



招 标 文 件

项目名称：2024 年局网络安全保障和局机关信息化系
统运维服务项目

招标编号：TC241953H/G24-1003

采 购 人：国家知识产权局

采购代理机构：中招国际招标有限公司

日期：2024 年 5 月

目 录

第一章	招标公告	2
第二章	投标须知前附表	4
第三章	投标人须知	8
第四章	项目采购合同	28
第五章	附件——投标文件格式	72
第六章	评标办法	102
第七章	采购需求	110

第一章 招标公告

招标公告

中招国际招标有限公司受国家知识产权局的委托，对 2024 年局网络安全保障和局机关信息化系统运维服务项目 进行国内公开招标。现邀请合格投标人参加投标。

一、项目基本情况

1.项目名称：2024 年局网络安全保障和局机关信息化系统运维服务项目

2.项目编号：TC241953H/G24-1003

3.资金来源：财政资金；

财政批复金额：预算金额为¥1175.14 万元，人民币：壹仟壹佰柒拾伍万壹仟肆佰元整。投标价格超过预算金额的投标将无效。

4.本次招标采购需求如下：为保障国家知识产权局网络安全工作的正常开展，确保局机关有关信息化系统的安全稳定运行，启动本项目。项目内容包括面向全局各部门单位，提供互联网网络安全技术监测、网络攻防演练、统一网络安全监测平台运营等服务，开展网络安全通报预警、远程应急指导、自查整改、宣传培训等工作；负责局机关信息化系统运维服务范围内相关系统的网络安全工作，包括网络安全云防护、病毒防护、统一访问控制、应急处置、重要时期保障、等保测评、IPv6 转换等服务。对局机关 9 个信息化系统提供包括基础环境运维、应用系统运维等相关服务，以及局机关用户使用办公终端设备的维护服务。

5.合同履行期限：2024 年 6 月 17 日至 2025 年 6 月 16 日。

二、投标人资格要求：

1. 满足《中华人民共和国政府采购法》第二十二条规定；

2. 落实政府采购政策需满足的资格要求：

(1) 本项目为专门面向中小企业预留份额采购项目，预留中小企业份额应占总金额不低于 30%，其中预留给小微企业的比例不低于 60%。

(2) 供应商被“信用中国”网站（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的，不得参与本项目的政府采购活动。

3. 本项目的特定资格要求：无。

4. 本项目不接受联合体投标。

三、其他事项

1.招标文件售价（人民币）：500 元，售后不退。

2.招标文件发售时间：2024 年 5 月 20 日至 2024 年 5 月 27 日，每天上午 09：00 至下午 17：00（北京时间）。

标书发售网址：<http://www.365trade.com.cn>。（详见特别告知）

纸质版文件请至北京市海淀区学院南路 62 号中关村资本大厦 9 层 911A 领取。

3.递交投标文件截止时间：2024 年 6 月 11 日下午 14：00（北京时间）。

4.投标文件的递交：北京市海淀区学院南路 62 号中关村资本大厦 6 层会议室第七会议室。

5.开标时间：2024 年 6 月 11 日下午 14：00（北京时间）。

6.开标地点：北京市海淀区学院南路 62 号中关村资本大厦 6 层会议室第七会议室。

7.公告日期：5 个工作日

8.落实的政府采购政策：

本项目落实节约能源、保护环境、促进中小企业发展、支持监狱企业发展、促进残疾人就业、扶持不发达地区和少数民族地区等政府采购政策。

9. 特别告知

各潜在投标人：

本项目采取网上发售电子版招标文件和线下同步售标方式，电子版文件和纸质版文件内容一致，现将有关注意事项特别告知如下：

凡有意购买文件的潜在投标人/资格预审申请人，请前往“中招联合招标采购平台”进行投标人注册（网址：<http://www.365trade.com.cn>）、购买并下载电子版招标文件/资格预审文件。投标人需将**标书款汇款底单**在报名阶段作为报名审核资料在系统中提交**购标上传附件**，标书款如需开具增值税专用发票请一并提交可编辑版（非图片形式）**专票信息和邮寄地址**，如不提交专票信息则默认开具普通发票。代理机构工作人员会在审查无误后通过购买申请，投标人即可自行在网站下载招标文件。

潜在投标人/资格预审申请人请在标书发售截止时间前登录中招联合招标采购平台完成注册、标书购买操作，否则将无法保证获取电子版招标文件或资格预审文件。如遇平台操作问题请咨询平台客服 010-86397110。

纸质版文件请至北京市海淀区学院南路 62 号院中关村资本大厦 911A 领取。纸

质版文件与电子版文件内容一致。

标书款汇款信息如下：

账户名称：中招国际招标有限公司

开户行：中国工商银行北京海淀支行营业部

账号：0200049619200362296

10. 采购代理机构：中招国际招标有限公司

地 址：北京市海淀区学院南路 62 号中关村资本大厦 911A

电 话：010-61954143/62108043

传 真：010-61954100

电子信箱：liuhuimin@cntcitic.com.cn

联 系 人：刘慧敏、邓嘉莹、蒋雪娜、陈思佳、张涵睿

第二章 投标须知前附表

投标须知前附表

本表是关于服务采购的具体资料，是对投标人须知的具体补充和修改，如有矛盾，应以本资料表为准。

	编 制 内 容
1.1	采购人名称：国家知识产权局 采购人地址：北京市海淀区蓟门桥西土城路 6 号 联系人和联系电话：俞骁航、陶怀轮 010-62088129、62083364
1.3.3	本项目是否属于政府购买服务项目： <u>是</u>
1.3.4	投标人资格要求：见第一章招标公告“投标人资格要求”
1.4.1	本项目采购标的对应的中小企业划分标准所属行业为：软件和信息技术服务业。
1.4.2	是否为专门面向中小企业采购： <u>否</u>
1.4.3	是否为面向中小企业采购预留份额： <u>是</u> ，未达到下面比例的投标将被认定为投标无效。 √要求供应商以分包形式参加采购活动，且分包企业中中小企业承担部分达到比例为不低于 30%，其中预留给小微企业的比例不低于 60%。 投标人为大型企业分包规则：分包企业中中小企业承担部分达到比例为不低于 30%，其中预留给小微企业的比例不低于 60%； 投标人为中型企业分包规则：分包企业中预留给小微企业的比例不低于 18%。
1.5	是否允许联合体投标： <u>否</u>
1.5.8	联合体的其他资格要求：无
2.2	资金来源：财政资金。 预算金额：预算金额为¥1175.14 万元，人民币：壹仟壹佰柒拾伍万壹仟肆佰元整。投标价格超过预算金额的投标将无效。
8.1	如投标人对多个包进行投标，可以中标 <u>1</u> 包
9.1	提供投标人的近半年内的任意 1 个月纳税和社保记录； 在法规范围内不需提供的，应做书面说明和提交证明文件。
12	保证金形式：投标保证金应当以支票、汇票、本票或者金融机构、担保机构出具的保函等非现金形式提交。 保证金数额：壹拾万元

	<p>保证金收款人：中招国际招标有限公司</p> <p>若采用电汇方式缴纳保证金，在线购买电子版招标文件的投标人，在线支付标书款并下载招标文件后，进入中招联合电子招标采购平台“缴纳保证金”功能模块，填写相关信息后通过平台自动获取保证金收款账户信息。请投标人按此信息将保证金电汇或银行转账至指定账户（该账号为虚拟账号，仅针对本投标人本项目分包有效，对于其他投标人、其他项目或分包无效）。</p> <p>中招国际招标有限公司委托中招联合信息股份有限公司及平安银行股份有限公司北京分行办理投标保证金收、退、转及结账、结算等相关业务。保证金办理相关问题请咨询中招联合（010-86397110）。</p>
13.1	投标有效期：自投标截止日期起，投标文件有效期为 <u>90</u> 个自然日。
14	<p>投标文件：</p> <p>第一部分投标文件：正本： <u>1</u> 份、副本： <u>3</u> 份；</p> <p>第二部分投标文件：正本： <u>1</u> 份、副本： <u>3</u> 份；</p> <p>除上述文件外，还须密封递交投标文件电子文档 <u>1</u> 份（电子文档须提供包含 Word 或 Excel 可编辑版，和正本签字盖章版的 pdf 扫描版，存储在 U 盘 中提交）。</p>
16.1	<p>投标截止时间及开标时间：见第一章招标公告</p> <p>开标地点：见第一章招标公告</p>
19.2	信用查询时间：递交投标文件截止时间后一个小时。
23.2	评审方法：采用综合评分法进行评审。
31.1	是否提交履约保证金：否。
33	中标供应商须参照《招标代理服务收费管理暂行办法》（国家计委计价格〔2002〕1980号）和《国家发改委关于降低部分建设项目收费标准规范收费行为等有关问题的通知》（发改价格〔2011〕534号）规定标准执行，在领取中标通知书时向中招国际招标有限公司一次性支付中标服务费。
34.4	<p>政府采购信用担保机构：</p> <p>所有政府采购项目的信用担保专业的担保公司</p> <p>中国投融资担保股份有限公司</p> <p>地址：北京市海淀区西三环北路 100 号光耀东方写字楼 9 层</p> <p>联系电话：010-88822888 传真：010-68437040</p> <p>电子邮箱：ztbxf@guaranty.com.cn</p> <p>北京市政府采购项目增加的信用担保公司</p> <p>1.北京首创融资担保有限责任公司</p>

	地址：北京市西城区闹市口大街一号长安兴融中心四号楼三层 联系电话： 58528799 传真：58528448 电子邮箱：yangyang@scdb.com.cn； chenhaoran@scdb.com.cn
	2.北京中关村科技融资担保有限公司 地址：北京市海淀区中关村南大街乙 12 号天作国际大厦 A 座 28 层 联系电话： 59705600-6950 传真：59705606 电子邮箱： li_yuchu@126.com
	3.本项目采购人本级和上级财政部门政府采购有关规定增加的担保机构。
35.3	反腐倡廉监督电话： <u>010-62108085</u>
37.2	针对同一采购程序环节的质疑次数： <input checked="" type="checkbox"/> 一次性提出 <input type="checkbox"/> 多次提出
备注	无

第三章 投标人须知

投标人须知

一 说 明

1. 采购人、采购代理机构及投标人

- 1.1 采购人：是指依法进行政府采购的国家机构、事业单位、团体组织。
- 1.2 采购代理机构：是指在中国政府采购网或其省级分网站网上登记的代理机构。本次招标的采购代理机构为中招国际招标有限公司。
- 1.3 投标人：是指响应招标、参加投标竞争的法人、非法人组织或者自然人。
潜在投标人：以招标文件规定的方式获取本项目招标文件的法人、非法人组织或者自然人。投标人须满足以下条件：
 - 1.3.1 在中华人民共和国境内注册，能够独立承担民事责任，有生产或供应能力的本国供应商，包括法人、非法人组织或者自然人。
 - 1.3.2 具备《中华人民共和国政府采购法》第二十二条关于供应商条件的规定，遵守国家、本项目采购人本级和上级财政部门政府采购的有关规定。
 - 1.3.3 对于政府购买服务项目，公益一类事业单位、使用事业单位编制且由财政拨款保障的群团组织，不得作为承接主体。本项目是否属于政府购买服务项目，见投标人须知资料表。
 - 1.3.4 以招标文件规定的方式获得了本项目的招标文件，并符合投标须知前附表中规定的其他要求。
- 1.4 投标人提供的服务由中小企业承接，即提供服务的人员为中小企业依照《中华人民共和国劳动合同法》订立劳动合同的从业人员，享受中小企业扶持政策。投标人根据《工业和信息化部、国家统计局、国家发展和改革委员会、财政部关于印发中小企业划型标准规定的通知》（工信部联企业[2011]300号）确定企业类型；也可在工业和信息化部网站（<https://www.miit.gov.cn/>）的“中小企业规模类型自测小程序”自助查询到企业类型。
 - 1.4.1 投标标的所属行业见投标须知前附表。
 - 1.4.2 若投标须知前附表中写明专门面向中小企业采购的，如投标人所提供的服务为非中小企业承接，其投标将被认定为投标无效。承接企业如为监狱企业或残疾人福利性单位的，视同为小型、微型企业。

