51. 访问控制服务

区光纤专网街道接入区二层协议进行访问控制服务，针对 PPP、 QinQ、MPLS 等协议进行屏蔽，对非 IP 协议进行访问控制服务、基于源安全区、目的安全区、源地址、目的地址、源端口、目的端口、协议等，模拟运行直接获得策略的命中信息，并可对命中的策略信息进行编辑服务

服务时间：现场服务：工作日 5×8 小时；远程服务：全年 7×24 小时策略运行监控。策略变更按需执行，策略审计每季度开展 1 次。

交付成果和标准：交付成果:《访问控制策略台账》《策略变更记录》。交付标准：台账应包含策略编号、源/目的安全区、源/目的地址、端口、协议、动作、启用状态等信息。

52. 应用识别服务

区光纤专网街道接入区应用特征识别库服务，对应用进行识别和控制，应用属性不少于类别、风险等级、标签、详细信息、实现技术等的服务

服务时间：远程服务：全年 7×24 小时应用识别；现场服务：工作日 5×8 小时。应用特征库更新按需推送。

交付成果和标准：交付成果:《安全分析报告》《应用控制策略台账》。交付标准：月度报告应包含本月应用识别覆盖率、应用类别分布、高风险应用提示、识别库更新情况、策略优化建议等内容。

53. URL 过滤服务

区光纤专网街道接入区提供云端 URL 分类库，提供 64+种精细分类（广告及弹出窗口、烟酒、匿名网站、艺术、聊天、盗用网站、犯罪活动等）

服务时间：远程服务：全年 7×24 小时 URL 过滤；现场服务：工作日 5×8 小时。URL 分类库更新按需推送。

交付成果和标准：交付成果:《安全分析报告》。交付标准：月度报告应包含本月 URL 访问统计、分类分布、阻断/告警统计、误报情况、白名单管理、策略优化建议等内容。

54. DNS 过滤服务

区光纤专网街道接入区针对 DNS 的 URL 过滤和分类识别服务

服务时间：远程服务：全年 7×24 小时 DNS 过滤；现场服务：工作日 5×8 小时。DNS 过滤规则每季度评估 1 次。

交付成果和标准：交付成果:《安全分析报告》。交付标准：月度报告应包含本月 DNS 请求统计、过滤分类分布、阻断/告警统计、异常 DNS 请求提示、策略优化建议等内容。

55. 内容过滤服务

区光纤专网街道接入区网页浏览、论坛发帖、电子邮件、即时通讯、文件传输、服务器操作等

信息关键字的实时检测和过滤服务

服务时间：远程服务：全年 7×24 小时内容过滤；现场服务：工作日 5×8 小时。过滤关键字每季度评估 1 次。

交付成果和标准：交付成果：《安全分析报告》。交付标准：月度报告应包含本月内容过滤事件统计、过滤类型分布、关键字命中情况、误报分析、策略优化建议等内容。

56. 敏感数据发现服务

区光纤专网街道接入区敏感信息过滤服务，对用户的个人隐私信息（手机号、身份证号码、社保号等）泄露进行检测或阻断服务

服务时间：现场服务：工作日 5×8 小时；远程服务：全年 7×24 小时监控。敏感数据扫描每季度开展 1 次。

交付成果和标准：交付成果：《安全分析报告》。交付标准：报告应包含、敏感数据类型统计、敏感数据分布、风险等级、整改建议等内容。

57. 边界控制管理服务

区光纤专网核心接入区从 802.1x 、 PBR（Policy – Based - Routing）、MVG 的各种边界控制服务、利用各种网络控制技术，实现在各种网络环境下适应性， IAC 能够帮助用户快速实现对于内网边界的规划。可以实现基于接入层边界的控制和基于重要资源边界的控制服务；

服务时间：现场服务：工作日 5×8 小时；远程服务：全年 7×24 小时边界监控。策略每季度评估 1 次。

交付成果和标准：交付成果：《接入设备清单》。交付标准：报告应包含边界控制覆盖范围、接入设备合规率、异常接入事件、策略优化建议等内容。

58. 人员认证管理服务

区光纤专网核心接入区本地用户名/密码、Email、Radius、LDAP、 AD 域、短信、生物指纹管理服务

服务时间：现场服务：工作日 5×8 小时；远程服务：全年 7×24 小时认证服务运行

交付成果和标准：交付成果：《接入设备清单》。交付标准：报告应包含各认证方式使用情况、认证成功率、异常认证事件、系统优化建议等内容。

59. 设备规范管理服务

区光纤专网核心接入区 IE 控件检查、IE 主页检查、IP/MAC 绑定检查、Windows 防火墙检测、操作系统版本检查、磁盘使用检查、计算机名称检查、垃圾文件检查、杀毒软件检查、网络监听端口检查、网络连接检查、系统补丁检查、系统时间检查、域用户检查、远程桌面检查、 P2P 软件检查、必须安装软件检查、必须运行进程检查、禁止安装软件检查、禁止运行进程检查、客户端运行状态检查、系统服务检查、软件授权检查、Guest 来宾账户检查、WSUS 更新配置检查、密码策

略设置检查、屏幕保护设置检查、弱口令账户检查、网卡绑定检查、系统共享资源检查服务

服务时间：现场服务：工作日 5×8 小时；远程服务：全年 7×24 小时终端合规监控。

交付成果和标准：交付成果:《不合规设备清单》。交付标准：应包含重点不合规设备、整改进度跟踪、改进建议等内容。

60. 操作行为管理服务

区光纤专网核心接入区用户各种操作的监控和响应服务：ip 更改、违规软件使用、必须安装软件随意卸载、安全检查违规；计算机设备的统一维护管理服务：类别管理、设备信息管理、软件分发、服务管理、终端探测；任务管控服务：终端软件安装包分发、终端批处理脚本分发、终端消息通知分发服务

服务时间：远程服务：全年 7×24 小时行为监控；现场服务：工作日 5×8 小时。

交付成果和标准：交付成果:《月度操作行为管理报告》。交付标准：月度报告应包含本月操作行为统计、违规事件分析、软件分发执行情况、终端在线率、管理优化建议等内容。

61. 视角报表管理服务

区光纤专网核心接入区资源报表、违规操作记录、检查结果报表、入网安全检查评估报告、用户认证记录报表、排行统计报表、资产统计报表

服务时间：远程服务：全年 7×24 小时报表系统运行；现场服务：工作日 5×8 小时。

交付成果和标准：交付成果:、《接入设备清单》。交付标准：报告应包含各认证方式使用情况、认证成功率、异常认证事件、系统优化建议等内容。

62. 边界控制管理服务

区光纤专网街道接入区从 802.1x 、 PBR（Policy – Based - Routing）、MVG 的各种边界控制服务、利用各种网络控制技术，实现在各种网络环境下适应性， IAC 能够帮助用户快速实现对于内网边界的规划。可以实现基于接入层边界的控制和基于重要资源边界的控制服务

服务时间：现场服务：工作日 5×8 小时；远程服务：全年 7×24 小时边界监控。策略每季度评估 1 次。

交付成果和标准：交付成果:《接入设备清单》。交付标准：报告应包含边界控制覆盖范围、接入设备合规率、异常接入事件、策略优化建议等内容。

63. 人员认证管理服务

区光纤专网街道接入区本地用户名/密码、Email、Radius、LDAP、 AD 域、短信、生物指纹管理服务

服务时间：现场服务：工作日 5×8 小时；远程服务：全年 7×24 小时认证服务运行

交付成果和标准：交付成果:、《接入设备清单》。交付标准：报告应包含各认证方式使用情况、认证成功率、异常认证事件、系统优化建议等内容。

64. 设备规范管理服务

区光纤专网街道接入区 IE 控件检查、IE 主页检查、IP/MAC 绑定检查、Windows 防火墙检测、操作系统版本检查、磁盘使用检查、计算机名称检查、垃圾文件检查、杀毒软件检查、网络监听端口检查、网络连接检查、系统补丁检查、系统时间检查、域用户检查、远程桌面检查、 P2P 软件检查、必须安装软件检查、必须运行进程检查、禁止安装软件检查、禁止运行进程检查、客户端运行状态检查、系统服务检查、软件授权检查、Guest 来宾账户检查、WSUS 更新配置检查、密码策略设置检查、屏幕保护设置检查、弱口令账户检查、网卡绑定检查、系统共享资源检查服务

服务时间：现场服务：工作日 5×8 小时；远程服务：全年 7×24 小时终端合规监控。

交付成果和标准：交付成果：《不合规设备清单》。交付标准：应包含重点不合规设备、整改进度跟踪、改进建议等内容。

65. 操作行为管理服务

区光纤专网街道接入区用户各种操作的监控和响应服务：ip 更改、违规软件使用、必须安装软件随意卸载、安全检查违规；计算机设备的统一维护管理服务：类别管理、设备信息管理、软件分发、服务管理、终端探测；任务管控服务：终端软件安装包分发、终端批处理脚本分发、终端消息通知分发服务

服务时间：远程服务：全年 7×24 小时行为监控；现场服务：工作日 5×8 小时。

交付成果和标准：交付成果：《月度操作行为管理报告》。交付标准：月度报告应包含本月操作行为统计、违规事件分析、软件分发执行情况、终端在线率、管理优化建议等内容。

66. 视角报表管理服务

区光纤专网街道接入区资源报表、违规操作记录、检查结果报表、入网安全检查评估报告、用户认证记录报表、排行统计报表、资产统计报表

服务时间：远程服务：全年 7×24 小时报表系统运行；现场服务：工作日 5×8 小时。

交付成果和标准：交付成果：《接入设备清单》。交付标准：报告应包含各认证方式使用情况、认证成功率、异常认证事件、系统优化建议等内容。

67. 代码审计服务

代码缺陷自动分析服务；代码缺陷人工审计服务 ；代码缺陷加固及复测服务

服务时间：现场服务：工作日 5×8 小时；远程服务：全年 7×24 小时接收审计申请。审计任务按需执行，在采购人约定的期限内完成。

交付成果和标准：交付成果：《代码审计申请单》《代码审计报告》《复测报告》（按需）。交付标准：审计报告应包含审计范围、审计方法、发现的缺陷清单（缺陷名称、风险等级、位置、描述、修复建议）、整体安全评估、整改优先级建议等内容。

68. 整体安全管理制度优化更新服务

区光纤专网安全管理制度优化与更新；区光纤专网应用安全接入规范编制和更新。

服务时间：现场服务：工作日 5×8 小时；远程服务：全年 7×24 小时沟通协作。制度优化每半年开展 1 次，按需更新。

交付成果和标准：交付成果：《区光纤专网安全管理制度文档》《区光纤专网应用安全接入规范文档》。交付标准：制度文档应符合国家相关法律法规与等级保护要求，结构完整、内容明确、可操作性强，经采购人审核确认后发布。

69. 安全意识和技术培训服务

网络安全法律法规解读培训；网络安全等级保护 2.0 解读培训；个人安全意识培训； 网络黑客攻击攻防技能培训；重保和护网专项培训。

服务时间：现场服务：工作日 5×8 小时，培训地点由采购人指定；远程服务：按需提供线上培训支持。全年不少于 1 次

交付成果和标准：交付成果：《培训签到表》《培训 PPT 课件》。交付标准：签到表应包含参训人员姓名、单位、职务、签到时间等信息；课件内容专业、准确、贴合采购人实际需求。

70. 应急预案体系和应急演练服务

应急响应保障制度体系优化和修订；应急演练场景和方案优化设计与编制；定期应急或攻防演练

服务时间：现场服务：工作日 5×8 小时；远程服务：全年 7×24 小时应急响应支持。应急演练每年开展 1 次。

交付成果和标准：交付成果：《应急演练方案》《应急演练结果报告》《应急演练签到表》。交付标准：演练方案应包含演练目标、场景设计、参与人员、时间安排、操作步骤、评估标准、安全措施等内容；结果报告应包含演练执行情况、目标达成情况、发现的问题、改进措施与建议等内容。

71. 网络安全应急响应服务

安全威胁事件应急响应处置服务；安全威胁事件研判与溯源服务；安全威胁事件总结建议报告服务。

服务时间：远程服务：全年 7×24 小时应急响应；现场服务：工作日 5×8 小时，重大安全事件按需到场（非工作时段到场时间双方协商）。

交付成果和标准：交付成果：《应急响应总结报告》（每次事件后）、《应急响应工单台账》。交付标准：总结报告应包含事件概述、事件时间线、影响范围、处置过程、原因分析、经验教训、改进建议与防范措施等内容。

72. 重大活动、护网期间安全保障专项服务

重保、护网安全保障方案设计；重保、护网安全防护布防措施实施；重保、护网安全防护自查服务；重保、护网安全应急演练；重保、护网期间现场安全值守和预警服务；重保、护网期间现场

安全事件应急响应和处置服务。

服务时间：远程服务：重保/护网期间 7×24 小时全程保障；现场服务：重保/护网期间按需现场值守（值守时间与人数由双方协商确定）

交付成果和标准：交付成果：《重保/护网安全保障方案》《重保/护网值班表》《签到表》《重保/护网安全保障总结报告》。交付标准：保障方案应包含保障目标、时间范围、组织架构、防护措施、值守安排、应急响应流程、沟通机制等内容；总结报告应包含保障期间安全态势、事件处置情况、值守情况、经验总结、改进建议等内容。

73. 安全检测系统服务

挂马检测服务

服务时间：远程服务：全年 7×24 小时挂马检测；现场服务：工作日 5×8 小时。

交付成果和标准：交付成果：《挂马检测安全分析报告》（按需）。交付标准：报告应包含检测范围、检测时间、检测结果（是否发现挂马、挂马位置、挂马类型、风险等级）、处置建议等内容。

74. 安全检测系统服务

黑链检测服务

服务时间：远程服务：全年 7×24 小时黑链检测；现场服务：工作日 5×8 小时。

交付成果和标准：交付成果：《黑链检测安全分析报告》（按需）。交付标准：报告应包含检测范围、检测时间、检测结果（是否发现黑链、黑链位置、黑链类型、风险等级）、处置建议等内容。

75. 安全检测系统服务

钓鱼检测服务

服务时间：远程服务：全年 7×24 小时钓鱼检测；现场服务：工作日 5×8 小时。

交付成果和标准：交付成果：《钓鱼检测安全分析报告》（按需）。交付标准：报告应包含监测范围、监测时间、发现的钓鱼网站清单（URL、仿冒对象、发现时间、风险等级）、处置建议与进展等内容。

76. 资产探测系统服务

资产探测服务

服务时间：现场服务：工作日 5×8 小时；远程服务：全年 7×24 小时资产探测。资产探测每季度至少 1 次，日常变更实时更新。

交付成果和标准：交付成果：《资产清单》（每季度更新）。交付标准：资产清单应包含资产 IP 地址、MAC 地址、设备类型、厂商型号、操作系统、开放端口、所属区域、责任人等字段；探测报告应包含本季度资产变化、新增资产、下线资产、异常资产提示等内容。

77. 网络病毒监测预警系统服务

病毒入侵监测服务； 防病毒检测服务；威胁情报检测服务；病毒攻击监测防护服务；安全行

为管理服务。

服务时间：远程服务：全年 7×24 小时病毒监测；现场服务：工作日 5×8 小时。

交付成果和标准：交付成果:《安全分析报告》。交付标准：月度报告应包含本月病毒检测统计、病毒类型分布、感染资产、病毒来源分析、处置情况、威胁情报更新、防护建议等内容。

78. 脆弱性扫描系统服务

脆弱性扫描服务

服务时间：现场服务：工作日 5×8 小时；远程服务：全年 7×24 小时扫描任务监控。脆弱性扫描每季度至少 1 次，在采购人指定维护窗口内执行。

交付成果和标准：交付成果:《漏洞扫描报告》（季度）。交付标准：报告应包含扫描范围、扫描时间、漏洞统计（按风险等级、按资产、按类型）、漏洞详情（漏洞名称、CVE 编号、风险等级、影响资产、漏洞描述、修复建议）、整体安全评估与改进建议等内容。

79. 威胁发现设备服务

威胁监测服务；威胁分析服务。

服务时间：远程服务：全年 7×24 小时威胁监测与分析；现场服务：工作日 5×8 小时。威胁分析报告每月出具 1 次。

交付成果和标准：交付成果:《安全分析报告》。交付标准：月度报告应包含本月威胁监测统计、威胁类型分布、重点威胁事件分析、攻击源分析、威胁趋势、设备运行状态、规则库更新情况、防护建议等内容。

其他要求：

1. **现网无缝过渡要求：本项目为在运行系统的年度安全运营服务。投标人须承诺：中标后 10 个工作日内完成与现网已部署安全设备（包括但不限于上网行为管理、入侵检测、日志审计、堡垒机、漏洞扫描、终端准入管理等设备）的策略对接、日志对接和账号交接，不改变现网网络拓扑和业务配置，并提供《现网无缝过渡方案》，服务所需工具和设备由中标方自行提供。未提供本承诺或承诺内容不满足本项要求的，作无效投标处理。**
2. **驻场服务要求：投标人须承诺：服务期内安排至少 1 名驻场工程师在采购人指定地点（上海市普陀区同普路 602 号）工作日 5×8 小时驻场。未提供本承诺的，作无效投标处理。**
3. **故障恢复时限承诺：投标人须承诺其服务满足第四章质量考核指标全部要求，包括：一般故障响应时间不超过 15 分钟、事件处置时限不超过 4 小时、问题解决不超过 3 天；紧急故障响应时间不超过 15 分钟、事件处置时限不超过 2 小时、问题解决不超过 2 天；重大故障响应时间不超过 15 分钟、普通应急处置时限不超过 1 小时、4 小时内应急恢复、问题解决不超过 1 天。未提供本承诺的，作无效投标处理。**

（二）交付物清单

序	服务名称	需求描述	服务范围	服务时段	交付物

号					
1	资产管理服务	区光纤专网核心接入区资产发现服务、入库资产管理服务、待入库资产管理服务、资产画像服务、资产主机资产画像服务、异常资产分析服务、环境要素识别服务	核心机房	现场服务：工作日时段 5*8 小时 远程服务：7*24 小时	《资产清单》(每季度更新)
2	漏洞脆弱性管理服务	区光纤专网核心接入区脆弱性配置服务、扫描任务管理服务、漏洞处置工单生成服务、漏洞利用热度展示服务	核心机房	现场服务：工作日时段 5*8 小时	《季度漏洞扫描报告》《漏洞处置工单台账》《高危漏洞应急处置报告》（按需）
3	安全威胁分析服务	区光纤专网核心接入区威胁事件研判服务、威胁事件研判配置服务、威胁攻击者画像服务、风险行为分析服务	核心机房	远程服务：7*24 小时	《月度安全威胁分析报告》《重大威胁事件专项分析报告》（按需）
4	安全事件溯源分析服务	区光纤专网核心接入区溯源流量取证服务、溯源日志搜索服务、威胁狩猎服务	核心机房	现场服务：工作日时段 5*8 小时	《安全事件溯源分析报告》（按需）、《威胁狩猎报告》（按需）
5	安全威胁监控服务	区光纤专网核心接入区攻击者监控服务、防护资产监控服务、攻击行为监控服务、自动化响应监控服务、监控配置服务、重点事件监控服务、目标 IP 跟踪服务	核心机房	远程服务：7*24 小时	《月度安全威胁分析报告》《重大告警事件处置记录》（按需）
6	安全态势感知服务	区光纤专网核心接入区综合态势可视化服务、环境感知服务、威胁态势呈现服务、运维响应态势展示服务、脆弱性态势感知服务、日志审计态势展现服务	核心机房	现场服务：工作日时段 5*8 小时	《月度安全态势分析报告》
7	安全威胁规则库运营服务	区光纤专网核心接入区预判规则服务、攻击识别规则配置服务、攻击识别实例配置服务、攻击识别规则管理服务、攻击识别规则调试服务、攻击识别防护策略配置服务、攻击识别全局配置服务、攻击识别简易模式自定义规则服务、攻击识别策略配置服务、规则升级服务	核心机房	远程服务：7*24 小时	《规则库运营台账》《规则升级记录》
8	漏洞库运营服务	区光纤专网核心接入区漏洞模板管理服务、漏洞分类服务、配置模板管理服务、密码字典管理服务、漏洞库升级服务	核心机房	现场服务：工作日时段 5*8 小时	《规则升级台账》
9	流量采集	区光纤专网核心接入区及街	核心机房	远程服务：7*24	《月度流量采集

	服务	道接入区 IPV4/IPV6 流量解析服务、VXLAN、MPLS、GRE、VLAN 流量解析服务、常见协议的深度解析服务、工控协议的深度解析服务、物联网协议的深度解析服务、数据库协议的解析服务、应用识别服务		小时	分析报告》《流量采集策略配置文档》
10	流量还原服务	区光纤专网核心接入区及街道接入区常规协议元数据还原服务、流量中出现的文件进行发现和还原服务	核心机房	现场服务：工作日时段 5*8 小时	《流量还原分析报告》（按需）、《还原文件清单》（按需）
11	流量威胁检测服务	区光纤专网核心接入区及街道接入区 webshell 检测服务、加密代理识别服务务、webshell 加密通信识别服务、钓鱼邮件检测服务、隐蔽隧道检测服务、dga 域名检测服务、	核心机房	远程服务：7*24 小时	《月度流量威胁检测分析报告》
12	流量风险行为分析服务	区光纤专网核心接入区及街道接入区暴力破解行为检测服务、弱口令行为检测服务、侦查探测行为检测服务、翻墙行为检测服务、主机外联行为检测服务、违规网站行为检测服务、异地登录行为检测服务、	核心机房	现场服务：工作日时段 5*8 小时	《月度流量风险行为分析报告》
13	流量留存服务	区光纤专网核心接入区及街道接入区元数据存储服务、原始 pcap 包存储服务、威胁包存储服务、恶意文件存储服务	核心机房	远程服务：7*24 小时	《季度流量留存策略评估报告》
14	流量检索服务	区光纤专网核心接入区及街道接入区流量日志查询服务、流量全局检索服务	核心机房	现场服务：工作日时段 5*8 小时	《流量检索结果报告》（按需）
15	设备日志接入服务	区光纤专网核心接入区设备海量日志数据采集服务、保存原始日志数据服务、异构日志格式进行统一化处理服务、保存统一化处理后的日志数据服务、界面配置未识别日志接入服务	核心机房	远程服务：7*24 小时	《设备接入清单》、《月度日志接入情况报告》
16	设备日志备份恢复服务	区光纤专网核心接入区设备手动或自动备份日志服务、 设置日志存储备份策略服务、 备份日志导入查询服务 日志备份至远程服务器服务	核心机房	现场服务：工作日时段 5*8 小时	《日志备份策略文档》、《季度备份恢复测试报告》、《备份任务执行台账》
17	设备日志检索服务	区光纤专网核心接入区设备实时日志查询服务、历史日志查询服务、原始日志范式化日志查询服务、自定义查询规则服务、全文检索模糊检索正则	核心机房	远程服务：7*24 小时	《日志检索结果报告》（按需）

		检索日志服务			
18	设备日志报表分析服务	区光纤专网核心接入区多种维度统计日志信息服务、统计分析报表与多种文件格式导出服务	核心机房	现场服务：工作日时段 5*8 小时	《月度日志分析报表》
19	设备日志事件告警服务	区光纤专网核心接入区多源事件关联分析服务、查询实时事件服务、告警抑制服务	核心机房	远程服务：7*24 小时	《月度日志告警分析报告》
20	设备主机漏洞扫描服务	区光纤专网核心接入区设备主机操作系统、数据库、中间件等进行漏洞扫描服务	核心机房	现场服务：工作日时段 5*8 小时	《季度漏洞扫描报告》
21	设备弱口令漏洞扫描服务	区光纤专网核心接入区设备系统进行弱口令扫描服务	核心机房	远程服务：7*24 小时	《季度漏洞扫描报告》
22	设备漏洞扫描任务管理服务	区光纤专网核心接入区设备已下发任务的列表展示，任务暂停、断点续扫等管理服务、任务参数展示，任务综述信息汇总分析展示，主机信息列表展示服务	核心机房	现场服务：工作日时段 5*8 小时	《漏洞扫描任务执行台账》
23	设备漏洞报表分析服务	区光纤专网核心接入区设备漏洞报表报表任务下发服务、报表类型选择服务、报表内容设置服务、对比分析服务、任务信息对比服务、漏洞对比服务，脆弱性账号对比服务	核心机房	远程服务：7*24 小时	《季度漏洞分析报表》、《季度漏洞对比分析报告》
24	设备漏洞验证服务	区光纤专网核心接入区设备对漏洞对取证性质的验证服务、支持漏洞库中标记可验证漏洞服务、漏洞验证漏洞利用原始结果服务	核心机房	现场服务：工作日时段 5*8 小时	《漏洞验证报告》（按需）
25	设备漏洞资产管理服务	区光纤专网核心接入区设备资产树对象的资产风险统计分析服务，展示整体资产范围的风险等级、风险评分服务	核心机房	远程服务：7*24 小时	《资产风险统计报告》（季度）、《高风险资产清单》（季度更新）
26	设备运维权限托管服务	区光纤专网核心接入区高价值设备登录运维和高危命令操作指定级金库授权服务、运维工单管理服务	核心机房	现场服务：工作日时段 5*8 小时	《月度运维权限审计分析报告》
27	设备字符运维审计服务	区光纤专网核心接入区设备 Telnet、SSH、Rlogin 等字符运维管理协议服务、密钥和密码方式SSH运维登录目标设备服务、对监控到的非法操作实时手工切断服务	核心机房	远程服务：7*24 小时	《月度审计分析报告》
28	设备文件运维审计服务	区光纤专网核心接入区设备 FTP、SFTP、Samba、SCP 等文件运维协议运维管理服务、web 文件插件方式运维目标服	核心机房	现场服务：工作日时段 5*8 小时	《月度审计分析报告》