- 1.4.3 本项目是否面向中小企业采购预留份额、措施及比例见投标须知前附表，未达到上述比例的投标将被认定为投标无效。承接企业如为监狱企业或残疾人福利性单位的，视同为小型、微型企业。
- 1.4.4 享受中小企业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。
- 1.5 如投标须知前附表中允许联合体投标，对联合体规定如下：
- 1.5.1 两个以上供应商可以组成一个投标联合体，以一个投标人的身份投标。
- 1.5.2 联合体各方均应符合《中华人民共和国政府采购法》第二十二条规定的条件，遵守国家、本项目采购人本级和上级财政部门政府采购的有关规定。
- 1.5.3 采购人根据采购项目对投标人的特殊要求，联合体中至少应当有一方符合相关规定。
- 1.5.4 联合体各方应签订共同投标协议，明确约定联合体各方承担的工作和相应的责任，并将共同投标协议连同投标文件一并提交招标采购单位。
- 1.5.5 大中型企业、其他自然人、法人或者非法人组织与小型、微型企业组成联合体共同参加投标，共同投标协议中应写明小型、微型企业的协议合同金额占到共同投标协议投标总金额的比例。联合体各方均为中小企业的，联合体视同中小企业。其中，联合体各方均为小微企业的，联合体视同小微企业。
- 1.5.6 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，按照资质等级较低的供应商确定资质等级。
- 1.5.7 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本项目投标，否则相关投标将被认定为**投标无效**。
- 1.5.8 对联合体投标的其他资格要求见投标须知前附表。
- 1.6 单位负责人为同一人或者存在直接控股、管理关系的不同供应商，其投标将被认定为**投标无效**。
- 1.7 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，其投标将被认定为**投标无效**。

2. 资金来源

- 2.1 本项目的采购人已获得足以支付本次招标后所签订的合同项下的资金（包括财政性资金和本项目采购中无法与财政性资金分割的非财政性资金）。
- 2.2 项目预算金额和分项或分包最高限价见投标须知前附表。
- 2.3 投标人报价超过招标文件规定的预算金额或者最高限价的，其投标将被认定为**投标无效**。

3. 投标费用

投标人应承担所有与准备和参加投标有关的费用，不论投标的结果如何，采购人和采购代理机构均无承担的义务和责任。

4. 适用法律

本项目采购人、采购代理机构、投标人、评标委员会的相关行为均受《中华人民共和国政府采购法》、《中华人民共和国政府采购法实施条例》及本项目本级和上级财政部门政府采购有关规定的约束和保护。

二 招标文件

5. 招标文件构成

- 5.1 要求提供服务及伴随货物及工程的内容及详细技术需求、投标须知和合同条件等在招标文件中均有说明。

招标文件共七章，共一册。内容如下：

第一章 招标公告

第二章 投标须知前附表

第三章 投标人须知

第四章 项目采购合同

第五章 附件——投标文件格式

第六章 评标办法

第七章 采购需求

- 5.2 招标文件中有不一致的，有澄清的部分以最终的澄清更正内容为准；未

澄清的，以投标须知前附表为准；投标须知前附表不涉及的内容，以编排在后的最后描述为准。

5.3 投标人应认真阅读招标文件所有的事项、格式、条款和技术规范等。如投标文件没有对招标文件的实质性要求做出响应，其投标将被认定为投标无效。

5.4 现场考察或者答疑会及相关事项见投标须知前附表。

5.5 原则上采购人、采购代理机构不要求投标人提供样品。除仅凭书面方式不能准确描述采购需求，或者需要对样品进行主观判断以确认是否满足采购需求等特殊情况除外。

6. 招标文件的澄清与修改

6.1 采购人可主动地或在解答投标人提出的澄清问题时对招标文件进行澄清或修改。采购代理机构将以发布澄清（更正）公告的方式，澄清或修改招标文件，澄清或修改内容作为招标文件的组成部分。

6.2 澄清或者修改的内容可能影响投标文件编制的，采购代理机构将以书面形式通知所有获取招标文件的潜在投标人，并对其具有约束力。投标人在收到上述通知后，应及时向采购代理机构确认。投标人未回复的，视同已知晓澄清或者修改的内容。

因潜在投标人原因或通讯线路故障导致通知逾期送达或无法送达，采购代理机构不因此承担任何责任，有关的招标采购活动可以继续有效进行。

7. 投标截止时间的顺延

为使投标人有足够的时间对招标文件的澄清或者修改部分进行研究而准备投标或因其他原因，采购人将依法决定是否顺延投标截止时间。

三 投标文件的编制

8. 投标范围及投标文件中标准和计量单位的使用

8.1 投标人可对招标文件中一个或几个分包服务进行投标，除非在投标须知前附表中另有规定。

8.2 投标人应当对所投分包招标文件中“服务及其伴随的货物和工程”所列的所有内容进行投标，如仅响应分包中的部分内容，其该包投标将被认定为

投标无效。

8.3 无论招标文件中是否要求，投标人所投服务及其伴随的货物和工程均应符合国家强制性标准。

8.4 除招标文件中有特殊要求外，投标文件中所使用的计量单位，应采用中华人民共和国法定计量单位。

9. 投标文件构成

9.1 投标文件由“第一部分开标一览表及资格证明文件”和“第二部分商务及技术文件”组成。投标人应完整地按照招标文件提供的投标文件格式及要求编写投标文件。其中第一部分开标一览表及资格证明文件中“依法缴纳税收和社会保障资金的记录”具体要求详见投标须知前附表。投标文件中资格审查和符合性审查涉及的事项不满足招标文件要求的，其投标将被认定为投标无效。

9.2 上述文件应按照招标文件的规定签署和盖公章或经公章授权的其他单位章（以下统称公章）。采用公章授权方式的，应当在投标文件第一部分附公章授权书（格式自定）。

10. 证明服务的合格性和符合招标文件规定的文件的其他文件。

10.1 投标人应提交证明文件，证明其拟提供的合同项下的服务的合格性符合招标文件规定。该证明文件是投标文件的一部分。

10.2 前款所述的证明文件，可以是文字资料、图纸和数据。

10.3 本条所指证明文件不得为对招标文件相关部分的文字、图标复制。

11. 投标报价

11.1 投标人的报价应当包括满足本次招标全部采购需求所应提供的服务，以及伴随的货物和工程。所有投标均应以人民币报价投标人的投标报价应遵守《中华人民共和国价格法》。

11.2 投标人应在投标分项报价表上标明服务内容、伴随的货物和工程的价格（如适用）和总价，并由法定代表人或委托代理人签署。

11.3 投标人所报的各分项投标单价在合同履行过程中是固定不变的，不得以任何理由予以变更。任何包含价格调整要求的投标，其投标将被认定为投标无效。

11.4 本项目只能有一个投标报价。招标采购单位不接受具有附加条件的报价。

12. 投标保证金

12.1 投标人应提供投标须知前附表中规定的投标保证金，并作为其投标的一部分。

12.2 投标保证金是为了保护采购人和采购代理机构免遭因投标人的行为蒙受损失而要求的。

下列任何情况发生，投标保证金不予退还：

- (1) 在投标有效期内，投标人撤回投标的；
- (2) 中标人不按本须知第 30 条的规定与采购人签订合同的；
- (3) 中标人不按本须知第 31 条的规定提交履约保证金的；
- (4) 中标人不按本须知第 32 条的规定缴纳中标服务费；
- (5) 存在串通投标情形的；
- (6) 存在向采购人、代理机构或评标专家行贿事实的。

12.3 投标保证金可采用下列形式之一：

北京地区：电汇、支票，以及投标须知前附表中可接受的其他形式；

外埠：电汇，以及投标须知前附表中可接受的其他形式；

接受符合财政部门规定的投标担保函正本。

12.4 凡没有根据本须知 12.1 和第 12.3 条的规定，随附投标保证金的投标，将被视为无效投标被拒绝。

采用电汇形式提交投标保证金的，一般可以实时入账。采用支票形式的，投标人则应充分考虑支票入账时间，以确保投标保证金能按时进入指定账户。根据银行信息交换和付款时间，支票从递交至实际入账一般需要 4-5 个工作日。如投标人未及时提交支票或支票不符合银行委托收款要求（如污损、折叠、胶装等），导致投标保证金不能按时进入指定账户的，将按照招标文件的第 22.2 条相关规定处理。

12.5 联合体投标的，可以由联合体中的一方或者共同提交投标保证金，以一方名义提交投标保证金的，对联合体各方均具有约束力。

12.6 采购代理机构应在中标人应在与采购人签订合同之日起 5 个工作日内及时办理投标保证金无息退还手续。

未中标投标人的投标保证金将在中标通知书发出之日暨中标结果公告公布之日起5个工作日内，采购代理机构办理无息退还投标保证金手续，因投标人自身原因导致无法及时退还的，采购人或采购代理机构将不承担资金占用费。

政府采购投标信用担保函正本不予退回。

13. 投标有效期

13.1 投标应在规定的提交投标文件截止之日起，按照投标须知前附表中规定时间内保持有效。投标有效期不满足要求的投标，将被视为**无效投标**被拒绝。

13.2 采购人或采购代理机构可根据实际情况，在原投标有效期截止之前，要求投标人延长投标文件的有效期。接受该要求的投标人将不会被要求和允许修正其投标，且本须知中有关投标保证金的要求须在延长的有效期内继续有效。投标人也可以拒绝延长投标有效期的要求，其投标保证金将不会被没收。上述要求和答复都应以书面形式提交。

14. 投标文件的签署及规定

14.1 投标人应按投标须知前附表中的规定准备和递交投标文件资格证明文件、商务和技术文件正本、副本和电子文档，每份资格证明文件、商务和技术文件须清楚地标明“正本”或“副本”。若正本和副本不符，以正本为准。资格证明文件需要单独成册，商务和技术部分投标人可自主装订。若项目为电子标则按电子标要求执行。

14.2 投标文件的正本需打印或用不褪色墨水书写，并由投标人的法定代表人或经其正式授权的代表按招标文件规定在投标文件上签字并加盖单位印章。授权代表须持有书面的“法定代表人授权书”（标准格式附后），并将其附在投标文件中。如对投标文件进行了修改，则应由投标人的法定代表人或经其正式授权的代表在每一修改处签字。投标文件的副本可采用正本的复印件。若项目为电子标则按电子标要求执行。