		务器服务、WEB 界面直接调用 WinSCP、xsftp 等三分工具运维目标设备服务			
29	设备图形运维审计服务	区光纤专网核心接入区设备 RDP、VNC、X11 等图形运维协议运维管理服务、web 图形插件方式运维目标服务器服务、RDP、VNC 客户端软件直接登录堡垒机 MSTSC、Vnc Viewer 等客户端服务	核心机房	远程服务：7*24 小时	《月度审计分析报告》
30	设备数据库运维审计服务	区光纤专网核心接入区设备 Oracle、MS SQL Server、IBM DB2、Sybase、IBM Informix Dynamic Server、MySQL 等数据库类型运维管理服务、数据库图形方式操作审计与字符方式（数据库操作命令级）操作审计服务、数据库操作命令审计定位数据库图形审计服务	核心机房	现场服务：工作日时段 5*8 小时	《月度审计分析报告》
31	入侵检测防护服务	区光纤专网核心接入区入侵规则分类防护服务，制定分类防护策略。包含勒索、挖矿、SQL 注入、XSS 注入、webshell、命令代码执行、内存破坏、类型混淆、反序列化、信息泄露、目录遍历、文件操作漏洞、注入攻击、重定向漏洞、CSRF、僵木蠕、拒绝服务、弱口令、欺骗劫持、扫描类攻击等防护服务、SQL 注入、XSS 注入、webshell 等多种常见的应用层安全威胁抵御服务	核心机房	远程服务：7*24 小时	《月度入侵检测防护分析报告》、《防护策略配置台账》、《入侵事件处置记录》（按需）
32	DDOS 攻击检测防护服务	区光纤专网核心接入区 DoS/DDoS 攻击防护服务，支持 PING/UDP/SYN/ACK/DNS Reply/DNS Req Flood，支持 TCP Port Scan/UDP Port Scan，支持 PING Sweep，支持 ARP Spoof 以及 HTTP GET/HTTP POST FLood 等常见的 DoS/DDoS 的攻击抵御服务	核心机房	现场服务：工作日时段 5*8 小时	《月度入侵检测防护分析报告》《DDoS 防护策略配置文档》《重大 DDoS 攻击事件处置报告》（按需）
33	服务器外联防护服务	区光纤专网核心接入区服务器外联异常告警功能，可以手动添加或自学习服务器外联行为，并以此为基线检测服务器非法外联行为并告警服务	核心机房	远程服务：7*24 小时	《月度入侵检测防护分析报告》
34	应用管理服务	区光纤专网核心接入区主流的应用程序识别服务，识别不	核心机房	现场服务：工作日时段 5*8 小时	《月度入侵检测防护分析报告》

		少于 6000 个应用、多种抗逃避或欺骗检测技术识别服务，能检测出的躲避行为包括但不限于：IP 数据包乱序分片、TCP 报文乱序分段、RPC 分片分段、SMB 分片分段、FTP 无效命令混淆、HTTP 响应消息异常、HTML 文件内容多种字符编码混淆、数据流分隔、 协议端口重定位、URL 混淆、shell 代码变形等。			
35	数据泄露防护	敏感数据保护服务，能够识别、阻断、告警超过阈值的敏感数据信息，其中敏感数据包括身份证号、银行卡、电话号码等，且支持自定义敏感数据、关键文件保护服务，能够识别、阻断通过自身的关键文件，以防止非法外传行为。	核心机房	远程服务：7*24 小时	《月度入侵检测防护分析报告》
36	安全策略管理服务	区光纤专网核心接入区一体化入侵防护策略管理服务、超过 1000 条访问控制策略服务，可基于 IP 地址、端口（单个、多个和范围）、协议、动作（阻断、允许）进行访问策略配置，并可支持是否生成访问控制策略的会话日志生成。	核心机房	现场服务：工作日时段 5*8 小时	《安全策略台账》《策略变更记录》
37	流量管理服务	区光纤专网核心接入区带宽管理服务，可以根据用户、应用、时间及带宽等因素，实现基于应用、面向对象的流量保护策略；全面的流量分析服务，可查看流量完整性分布情况		远程服务：7*24 小时	《月度流量管理分析报告》《流量管理策略配置文档》
38	入侵检测防护服务	区光纤专网街道接入区入侵规则分类防护服务，制定分类防护策略。包含勒索、挖矿、SQL 注入、XSS 注入、webshell、命令代码执行、内存破坏、类型混淆、反序列化、信息泄露、目录遍历、文件操作漏洞、注入攻击、重定向漏洞、CSRF、僵木蠕、拒绝服务、弱口令、欺骗劫持、扫描类攻击等防护服务、SQL 注入、XSS 注入、webshell 等多种常见的应用层安全威胁抵御服务	10 个街道镇	现场服务：工作日时段 5*8 小时	《月度入侵检测防护分析报告》《防护策略配置台账》《入侵事件处置记录》（按需）
39	DDOS 攻击检测防护	区光纤专网街道接入区 DoS/DDoS 攻击防护服务，支持	10 个街道镇	远程服务：7*24 小时	《月度入侵检测防护分析报告》

	服务	PING/UDP/SYN/ACK/DNS Reply/DNS Req Flood，支持 TCP Port Scan/UDP Port Scan，支持 PING Sweep，支持 ARP Spoof 以及 HTTP GET/HTTP POST FLood 等常见的 DoS/DDoS 的攻击抵御服务			《DDoS 防护策略配置文档》《重大 DDoS 攻击事件处置报告》（按需）
40	服务器外联防护服务	区光纤专网街道接入区服务器外联异常告警功能，可以手动添加或自学习服务器外联行为，并以此为基线检测服务器非法外联行为并告警服务	10 个街道镇	现场服务：工作日时段 5*8 小时	《月度入侵检测防护分析报告》
41	应用管理服务	区光纤专网街道接入区主流的应用程序识别服务，识别不少于 6000 个应用、多种抗逃避或欺骗检测技术识别服务，能检测出的躲避行为包括但不限于：IP 数据包乱序分片、TCP 报文乱序分段、RPC 分片分段、SMB 分片分段、FTP 无效命令混淆、HTTP 响应消息异常、HTML 文件内容多种字符编码混淆、数据流分隔、 协议端口重定位、URL 混淆、shell 代码变形等。	10 个街道镇	远程服务：7*24 小时	《月度入侵检测防护分析报告》
42	数据泄露防护	区光纤专网街道接入区敏感数据保护服务，能够识别、阻断、告警超过阈值的敏感数据信息，其中敏感数据包括身份证号、银行卡、电话号码等，且支持自定义敏感数据、关键文件保护服务，能够识别、阻断通过自身的关键文件，以防止非法外传行为。	10 个街道镇	现场服务：工作日时段 5*8 小时	《月度入侵检测防护分析报告》
43	安全策略管理服务	区光纤专网街道接入区一体化入侵防护策略管理服务、超过 1000 条访问控制策略服务，可基于 IP 地址、端口（单个、多个和范围）、协议、动作（阻断、允许）进行访问策略配置，并可支持是否生成访问控制策略的会话日志生成。	10 个街道镇	远程服务：7*24 小时	《安全策略台账》《策略变更记录》
44	流量管理服务	区光纤专网街道接入区带宽管理服务，可以根据用户、应用、时间及带宽等因素，实现基于应用、面向对象的流量保护策略；全面的流量分析服务，可查看流量完整性分布情况	10 个街道镇	现场服务：工作日时段 5*8 小时	《月度流量管理分析报告》《流量管理策略配置文档》

45	访问控制服务	区光纤专网核心接入区二层协议进行访问控制服务，针对PPP、QinQ、MPLS 等协议进行屏蔽，对非 IP 协议进行访问控制服务、基于源安全区、目的安全区、源地址、目的地址、源端口、目的端口、协议等，模拟运行直接获得策略的命中信息，并可对命中的策略信息进行编辑服务	核心机房	远程服务：7*24小时	《访问控制策略台账》《策略变更记录》
46	应用识别服务	区光纤专网核心接入区应用特征识别库服务，对应用进行识别和控制，应用属性不少于类别、风险等级、标签、详细信息、实现技术等的服务	核心机房	现场服务：工作日时段 5*8 小时	《安全分析报告》《应用控制策略台账》
47	URL 过滤服务	区光纤专网核心接入区提供云端 URL 分类库，提供 64+种精细分类（广告及弹出窗口、烟酒、匿名网站、艺术、聊天、盗用网站、犯罪活动等）	核心机房	远程服务：7*24小时	《安全分析报告》
48	DNS 过滤服务	区光纤专网核心接入区针对 DNS 的 URL 过滤和分类识别服务	核心机房	现场服务：工作日时段 5*8 小时	《安全分析报告》
49	内容过滤服务	区光纤专网核心接入区网页浏览、论坛发帖、电子邮件、即时通讯、文件传输、服务器操作等信息关键字的实时检测和过滤服务	核心机房	远程服务：7*24小时	《安全分析报告》
50	敏感数据发现服务	区光纤专网核心接入区敏感信息过滤服务，对用户的个人隐私信息（手机号、身份证号码、社保号等）泄露进行检测或阻断服务	核心机房	现场服务：工作日时段 5*8 小时	《安全分析报告》
51	访问控制服务	区光纤专网街道接入区二层协议进行访问控制服务，针对PPP、QinQ、MPLS 等协议进行屏蔽，对非 IP 协议进行访问控制服务、基于源安全区、目的安全区、源地址、目的地址、源端口、目的端口、协议等，模拟运行直接获得策略的命中信息，并可对命中的策略信息进行编辑服务	10 个街道镇	远程服务：7*24小时	《访问控制策略台账》《策略变更记录》
52	应用识别服务	区光纤专网街道接入区应用特征识别库服务，对应用进行识别和控制，应用属性不少于类别、风险等级、标签、详细信息、实现技术等的服务	10 个街道镇	现场服务：工作日时段 5*8 小时	《安全分析报告》《应用控制策略台账》
53	URL 过滤	区光纤专网街道接入区提供	10 个街道	远程服务：7*24	《安全分析报

	服务	云端 URL 分类库，提供 64+种精细分类（广告及弹出窗口、烟酒、匿名网站、艺术、聊天、盗用网站、犯罪活动等）	镇	小时	告》
54	DNS 过滤服务	区光纤专网街道接入区针对 DNS 的 URL 过滤和分类识别服务	10 个街道镇	现场服务：工作日时段 5*8 小时	《安全分析报告》
55	内容过滤服务	区光纤专网街道接入区网页浏览、论坛发帖、电子邮件、即时通讯、文件传输、服务器操作等信息关键字的实时检测和过滤服务	10 个街道镇	远程服务：7*24 小时	《安全分析报告》
56	敏感数据发现服务	区光纤专网街道接入区敏感信息过滤服务，对用户的个人隐私信息（手机号、身份证号码、社保号等）泄露进行检测或阻断服务	10 个街道镇	现场服务：工作日时段 5*8 小时	《安全分析报告》
57	边界控制管理服务	区光纤专网核心接入区从 802.1x 、 PBR （ Policy - Based - Routing）、MVG 的各种边界控制服务、利用各种网络控制技术，实现在各种网络环境下适应性，IAC 能够帮助用户快速实现对于内网边界的规划。可以实现基于接入层边界的控制和基于重要资源边界的控制服务	核心机房	远程服务：7*24 小时	《接入设备清单》
58	人员认证管理服务	区光纤专网核心接入区本地用户名/密码、Email、Radius、LDAP、AD 域、短信、生物指纹管理服务	核心机房	现场服务：工作日时段 5*8 小时	《接入设备清单》
59	设备规范管理服务	区光纤专网核心接入区 IE 控件检查、IE 主页检查、IP/MAC 绑定检查、Windows 防火墙检测、操作系统版本检查、磁盘使用检查、计算机名称检查、垃圾文件检查、杀毒软件检查、网络监听端口检查、网络连接检查、系统补丁检查、系统时间检查、域用户检查、远程桌面检查、P2P 软件检查、必须安装软件检查、必须运行进程检查、禁止安装软件检查、禁止运行进程检查、客户端运行状态检查、系统服务检查、软件授权检查、Guest 来宾账户检查、WSUS 更新配置检查、密码策略设置检查、屏幕保护设置检查、弱口令账户检	核心机房	远程服务：7*24 小时	《不合规设备清单》

		查、网卡绑定检查、系统共享资源检查服务			
60	操作行为管理服务	区光纤专网核心接入区用户各种操作的监控和响应服务：ip 更改、违规软件使用、必须安装软件随意卸载、安全检查违规； 计算机设备的统一维护管理服务：类别管理、设备信息管理、软件分发、服务管理、终端探测；任务管控服务：终端软件安装包分发、终端批处理脚本分发、终端消息通知分发服务	核心机房	现场服务：工作日时段 5*8 小时	《月度操作行为管理报告》
61	视角报表管理服务	区光纤专网核心接入区资源报表、违规操作记录、检查结果报表、入网安全检查评估报告、用户认证记录报表、排行统计报表、资产统计报表	核心机房	远程服务：7*24 小时	《接入设备清单》
62	边界控制管理服务	区光纤专网街道接入区从 802.1x 、 PBR （ Policy - Based - Routing）、MVG 的各种边界控制服务、利用各种网络控制技术，实现在各种网络环境下适应性，IAC 能够帮助用户快速实现对于内网边界的规划。可以实现基于接入层边界的控制和基于重要资源边界的控制服务	10 个街道镇	现场服务：工作日时段 5*8 小时	《接入设备清单》
63	人员认证管理服务	区光纤专网街道接入区本地用户名/密码、Email、Radius、LDAP、AD 域、短信、生物指纹管理服务	10 个街道镇	远程服务：7*24 小时	《接入设备清单》
64	设备规范管理服务	区光纤专网街道接入区 IE 控件检查、IE 主页检查、IP/MAC 绑定检查、Windows 防火墙检测、操作系统版本检查、磁盘使用检查、计算机名称检查、垃圾文件检查、杀毒软件检查、网络监听端口检查、网络连接检查、系统补丁检查、系统时间检查、域用户检查、远程桌面检查、P2P 软件检查、必须安装软件检查、必须运行进程检查、禁止安装软件检查、禁止运行进程检查、客户端运行状态检查、系统服务检查、软件授权检查、Guest 来宾账户检查、WSUS 更新配置检	10 个街道镇	现场服务：工作日时段 5*8 小时	《不合规设备清单》

		查、密码策略设置检查、屏幕保护设置检查、弱口令账户检查、网卡绑定检查、系统共享资源检查服务			
65	操作行为管理服务	区光纤专网街道接入区用户各种操作的监控和响应服务：ip 更改、违规软件使用、必须安装软件随意卸载、安全检查违规； 计算机设备的统一维护管理服务：类别管理、设备信息管理、软件分发、服务管理、终端探测；任务管控服务：终端软件安装包分发、终端批处理脚本分发、终端消息通知分发服务	10 个街道镇	远程服务：7*24 小时	《月度操作行为管理报告》
66	视角报表管理服务	区光纤专网街道接入区资源报表、违规操作记录、检查结果报表、入网安全检查评估报告、用户认证记录报表、排行统计报表、资产统计报表	10 个街道镇	现场服务：工作日时段 5*8 小时	《接入设备清单》
67	代码审计服务	代码缺陷自动分析服务；代码缺陷人工审计服务 ；代码缺陷加固及复测服务	核心机房+10 个街道镇	远程服务：7*24 小时	《代码审计申请单》、《代码审计报告》、《复测报告》（按需）
68	整体安全管理制度优化更新服务	区光纤专网安全管理制度优化与更新；区光纤专网应用安全接入规范编制和更新。	核心机房+10 个街道镇	现场服务：工作日时段 5*8 小时	《区光纤专网安全管理制度文档》、《区光纤专网应用安全接入规范文档》
69	安全意识和技术培训服务	网络安全法律法规解读培训；网络安全等级保护 2.0 解读培训；个人安全意识培训；网络黑客攻击攻防技能培训；重保和护网专项培训。	核心机房+10 个街道镇	远程服务：7*24 小时	《培训签到表》、《培训 PPT 课件》
70	应急预案体系和应急演练服务	应急响应保障制度体系优化和修订；应急演练场景和方案优化设计与编制；定期应急或攻防演练	核心机房+10 个街道镇	现场服务：工作日时段 5*8 小时	《应急演练方案》、《应急演练结果报告》、《应急演练签到表》
71	网络安全应急响应服务	安全威胁事件应急响应处置服务；安全威胁事件研判与溯源服务；安全威胁事件总结建议报告服务。	核心机房+10 个街道镇	远程服务：7*24 小时	《应急响应总结报告》（每次事件后）、《应急响应工单台账》
72	重大活动、护网期间安全保障专项服务	重保、护网安全保障方案设计；重保、护网安全防护布防措施实施；重保、护网安全防护自查服务；重保、护网安全应急演练；重保、护网期间现	核心机房+10 个街道镇	重保/护网期间 7×24 小时全程保障； 现场服务：	《重保/护网安全保障方案》《重保/护网值班表》《签到表》《重保/护网安全保

		场安全值守和预警服务；重保、护网期间现场安全事件应急响应和处置服务。		按需现场值守（值守时间与人数由双方协商确定）	障总结报告》
73	安全检测系统服务	挂马检测服务	核心机房+10 个街道镇	远程服务：7*24 小时	《挂马检测安全分析报告》（按需）
74	安全检测系统服务	黑链检测服务	核心机房+10 个街道镇	现场服务：工作日时段 5*8 小时	《黑链检测安全分析报告》（按需）
75	安全检测系统服务	钓鱼检测服务	核心机房+10 个街道镇	远程服务：7*24 小时	《钓鱼检测安全分析报告》（按需）
76	资产探测系统服务	资产探测服务	核心机房+10 个街道镇	现场服务：工作日时段 5*8 小时	《资产清单》(每季度更新）
77	网络病毒监测预警系统服务	病毒入侵监测服务；防病毒检测服务；威胁情报检测服务；病毒攻击监测防护服务；安全行为管理服务。	核心机房+10 个街道镇	远程服务：7*24 小时	《安全分析报告》
78	脆弱性扫描系统服务	脆弱性扫描服务	核心机房+10 个街道镇	现场服务：工作日时段 5*8 小时	《漏洞扫描报告》（季度）
79	威胁发现设备服务	威胁监测服务；威胁分析服务。	核心机房+10 个街道镇	远程服务：7*24 小时	《安全分析报告》（每月）
80	驻场服务	服务有效期内，提供 1 名驻场服务人员进行服务范围内设备的运行管理维护，在采购人指定地点工作时间内提供现场运维服务，及时提供响应服务同时按用户方需求提供个性化服务。	核心机房+10 个街道镇	现场服务：工作日时段 5*8 小时	驻场服务人员工作相关信息安全服务资质证书、中标方委派驻场工作证明。

（三）质量考核指标

序号	指标名称	指标描述
1	重大责任事件	全年重大责任事件数为 0
2	服务满意度	事件处理满意度达到 98%以上
3	事件处置效率	事件升级为故障的件数/事件台账总数*故障等级权重系数
4	工作时段响应	15 分钟内响应

5	非工作时段响应	2 小时内响应
6	应急响应	全年 7*24 小时响应，并做好应急保障工作
7	故障恢复时间	（1）一般故障： 响应时间≤15 分钟，事件处置时限≤4 小时，问题解决≤3 天。 （2）紧急故障： 响应时间≤15 分钟，事件处置时限≤2 小时，问题解决≤2 天。 （3）重大故障： 响应时间≤15 分钟，普通应急处置时限≤1 小时，重大故障（除自然灾害等不可抗力影响导致）4 小时内应急恢复，问题解决≤1 天。

序号	类别	考核项	权重分数	指标公式/来源	内容	整体目标值
1	维护质量	系统可用率	30	系统可用率=每日设备可用时长/当月总时长	设备可用指设备在线、功能正常	≥95%
2		巡检完成率	20	1.巡检完成率=实际完成巡检次数/半年按要求完成巡检总次数； 2.巡检完成率达标的情况下得满分。如不达标，实际得分=巡检完成率/达标值*权重分	平台巡检工作为每年巡检工作内容。	≥95%
3		问题处理及时率	20	1.工单处理及时率=考核周期内按时处理完成工单数/总工单次数；2. 总得分=故障处理及时率/达标值*权重分	问题发现和处理工作内容	≥95%
4		客户满意度评分	10	客户满意度评分达标情况下得满分，如未达标，考核项得分=客户满意度评分/达标值*权重分	客户满意度回访调查	≥95%
5	基础管理	维护资料提交完整率	5	1. 每年向客户提交：“故障处理及时率”“巡检完成率”共 2 份表格； 2. “维护资料提交完整率”达标的情况下得满分，如未达标则按以下公式计算：得分=实际提交资料数量/应提交资料数量*权重分	故障处理及时率及巡检完成率报表	≥95%
6		人员稳	15	参与服务人员变更，未向客户	运维人员在	≥95%

		定性		报备，或报备未经客户同意的，每次扣 5 分。人员变更不超过 3 次。	岗考核	
总分			**100 分**			

第五章　评标办法及评分标准

根据《中华人民共和国政府采购法》等有关法律法规，结合本项目的实际需求，制定本办法。

一、评标依据和原则：

1、本评标办法作为本项目择优选定中标人的依据，在评标全过程中应遵照执行。

2、评标委员会由招标人或其委托的集采机构依法组建。评标委员会由招标人代表和评审专家组成，成员人数为 5 人单数，其中评审专家不得少于成员总数的三分之二，采购人代表不参加评审的，则评标委员会均由评审专家组成 ，评审专家将从上海市政府采购评审专家库内的专家名单中随机抽取。

3、本项目评标由评委根据本评标办法的规定，按顺序依次分技术因素和价格因素二个 阶段各自打分，分项计分。技术因素占 90%、价格因素占 10%。

4、评审要点的相应权重设置如下，价格因素中打分精确到 0.1 分，其他各项评审要点均精确到 0.1 分。各项评审要点得分不得超过该项的总分值。

5、各评委须严格按照上述办法打分。

6、评标委员会成员必须本人参加评标会。

7、任何人不得干预评委的评分权利，评分表要保存备查。

8、评标委员会根据本招标文件的规定否决不合格投标，因有效标不足三家使得投标明显缺乏竞争的，评标委员会可以否决全部投标。

二、评标决标程序

1、资格性审查：由招标人依据法律法规和招标文件，对投标人进行资格审查；资格审查不合格者，投标无效；若资格审查合格的投标人不满三家，则本项目按废标处理。

2、符合性审查：由评标委员会根据公开招标文件要求，对各通过资格性审查的投标人的文件进行符合性审查，符合性审查不满足要求的将不进入评分阶段，符合性审查合格者进入技术因素和价格因素评分阶段。

3、异常低价审查：评审中出现下列情形之一的，评标委员会应当对投标报价启动异常低价投标审查程序；

标项 1

是否启用异常低价审查程序：是

1.投标（响应）报价低于全部通过符合性审查供应商投标（响应）报价平均值 50%的，即投标（响应）报价<全部通过符合性审查供应商投标（响应）报价平均值×50%；

2.投标（响应）报价低于通过符合性审查的次低报价供应商投标（响应）报价 50%的，即投标（响应）报价<通过符合性审查的次低报价供应商投标（响应）报价×50%；

3.投标（响应）报价低于采购项目最高限价45%的，即投标（响应）报价<采购项目最高限价×45%；

4.评审委员会基于专业判断，认为供应商报价过低，有可能影响产品质量或者不能诚信履约的其他情形。

评标委员会启动异常响应低价审查后，属于前述第1 项至第4 项情形的，应当要求相关供应商在评审现场合理的时间内对响应价格作出解释，提供项目具体成本测算等与报价合理性相关的书面说明及必要的证明材料，包括但不限于原材料成本、人工成本、制造费用等，给予相关供应商的合理时间一般不少于30 分钟。其中，属于第3 项情形，供应商已随响应文件一并提交相关书面说明及必要的证明材料的，在评审现场可不再重复提交。

评标委员会依据专业经验，参考同类项目成交价格、类似产品市场价格水平、行业人工费用标准、国家有关部门指导行业协会发布的行业平均成本等情况，对报价合理性进行判断。供应商不能提供书面说明、证明材料，或者提供的书面说明、证明材料不能证明其报价合理性的，评标委员会应当将其作为无效响应处理。异常低价投标审查的启动原因、审查意见和审查结果应当在评审报告中记录，并随供应商提供的相关书面说明及证明材料，以及评审委员会有关互联网浏览、查询历史一并归档。

4、评标委员会要求供应商澄清、说明或者更正投标文件将以书面形式作出。供应商的澄清、说明或者更正应当由法定代表人（负责人）或其授权代表签字或者加盖公章。由授权代表签字的，应当附法定代表人（负责人）授权书。供应商为自然人的，应当由本人签字并附身份证明。

5、详细评审：根据评标办法，主观分由各评审专家根据投标文件进行打分。

6、最低报价并不能作为授予合同的保证。

三、评标内容及标准

智联普陀光纤专网安全加固政务信息化购买服务项目（2026年度）评分规则：

综合评分法

智联普陀光纤专网安全加固政务信息化购买服务项目（2026年度）包1评分规则：

评分项目	分值区间	评分办法
报价得分	0~10	（1）确定评标基准价：经评标委员会甄别确认，满足招标文件要求的合理的最低有效报价为评标基准价。 （2）其他报价得分计算公式：报价得分＝（评标基准价／经评

		审后的投标报价）×10%×100，分值计算保留一位小数。
项目现状分析及需求理解	0~5	1.对项目现状及服务需求理解透彻，明确服务定位和目标，并能具体说明： ①本项目 10 个街道镇汇聚机房与核心机房的现网拓扑及安全边界现状； ②现网等保三级（依据 GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》）差距项； ③上一年度已发现高危漏洞及整改情况； ④护网、重保期间暴露的安全问题。全部覆盖得 4～5 分； 2.覆盖其中两项以上但不够全面，得 2～3 分； 3.仅作一般性描述、无具体内容，得 1 分； 4.未做说明得 0 分。
重点、难点分析及合理化建议	0~5	1.对本项目在运行系统无缝交接、10 个街道节点分散运维、7×24 小时值守、重大活动保障等重难点分析到位，合理化建议能落地解决实际问题，得 4～5 分； 2.分析较清晰、建议可部分解决问题，得 2～3 分； 3.分析简单、无具体建议，得 1 分；4.未作说明得 0 分。

服务交付流程设计情况	0~4	1.服务交付流程设计思路条理清晰，覆盖服务启动、交接、日常运维、月度/季度/年度报告、考核改进全流程，且针对本项目具有可操作性，得 4 分； 2.流程基本完整、针对性一般，得 2～4 分； 3.流程存在明显缺漏，得 1 分； 4.未做说明得 0 分。
安全服务方案	0~5	1.安全服务方案内容完整，包含核心机房与 10 个街道镇分层防护矩阵、7×24 小时监控值班安排、月度/季度/年度报告模板样例、与现网安全管理平台对接方案，贴合项目实际，得 4～5 分； 2.方案内容简单、基本满足需求，得 2～3 分； 3.方案缺漏或缺乏针对性，得 1 分； 4.未做说明得 0 分。
服务成果及交付物	0~4	1.服务成果及交付物覆盖招标需求全部交付清单，交付模板规范、流程合理，得 4 分； 2.基本覆盖交付清单、模板欠规范，得 2～3 分； 3.交付物内容不完整，得 1 分； 4.未做说明得 0 分。
项目进度计划安排	0~5	1.对项目整体实施及分项进度