14.3 所有投标文件采用不可拆装的胶订方式装订，否则将被视为**无效投标**被拒绝。若项目为电子标则按电子标要求执行。

14.4 任何行间插字、涂改和增删，必须由投标人的法定代表人或经其正式授

权的代表签字或盖章后才有效。

- 14.5 投标文件因字迹潦草、表达不清或装订不当所引起的后果由投标人负责。

四 投标文件的递交

15. 投标文件的密封和标记

- 15.1 投标文件封皮正面标明“正本”或“副本”字样。

- 15.2 所有包装封皮和信封上均应：

(1) 注明招标公告或投标邀请书中指明的项目名称、招标编号、投标人名称和“在（投标须知前附表中规定开标时间）之前不得启封”的字样。

(2) 在封口处加盖投标人公章，或由法定代表人（或其授权代表）签字。

- 15.3 如果投标人未按上述要求密封，或者资格证明文件密封装订在其他投标文件中，其投标将作为**无效投标**被否决。

16. 投标截止期

- 16.1 投标人应在招标公告或投标邀请书中规定的截止日期和时间内，派人将投标文件递交到招标公告或投标邀请书中规定的地址。

- 16.2 采购人和采购代理机构有权按本须知的规定，通过修改招标文件，延长投标截止期。在此情况下，采购人、采购代理机构和投标人受投标截止期制约的所有权利和义务均应延长至新的截止期。

- 16.3 采购人和采购代理机构将拒绝并原封退回在投标截止期后送达的任何投标文件。

17. 投标文件的接收、修改与撤回

- 17.1 采购人或者采购代理机构收到投标文件后，应当如实记载投标文件的送达时间和密封情况，并向投标人出具以下签收回执。

接收投标文件回执单

招标编号			
项目名称			
投标人名称			
递交时间		投标文件密封情况	
接收单位	中招国际招标有限公司		
接收人签字			

投标人不足 3 家的，不得开封。

- 17.2 递交投标文件以后，如果投标人要进行修改，须提出书面通知并在投标截止时间前送达开标地点，投标人对投标文件的修改通知应按本须知规定编制、签署、密封、标记。采购人和采购代理机构将予以接收，并视为投标文件的组成部分。

递交投标文件以后，如果投标人要进行撤回的，须提出书面通知并在投标截止时间前送达开标地点，采购人和采购代理机构将予以接受。

- 17.3 在投标截止时间之后，投标人不得对其投标文件做任何修改。

- 17.4 除投标人不足 3 家未开标外，采购人和采购代理机构对所接收投标文件概不退回。

五 开标及评标

18. 开标

- 18.1 采购人和采购代理机构将按投标须知前附表中规定的开标时间和地点组织公开开标并邀请所有投标人代表参加。

- 18.2 开标时，由投标人或其推选的代表检查自己或所代表的投标文件的密封情况，经记录后，由采购人或采购代理机构当众拆封、宣读投标人名称、投标价格及招标文件规定的内容。对于投标人在投标截止期前递交的投标声明，在开标时当众宣读，评标时有效。

未宣读的投标价格、价格折扣、备选方案等实质内容，评标时不予承认。

- 18.3 采购人或采购代理机构将对开标过程进行记录，由参加开标的各投标人代表和相关工作人员签字确认，并存档备查。

投标人未派代表参加开标的，视同投标人认可开标结果。

- 18.4 投标人代表对开标过程和开标记录有疑义，以及认为开标现场采购人、采购代理机构相关工作人员有需要回避的情形的，应当场提出询问或者回避申请。

19. 资格审查及组建评标委员会

- 19.1 采购人或采购代理机构依据法律法规和招标文件中规定的内容，对投标人的资格进行审查。未通过资格审查的投标人不进入评标；通过资格审

查的投标人少于三家的，不进行评标。

19.2 采购人或采购代理机构将按投标须知前附表中规定的时间查询投标人的信用记录。

19.2.1 投标人在中国政府采购网（www.ccgp.gov.cn）被列入政府采购严重违法失信行为记录名单，或在“信用中国”网站（www.creditchina.gov.cn）被列入失信被执行人、重大税收违法案件当事人名单，以及存在《中华人民共和国政府采购法实施条例》第十九条规定的行政处罚记录，投标将被认定为投标无效。

以联合体形式参加投标的，联合体任何成员存在以上不良信用记录的，联合体投标将被认定为投标无效。

19.2.2 采购人或采购代理机构经办人将查询网页打印、签字并存档备查。投标人不良信用记录以采购人或采购代理机构查询结果为准。投标人自行提供的与网站信息不一致的其他证明材料亦不作为资格审查依据。

在本招标文件规定的查询时间之外，网站信息发生的任何变更均不作为资格审查依据。

19.3 按照《中华人民共和国政府采购法》、《中华人民共和国政府采购法实施条例》及本项目本级和上级财政部门的有关规定依法组建的评标委员会，负责评标工作。

20. 投标文件的符合性检查与澄清

20.1 符合性检查是指依据招标文件的规定，从商务和技术角度对投标文件的有效性和完整性进行审查，以确定是否对招标文件的实质性要求做出响应。

20.2 投标文件的澄清

20.2.1 在评标期间，评标委员会将以书面方式要求投标人对其投标文件中含义不明确、对同类问题表述不一致或者有明显文字和计算错误的内容，以及评标委员会认为投标人的报价明显低于其他通过符合性审查投标人的报价，有可能影响履约的情况作必要的澄清、说明或补正。投标人的澄清、说明或补正应在评标委员会规定的时间内以书面方式进行，并不得超出投标文件范围或者改变投标文件的实质性内容。

20.2.2 投标人的澄清、说明或补正将作为投标文件的一部分。

20.2.3 投标文件报价出现前后不一致的，按照下列规定修正：

（一）投标文件中开标一览表（报价表）内容与投标文件中相应内容不一致的，以开标一览表（报价表）为准；

（二）大写金额和小写金额不一致的，以大写金额为准；

（三）单价金额小数点或者百分比有明显错位的，以开标一览表的总价为准，并修改单价；

（四）总价金额与按单价汇总金额不一致的，以单价金额计算结果为准。

同时出现两种以上不一致的，按照前款规定的顺序修正。修正后的报价按照第 20.2 条的规定经投标人确认后产生约束力，投标人不确认的，将被视为**无效投标**被拒绝。

对不同文字文本投标文件的解释发生异议的，以中文文本为准。

20.3 投标人所投服务所伴随的货物如被列入财政部与国家主管部门颁发的节能产品或环境标志产品品目清单或无线局域网产品清单，应提供处于有效期之内的认证证书等相关证明，在评标时予以优先采购，具体优先采购办法见第 6 章评标方法和标准。

如采购人所投服务所伴随的货物为政府强制采购的产品，投标人所投产品应属于品目清单的强制采购部分。投标人应提供有效期内的认证证书，否则其投标将被认定为投标无效。

如采购人所投服务所伴随的货物属于信息安全产品的，投标人所投产品应为经国家认证的信息安全产品，并提供由中国信息安全认证中心按国家标准认证颁发的有效认证证书，否则其投标将被认定为投标无效。

20.4 政府采购货物、工程和服务项目中涉及商品包装和快递包装的，供应商提供产品及相关快递服务的具体包装要求请详见《商品包装政府采购需求标准（试行）》、《快递包装政府采购需求标准（试行）》。

21. 投标偏离

对于投标文件中不构成实质性偏差的不正规、不一致或不规则，评标委员会可以接受，但这种接受不能损坏或影响任何投标人的相对排序。

22. 无效投标

22.1 在比较与评价之前，根据本须知的规定，评标委员会要审查每份投标文件是否实质上响应了招标文件的要求。实质上响应的投标应该是与招标文件要求的全部条款、条件和规格相符，没有重大偏离的投标。对关键条款的偏离、保留和反对，将被认为是实质上的偏离，属于**无效投标**被拒绝。评标委员会决定投标的响应性只根据招标文件要求、投标文件内容及财政主管部门指定相关信息发布媒体。

22.2 实质上没有响应招标文件要求的投标将被作为**无效投标**被拒绝。投标人不得通过修正或撤销不符合要求的偏离或保留从而使其投标成为实质上响应的投标。如发现下列情况之一的，其投标将被作为**无效投标**被拒绝：

- (1) 未按招标文件规定的形式和金额交纳投标保证金的；
- (2) 未按照招标文件规定要求签署、盖章的；
- (3) 未满足招标文件中技术条款的实质性要求；
- (4) 属于串通投标，或者依法被视为串通投标；
- (5) 投标文件含有采购人不能接受的附加条件的；
- (6) 评标委员会认为投标人的报价明显低于其他通过符合性检查投标人的报价，有可能影响履约的，且投标人未按照规定证明其报价合理性的；
- (7) 属于招标文件规定的其他无效投标情形；
- (8) 不符合法规和招标文件中规定的其他实质性要求的。

23. 比较与评价

23.1 经符合性检查合格的投标文件，评标委员会将根据招标文件确定的评标方法和标准，对其技术部分和商务部分作进一步的比较和评价。

23.2 评标严格按照招标文件的要求和条件进行。根据实际情况，在投标须知前附表中规定采用下列一种评标方法，详细评标标准见招标文件第六章：

- (1) 最低评标价法，是指投标文件满足招标文件全部实质性要求，且投标报价最低的投标人为中标候选人的评标方法。
- (2) 综合评分法，是指投标文件满足招标文件全部实质性要求，且按照

评审因素的量化指标评审得分最高的投标人为中标候选人的评标方法。

- 23.3 根据《政府采购促进中小企业发展管理办法》（财库[2020]46号）、《财政部司法部关于政府采购支持监狱企业发展有关问题的通知》（财库〔2014〕68号）和《三部门联合发布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，对满足价格扣除条件且在投标文件中提交了《中小企业声明函》或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的投标人，其投标报价扣除10%-20%后参与评审。

24. 废标

出现下列情形之一，将导致项目废标即本项目的所有投标被拒绝：

- （1）符合专业条件的供应商或者对招标文件做实质性响应的供应商不足三家；
- （2）出现影响采购公正的违法、违规行为的；
- （3）投标人的报价均超过了采购预算，采购人不能支付的；
- （4）因重大变故，采购任务取消的。

25. 保密原则

- 25.1 评标将在严格保密的情况下进行。
- 25.2 政府采购评审专家应当遵守评审工作纪律，不得泄露评审文件、评审情况和评审中获悉的商业秘密。
- 25.3 投标人试图影响采购人、采购代理机构和评标委员会的任何活动，将导致其**投标被拒绝**，并承担相应的法律责任。

六 确定中标

26. 中标候选人的确定原则及标准

除评标委员会受采购人委托直接确定中标人的情形外，对实质上响应招标文件的投标人按下列方法进行排序，确定中标候选人：

- （1）采用最低评标价法的，除了算数修正和落实政府采购政策需进行的价格扣除外，不对投标人的投标价格进行任何调整。评标结果按投标报价由低到高顺序排列。报价相同的并列。

(2) 采用综合评分法的，评标结果按评审后得分由高到低顺序排列。得分相同的，按投标报价由低到高顺序排列。得分与投标报价均相同的，按技术指标优劣排列。

27. 确定中标候选人和中标人

评标委员会将根据评标标准，按投标须知前附表中规定数量推荐中标候选人；或根据采购人的委托，直接确定中标人。

28. 发出中标通知书

在投标有效期内，中标人确定后，采购人或者采购代理机构发布中标公告。在公告中标结果的同时，向中标人发出中标通知书，中标通知书是合同的组成部分。

29. 告知招标结果

在公告中标结果的同时，告知未通过资格审查投标人未通过的原因；采用综合评分法评审的，还将告知未中标人本人的评审得分和排序。

中标公告发布后，各投标人登录中招联合招标采购平台：<http://www.365trade.com.cn> 获取结果通知书。

30. 签订合同

30.1 中标人应当自发出中标通知书之日起 30 日内，与采购人签订合同。

30.2 招标文件、中标人的投标文件及其澄清文件等，均为签订合同的依据。

30.3 中标人拒绝与采购人签订合同的，采购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人，也可以重新开展政府采购活动。