		计划安排合理，明确交接期、各季度服务节点、重大活动保障节点，具有科学性和可操作性，得5分； 2.进度安排基本合理、可操作性欠佳，得2～4分； 3.进度安排不合理或缺失，得1分； 4.未做说明得0分。
应急处理方案	0~5	1.针对DDoS攻击、勒索病毒、webshell入侵、数据泄漏四类场景均提供具体处置SOP，并与采购人现有应急预案衔接，应急响应步骤详细可执行，得4～5分； 2.方案合理、覆盖部分场景，得2～3分； 3.方案不完整，得1分； 4.未作说明得0分。
安全保密措施	0~5	1.安全保密措施描述清晰完整，包含数据不出域、涉密信息管理、驻场人员保密承诺、离场信息清理等可操作措施，得5分； 2.描述基本满足要求、操作性一般，得2～4分； 3.缺漏或描述不清，得1分；4.未做说明得0分。
重保、护网安全保障方案	0~5	1.重保/护网安全保障方案完整，包含保障目标、组织架构、防护

		布防、值守安排、应急响应流程;得 4~5 分;2.方案基本完整;得 2~3 分;3.方案缺漏，得 1 分;4.未做说明得 0 分。
运营服务承诺及奖罚措施	0~4	1.运营服务承诺满足项目要求，奖惩措施完善、明确、可操作，得 4 分； 2.承诺与奖惩基本合理，得 2～3 分； 3.承诺简单、奖惩缺漏，得 1 分； 4.未做说明得 0 分。
培训方案	0~3	1.培训大纲内容详细，培训人员经验丰富、培训次数不少于采购需求要求，得 3 分； 2.培训内容简单、次数较少，得 2 分； 3.培训方案缺漏，得 1 分； 4.未做说明得 0 分。
验收方案	0~3	1.验收方案内容全面、程序科学、各环节措施详尽，得 3 分； 2.验收方案有缺漏，得 2 分； 3.验收方案缺失，得 1 分； 4.未做说明得 0 分。
各类规章制度	0~4	1.提供与安全运营服务相关的规章制度全面、合理、科学（含值班制度、交接班制度、应急值守制度、报告审核制度等），得 4 分； 2.制度较全面、基本合理，得 2～3 分；

		3.制度不完善，得 1 分； 4.未做说明得 0 分。
项目负责人	0~9	项目负责人同时满足以下条件的得 6 分： ①提供本科及以上学历的，得 3 分；未提供的不得分； ②提供具备中级工程师（及以上）工程系列职称的，得 1-3 分；未提供的不得分； ③提供近三年（以合同签订日期计）作为项目负责人完成过至少 1 个合同的网络安全运营服务或等级保护三级系统安全运维项目的，得 3 分；未提供的不得分； 注：项目负责人须提供本单位投标截止日前近六个月内任意一个月社会保险缴纳证明材料，未提供的或证书、合同、社保非同一主体的不予认可。
项目团队	0~3	本项目投入整体服务团队不少于 12 人，出具正式承诺函，覆盖项目经理、驻场运维、安全分析、漏洞处置、应急响应岗位，得 1-3 分；人数不足或无承诺函不得分。
团队网络与技术力量	0~6	团队网络与技术力量（本小项最高 6 分）：除项目经理外，团队人员满足下面任意一项，每 1 人得 1 分，本小项最高 6 分；同

		一人员多项证书不重复计分。满足条件（任意一项即可）： ①人社/工信颁发中级及以上工程师职称（计算机、通信、网络相关方向）； ②计算机技术与软件专业技术资格（软考）中级及以上； 备注：职称以人社部门正规评审证书为准；所有人员须提供投标单位近 6 个月社保缴纳证明。
类似项目业绩	0~3	1.提供清晰可辨的自响应公告发布之日前 36 个月内的同类项目的业绩材料，时间以合同签订日期为准。业绩证明以供应商实际提供的合同扫描件为准（供应商提供的合同案例应包含合同首页、金额所在页和签字盖章页等）； 2.供应商每提供一个符合要求的业绩及证明材料得 1 分，满分 3 分，未提供或提供的不符合要求不得分。
企业综合实力	0~6	评分范围：0-6 分 根据投标单位的社会信誉、履约能力、综合经营能力、本地化服务能力等情况进行综合评审。 评分标准： 投标单位综合服务能力、诚信经营履约能力、项目实施能力均符合本项目需要的证明文件齐全

		的，得 5-6 分； 投标单位综合服务能力、诚信经营履约能力、项目实施能力均符合本项目需要的证明文件缺少的，得 3-4 分； 企业相关信息提供不完善或无法有效证明其综合能力的，得 1-2 分。 无相关内容的不得分。
响应时间	0~6	评分范围：0-6 分 根据投标单位提供的服务保障方案、应急排班表等证明文件就行评分： 1. 承诺到场响应时间≤45 分钟内的，得 4-6 分； 2. 承诺到场响应时间＞45 分钟至≤90 分钟内的，得 1-3 分； 3. 承诺到场响应时间＞120 分钟，或未承诺的，得 0 分；

第六章　政府采购合同主要条款指引

包 1 合同模板：

[合同中心-合同名称]

合同统一编号：［合同中心-合同编码］

合同内部编号：

合同各方：

甲方：[合同中心-采购单位名称]	**乙方：[合同中心-供应商名称]**
地址：[合同中心-采购单位所在地]	**地址：[合同中心-供应商所在地]**
邮政编码：[合同中心-采购人单位邮编]	**邮政编码：[合同中心-供应商单位邮编]**
电话：[合同中心-采购单位联系人电话]	**电话：[合同中心-供应商联系人电话]**
传真：[合同中心-采购人单位传真]	**传真：[合同中心-供应商单位传真]**
联系人：[合同中心-采购单位联系人]	**联系人：[合同中心-供应商联系人]**

根据《中华人民共和国政府采购法》、《中华人民共和国民法典》之规定，本合同当事人在平等、自愿的基础上，经协商一致，同意按下述条款和条件签署本合同：

1．乙方根据本合同的规定向甲方提供以下服务：

1．1 乙方所提供的服务其来源应符合国家的有关规定，服务的内容、要求、服务质量等详见合同附件。

2. 合同价格、服务地点和服务期限

2．1 合同价格

本合同价格为**[合同中心-合同总价]**元整（**[合同中心-合同总价大写]**）。

乙方为履行本合同而发生的所有费用均应包含在合同价中，甲方不再另行支付其它任何费用。

2．2 服务地点:甲方指定地点。

2．3 服务期限
本服务的服务期限：[合同中心-合同有效期]。

3．质量标准和要求
3．1 乙方所提供的服务的质量标准按照国家标准、行业标准或制造厂家企业标准确定，上述标准不一致的，以严格的标准为准。没有国家标准、行业标准和企业标准的，按照通常标准或者符合合同目的的特定标准确定。
3．2 乙方所交付的服务还应符合国家和上海市有关安全、环保、卫生之规定。

4．权利瑕疵担保
4．1 乙方保证对其交付的服务享有合法的权利。
4．2 乙方保证在服务上不存在任何未曾向甲方透露的担保物权，如抵押权、质押权、留置权等。
4．3 乙方保证其所交付的服务没有侵犯任何第三人的知识产权和商业秘密等权利。
4．4 如甲方使用该服务构成上述侵权的，则由乙方承担全部责任。

5．验收
5．1 服务根据合同的规定完成后，甲方应及时进行根据合同的规定进行服务验收。乙方应当以书面形式向甲方递交验收通知书，甲方在收到验收通知书后的 10 个工作日内，确定具体日期，由双方按照本合同的规定完成服务验收。甲方有权委托第三方检测机构进行验收，对此乙方应当配合。
5．2 如果属于乙方原因致使系统未能通过验收，乙方应当排除故障，并自行承担相关费用，同时进行试运行，直至服务完全符合验收标准。
5．3 如果属于甲方原因致使系统未能通过验收，甲方应在合理时间内排除故障，再次进行验收。如果属于故障之外的原因，除本合同规定的不可抗力外，甲方不愿或未能在规定的时间内完成验收，则由乙方单方面进行验收，并将验收报告提交甲方，即视为验收通过。
5．4 甲方根据《采购需求》中考核办法等相关要求进行考核验收。

5．5 甲方根据合同的规定对服务验收合格后，甲方收取发票并签署验收意见。

6．保密
6．1 如果甲方或乙方提供的内容属于保密的，应签订保密协议，甲乙双方均有保密义务。

7．付款
7．1 本合同以人民币付款（单位：元）。
7．2 本合同款项按照以下方式支付。
7．2．1 付款内容：（分期付款）
7．2．2 付款条件：

[合同中心-支付方式名称]

付款方式：

签订服务合同支付合同金额 20%费用，服务期满半年后支付合同金额 50%费用，服务期满后支付合同金额 30%尾款。

8．甲方（甲方）的权利义务

8．1、甲方有权在合同规定的范围内享受，对没有达到合同规定的服务质量或标准的服务事项，甲方有权要求乙方在规定的时间内加急提供服务，直至符合要求为止。

8．2 如果乙方无法完成合同规定的服务内容、或者服务无法达到合同规定的服务质量或标准的，造成的无法正常运行，甲方有权邀请第三方提供服务，其支付的服务费用由乙方承担；如果乙方不支付，甲方有权在支付乙方合同款项时扣除其相等的金额。

8．3 由于乙方服务质量或延误服务的原因，使甲方有关或设备损坏造成经济损失的，甲方有权要求乙方进行经济赔偿。

8．4 甲方在合同规定的服务期限内有义务为乙方创造服务工作便利，并提供适合的工作环境，协助乙方完成服务工作。

8．5 当或设备发生故障时，甲方应及时告知乙方有关发生故障的相关信息，以便乙方及时分析故障原因，及时采取有效措施排除故障，恢复正常运行。

8． 6 如果甲方因工作需要对原有进行调整，应有义务并通过有效的方式及时通知乙方涉及合同服务范围调整的，应与乙方协商解决。

9．乙方的权利与义务

9．1 乙方根据合同的服务内容和要求及时提供相应的服务，如果甲方在合同服务范围外增加或扩大服务内容的，乙方有权要求甲方支付其相应的费用。

9．2 乙方为了更好地进行服务，满足甲方对服务质量的要求，有权利要求甲方提供合适的工作环境和便利。在进行故障处理紧急服务时，可以要求甲方进行合作配合。

9．3 如果由于甲方的责任而造成服务延误或不能达到服务质量的，乙方不承担违约责任。

9．4 由于因甲方工作人员人为操作失误、或供电等环境不符合合同设备正常工作要求、或其他不可抗力因素造成的设备损毁，乙方不承担赔偿责任。

9．5 乙方保证在服务中，未经甲方许可不得使用含有可以自动终止或妨碍系统运作的软件和硬件，否则，乙方应承担赔偿责任。

9． 6 乙方在履行服务时，发现存在潜在缺陷或故障时，有义务及时与甲方联系，共同落实防范措施，保证正常运行。

9．7 如果乙方确实需要第三方合作才能完成合同规定的服务内容和服务质量的，应事先征得甲方的同意，并由乙方承担第三方提供服务的费用。

9．8 乙方保证在服务中提供更换的部件是全新的、未使用过的。如果或证实服务是有缺陷的，包括潜在的缺陷或使用不符合要求的材料等，甲方可以根据本合同第 10 条规定以书面形式向乙方提出补救措施或索赔。

10．补救措施和索赔

10．1 甲方有权根据质量检测部门出具的检验证书向乙方提出索赔。

10．2 在服务期限内，如果乙方对提供服务的缺陷负有责任而甲方提出索赔，乙方应按照甲方同意的下列一种或多种方式解决索赔事宜：

（1）根据服务的质量状况以及甲方所遭受的损失，经过买卖双方商定降低服务的价格。

（2）乙方应在接到甲方通知后七天内，根据合同的规定负责采用符合规定的规格、质量和性能要求的新零件、部件和设备来更换在服务中有缺陷的部分或修补缺陷部分，其费用由乙方负担。

（3）如果在甲方发出索赔通知后十天内乙方未作答复，上述索赔应视为已被乙方接受。如果乙方未能在甲方发出索赔通知后十天内或甲方同意延长的期限内，按照上述规定的任何一种方法采取补

救措施，甲方有权从应付的合同款项中扣除索赔金额，如不足以弥补甲方损失的，甲方有权进一步要求乙方赔偿。

11．履约延误

11．1 乙方应按照合同规定的时间、地点提供服务。

11．2 如乙方无正当理由而拖延服务，甲方有权没收乙方提供的履约保证金，或解除合同并追究乙方的违约责任。

11．3 在履行合同过程中，如果乙方可能遇到妨碍按时提供服务的情况时，应及时以书面形式将拖延的事实、可能拖延的期限和理由通知甲方。甲方在收到乙方通知后，应尽快对情况进行评价，并确定是否同意延期提供服务。

12．误期赔偿

12．1 除合同第 13 条规定外，如果乙方没有按照合同规定的时间提供服务，甲方可以应付的合同款项中扣除误期赔偿费而不影响合同项下的其他补救方法，赔偿费按每（天）赔偿延期服务的服务费用的百分之零点五（0.5%）计收，直至提供服务为止。但误期赔偿费的最高限额不超过合同价的百分之五（5%）。（一周按七天计算，不足七天按一周计算。）一旦达到误期赔偿的最高限额，甲方可考虑终止合同。

13．不可抗力

13．1 如果合同各方因不可抗力而导致合同实施延误或不能履行合同义务的话，不应该承担误期赔偿或不能履行合同义务的责任。

13．2 本条所述的“不可抗力”系指那些双方不可预见、不可避免、不可克服的事件，但不包括双方的违约或疏忽。这些事件包括但不限于：战争、严重火灾、洪水、台风、地震、国家政策的重大变化，以及双方商定的其他事件。

13．3 在不可抗力事件发生后，当事方应尽快以书面形式将不可抗力的情况和原因通知对方。合同各方应尽可能继续履行合同义务，并积极寻求采取合理的措施履行不受不可抗力影响的其他事项。合同各方应通过友好协商在合理的时间内达成进一步履行合同的协议。