30.4 当出现法规规定的中标无效或中标结果无效情形时，采购人可与排名下一位的中标候选人另行签订合同，或依法重新开展采购活动。

31. 履约保证金

31.1 中标人应按照投标须知前附表规定的金额、形式和时间向采购人缴纳履约保证金（如采用保函形式，格式见本章附件 1）。经采购人同意，中标人也可以自愿采用其他履约保证金的提供方式。

31.2 中标人除 31.1 规定的情形外，也可以按照财政部门的规定，向采购人提供合格的履约担保函（格式见本章附件 2）。

- 31.3 如果中标人没有按照上述第 30 条或 31.1 条的规定执行,将视为放弃中标资格,中标人的投标保证金将被没收。在此情况下,采购人可确定下一候选人为中标人,也可以重新开展政府采购活动。

32.预付款

- 32.1 政府采购合同签订后,采购人向中标人预先支付部分合同款项,预付款金额按照采购人当年财政预算情况执行。

33. 招标代理费

本项目是否由中标人向采购代理机构支付招标代理费,按照投标须知前附表规定执行。

34. 政府采购信用担保

- 34.1 中小型企业投标人可以自由按照财政部门的规定,采用投标担保、履约担保和融资担保。
- 34.2 投标人递交的投标担保函和履约担保函应符合本招标文件的规定。
- 34.3 投标人可以采取融资担保的形式为政府采购项目履约进行融资。
- 34.4 合格的政府采购专业信用担保公司名单见第二章投标须知前附表。

35. 廉洁自律规定

- 35.1 采购代理机构工作人员不得以不正当手段获取政府采购代理业务,不得与采购人、供应商恶意串通。
- 35.2 采购代理机构工作人员不得接受采购人或者供应商组织的宴请、旅游、娱乐,不得收受礼品、现金、有价证券等,不得向采购人或者供应商报销应当由个人承担的费用。
- 35.3 为强化内部监督机制,供应商可按投标须知前附表中代理机构的反腐倡廉监督电话/邮箱,反映采购代理机构的廉洁自律等问题。

36. 人员回避

潜在投标人认为招标文件使自己的权益受到损害的,投标人认为采购人员及其相关人员有法律法规所列与其他供应商有利害关系的,均可以向采购人或采购代理机构书面提出回避申请,并说明理由。

37. 质疑的提出与接收

- 37.1 投标人认为招标文件、招标过程和中标结果使自己的权益受到损害的,

可以根据《中华人民共和国政府采购法》、《中华人民共和国政府采购法实施条例》和《政府采购质疑和投诉办法》的有关规定，依法向采购人或其委托的采购代理机构提出质疑。

- 37.2 质疑供应商应按照财政部制定的《政府采购质疑函范本》格式（可从财政部官方网站下载）和《政府采购质疑和投诉办法》的要求，在法定质疑期内以书面形式提出质疑，针对同一采购程序环节的质疑次数应符合投标须知前附表的规定。

超出法定质疑期提交的质疑将被拒绝。

重复或分次提出的、内容或形式不符合《政府采购质疑和投诉办法》的，质疑供应商将依法承担不利后果。

- 37.3 采购代理机构质疑函接收部门、联系电话和通讯地址

联系部门：中招国际招标有限公司综合发展部

联系电话：62108164、62108058

通讯地址：北京市海淀区学院南路 62 号院中关村资本大厦

附件 1：履约保证金保函（格式）

（中标后开具）

致：（买方名称）

_____号合同履行保函

本保函作为贵方与（卖方名称）（以下简称卖方）于_____年_____月_____日就_____项目（以下简称项目）项下提供（货物名称）（以下简称货物）签订的（合同号）号合同的履约保函。

（出具保函的银行名称）（以下简称银行）无条件地、不可撤销地具结保证本行、其继承人和受让人无追索地向贵方以（货币名称）支付总额不超过（货币数量），即相当于合同价格的_____%，并以此约定如下：

- 1.只要贵方确定卖方未能忠实地履行所有合同文件的规定和双方此后一致同意的修改、补充和变动，包括更改和/或修补贵方认为有缺陷的货物（以下简称违约），无论卖方有任何反对，本行将凭贵方关于卖方违约说明的书面通知，立即按贵方提出的累计总额不超过上述金额的款项和按贵方通知规定的方式付给贵方。
- 2.本保函项下的任何支付应为免税和净值。对于现有或将来的税收、关税、收费、费用扣减或预提税款，不论这些款项是何种性质和由谁征收，都不应从本保函项下的支付中扣除。
- 3.本保函的条款构成本行无条件的、不可撤销的直接责任。对即将履行的合同条款的任何变更、贵方在时间上的宽限、或由贵方采取的如果没有本款可能免除本行责任的任何其它行为，均不能解除或免除本行在本保函项下的责任。
- 4.本保函在本合同规定的保证期期满前完全有效。

谨启

出具保函银行名称：_____

签字人姓名和职务：_____

签字人签名：_____

公章：_____

附件 2：履约担保函格式

(如采用政府采购信用担保形式时使用)

政府采购履约担保函（项目用）

编号：

_____（采购人）：

鉴于你方与_____（以下简称供应商）于____年__月__日签定编号为_____的《_____政府采购合同》（以下简称主合同），且依据该合同的约定，供应商应在____年____月____日前向你方交纳履约保证金，且可以履约担保函的形式交纳履约保证金。应供应商的申请，我方以保证的方式向你方提供如下履约保证金担保：

一、保证责任的情形及保证金额

（一）在供应商出现下列情形之一时，我方承担保证责任：

1. 将中标项目转让给他人，或者在投标文件中未说明，且未经采购招标机构同意，将中标项目分包给他人的；

2. 主合同约定的应当缴纳履约保证金的情形：

（1）未按主合同约定的质量、数量和期限供应货物/提供服务/完成工程的；

（2）_____。

（二）我方的保证范围是主合同约定的合同价款总额的_____%数额为元（大写_____），币种为_____。（即主合同履约保证金金额）

二、保证的方式及保证期间

我方保证的方式为：连带责任保证。

我方保证的期间为：自本合同生效之日起至供应商按照主合同约定的供货/完工期限届满后____日内。

如果供应商未按主合同约定向贵方供应货物/提供服务/完成工程的，由我方在保证金额内向你方支付上述款项。

三、承担保证责任的程序

1. 你方要求我方承担保证责任的，应在本保函保证期间内向我方发出书面索赔通知。索赔通知应写明要求索赔的金额，支付款项应到达的帐号。并附有证明供应商违约事实的证明材料。

如果你方与供应商因货物质量问题产生争议，你方还需同时提供_____部门出具的质量检测报告，或经诉讼（仲裁）程序裁决后的裁决书、调解书，本保证人即按照检测结果或裁决书、调解书决定是否承担保证责任。

2. 我方收到你方的书面索赔通知及相应证明材料，在____个工作日内进行核定后按照本保函的承诺承担保证责任。

四、保证责任的终止

1. 保证期间届满你方未向我方书面主张保证责任的，自保证期间届满次日起，我方保证责任自动终止。保证期间届满前，主合同约定的货物\工程\服务全部验收合格的，自验收合格日起，我方保证责任自动终止。

2. 我方按照本保函向你方履行了保证责任后，自我方向你方支付款项（支付款项从我方账户划出）之日起，保证责任即终止。

3. 按照法律法规的规定或出现应终止我方保证责任的其它情形的，我方在本保函项下的保证责任亦终止。

4. 你方与供应商修改主合同，加重我方保证责任的，我方对加重部分不承担保证责任，但该等修改事先经我方书面同意的除外；你方与供应商修改主合同履行期限，我方保证期间仍依修改前的履行期限计算，但该等修改事先经我方书面同意的除外。

五、免责条款

1. 因你方违反主合同约定致使供应商不能履行义务的，我方不承担保证责任。

2. 依照法律法规的规定或你方与供应商的另行约定，全部或者部分免除供应商应缴纳的保证金义务的，我方亦免除相应的保证责任。

3. 因不可抗力造成供应商不能履行供货义务的，我方不承担保证责任。

六、争议的解决

因本保函发生的纠纷，由你我双方协商解决，协商不成的，通过诉讼程序解决，诉讼管辖地法院为_____法院。

七、保函的生效

本保函自我方加盖公章之日起生效。

保证人：（公章）

年 月 日

第四章 项目采购合同

2024 年局网络安全保障和局机关 信息化系统运维服务项目 合同

甲方：国家知识产权局

乙方：XXXXXX

签约地点：北京

注：本合同为中小企业预留合同

国家知识产权局（以下简称“甲方”）与 XXXXXX（以下简称“乙方”）根据《中华人民共和国政府采购法》、《中华人民共和国民法典》等相关法律法规以及本项目招标文件的规定，就“2024 年局网络安全保障和局机关信息化系统运维服务项目”的相关工作，同意按下述条款和条件签署本项目合同（以下简称“合同”）。

一、基本原则

乙方应坚持用户利益第一的原则，全面承接甲方信息化运行维护服务统筹管理及执行层面的工作，做好网络安全保障相关服务，不断加强内部管理，提高服务水平及服务意识，指派专人或成立专门部门负责甲方信息化运行维护的人员投入服务、配套服务和协调工作，保障甲方信息化系统的稳定运行。

二、服务范围及内容

乙方应整体承接甲方信息化系统运行维护和网络安全保障工作。保障甲方有关信息化基础设施及应用系统的高效、安全、稳定运行，为甲方履行政府职能，对社会公众服务提供信息化基础性保障。服务内容包括两部分：局机关信息化运行维护保障服务、全局网络安全保障服务。主要服务范围及内容概括如下，具体服务范围及内容详见：附件 B：工作说明书。

（一）局机关信息化运行维护保障服务：包括甲方委托维护范围内系统的基础环境运维、应用系统集成运维、网络安全保障相关服务以及办公终端设备维护服务。

本项目信息化维护服务范围包括：全国专利管理信息平台、专利代理管理系统、全国专利代理师资格考试考务系统、知识产权数据资源公共服务系统、公文智能交换管理系统、离退休干部工作管理信息系统、老干部活动中心信息化项目、外观设计专利检索公共服务系统、档案管理系统和公共服务网，共 10 个信息化系统及基础环境。

1.基础环境运维：乙方需对服务器、网络设备、安全设备等硬件设备开展定期巡检、日常维护及故障处理，提供不低于原功能性能的设备备件及配件，

根据现场紧急状况提供备机；对操作系统、数据库、中间件等软件进行版本升级、日常维护及故障处理，保障系统软件正常运行；提供内外网各一条连接局蓟门桥办公区至老干部活动中心的 10M 专线链路，保障链路的正常通信使用及网络安全。提供知识产权数据资源公共服务系统运行所需云平台租用，并负责公有云产品日常运行维护，保障系统运行环境安全。

2.应用系统集成运维：乙方需对应用系统故障提供热线电话、远程在线诊断和故障排除、现场响应等支持服务；提供每月预防性现场巡检服务；对系统基础资源进行监控和管理，及时掌握系统资源现状、运行状态、配置信息、可用性等信息；重要敏感时期按需提供现场值守服务；提供系统整合、优化方案建议并配合实施，提供用户咨询等服务。