14．履约保证金

14．1 在本合同签署之前，乙方应向甲方提交一笔金额为 0 元人民币的履约保证金。履约保证金应自出具之日起至全部服务按本合同规定验收合格后三十天内有效。在全部服务按本合同规定验收合格后 15 日内，甲方应一次性将履约保证金无息退还乙方。

14．2 履约保证金可以采用支票或者甲方认可的银行出具的保函。乙方提交履约保证金所需的有关费用均由其自行负担。

14．3 如乙方未能履行本合同规定的任何义务，则甲方有权从履约保证金中得到补偿。履约保证金不足弥补甲方损失的，乙方仍需承担赔偿责任。

15．争端的解决

15.1 合同各方应通过友好协商，解决在执行本合同过程中所发生的或与本合同有关的一切争端。如从协商开始十天内仍不能解决，可以向同级政府采购监管部门提请调解。

15．2 调解不成则提交上海仲裁委员会根据其仲裁规则和程序进行仲裁。

15．3 如仲裁事项不影响合同其它部分的履行，则在仲裁期间，除正在进行仲裁的部分外，本合同的其它部分应继续执行。

16．违约终止合同

16．1 在甲方对乙方违约而采取的任何补救措施不受影响的情况下，甲方可在下列情况下向乙方发出书面通知书，提出终止部分或全部合同。

（1）如果乙方未能在合同规定的期限或甲方同意延长的期限内提供部分或全部服务。

（2）如果乙方未能履行合同规定的其它义务。

16．2 如果乙方在履行合同过程中有不正当竞争行为，甲方有权解除合同，并按《中华人民共和国反不正当竞争法》之规定由有关部门追究其法律责任。

17．破产终止合同

17．1 如果乙方丧失履约能力或被宣告破产，甲方可在任何时候以书面形式通知乙方终止合同而不给乙方补偿。该终止合同将不损害或影响甲方已经采取或将要采取任何行动或补救措施的权利。

18．合同转让和分包

18.1 除甲方事先书面同意外，乙方不得转让和分包其应履行的合同义务。

19．合同生效

19．1 本合同在合同各方签字盖章并且甲方收到乙方提供的履约保证金后生效。

19．2 本合同一式三份，甲乙双方各执一份。一份送同级政府采购监管部门备案。

20．合同附件

20．1 本合同附件包括： 招标(采购)文件、投标（响应）文件

20．2 本合同附件与合同具有同等效力。

20．3 合同文件应能相互解释，互为说明。若合同文件之间有矛盾，则以最新的文件为准。

21．合同修改

21．1 除了双方签署书面修改协议，并成为本合同不可分割的一部分之外，本合同条件不得有任何变化或修改。

[合同中心-补充条款列表]

签约各方：

甲方（盖章）：

法定代表人或授权委托人（签章）：

乙方（盖章）：

法定代表人或授权委托人（签章）：

合同签订点:网上签约

第七章　投标文件格式附件

附件 1

投标函（格式）

致____（招标人）_____：

根据贵方为_____ 采购项目（项目编号：_____ ）的投标邀请，签字代表_____（全名职务）经正式授权并代表投标人_____（投标人名称、地址）提交投标文件。

全权代表宣布如下：

（1）我方针对本次项目的投标总价为_____（注明币种，并用文字和数字表示的投标总价）。

（2）我方将按招标文件的规定履行合同责任和义务。

（3）我方已详细研究了全部招标文件，包括招标文件的澄清和修改文件（如果有的话）、参考资料及有关附件，我们已完全理解并接受招标文件的各项规定和要求，对招标文件的合理性、合法性不再有异议。

（4）投标有效期为投标截止之日起 90 个日历日。

（5）我方按照招标文件要求递交投标保证金人民币 0 元整。

（6）如果在规定的开标时间后，我方在投标有效期内撤回投标，投标保证金将被贵方没收。

（7）我方同意提供按照贵方可能要求的与投标有关的一切数据或资料，完全理解贵方不一定要接受最低价的投标或收到的任何投标。

（8）与本投标有关的一切正式往来通讯请寄：

地址：_____　　邮编：_____

电话：_____　　传真：_____

投标人授权代表姓名、职务（印刷体）_____

投标人名称：_____

（公章）：_____

（法定代表人（负责人）签字或盖章）：_____

日期：____年____月____日

授权代表签字：_____

附件 2

法定代表人（负责人）资格证明书

致：_____

姓名：_____ 性别：_____ 年龄：_____ 职务：_____ 身份证号码：_____

系 投标人名称 的法定代表人（负责人）。为 项目名称 （项目编号：_____）项目签署投标文件、进行合同洽谈、签署合同和处理与之有关的一切事务。

特此证明。

投标人名称：

（盖公章）

日期： 年 月 日

注：

1. 本证明书投标人必须提供。此处所述“法定代表人”或“负责人”，须与投标人的“营业执照”上的内容一致。

粘贴法定代表人（负责人）（身份证复印件）

法定代表人（负责人）授权委托书

致：_____

本授权书委托书声明：我_____(姓名)系_____(投标人名称)的法定代表人（负责人）,现授权委托_____(单位名称)的_____(姓名)为我公司代理人，以本公司的名义参加_____项目名称　　（项目编号：_____）的招标活动。代理人在投标过程中所签署的一切文件和处理与之有关的一切事务，我均予以承认。

被授权人无转委托权。

特此委托。

被授权人：_____性别：_____年龄：_____

单位：_____部门：_____职务：_____

投标人名称（盖章）：_____

法定代表人（负责人）（签字或盖章：）_____

日期：_____

注：

1.投标人“法定代表人”或“负责人”参加投标和签署投标文件的不须提供该委托书。

2.此处所述“法定代表人”或“负责人”，须与投标人“营业执照”上的内容一致。

3.所指被授权人即为投标代表人。

粘贴被授权人（身份证复印件）

附件 3

开标一览表（格式）

投标人名称：_____

项目编号：_____

货币单位：

元（人民币）

智联普陀光纤专网安全加固政务信息化购买服务项目（2026 年度）包 1

项目名称	服务周期（年）	拟派项目负责人（姓名）	最终报价(总价、元)

备注：

（1）所有价格均系用人民币表示，单位为元，保留到个数位。

（2）开标一览表内容与投标文件其它部分内容不一致时以开标一览表内容为准。

（3）本招标文件所要求的服务内容、服务期限、工作范围和要求。

（4）投标人应当按照国家和上海市有关行业管理服务收费的相关规定，结合自身服务水平和承受能力进行报价。

投标人：（盖章）

法定代表人（负责人）或其授权委托人：（签字或盖章）

日期：　　年　月　日

附件 4

报价分类表

投标人名称：_____

项目编号：_____

货币单位：元（人民币）

序号	服务名称	需求描述	单价 元/月	小计 元	服务周期/月
1	资产管理服务	区光纤专网核心接入区资产发现服务、入库资产管理服务、待入库资产管理服务、资产画像服务、资产主机资产画像服务、异常资产分析服务、环境要素识别服务			
2	漏洞脆弱性管理服务	区光纤专网核心接入区脆弱性配置服务、扫描任务管理服务、漏洞处置工单生成服务、漏洞利用热度展示服务			
3	安全威胁分析服务	区光纤专网核心接入区威胁事件研判服务、威胁事件研判配置服务、威胁攻击者画像服务、风险行为分析服务			
4	安全事件溯源分析服务	区光纤专网核心接入区溯源流量取证服务、溯源日志搜索服务、威胁狩猎服务			
5	安全威胁监控服务	区光纤专网核心接入区攻击者监控服务、防护资产监控服务、攻击行为监控服务、自动化响应监控服务、监控配置服务、重点事件监控服务、目标 IP 跟踪服务			
6	安全态势感知服务	区光纤专网核心接入区综合态势可视化服务、环境感知服务、威胁态势呈现服务、运维响应态势展示服务、脆弱性态势感知服务、日志审计态势展现服务			
7	安全威胁规则库运营服务	区光纤专网核心接入区预判规则服务、攻击识别规则配置服务、攻击识别实例配置服务、攻击识别规则管理服务、攻击识别规则调试服务、攻击识别防护策略配置服务、攻击识别全局配置服务、攻击识别简易模式自定义规则服务、攻击识别策略配置服务、规则升级服务			
8	漏洞库运营服务	区光纤专网核心接入区漏洞模板管理服务、漏洞分类服务、配置模板管理服务、密码字典管理服务、漏洞库升级服务			
9	流量采集服务	区光纤专网核心接入区及街道接入区 IPV4/IPV6 流量解析服务、VXLAN、MPLS、GRE、VLAN 流量解析服务、常见协议的深度解析服务、工控协议的深度解析服务、物联网协议的深度解析服务、数据库协议的解析服务、应用识别服务			
10	流量还原服务	区光纤专网核心接入区及街道接入区常规协议元数据还原服务、流量中出现的文件进行发现和还原服务			
11	流量威胁检测服务	区光纤专网核心接入区及街道接入区 webshell 检测服务、加密代理识别服务、webshell 加密通信识别服务、钓鱼邮件检测服务、隐蔽隧道检测服务、dga 域名检测服务、			
12	流量风险行为分析服务	区光纤专网核心接入区及街道接入区暴力破解行为检测服务、弱口令行为检测服务、侦查探测行为检测服务、翻墙行为检测服务、主机外联行为检测服务、违规网站行为检测服务、异地登录行为检测服务、			
13	流量留存服务	区光纤专网核心接入区及街道接入区元数据存储服务、原始 pcap 包存储服务、威胁包存储服务、恶意文件存储服务			

14	流量检索服务	区光纤专网核心接入区及街道接入区流量日志查询服务、 流量全局检索服务			
15	设备日志接入服务	区光纤专网核心接入区设备海量日志数据采集服务、保存原始日志数据服务、异构日志格式进行统一化处理服务、保存统一化处理后的日志数据服务、界面配置未识别日志接入服务			
16	设备日志备份恢复服务	区光纤专网核心接入区设备手动或自动备份日志服务、 设置日志存储备份策略服务、备份日志导入查询服务 日志备份至远程服务器服务			
17	设备日志检索服务	区光纤专网核心接入区设备实时日志查询服务、历史日志查询服务、原始日志范式化日志查询服务、自定义查询规则服务、全文检索模糊检索正则检索日志服务			
18	设备日志报表分析服务	区光纤专网核心接入区多种维度统计日志信息服务、 统计分析报表与多种文件格式导出服务			
19	设备日志事件告警服务	区光纤专网核心接入区多源事件关联分析服务、查询实时事件服务、告警抑制服务			
20	设备主机漏洞扫描服务	区光纤专网核心接入区设备主机操作系统、数据库、中间件等进行漏洞扫描服务			
21	设备弱口令漏洞扫描服务	区光纤专网核心接入区设备系统进行弱口令扫描服务			
22	设备漏洞扫描任务管理服务	区光纤专网核心接入区设备已下发任务的列表展示，任务暂停、断点续扫等管理服务、任务参数展示，任务综述信息汇总分析展示，主机信息列表展示服务			
23	设备漏洞报表分析服务	区光纤专网核心接入区设备漏洞报表报表任务下发服务、报表类型选择服务、报表内容设置服务、对比分析服务、任务信息对比服务、漏洞对比服务，脆弱性账号对比服务			
24	设备漏洞验证服务	区光纤专网核心接入区设备对漏洞对取证性质的验证服务、支持漏洞库中标记可验证漏洞服务、漏洞验证漏洞利用原始结果服务			
25	设备漏洞资产管理服务	区光纤专网核心接入区设备资产树对象的资产风险统计分析服务，展示整体资产范围的风险等级、风险评分服务			
26	设备运维权限托管服务	区光纤专网核心接入区高价值设备登录运维和高危命令操作指定级金库授权服务、运维工单管理服务			
27	设备字符运维审计服务	区光纤专网核心接入区设备 Telnet、SSH、Rlogin 等字符运维管理协议服务、密钥和密码方式 SSH 运维登录目标设备服务、对监控到的非法操作实时手工切断服务			
28	设备文件运维审计服务	区光纤专网核心接入区设备 FTP、SFTP、Samba、SCP 等文件运维协议运维管理服务、web 文件插件方式运维目标服务器服务、WEB 界面直接调用 WinSCP、xsftp 等三分工具运维目标设备服务			
29	设备图形运维审计服务	区光纤专网核心接入区设备 RDP、VNC、X11 等图形运维协议运维管理服务、web 图形插件方式运维目标服务器服务、RDP、VNC 客户端软件直接登录堡垒机 MSTSC、Vnc Viewer 等客户端服务			
30	设备数据库运维审计服务	区光纤专网核心接入区设备 Oracle、MS SQL Server、IBM DB2、Sybase、IBM Informix Dynamic Server、MySQL 等数据库类型运维管理服务、数据库图形方式操作审计与字符方式（数据库操作命令级）操作审计服务、数据库操作命令审计定位数据库图			