3.局机关信息化网络安全保障服务：乙方需对运维范围内系统开展网络安全技术防护、统一访问控制、病毒防护、网络安全应急处置、重要时期保障、等保测评、IPv6 转换、网站 HTTPS 安全证书、电子政务外网网络安全保障等服务，保障相关系统的可靠、稳定、安全运行。

4.办公终端设备维护服务：乙方需提供甲方局机关用户使用的台式计算机、便携式计算机、打印机、传真机等办公终端设备的现场维护和维修；负责鼠标、键盘等配件，打印机硒鼓、墨盒等耗材及 IP 电话等的配发及维护。

（二）全局网络安全保障服务：乙方需面向甲方全局范围内，提供网络安全通报、应急、检查、培训及宣传等服务；负责网络安全监测平台运营、网络攻防演练、网络安全监测技术等服务。

三、服务期限

本项目运维整体服务期限：2024 年 6 月 17 日至 2025 年 6 月 16 日。各项服务内容具体服务期限详见附件 B：工作说明书

四、合同金额及付款方式

（一）合同总额为¥XXXXXXX 元，人民币大写：XXXXXXX。

（二）支付方式：

1.首付款：合同签订后，甲方在收到乙方提交的首付款技术服务发票后 30 日内向乙方支付合同首付款：¥4,119,200 元，人民币大写：肆佰壹拾壹万玖仟贰佰元整。

2.尾款：合同履行期限届满后，双方完成最终验收并出具验收报告，甲方在收到乙方提供的尾款技术服务发票后 30 日内向乙方支付合同尾款：¥XXXXXX 元，人民币大写：XXXXXX。

（三）如乙方根据本合同规定有责任向甲方支付违约金或其它赔偿时，甲方在书面通知乙方后，将从合同款中扣减。

（四）甲方每次付款前乙方须向甲方出具等额的中华人民共和国法定发票，乙方出示的发票应包含甲方应向乙方支付的各项款项所有金额，并应包含足够详细的内容，使甲方能够确定金额的准确性，甲方根据乙方提供的合格发票支付相应款项，如乙方提交的发票不正确，甲方可延迟付款（但不承担违约责任）。因财政国库支付受限时，结算支付相应顺延，甲方不承担违约责任，但应当及时通知乙方。障碍消除后，甲方应当及时恢复支付。乙方不得因此延迟、暂停、拒绝、终止义务的履行

（五）乙方账户信息

帐户名称：XXXXXX

开户银行：XXXXXX

帐号：XXXXXX

若乙方支付信息发生变更，须提前 20 个工作日书面通知甲方。否则，甲方按照按照上述银行账户付款或由此延期支付的，责任由乙方自行承担。

五、双方的责任和义务

（一）甲方的责任和义务

甲方完全理解乙方完成本项目需要甲方的全力支持和及时配合，因此甲方将指定专人或团队作为代表与乙方配合，定期与乙方代表对服务状况进行沟通。甲方应向乙方提供本合同所需的信息或给乙方提供获取信息的条件。

（二）乙方的责任和义务

乙方根据本合同及其本合同的附件中的条款履行义务，接受相关条款的约

束，并承担合同约定的相应义务。乙方及服务人员在项目合同执行期间需严格遵守甲方制定的工作规定和安全生产管理制度。乙方具体责任如下：

1.乙方服务过程中应当遵循甲方所颁布的相关管理规则并执行局信息化建设的有关规定或决议。

2.完善乙方相关工作规范，提交甲方审核，并按甲方要求修改，包括：

制定运行服务工作的服务流程和规范；

根据各系统的特点制定应急预案；

制定故障上报制度及流程；

制定详细的工作岗位说明书；

制定甲方要求的其它工作规范；

乙方应配合做好重要敏感时期网络安全保障工作，制定特殊情况下，相关系统的正常运行的保障计划。

3.规范服务

乙方工作人员对用户进行服务时应当明示身份，规范服务用语，配备统一标识。

乙方应指定技术联系人并提供联系方式，负责协调联系跨处室或跨部门的工作。

4.对甲方其它业务应用系统服务部门服务工作给予督促、监督、配合。

5.对涉及的设备及系统建立服务、运行档案；并以应用系统为主线理出相关设备、软件文档。

6.服务队伍

乙方应为甲方配备熟悉甲方系统环境的技术服务支持团队，并指派专人负责协调完成各种技术服务。

六、服务总体要求

1.维护职责范围

乙方需负责整体承接范围内信息化系统的运行维护及整体网络安全保障工作，根据我局网络安全和信息化相关管理制度要求，制定运维保障、应急处置等各类制度、规范、及技术标准，并贯彻实施，保障有关信息化基础设施及应

用系统的高效、安全、稳定运行，为我局履行政府职能，对社会公众服务提供信息化支撑保障。乙方需建立运维流程，进行日常监控和故障记录，保障设备、系统软件和应用系统正常工作，做到“事前监控、事中掌控、事后追踪”。完成各类故障处理、信息统计、配置管理、项目配合等工作。乙方需负责详细清理盘点甲方委托维护范围内信息化系统的基本情况，建立系统底数台账并及时更新。

2.维护时间要求

乙方整体服务需提供 7×24 小时电话技术支持，30 分钟内响应，根据设备和系统的重要性，提供不同级别的现场服务，具体服务指标明细详见附件 B：工作说明书。

3. 系统可用性要求

系统非连续正常运行时间要求，核心系统不超过 2 小时、重要系统不超过 4 小时、一般系统不超过 6 小时，全年系统非正常运行中断不得超过 3 次。

4. 服务方式要求

乙方需提供热线、远程、现场以及 Email 和传真支持服务。根据设备和系统的重要性，提供不同级别的现场巡检服务。按照附件 B：工作说明书提供不同级别的驻场值守服务。

5.人员要求

在整体服务期间，乙方需提供不少于____人驻场服务团队，北京驻场人员中包括乙方在甲方北京办公地点派驻不少于____人项目管理团队，并需要保持团队稳定性。乙方需派至少两名项目经理且具有与本项目类似领域的项目管理工作 8 年及以上经验，具有 CISP 证书且具有副高级（含）以上专业技术任职资格或同等资质（包括取得副研究员（含）、高级工程师（含）以上职称）。

未经甲方同意,项目经理和核心项目技术人员不做变更。

七、违约责任

1.甲方的违约责任：

甲方不按合同约定付款的，视为违约，乙方有权不向甲方提供条款六中约定的技术支持与服务。

2.乙方的违约责任：

乙方违背合同条款二、五或未能按照合同条款六中约定向甲方提供合乎甲方标准的技术支持与服务（具体服务内容及标准详见附件 B：工作说明书），视为违约，甲方有权将此视为技术支持和服务中断，并保留进一步向乙方索赔由于技术支持和服务中断给甲方造成的损失的权利。对于技术支持和服务中断，每中断一次，扣除合同价款中对应该类服务款项的 1‰作为违约金。

由于乙方违反合同约定，并造成甲方用户的无法正常使用各系统（后台系统及业务应用系统）且在规定恢复时间以内无法解决的，视为违约。依照影响面的大小，违约金具体执行标准如下表：

影响面（以无法正常使用的用户数计量）	违约金比例（合同价款中对应服务的该类款项的千分数）
20 个以内	1‰
20 个以上 50 个以内	2‰
50 个以上 200 个以内	4‰
200 个以上 1000 个以内	10‰
1000 个以上 5000 个以内	50‰

3. 当违约行为发生后，违约金额达到合同总金额的 10%，甲方有权解除本合同。甲方未全部付清项目价款的，则甲方有权直接从应付款项中直接扣除相应违约金；违约金超出未支付款项的部分，由乙方在收到通知后 10 日内补足。如违约金额仍不足以赔偿甲方因技术支持和服务中断所遭受的实际直接损失，甲方有权要求乙方以实际直接损失价值进行赔偿，包括但不限于：甲方直接经济利益的减损、可得利益损失、甲方支付的调查取证费、公证费、评估费、鉴定费、诉讼费、保全费、 律师代理费、咨询费、执行费、差旅费以及甲方向第三方支付的赔偿款、向行政机关缴纳的罚款等。

八、验收

（一）合同期满 10 个工作日内，乙方应向甲方提出验收请求并提交验收文档。

（二）验收文档应包括：

乙方需提供系统运维服务周报、月报、季报、年报，记录系统运行、资源使用、故障处置、巡检情况和维护记录等，按月提供统一监测平台运行统计分析报告，对于重大故障或安全事件，提交专项处置报告。提供重要敏感时期安全保障情况报告、网络安全等级保护测评报告、攻防演练专项报告等。服务内容及服务标准的要求，需严格按照附件 B：工作说明书提供。

（三）验收要求：

在上述第（一）条和第（二）条完成情形下甲方组织验收，验收合格后由双方授权代表签署验收报告。如验收不合格，甲方有权暂不签署验收报告并暂缓支付相应服务款项，乙方应按照验收标准在十个工作日内进行弥补、改进或完善，待甲方重新组织验收并且验收合格后，甲方再向乙方支付相关费用。如果乙方经三次改进仍达不到验收标准的，甲方有权拒绝支付相应服务款，且不承担任何责任。

九、保密条款

1.任何一方对其获知的本合同及附件中其他各方的商业秘密和国家秘密负有保密义务。

2.除法律、法规另有规定或得到本合同之其他各方的书面许可，任何一方不得向第三人泄露前款规定的商业秘密和国家秘密。保密期限自任何一方获知该商业秘密和国家秘密之日起至本条规定的秘密成为公众信息之日止。

十、 知识产权

1.本合同涉及的全部及/或任何部分的相关知识产权、软件著作权、相关权益，包括本合同相关的且为履行本合同而新形成的商业秘密信息、技术资料和技术诀窍等，均归甲方所有。

2.乙方有不可争议的义务确保甲方依据本合同所获得的知识产权在中国境内（香港、澳门、台湾地区除外）不存在任何瑕疵并且可以不受限制地行使相关权利，包括各项延伸权利。若因此发生任何争议均应由乙方独自承担全部及/

或任何责任,包括但不限于承担其自身及甲方为解决任何争议及/或瑕疵及/或缺陷所应当或所需要支付的一切相关及/或由此引起的费用。

3.甲方将拥有其在本合同项下所从事的所有工作(包括各类纸质文档,电子文档及其它可交付物)中所包含的或与之相关的全部版权、专利权、商业秘密、商标权和其它知识产权以及所有权和其它权益。

4.在本合同生效日前业已存在的版权及其它知识产权和技术秘密应属于本合同生效前即拥有该等权利的一方或与该方有协议关系的第三方。任何一方均无权凭借本合同取得另一方此前所拥有且根据本合同不应被合理的推论为其已经同意转移的版权、专利权、商业秘密、商标权或其它知识产权的所有权。

5.若本条第4款涉及的权利已构成可交付物的一部分或甲方为实现本合同目的而必须使用的,乙方将就该等权利授予甲方非专有的、免付任何费用的、可授予分许可的、不可撤销的、永久性的许可,以确保甲方对可交付物的制作、复制、修改、使用和销售等。

6.乙方应当保证其提交的可交付物及有关参与本合同的任何活动,以及本合同终止后的任何涉及本合同的任何行为,在中国境内(香港、澳门、台湾地区除外)均不会侵犯任何第三方的知识产权。若因此发生任何争议、侵权,均应当由乙方独自承担全部及/或任何责任。

十一、其它约定事项

(一) 不可抗力

1.合同任何一方由于受诸如战争、严重火灾、洪水、台风、地震等不可抗力事件的影响而不能执行合同时,履行合同的期限应予以延长。延长的期限应相当于事件所影响的时间。不可抗力系指双方在签署合同时不能预见的、不能避免并无法克服的客观情况。