		形审计服务			
31	入侵检测防护服务	区光纤专网核心接入区入侵规则分类防护服务，制定分类防护策略。包含勒索、挖矿、SQL 注入、XSS 注入、webshell、命令代码执行、内存破坏、类型混淆、反序列化、信息泄露、目录遍历、文件操作漏洞、注入攻击、重定向漏洞、CSRF、僵木蠕、拒绝服务、弱口令、欺骗劫持、扫描类攻击等防护服务、SQL 注入、XSS 注入、webshell 等多种常见的应用层安全威胁抵御服务			
32	DDOS 攻击检测防护服务	区光纤专网核心接入区 DoS/DDoS 攻击防护服务，支持 PING/UDP/SYN/ACK/DNS Reply/DNS Req Flood，支持 TCP Port Scan/UDP Port Scan，支持 PING Sweep，支持 ARP Spoof 以及 HTTP GET/HTTP POST FLood 等常见的 DoS/DDoS 的攻击抵御服务			
33	服务器外联防护服务	区光纤专网核心接入区服务器外联异常告警功能，可以手动添加或自学习服务器外联行为，并以此为基线检测服务器非法外联行为并告警服务			
34	应用管理服务	区光纤专网核心接入区主流的应用程序识别服务，识别不少于 6000 个应用、多种抗逃避或欺骗检测技术识别服务，能检测出的躲避行为包括但不限于：IP 数据包乱序分片、TCP 报文乱序分段、RPC 分片分段、SMB 分片分段、FTP 无效命令混淆、HTTP 响应消息异常、HTML 文件内容多种字符编码混淆、数据流分隔、 协议端口重定位、URL 混淆、shell 代码变形等。			
35	数据泄露防护	敏感数据保护服务，能够识别、阻断、告警超过阈值的敏感数据信息，其中敏感数据包括身份证号、银行卡、电话号码等，且支持自定义敏感数据、关键文件保护服务，能够识别、阻断通过自身的关键文件，以防止非法外传行为。			
36	安全策略管理服务	区光纤专网核心接入区一体化入侵防护策略管理服务、超过 1000 条访问控制策略服务，可基于 IP 地址、端口（单个、多个和范围）、协议、动作（阻断、允许）进行访问策略配置，并可支持是否生成访问控制策略的会话日志生成。			
37	流量管理服务	区光纤专网核心接入区带宽管理服务，可以根据用户、应用、时间及带宽等因素，实现基于应用、面向对象的流量保护策略；全面的流量分析服务，可察看流量完整性分布情况			
38	入侵检测防护服务	区光纤专网街道接入区入侵规则分类防护服务，制定分类防护策略。包含勒索、挖矿、SQL 注入、XSS 注入、webshell、命令代码执行、内存破坏、类型混淆、反序列化、信息泄露、目录遍历、文件操作漏洞、注入攻击、重定向漏洞、CSRF、僵木蠕、拒绝服务、弱口令、欺骗劫持、扫描类攻击等防护服务、SQL 注入、XSS 注入、webshell 等多种常见的应用层安全威胁抵御服务			
39	DDOS 攻击检测防护服务	区光纤专网街道接入区 DoS/DDoS 攻击防护服务，支持 PING/UDP/SYN/ACK/DNS Reply/DNS Req Flood，支持 TCP Port Scan/UDP Port Scan，支持 PING Sweep，支持 ARP Spoof 以及 HTTP GET/HTTP POST FLood 等常见的 DoS/DDoS 的攻击抵御服务			
40	服务器外联防护服务	区光纤专网街道接入区服务器外联异常告警功能，可以手动添加或自学习服务器外联行为，并以此为基线检测服务器非法外联行为并告警服务			

41	应用管理服务	区光纤专网街道接入区主流的应用程序识别服务，识别不少于6000 个应用、多种抗逃避或欺骗检测技术识别服务，能检测出的躲避行为包括但不限于：IP 数据包乱序分片、TCP 报文乱序分段、RPC 分片分段、SMB 分片分段、FTP 无效命令混淆、HTTP 响应消息异常、HTML 文件内容多种字符编码混淆、数据流分隔、 协议端口重定位、URL 混淆、shell 代码变形等。			
42	数据泄露防护	区光纤专网街道接入区敏感数据保护服务，能够识别、阻断、告警超过阈值的敏感数据信息，其中敏感数据包括身份证号、银行卡、电话号码等，且支持自定义敏感数据、关键文件保护服务，能够识别、阻断通过自身的关键文件，以防止非法外传行为。			
43	安全策略管理服务	区光纤专网街道接入区一体化入侵防护策略管理服务、超过1000 条访问控制策略服务，可基于 IP 地址、端口（单个、多个和范围）、协议、动作（阻断、允许）进行访问策略配置，并可支持是否生成访问控制策略的会话日志生成。			
44	流量管理服务	区光纤专网街道接入区带宽管理服务，可以根据用户、应用、时间及带宽等因素，实现基于应用、面向对象的流量保护策略；全面的流量分析服务，可察看流量完整性分布情况			
45	访问控制服务	区光纤专网核心接入区二层协议进行访问控制服务，针对 PPP、QinQ、MPLS 等协议进行屏蔽，对非 IP 协议进行访问控制服务、基于源安全区、目的安全区、源地址、目的地址、源端口、目的端口、协议等，模拟运行直接获得策略的命中信息，并可对命中的策略信息进行编辑服务			
46	应用识别服务	区光纤专网核心接入区应用特征识别库服务，对应用进行识别和控制，应用属性不少于类别、风险等级、标签、详细信息、实现技术等的服务			
47	URL 过滤服务	区光纤专网核心接入区提供云端 URL 分类库，提供 64+种精细分类（广告及弹出窗口、烟酒、匿名网站、艺术、聊天、盗用网站、犯罪活动等）			
48	DNS 过滤服务	区光纤专网核心接入区针对 DNS 的 URL 过滤和分类识别服务			
49	内容过滤服务	区光纤专网核心接入区网页浏览、论坛发帖、电子邮件、即时通讯、文件传输、服务器操作等信息关键字的实时检测和过滤服务			
50	敏感数据发现服务	区光纤专网核心接入区敏感信息过滤服务，对用户的个人隐私信息（手机号、身份证号码、社保号等）泄露进行检测或阻断服务			
51	访问控制服务	区光纤专网街道接入区二层协议进行访问控制服务，针对 PPP、QinQ、MPLS 等协议进行屏蔽，对非 IP 协议进行访问控制服务、基于源安全区、目的安全区、源地址、目的地址、源端口、目的端口、协议等，模拟运行直接获得策略的命中信息，并可对命中的策略信息进行编辑服务			
52	应用识别服务	区光纤专网街道接入区应用特征识别库服务，对应用进行识别和控制，应用属性不少于类别、风险等级、标签、详细信息、实现技术等的服务			
53	URL 过滤服务	区光纤专网街道接入区提供云端 URL 分类库，提供 64+种精细分类（广告及弹出窗口、烟酒、匿名网站、艺术、聊天、盗用网站、犯罪活动等）			

54	DNS 过滤服务	区光纤专网街道接入区针对 DNS 的 URL 过滤和分类识别服务			
55	内容过滤服务	区光纤专网街道接入区网页浏览、论坛发帖、电子邮件、即时通讯、文件传输、服务器操作等信息关键字的实时检测和过滤服务			
56	敏感数据发现服务	区光纤专网街道接入区敏感信息过滤服务，对用户的个人隐私信息（手机号、身份证号码、社保号等）泄露进行检测或阻断服务			
57	边界控制管理服务	区光纤专网核心接入区从 802.1x、PBR（Policy – Based - Routing）、MVG 的各种边界控制服务、利用各种网络控制技术，实现在各种网络环境下适应性，IAC 能够帮助用户快速实现对于内网边界的规划。可以实现基于接入层边界的控制和基于重要资源边界的控制服务			
58	人员认证管理服务	区光纤专网核心接入区本地用户名/密码、Email、Radius、LDAP、AD 域、短信、生物指纹管理服务			
59	设备规范管理服务	区光纤专网核心接入区 IE 控件检查、IE 主页检查、IP/MAC 绑定检查、Windows 防火墙检测、操作系统版本检查、磁盘使用检查、计算机名称检查、垃圾文件检查、杀毒软件检查、网络监听端口检查、网络连接检查、系统补丁检查、系统时间检查、域用户检查、远程桌面检查、P2P 软件检查、必须安装软件检查、必须运行进程检查、禁止安装软件检查、禁止运行进程检查、客户端运行状态检查、系统服务检查、软件授权检查、Guest 来宾账户检查、WSUS 更新配置检查、密码策略设置检查、屏幕保护设置检查、弱口令账户检查、网卡绑定检查、系统共享资源检查服务			
60	操作行为管理服务	区光纤专网核心接入区用户各种操作的监控和响应服务：ip 更改、违规软件使用、必须安装软件随意卸载、安全检查违规；计算机设备的统一维护管理服务：类别管理、设备信息管理、软件分发、服务管理、终端探测；任务管控服务：终端软件安装包分发、终端批处理脚本分发、终端消息通知分发服务			
61	视角报表管理服务	区光纤专网核心接入区资源报表、违规操作记录、检查结果报表、入网安全检查评估报告、用户认证记录报表、排行统计报表、资产统计报表			
62	边界控制管理服务	区光纤专网街道接入区从 802.1x、PBR（Policy – Based - Routing）、MVG 的各种边界控制服务、利用各种网络控制技术，实现在各种网络环境下适应性，IAC 能够帮助用户快速实现对于内网边界的规划。可以实现基于接入层边界的控制和基于重要资源边界的控制服务			
63	人员认证管理服务	区光纤专网街道接入区本地用户名/密码、Email、Radius、LDAP、AD 域、短信、生物指纹管理服务			
64	设备规范管理服务	区光纤专网街道接入区 IE 控件检查、IE 主页检查、IP/MAC 绑定检查、Windows 防火墙检测、操作系统版本检查、磁盘使用检查、计算机名称检查、垃圾文件检查、杀毒软件检查、网络监听端口检查、网络连接检查、系统补丁检查、系统时间检查、域用户检查、远程桌面检查、P2P 软件检查、必须安装软件检查、必须运行进程检查、禁止安装软件检查、禁止运行进程检查、客户端运行状态检查、系统服务检查、软件授权检查、Guest 来宾账户检查、WSUS 更新配置检查、密码策略设置检查、屏			

		幕保护设置检查、弱口令账户检查、网卡绑定检查、系统共享资源检查服务			
65	操作行为管理服务	区光纤专网街道接入区用户各种操作的监控和响应服务：ip 更改、违规软件使用、必须安装软件随意卸载、安全检查违规；计算机设备的统一维护管理服务：类别管理、设备信息管理、软件分发、服务管理、终端探测；任务管控服务：终端软件安装包分发、终端批处理脚本分发、终端消息通知分发服务			
66	视角报表管理服务	区光纤专网街道接入区资源报表、违规操作记录、检查结果报表、入网安全检查评估报告、用户认证记录报表、排行统计报表、资产统计报表			
67	代码审计服务	代码缺陷自动分析服务；代码缺陷人工审计服务 ；代码缺陷加固及复测服务			
68	整体安全管理制度优化更新服务	区光纤专网安全管理制度优化与更新；区光纤专网应用安全接入规范编制和更新。			
69	安全意识和技术培训服务	网络安全法律法规解读培训；网络安全等级保护 2.0 解读培训；个人安全意识培训；网络黑客攻击攻防技能培训；重保和护网专项培训。			
70	应急预案体系和应急演练服务	应急响应保障制度体系优化和修订；应急演练场景和方案优化设计与编制；定期应急或攻防演练			
71	网络安全应急响应服务	安全威胁事件应急响应处置服务；安全威胁事件研判与溯源服务；安全威胁事件总结建议报告服务。			
72	重大活动、护网期间安全保障专项服务	重保、护网安全保障方案设计；重保、护网安全防护布防措施实施；重保、护网安全防护自查服务；重保、护网安全应急演练；重保、护网期间现场安全值守和预警服务；重保、护网期间现场安全事件应急响应和处置服务。			
73	安全检测系统服务	挂马检测服务			
74	安全检测系统服务	黑链检测服务			
75	安全检测系统服务	钓鱼检测服务			
76	资产探测系统服务	资产探测服务			
77	网络病毒监测预警系统服务	病毒入侵监测服务；防病毒检测服务；威胁情报检测服务；病毒攻击监测防护服务；安全行为管理服务。			
78	脆弱性扫描系统服务	脆弱性扫描服务			
79	威胁发现设备服务	威胁监测服务；威胁分析服务。			
83	总报价（RNB）：				

注：投标人根据企业实力自报单价及折扣率，一旦中标后服务单价及折扣率为结算价。

投标人授权代表签字：_____

投标人（公章）：_____

日期：_____年_____月_____日

附件 5

资格条件响应表

项目名称：
项目编号：
包号：

项目内容	具备的条件说明	投标检查项（响应内容说明(是/否)）	详细内容所对应电子投标文件名称	备注
法定基本条件	1、符合《中华人民共和国政府采购法》第二十二条规定的条件：营业执照（或事业单位、社会团体法人证书)、税务登记证(若为三证合一的仅需提供营业执照）符合要求； 2、提供财务状况及税收、社会保障资金缴纳情况声明函； 3、未被列入“信用中国”网站(www.creditchina.gov.cn)失信被执行人名单、重大税收违法案件当事人名单和中国政府采购网(www.ccgp.gov.cn)政府采购严重违法失信行为记录名单的供应商。			
联合投标	本项目不接受联合投标。			
法定代表人（负责人）授权	1、在投标文件由法定代表人(单位负责人）授权代表签字（或盖章）的情况下，应按招标文件规定格式提供法定代表人（单位负责人）授权委托书； 2、按招标文件要求提供法定代表人（单位负责人)、被授权人身份证复印件。			

投标人授权代表签字：_____

投标人（公章）：_____

日期：_____年_____月_____日

符合性要求响应表

项目名称：
项目编号：
包号：

项目内容	具备的条件说明	投标检查项（响应内容说明(是/否)）	详细内容所对应电子投标文件名称	备注
投标文件内容、密封、签署等要求	符合招标文件规定： 1、投标文件按招标文件规定格式提供《投标函》、《开标一览表》、《资格条件响应表》及《符合性要求响应表》； 2、投标文件按招标文件要求密封（适用于纸质投标项目），电子投标文件须经电子加密（投标文件上传成功后，系统即自动加密）。			
投标有效期	不少于 90 天。			
投标报价	1、不得进行选择性报价（投标报价应是唯一的，招标文件要求提供备选方案的除外）； 2、不得进行可变的或者附有条件的投标报价； 3、投标报价不得超出招标文件标明的采购预算金额及项目最高限价； 4、投标报价出现前后不一致，投标人未按招标文件规定确认投标报价的修正； 5、投标报价明显低于其他通过符合性审查投标人的报价，投标人不能证明其报价合理性的； 6、投标报价有缺漏项的，缺漏项部分的报价按照其他投标人相同项的最高报价计算，计算出的缺漏项部分报价不得超过投标报价的 10%。			
合同履约期限	本项目服务周期为合同签订后一年。			
付款方法	签订服务合同支付合同金额 20%费用，服务期满半年后支付合同金额 50%费用，服务期满后支付合同金额 30%尾款。			
合同转让与分包	合同不得转让与分包。			
公平竞争和诚实信用	不得存在腐败、欺诈或其他严重违背公平竞争和诚实信用原则、妨碍其他投标人的竞争、损害采购人或者其他投标人的合法权益、扰乱政府采购正常秩序的行为。			
关联供应商	1、单位负责人或法定代表人为同一人，或者存在控股、管理关系的不同供应商，参加同一包件或者未划分包件的同一项目投标的，相关投标均无效。 2、与本项目采购集中采购机构的负责人为同一人或者存在直接控股和管理关系的供应商不得参加本次			

	政府采购活动。 3、为本项目提供整体设计、规范编制或者项目管理、监理、检测等服务的供应商不得参加本次政府采购活动。			

投标人授权代表签字：_____

投标人（公章）：_____

日期：_____年_____月_____日

附件 6

参加政府采购活动前 3 年内在经营活动中没有重大违法记录的书面声明

致：_____（招标人）_____

我公司承诺在参加本项目政府采购活动前三年内，在经营活动中没有重大违法记录，遵守国家其他有关的法律、法规和管理办法。

特此声明。

（注：重大违法记录是指供应商因违法经营受到刑事处罚或者责令停产停业、吊销许可证或者执照、较大数额罚款等行政处罚。

供应商在参加政府采购活动前 3 年内因违法经营被禁止在一定期限内参加政府采购活动，期限届满的，可以参加政府采购活动。）

投标人授权代表签字：_____

投标人（公章）：_____

日期：_____年_____月_____日

附件 7

近三年完成同类业绩一览表

年份	委托单位	项目名称	规模	合同金额（万元）	附件页码		证明联系方式
					中标通知书	合同	

注：扫描件中需体现合同的签约主体、项目名称及内容、合同金额、签订时间等合同要素的相关内容，需加盖业主公章，否则将不予认可。

投标人授权代表签字：_____

投标人（公章）：_____

日期：_____年_____月_____日

附件 8

中小企业声明函（服务）

本公司（联合体）郑重声明，根据《政府采购促进中小企业发展管理办法》（财库〔2020〕46 号）的规定，本公司（联合体）参加（单位名称）的（项目名称）采购活动，投标单位须符合政策要求的中小企业（或者：服务全部由符合政策要求的中小企业承接）。相关企业（含联合体中的中小企业、签订分包意向协议的中小企业）的具体情况如下：

1.（标的名称），属于（信息传输业）；承建（承接）企业为（企业名称），从业人员_____人，营业收入为_____万元，资产总额为____万元[1]，属于（中型企业、小型企业、微型企业）；

……

以上企业，不属于大企业的分支机构，不存在控股股东为大企业的情形，也不存在与大企业的负责人为同一人的情形。

本企业对上述声明内容的真实性负责。如有虚假，将依法承担相应责任。

企业名称（盖章）：

日期：

注：从业人员、营业收入、资产总额填报上一年度数据，无上一年度数据的新成立企业可不填报。

注：各行业划型标准：

（一）农、林、牧、渔业。营业收入 20000 万元以下的为中小微型企业。其中，营业收入 500 万元及以上的为中型企业，营业收入 50 万元及以上的为小型企业，营业收入 50 万元以下的为微型企业。

（二）工业（包括采矿业，制造业，电力、热力、燃气及水生产和供应业）。从业人员 1000 人以下或营业收入 40000 万元以下的为中小微型企业。其中，从业人员 300 人及以上，且营业收入 2000 万元及以上的为中型企业；从业人员 20 人及以上，且营业收入 300 万元及以上的为小型企业；从业人员 20 人以下或营业收入 300 万元以下的为微型企业。

（三）建筑业。营业收入 80000 万元以下或资产总额 80000 万元以下的为中小微型企业。其中，营业收入 6000 万元及以上，且资产总额 5000 万元及以上的为中型企业；营业收入 300 万元及以上，且资产总额 300 万元及以上的为小型企业；营业收入 300 万元以下或资产总额 300 万元以下的为微型企业。

（四）批发业。从业人员 200 人以下或营业收入 40000 万元以下的为中小微型企业。其中，从业人员 20 人及以上，且营业收入 5000 万元及以上的为中型企业；从业人员 5 人及以上，且营业收入 1000 万元及以上的为小型企业；从业人员 5 人以下或营业收入 1000 万元以下的为微型企业。

（五）零售业。从业人员 300 人以下或营业收入 20000 万元以下的为中小微型企业。其中，从业人员 50 人及以上，且营业收入 500 万元及以上的为中型企业；从业人员 10 人及以上，且营业收入 100 万元及以上的为小型企业；从业人员 10 人以下或营业收入 100 万元以下的为微型企业。

（六）交通运输业（不含铁路运输业）。从业人员 1000 人以下或营业收入 30000 万元以下的为中小微型企业。其中，从业人员 300 人及以上，且营业收入 3000 万元及以上的为中型企业；从业人员 20 人及以上，且营业收入 200 万元及以上的为小型企业；从业人员 20 人以下或营业收入 200 万元以下的为微型企业。

（七）仓储业。从业人员 200 人以下或营业收入 30000 万元以下的为中小微型企业。其中，从业人员 100 人及以上，且营业收入 1000 万元及以上的为中型企业；从业人员 20 人及以上，且营业收入 100 万元及以上的为小型企业；从业人员 20 人以下或营业收入 100 万元以下的为微型企业。

（八）邮政业。从业人员 1000 人以下或营业收入 30000 万元以下的为中小微型企业。其中，从业人员 300 人及以上，且营业收入 2000 万元及以上的为中型企业；从业人员 20 人及以上，且营业收入 100 万元及以上的为小型企业；从业人员 20 人以下或营业收入 100 万元以下的为微型企业。

（九）住宿业。从业人员 300 人以下或营业收入 10000 万元以下的为中小微型企业。其中，从业人员 100 人及以上，且营业收入 2000 万元及以上的为中型企业；从业人员 10 人及以上，且营业收入 100 万元及以上的为小型企业；从业人员 10 人以下或营业收入 100 万元以下的为微型企业。

（十）餐饮业。从业人员 300 人以下或营业收入 10000 万元以下的为中小微型企业。其中，从业人员 100 人及以上，且营业收入 2000 万元及以上的为中型企业；从业人员 10 人及以上，且营业收入 100 万元及以上的为小型企业；从业人员 10 人以下或营业收入 100 万元以下的为微型企业。

（十一）信息传输业（包括电信、互联网和相关服务）。从业人员 2000 人以下或营业收入 100000 万元以下的为中小微型企业。其中，从业人员 100 人及以上，且营业收入 1000 万元及以上的为中型企业；从业人员 10 人及以上，且营业收入 100 万元及以上的为小型企业；从业人员 10 人以下或营业收入 100 万元以下的为微型企业。

（十二）软件和信息技术服务业。从业人员 300 人以下或营业收入 10000 万元以下的为中小微型企业。其中，从业人员 100 人及以上，且营业收入 1000 万元及以上的为中型企业；从业人员 10 人及以上，且营业收入 50 万元及以上的为小型企业；从业人员 10 人以下或营业收入 50 万元以下的为微型企业。

（十三）房地产开发经营。营业收入 200000 万元以下或资产总额 10000 万元以下的为中小微型企业。其中，营业收入 1000 万元及以上，且资产总额 5000 万元及以上的为中型企业；营业收入 100 万元及以上，且资产总额 2000 万元及以上的为小型企业；营业收入 100 万元以下或资产总额 2000 万元以下的为微型企业。

（十四）物业管理。从业人员 1000 人以下或营业收入 5000 万元以下的为中小微型企业。其中，从业人 300 人及以上，且营业收入 1000 万元及以上的为中型企业；从业人员 100 人及以上，且营业收入 500 万元及以上的为小型企业；从业人员 100 人以下或营业收入 500 万元以下的为微型企业。

（十五）租赁和商务服务业。从业人员 300 人以下或资产总额 120000 万元以下的为中小微型企业。其中，从业人员 100 人及以上，且资产总额 8000 万元及以上的为中型企业；从业人员 10 人及以上，且资产总额 100 万元及以上的为小型企业；从业人员 10 人以下或资产总额 100 万元以下的为微型企业。

（十六）其他未列明行业（包括科学研究和技术服务业，水利、环境和公共设施管理业，居民服务、修理和其他服务业，社会工作，文化、体育和娱乐业等）。从业人员 300 人以下的为中小微型企业。其中，从业人员 100 人及以上的为中型企业；从业人员 10 人及以上的为小型企业；从业人员 10 人以下的为微型企业。

附件 9

财务状况及税收、社会保障资金

缴纳情况声明函

我方（供应商名称）符合《中华人民共和国政府采购法》第二十二条第一款第（二）项、第（四）项规定条件，具体包括：

1、具有健全的财务会计制度；

2.有依法缴纳税收和社会保障资金的良好记录。

特此声明。

我方对上述声明的真实性负责。如有虚假，将依法承担相应责任。

供应商名称（公章）

日期：

附件 10

残疾人福利性单位声明函

本单位郑重声明，根据《财政部 民政部 中国残疾人联合会关于促进残疾人就业政府采购政策的通知》（财库〔2017〕 141 号）的规定，本单位为符合条件的残疾人福利性单位，且本单位参加_____单位的_____项目采购活动提供本单位制造的货物（由本单位承担工程/提供服务），或者提供其他残疾人福利性单位制造的货物（不包括使用非残疾人福利性单位注册商标的货物）。

本单位对上述声明的真实性负责。如有虚假，将依法承担相应责任。

单位名称（盖章）：

日　期：

说明：根据《财政部民政部中国残疾人联合会关于促进残疾人就业政府采购政策的通 知》享受政府采购支持政策的残疾人福利性单位应当同时满足以下条件：

（1）安置的残疾人占本单位在职职工人数的比例不低于 25%（含 25%），并且安置的残 疾人人数不少于 10 人（含 10 人）；

（2）依法与安置的每位残疾人签订了一年以上（含一年）的劳动合同或服务协议；

（3）为安置的每位残疾人按月足额缴纳了基本养老保险、基本医疗保险、失业保险、工伤保险和生育保险等社会保险费；

（4）通过银行等金融机构向安置的每位残疾人，按月支付了不低于单位所在区县适用的经省级人民政府批准的月最低工资标准的工资；

（5）提供本单位制造的货物、承担的工程或者服务（以下简称产品），或者提供其他残 疾人福利性单位制造的货物（不包括使用非残疾人福利性单位注册商标的货物）。

如投标人不符合残疾人福利性单位条件，无需填写本声明。

附件 11

投标货物/服务报告
（包括但不限于以下内容）

包括但不限于以下内容：

1、针对本项目的总体要求理解；

2、针对本项目的具体实施方案；

3、针对本项目服务方案的具体内容和实施措施；

4、针对本项目的规章制度与应急预案；

5、针对本项目的日常管理服务措施及承诺；

6、针对本项目的服务质量保障措施及人员培训计划；

7、投标人的组织构架、内部管理规章制度等；

8、拟投入本项目人员安排（人员配置一览表）及项目经理及主要管理人员一览表；

9、承担同类项目情况及业主好评证明（以提供的中标通知书或合同复印件等证明材料为准）；

10、针对本项目提供的其他技术性资料、资格资料以及需要说明的其他事项。

附件 11-1

项目经理说明表

项目名称：

姓名		出生年月		文化程度		毕业时间	
毕业院校和专业			从事项目管理工作年限			联系方式	
执业资格			技术职称			聘任时间	
主要工作经历： 主要管理服务项目： 主要工作特点： 主要工作成绩： 胜任本项目经理的理由： 本项目经理管理思路和工作安排： 本项目经理每周现场工作时间：							
更换项目经理的方案							
更换项目经理的前提和客观原因： 更换项目经理的原则： 替代项目经理应达到的能力和资格： 替代项目经理应满足本项目管理服务的工作方案：							

投标人授权代表签字：

投标人（公章）：

日期：_____年_____月_____日

附件 11-2

投入项目的管理人员配备及相关工作经历、资质汇总表

项目名称：

项目组成员姓名	年龄	在项目组中的岗位	学历和毕业时间	职称及 资质	进入本单位时间	相关工作经历	
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							
……							

投标人授权代表签字：_____

投标人（公章）：_____

日期：_____年_____月_____日

附件 11-3

岗位、人员设置及要求表

项目名称：

类别	岗位	人数		岗位职责
	项目经理	1		全面负责

投标人授权代表签字：_____

投标人（公章）：_____

日期：_____年_____月_____日