2.受不可抗力事件影响的一方,应在不可抗力事件发生后尽快用电报、传真或电传通知对方,并于事件发生后14天内将有关机构出具的证明文件用特快专递或挂号信寄给对方予以确认。

3.若不可抗力事件的影响持续30天以上,甲方有权确定是否延期履行或终

止合同。

4.任何一方因受不可抗力影响而不能执行本合同时，双方对此互不承担违约责任。但当事人迟延履行后发生不可抗力的，不能免除责任。

5.若双方对是否属于不可抗力发生争执，则由受理案件的法院根据合同的含义解释发生的客观情况是否构成不可抗力。

（二）解决合同纠纷的方式

双方如因履行本合同发生争议，双方应尽量协商解决。协商不成时，任何一方均有权向甲方住所地人民法院提起诉讼。

（三）适用法律

1.本合同适用中华人民共和国的法律。

2.任何一方对本合同及其附件的解释均应遵循诚实信用原则，依照本合同签订时有效的中国法律、法规以及通常的理解进行。

3.在本合同履行期间，因中华人民共和国法律、法规、政策的变化致使本合同的部分条款相冲突、无效或失去可强制执行效力时，双方同意将密切合作，尽快修改本合同中相冲突或无效或失去强制执行效力的有关条款。

（四）中小企业政策

本项目为面向中小企业预留份额，本项目合同标的对应的中小企业划分标准所属行业为：软件和信息技术服务业。乙方应在本合同签订后将不低于 30% 比例分包给一家或者多家中小企业，其中预留给小微企业的比例不低于 60 %。乙方投标文件中提供的分包意向协议见附件 E：分包意向协议。

（五）通知

1.任何通知应以快递、电报、电传或传真的方式发送至合同中载明的地址，快递、电报、电传或传真须经对方签收。

2.通知以送达日期或通知书载明的日期为生效日期，两者中以日期在后者为准。

3.如有变更应及时通知对方，否则因此造成的有关文件、通知不能送达，由责任方自负。

4.凡甲方按本合同所列明的地址、传真、电话等联络信息发出的文件、通知，均视为甲方已完成有关文件、通知的送达义务。

甲方：国家知识产权局

联系人：李子行

地址：北京市海淀区西土城路 6 号

邮编：100088

电话：62084891

传真：62083680

乙方：XXXXXX

联系人：XXXX

地址：

邮编：

电话：

传真：

乙方联系人发生变更，应书面形式告知甲方，否则因甲方无法正确联系到乙方所造成的损失，由乙方承担。

（六）合同与补充合同的效力

1. 本合同中的附件均为本合同不可分割的部分，与本合同具有相同的法律效力。甲方招标文件的效力高于乙方的投标文件，二者有冲突的，以对甲方有利的规定及解释为准。

2. 本合同未尽事宜应依照相关法律法规，双方可签订补充合同及附件，补充合同及附件与本合同具有同等法律效力。如果本合同与补充合同相关条款存在冲突，除非双方另有约定，否则以补充合同为准。

3. 本合同经甲乙双方法定代表人或授权代表签字盖章后生效。

4. 本合同一式陆份，甲方执肆份，乙方执贰份，每份具有同等法律效力。

（七）本合同包含以下附件：

附件 A：服务费用清单

附件 B：工作说明书

附件 C：项目责任书

附件 D：保密承诺书

附件 E：分包意向协议

（正文结束）

甲方：国家知识产权局

乙方：XXXXXX

法定代表人/授权代表：

法定代表人/授权代表：

签约日期：

签约日期：

附件 A：服务费用清单

附件 B：工作说明书

一、总体要求

（一）服务内容及期限

乙方应整体承接甲方信息化系统运行维护和网络安全保障工作。保障甲方有关信息化基础设施及应用系统的高效、安全、稳定运行，为甲方履行政府职能，对社会公众服务提供信息化基础性保障。

服务内容包括两部分：局机关信息化运行维护保障服务、全局网络安全保障服务。

1.局机关信息化运行维护保障服务：包括甲方委托维护范围内系统的基础环境运维、数据专线保障、应用系统集成运维、网络安全保障相关服务以及办公终端设备维护服务。

（1）基础环境运维：对服务器、网络设备、安全设备等硬件设备开展定期巡检、日常维护及故障处理，提供不低于原功能性能的设备备件及配件，根据现场紧急状况提供备机；对操作系统、数据库、中间件等软件进行版本升级、日常维护及故障处理，保障系统软件正常运行；提供内外网各一条连接局蓟门桥办公区至老干部活动中心的 10M 专线链路，保障链路的正常通信使用及网络安全。提供知识产权数据资源公共服务系统运行所需云平台租用，并负责公有云产品日常运行维护，保障系统运行环境安全。

（2）应用系统集成运维：对应用系统故障提供热线电话、远程在线诊断和故障排除、现场响应等支持服务；提供每月预防性现场巡检服务；对系统基础资源进行监控和管理，及时掌握系统资源现状、运行状态、配置信息、可用性等信息；重要敏感时期按需提供现场值守服务；提供系统整合、优化方案建议并配合实施，提供用户咨询等服务。

（3）局机关信息化网络安全保障：乙方需对运维范围内系统开展网络安全技术防护、统一访问控制、病毒防护、网络安全应急处置、重要时期保障、等保测评、IPv6 转换、网站 HTTPS 安全证书、电子政务外网网络安全保障等服务，保障相关系统的可靠、稳定、安全运行。

（4）办公终端设备维护服务：乙方需提供甲方局机关用户使用的台式计算机、便携式计算机、打印机、传真机等办公终端设备的现场维护和维修；负责鼠标、键盘等配件，打印机硒鼓、墨盒等耗材及 IP 电话等的配发及维护；办公终端设备巡检清查。

2.全局网络安全保障服务：乙方需面向甲方全局范围内，提供网络安全通报、应急、检查、培训及宣传等服务；负责网络安全监测平台运营、网络攻防演练、网络安全监测技术服务等。

3.项目整体服务期限为：2024 年 6 月 17 日至 2025 年 6 月 16 日。

（二）服务管理要求

乙方作为技术总责方及项目管理方应坚持用户利益第一的原则，在甲方的管理、监督下开展日常运维工作，整体负责相关信息化系统的可用性、安全性，以及业务的连续性和稳定性保障。为甲方知识产权行政管理相关业务开展、履行政府职能、对社会公众提供服务等提供有力支撑。作为技术总责方及项目管理方，其主要职责目标应包括：

1.标准运维管理体系

按 ISO20000 标准建立规范的运维管理体系，建立结构合理、标准统一、层次清晰的运维服务队伍，持续优化标准化的维护管理流程和工作规范。

（1）工作规范管理要求

乙方应根据甲方的运维服务及网络安全相关管理制度要求，持续优化运维保障、应急处置等各类相关制度、规范、及技术标准，并贯彻实施。遵循流程和规范组织运维工作，保障各应用系统的稳定正常运行。

（2）流程制度管理

乙方应对流程制度进行管理，包括故障响应、故障处理、故障处理过程管控以及日常巡检，日常资源申请等流程。在重要节假日前，提供相应的应急保障预案和巡检报告，并进行归档。

（3）服务过程管理

乙方应对服务过程进行标准化管理，以确保提高运维服务质量，降低服务成本，降低因 IT 服务中断所导致的业务风险。包括：服务级别管理、配置管理、变更管理、发布管理、事件管理、问题管理等。

（4）系统底数台账管理

乙方需负责详细清理盘点甲方委托维护范围内信息化系统的基本情况，包括：各系统的信息化资产、应用架构、机房部署、网络拓扑结构、等级保护、安全防护情况等，按照甲方要求，建立系统底数台账并及时更新。

2.运维服务

（1）整体技术运维

负责信息化系统的可用性、安全性、稳定性及业务的连续性保障，确保各项运维服务保障工作有效落实和顺利开展。

(2) 运维需求及知识管理

负责接收用户服务保障要求，分派服务保障任务，跟踪服务保障过程；收集用户运维服务需求信息，接收和反馈用户投诉并报告甲方等；负责建立系统运维保障知识库，有效做好系统各类运维知识收集、管理、使用和共享发布。

(3) 运行状态监控

负责全方位监控系统基础环境和业务应用运行状态，及时发现并上报服务保障异常和业务运行风险情况，定期分析系统使用情况，根据甲方要求开展系统下线评估。

(4) 系统变更优化

负责根据用户需求开展业务系统的缺陷处理、变更和优化。

(5) 运维安全管理

承担系统运维安全保密责任，严格遵守系统运维保密要求，确保运维中的系统安全、数据安全、人员安全。负责严格落实运维请示报告制度，系统相关信息未经甲方允许，不得对外披露。

(6) 应急处置

负责按照甲方需求制定信息化系统重大突发事件应急预案，并报甲方备案。按照预案中关于运维事件分类和等级的要求，第一时间发现、受理各类系统运维事件并进行处置，及时按照有关规定进行分类分级上报和跟踪协调，在规定时限内完成应急事件处理。

(7) 特殊时期保障服务

在特殊时期，如巡视、审计等，提供可靠的终端支持以及配套的网络环境保障，并根据甲方要求增加巡检频次。

(8) 人员要求

在整体服务期间，乙方需提供总数不少于 41 人的服务团队，其中驻场服务人员不少于 37 人（含 2 名项目经理），项目管理团队不少于 4 人。项目管理团队需在北京办公地点驻场，并负责本项目中的信息化台账、账户、网络接入、资源调配等管理运营协调工作，网络安全通报、应急、演练、检查、宣传、培训等管理工作，以及办公设备管理、资产管理、软件正版化等工作，并需要保持团队稳定性。

未经甲方同意，项目经理和项目核心技术人员不做变更。

(三) 服务指标要求

乙方应按照甲方对运维服务及网络安全保障服务的总体要求，负责运维服务质量相关的程序、计划、报告的编制或生成。乙方应规范运维服务质量管理，加强运维服务质量管

理的有效性，为甲方提供高质量的运维服务，保障相关业务系统的平稳开展。

根据 ISO20000 服务管理体系、ITSS 运维系列标准（国家标准）、制定以下具体要求：

表格 1 服务指标明细表

服务内容	服务指标说明	服务指标
机房内 IT 设备巡检	日常巡检	不低于 2 次/天
	深度巡检	不低于 1 次/月
应用系统巡检	日常巡检	核心系统不低于 1 次/天；其他系统不低于 2 次/周
	深度巡检	不低于 1 次/月
应用系统故障处理	应用系统故障事件	30 分钟内响应，5×9 小时现场服务，7×24 小时电话咨询服务
	核心系统	2 小时解决，每 2 小时向甲方汇报故障处理进展情况，故障处理完毕后向甲方提供处理报告
	重要系统	4 小时解决，每 2 小时向甲方汇报故障处理进展情况，故障处理完毕后向甲方提供处理报告
	一般系统	6 小时解决，每 2 小时向甲方汇报故障处理进展情况，故障处理完毕后向甲方提供处理报告
系统非计划中断发生次数	在约定的服务时间内，发生系统非计划中断的次数	≤3 次
集中监控	现场集中监控服务	提供 7×24 小时现场集中监控服务，在 30 分钟内对监控告警作出响应
重要时期保障	重大节假日和特殊时期对应用系统、硬件、存储、网络安全提供保障服务	工程师人数不低于 37 人驻场服务
机房内设备备品/备件/备机服务	负责维保中涉及的机房内设备的备品备件的提供、部署或更换服务	7×24 小时机房内设备全天候备件服务，包括设备重要部件、常用机型易损配件等
办公终端设备维护驻场服务	工作日工作时间提供驻场服务	工作日 5×8 小时

服务内容	服务指标说明	服务指标
办公终端运维事件处理	事件响应时长和解决率	30 分钟响应并到达现场，事件平均 2 小时解决，且全年事件解决率不低于 90%
网络安全应急响应服务	网络安全事件应急处理	7×24 小时电话支持，5 分钟内响应，工作时间提供 5×9 小时驻场应急支持服务，非工作时间 2 小时内到场。
网络安全监测服务	提供日常网络安全监测、分析研判及配合处置服务	7×24 小时电话支持，30 分钟内响应，工作时间提供 5×9 小时驻场服务，非工作时间 2 小时内到场
网络攻防演练服务	提供网络攻防演练期间防守相关工作	7×24 小时现场值守，10 分钟内响应支持服务
服务报告	需提供系统运维服务周报、月报、季报、年报，记录系统运行、资源使用、故障处置、巡检情况和维护记录等，按月提供统一监测平台运行统计分析报告，对于重大故障或安全事件，提交专项处置报告。	保证服务文档的可读性、标准化和有效性，以及文档数据的准确性。 服务报告频次： 周报为次周 1 个工作日内提交； 月报为次月 5 个工作日内提交；季报为次季 10 个工作日内提交；年报为次年 20 个工作日内提交；故障或安全事件处置报告为事件解决后 5 个工作日内提交；重保、等保测评、攻防演练等专项报告为活动结束后 10 个工作日内提交。
	需提供重要敏感时期安全保障情况报告、网络安全等级保护测评报告、攻防演练专项报告等。	

二、局机关信息化运行维护保障服务内容

局机关信息化运行维护保障服务：包括基础环境运维、数据专线保障、应用系统集成运维、局机关信息化网络安全保障、办公终端设备维护服务等。具体情况详见下表：

表格 2 局机关信息化系统及基础环境维护服务范围清单

序号	系统名称	上线时间	系统级别	应用系统服务期限	软硬件服务期限	链路服务期限
1	全国专利管理信息平台	2011 年	重要	9 个月	9 个月	无
2	专利代理管理系统	2011 年	重要	9 个月	9 个月	无
3	全国专利代理师资格考试考务系统	2009 年	核心	9 个月	9 个月	无
4	知识产权数据资源公共服务系统	2023 年	重要	7.5 个月	无	无
5	公文智能交换管理系统	2023 年	重要	12 个月	12 个月	无
6	离退休干部工作管理信息	2009 年	一般	12 个月	12 个月	无

序号	系统名称	上线时间	系统级别	应用系统服务期限	软硬件服务期限	链路服务期限
	系统					
7	老干部活动中心信息化项目	2018 年	一般	无	12 个月	12 个月
8	外观设计专利检索公共服务系统	2023 年	一般	12 个月	12 个月	无
9	档案管理系统	2023 年	重要	12 个月	12 个月	无
10	公共服务网	2020 年	核心	12 个月	12 个月	无

重点备注：

- 乙方需提供内外网各一条连接甲方北京蓟门桥办公区至老干部活动中心的市内 10M 专线链路（上表序号 7），并保障链路网络安全。
- 知识产权数据资源公共服务系统所需环境在公有云服务中提供。
- 硬件未出保设备需提供日常运行维护服务，电子政务外网提供沟通协调服务。

（一）基础环境运维服务

1.制度流程管理

对属于招标范围内的 PC 服务器及小型机、存储、数据库、中间件、网络、安全相关的流程制度进行管理，包括故障响应、故障处理、故障处理过程管控以及日常巡检，日常资源申请等日常流程。执行故障响应流程，对范围内故障来源进行分析，满足各设备的故障响应条件和机制。执行故障处理流程，分为一般故障处理和重要故障处理流程，并形成相应的汇报机制。执行故障处理管控流程，形成对故障处理流程的执行规范，形成在流程执行过程中文档的存放及更新机制。执行日常巡检类流程，提供相应设备的巡检手册，包含标准、流程及记录模板。执行检查流程，提供设备的健康检查手册，包含标准、流程及记录模板等。执行深度巡检类流程，在重要节假日前，提供相应的应急保障预案和巡检报告，并进行归档。

2.硬件设备管理

PC 服务器和小型机日常巡检

工作日对 PC 服务器和小型机进行现场巡检、非工作时间通过监控平台处理告警信息。在特殊时期、巡视审计等时期根据甲方要求增加巡检频次。

PC 服务器和小型机深度巡检

对 PC 服务器和小型机进行现场深度巡检、预防性维护，以满足服务器的运行要求。

PC 服务器和小型机重要保障服务

重大节假日和特殊时期按要求对 PC 服务器和小型机提供保障服务。

网络设备日常巡检

通过集中监控平台、人工现场巡检等方式对网络设备硬件状态进行监控。在特殊时期、巡视审计等时期根据甲方要求增加巡检频次。

网络设备深度巡检

对网络设备进行现场深度巡检、预防性维护，以满足网络设备的运行要求。

网络设备重要保障服务

重大节假日和特殊时期按要求对网络设备提供保障服务。

安全设备日常巡检

对安全设备进行现场巡检，以满足安全设备的日常运行要求。在特殊时期、巡视审计等时期根据甲方要求增加巡检频次。

安全设备深度巡检

对安全设备进行现场深度巡检、预防性维护，以满足安全设备的运行要求。

安全设备重要保障服务

重大节假日和特殊时期按要求对安全设备提供保障服务。

存储设备和备份系统日常巡检

现场巡检，通过监控平台监控存储设备和备份系统运行情况。在特殊时期、巡视审计等时期根据甲方要求增加巡检频次。

存储设备和备份系统深度巡检

对存储设备和备份系统进行现场深度巡检、预防性维护，以满足存储设备和备份系统的运行要求。

存储设备和备份系统重要保障服务

重大节假日和特殊时期对存储设备和备份系统进行现场保障和健康检查，对监控平台中的重要报警进行实时响应。

3.基础软件管理

产品软件日常巡检

对操作系统、数据库、中间件等产品软件进行日常巡检。在特殊时期，如巡视审计等时期，根据甲方要求增加巡检频次。

服务器类产品软件补丁服务

按照甲方的补丁测试流程完成补丁测试评估报告，制定保障方案，在获得甲方认可的前提下，按照实施方案组织补丁安装实施工作。

4.故障处理

对甲方范围内的 PC 服务器及小型机、存储、备份、操作系统、数据库、中间件、网络设备、安全设备等发生的故障进行处理。对相关的故障信息进行沟通，记录故障发生时

间和其他相关信息，进行故障初步分析，对故障的影响做出评估，按照故障处理流程，协调完成故障处理工作，管理和记录相关信息，对结果进行审核和汇报。

5.维保服务

提供基础软硬件维保服务，包括服务器、操作系统、数据库、中间件、存储设备、网络设备和安全设备等。服务内容包括进行预防性维护服务，现场设备巡检；在规定的时限内排除硬件故障，进行备件备机等更换；提供操作系统、数据库、中间件的高可用性能优化服务；提供设备升级服务、产品升级在内的产品服务；提供网络设备监控和性能检测分析服务；提供安全设备策略调整优化技术支持服务。在甲方实施重大项目，如网络改造、系统切换、系统升级、机房搬迁或机房停电等时，需要乙方配合或协助时，提供运维支撑服务。

6.资源管理

对属于招标范围内的 PC 服务器及小型机、存储、备份、数据库、中间件等基础应用维护的资源进行管理，对相应的流程制度进行改进等。提供资源使用规划，执行资源回收、优化及调整，审核资源分配相关操作。

运维资料管理，按照甲方要求收集并审核运维相关的资料，包括收集网络安全系统配置信息、关联关系、基础数据、资源分配、权限管理等信息。

对属于招标范围内的硬件设备、基础软件、网络信息、安全信息及 VPN 配置信息进行管理，配置管理流程包括创建配置管理数据库，维护配置数据以及定期对配置信息进行检查和审核。制定合理的配置信息如：硬件基本信息、运行状态、软件版本号、操作系统，通过这些信息真实的反映出管理对象的技术指标和应用情况。保证数据的准确性、可靠性和有效性。按需给甲方提供配置数据。

7.数据专线保障

提供内外网各一条连接甲方北京蓟门桥办公区至老干部活动中心的市内 10M 专线链路，保障链路的正常通信使用。

8.公有云平台租用

为知识产权数据资源公共服务系统提供满足等级保护测评要求三级的公有云租用；并提供公有云产品日常运行维护，保障系统运行环境安全，服务内容包括共有云产品配置、日常巡检、故障处理、应急处置、漏洞修复、补丁升级、病毒查杀、核心数据备份、IPv6 转换服务、短信服务等。公有云产品及规格主要参数详见下表：

表格 3 公有云产品及规格明细表

序号	产品名称	参数及配置	数量
1	负载均衡	提供负载均衡服务	3
2	IPv6 服务	提供 IPv6/IPv4 转换服务	1
3	云服务器	4 核 8GiB, 40GiB, 数据盘 SSD: 64GiB	4
		2 核 8GiB, 40GiB, 数据盘 SSD: 64GiB	4
		2 核 4GiB, 40GiB, 数据盘 SSD: 64GiB	2
4	云数据库 MySQL	MySQL8.0, 高可用版, 4 核 8G, 40GB	1
5	文件存储	通用型 (50T)	1
6	弹性公网 IP	支持 BGP 线路	14
7	共享带宽	800M	1
8	主机安全	企业版	10
9	Web 应用防火墙	黑白名单个数: 20 个, 单域名 CC 防护规则个数: 5 个, 子域名数量: 10 个, 一级域名数: 1 个	1
10	云堡垒机	存储空间不小于 500G, 管理节点数量: 20	1
11	日志审计	存储空间不小于 500G, 支持日志源数量: 20	1
12	云防火墙	4 核/16G; 120G, 吞吐量: 2Gbps	2
13	数据库审计	合规性管理功能, 实现合规报告	1
14	SSL 证书	域名型 (DV) 通配符 SSL 证书	1
15	虚拟私有网络	专有网络 VPC	1
16	短信服务		1

(二) 应用系统集成运维服务

1. 系统相关情况简介

(1) 全国专利管理信息平台

全国专利管理信息平台为支撑我局与地方局之间业务交流所需的管理信息平台, 涵盖了法律规章及与知识产权相关文件公告、规划与计划管理、地方管理工作评价等业务内容, 方便各地方知识产权局更快、更及时的获取相关数据; 满足部分地方局对于数据特殊化的需求; 提高专利管理工作效率。

(2) 专利代理管理系统

专利代理管理系统主要实现了代理机构、代理人基本信息、管理信息的电子化, 管理流程的电子化; 实现电子审批及相关系统自动获得代理机构、代理人的相关信息, 为实现智能化代理审查提供数据基础; 建立更丰富数据指标的代理机构和代理人的评价体系; 最终达到专利审批与代理专利代理管理的业务充分融合。

(3) 全国专利代理师资格考试考务系统

全国专利代理师资格考试网上考务管理信息系统，以考务管理中心为平台，对各考点知识产权局的考务工作实行统一管理、全面规划，为考务管理工作提供便利服务，对社会公众提供考试网上报名和成绩查询等服务。

(4) 知识产权数据资源公共服务系统

知识产权数据资源公共服务系统是支撑国家知识产权局知识产权信息公共服务工作重要的信息系统。该系统为社会公众，知识产权公共服务节点网点单位，确有知识产权数据需求，且具备知识产权数据加工处理和分析利用能力的服务机构和创新主体等提供知识产权数据服务。实现对国家知识产权局拥有的各类数据的统一管理，工作人员可以对数据资源进行全面、及时的掌握；可根据区域/地方常态化以及个性化的数据请求，高效快捷的调配全局甚至全行业的专利数据资源；实现对常态化数据的定期分发，对个性化数据请求的及时分发。

本系统以我局原来的知识产权数据资源管理系统（下称“国数系统”）为基础，迁移了原专利数据服务试验系统的用户数据，优化了原国数系统的功能，国数系统升级优化为现在的知识产权数据资源公共服务系统，同时下线了原专利数据服务试验系统，提升了信息化资源利用效率，节约财政资金、增强网络安全防护能力、改善用户体验。

(5) 公文智能交换管理系统

公文智能交换管理系统是一套包含软硬件的机要文件管理系统，该系统利用条码和自动化识别技术，实现对机要文件和信件的信息化管理，从而动态、准确、全面的掌握与共享查询文件和信件的流转状态信息。该系统包括文件登记、业务管理、交换员自助、语音短信提醒等功能。

(6) 离退休干部工作管理信息系统

离退休干部工作管理信息系统主要功能为实现离退休干部工作人员各类信息资源的共享，该系统以离退休人员基本数据为基础，与有关功能模块中的特殊信息相结合，实现多种检索应用和综合统计功能。该系统实现离退休干部部各项工作的一体化、垂直化管理的目标，达到部门内部的无纸化办公要求。

(7) 中国外观设计检索公共服务系统

中国外观设计检索公共服务系统利用“基于内容的图像检索技术”，实现外观设计专利图像内容的检索，并与基于全文检索技术的文字检索功能结合，建立一套全新的检索模式。该检索系统依据一定的规则，对外观设计专利的图形图像进行自动识别和基本判断，保留

可作为对比文件的设计，过滤掉绝大多数没有价值的设计，把有价值的检出对象缩小到最小范围。用户范围涉及：地方局、代办处、保护中心、快速维权中心、省级知识产权公共服务机构、地市级综合性知识产权公共服务机构、TISC 机构、高校国家知识产权信息服务中心、国家知识产权信息公共服务网点，以及有需要的创新主体等。

（8）档案管理系统

档案管理系统主要实现电子档案接收采集、归档编目、检索利用、鉴定统计、档案编研等档案业务管理功能；实现对已有文件资料信息资源的科学整合、集中管理、长久保存、有效利用、安全共享，保障电子档案的真实性、完整性、有效性和可用性。

（9）公共服务网

公共服务网整合了局内现有知识产权公共服务资源平台，实现了专利、商标、地理标志、集成电路布图设计的申请、缴费、信息查询、检索及数据下载等服务“一网通办”，实现了全国知识产权公共服务机构一体化查询，为全国的创新创业主体和社会公众提供了便捷、高效的知识产权公共服务。实现了国务院客户端小程序、中国科学院知识服务平台等 120 余个外部网站链接公共服务网，实现公共服务网在副省级以上知识产权管理部门网站链接的全覆盖。公共服务网主要包括网上办事、信息服务、行政许可、在线公益课堂、公共服务机构查询、服务事项通知以及地方特色等栏目。

2.服务过程管理

（1）服务级别管理

乙方应与甲方就服务内容和指标达成协议，乙方按照双方达成的协议提供服务，应定期测量所提供的服务是否满足服务级别协议，并制定和实施服务改进计划，提高服务质量，保证系统运行的稳定性、可靠性。

（2）服务报告管理

乙方需按照甲方规定按时提供运维服务报告，服务报告分为定期和不定期，不定期的服务报告应根据相应事项规定的时限出具，定期服务报告按周期分为周报、月报、季报、年报。服务报告的范围包括但不限于运维周报、月报、季报、年报，记录系统故障情况、巡检情况和维护记录、重大事件处理报告等。服务报告的内容包括但不限于：

信息化系统整体运维工作情况；

信息化系统运行使用情况；

信息化系统运维服务情况；

对运行使用情况和运维服务情况的回顾与改进分析；

专项工作的专项报告。

乙方在提供服务期间需能够按照甲方需求调整运维服务报告内容。

(3) 事件管理

事件管理着重管理的是对事件的响应速度和尽快恢复业务运作的的能力。事件管理负责对事件进行查明和记录、分类和初步支持、调查和分析、解决和恢复，其目标是在尽可能短的时间内恢复业务系统的正常运转，同时记录事件并为其他流程提供支持。事件流程建设的目标为：规范生产事件管理工作流程，保证生产系统安全、稳定、高效运行。允许预先定义事件的分类（严重等级、影响程度、紧急程度的分类）和优先级信息。事件可以和问题、变更、配置等相互关联。

(4) 问题管理

问题管理的目标是将由业务系统错误引起的事件和问题对业务的影响减少到最低程度；查明事件或问题产生的根本原因，制定解决方案和防止事件再次发生的预防措施；实施主动问题管理，在事件发生之前发现和解决可能导致事件产生的问题。从问题申报、归类、分派、处理到最后结束，所有的过程均在问题管理中进行了严格合理的定义。其间所涉及到的各类人员：如最终用户、维护人员、二线支持人员和专家组、管理层等，都会在指定的范围和规范化的框架和流程下进行日常工作。从而保证问题处理的所有环节有条不紊，并具有最优效率。提供问题的分类（严重等级、影响程度、紧急程度的分类）和优先级。对已经找到根本原因但暂时无法根本解决的，通过独立的已知错误管理流程进行管理，要求提供临时解决方案。对于已经找到根本原因且有解决方案的问题，可以提交知识条目给知识管理。

问题审计：能够记录数据变化前后的修改人、时间进行记录保证数据的安全性。

乙方应构建运维服务知识库，实现知识的积累，便于查询和更新。知识库应使参与事件处理的所有人员可访问，帮助提高故障的一线解决率，帮助解决已知错误故障，有效减少故障恢复时间。知识库和知识管理流程应按规范管理，具有对知识条目进行规范管理的流程（创建，审核，发布，撤回等）；知识条目可按产品、用户群、业务领域、地点等进行分类，知识可设定维护责任人。

(5) 变更管理

变更管理是指为在最短的时间内，安全、准确地完成各业务系统的任一方面的变更而对其进行控制的服务管理流程。其目标主要是为了保证对变更的有效控制，确保在实施过程中使用标准的方法和步骤，准确高效地完成变更任务，减少由于变更引起的影响业务效

率的突发事件，降低可能带来的负面效应。提供变更的分类和优先级。

能够提供大量的字段记录变更的详细信息如：实施日期、相应资源、请求人、实施者、实施计划等。

提供变更风险评估功能，可以基于配置管理数据库提供的数据库模型进行影响模拟分析。

变更审计：能够记录数据变化前后的修改人、时间进行记录保证数据的安全性。

(6) 配置管理

乙方需为甲方建立维护服务档案，记录所有设备系统配置、维护记录等信息。乙方应定期进行配置审核，维护配置信息完整性、准确性。每个配置项的配置信息应包括：

唯一性标识；

配置项类型；

配置项描述；

与其它配置项的关系；

状态。

配置项应受控，配置项的变更应可追溯和可审计。配置项在进行相关的变更发布后，配置项应及时更新。

(7) 发布管理

发布管理的目的在于全盘了解 IT 服务的过程，并确保考虑到发布的所有方面，包括技术和非技术方面。适用于：

发布大型或关键硬件

发布主要软件

打包或成批的系列变更

通过发布成功率提高和业务中断率降低，从而改进服务的质量，降低使用非法、存在缺陷或未经授权软件的几率。

3.应用系统集成维护

乙方需保障应用系统的稳定运行，完成应用系统集成维护工作，维护工作包括但不限于以下内容：

(1) 日常例行维护

定期对应用系统进行预防性日常巡检，做好巡检记录，发现问题及时处理或上报。在特殊时期，如巡视审计等时期，根据甲方要求增加巡检频次。

通过自动化监控工具，包括但不限于集中监控系统，监控系统和设备的运行状况，及

时发现潜在隐患及故障等。

按甲方要求定期执行系统数据备份操作，并定期检查备份执行情况，做好记录。

负责日常故障导致的应用程序安装部署。运行环境变更和迁移导致的应用系统重新安装和部署不在本合同规定的工作范围内。

对具备演练条件的系统按照甲方的要求，配合甲方完成容灾演练。

重大节假日和特殊时期按要求对应用系统提供重点保障服务。

（2）事件及故障处理

按照甲方的工作流程处理用户关于应用系统的报修。对用户报修故障进行记录并跟踪，并将处理情况和结果反馈甲方。

应用系统故障的处理。对应用系统发生的故障，进行故障定位并协调跟踪处理，处理过程要遵循相应的服务流程规范执行，重大故障要按照故障上报制度及流程上报处理，管理和记录相关信息，对结果进行审核和汇报。

按照甲方的流程，实施应用系统的重大操作，如停启系统等。

按甲方要求，从应用系统层面评估防病毒软件或操作系统补丁对应用系统可用性的影响；在发生病毒事件时，从应用系统层面配合甲方处理病毒事件。

（3）咨询及答疑

为用户提供应用软件使用咨询，对在应用系统软件使用过程中出现的有关使用方面的疑问进行解答、培训、咨询。

（4）应用数据维护

根据用户要求，进行应用数据维护工作。数据维护的工作包括：

按要求进行业务数据的提取和统计。

按要求提供系统使用情况的统计数据。

按要求提供关于系统信息的统计数据。

按要求进行批量及个别数据的修正。

（5）数据更新服务

乙方需负责对知识产权数据资源公共服务系统涉及的数据资源（约 83 种），按照甲方要求的更新周期，制定更新计划，协调数据产品提供方、按照数据资源规范要求，完成数据资源核查、数据资源包组织、数据资源上传更新以及过档数据资源回收工作；及时监管数据资源上传、下载情况，处理数据资源上传、下载问题，维护并更新常见问题处理，分析统计数据资源上传、下载情况，并定期形成服务报告。

（6）系统完善及优化

乙方应负责维护范围内系统应用程序的 BUG 修复。对在用户使用过程中发现的系统 BUG 进行修改，并进行应用程序发布。按甲方要求提供应用系统的优化建议，必要时形成优化方案技术文档。

（7）项目配合

项目配合工作是指在项目开展的各个时期以甲方项目组为主，从有利于项目正常进展的角度，进行的一系列协助工作。主要包括以下内容：

甲方在实施重大项目，如系统切换、系统升级、服务器虚拟化系统迁移、机房搬迁或设备搬迁等时，需要乙方配合或协助，乙方积极响应及时指派资深系统人员现场协助及指导，提供现场技术支持和后续维护保障工作。必要时，形成技术方案建议等文档。

按照甲方要求及流程提供应用系统下线服务。

按照甲方要求，对其职能范围内中办专网、中纪委专线、党委督查专网、电子政务内网、电子政务外网等网络进行相关配置或协调工作。

（三）局机关信息化网络安全保障服务

1.网络安全云端及主机防护服务

针对甲方 5 个局机关重要互联网业务系统（域名）部署云端安全防护，包括全国专利代理师资格考试考务系统、公共服务网、全国专利管理信息平台、知识产权数据资源公共服务系统、外观设计专利检索公共服务系统等，对系统进行 Web 攻击防护，拦截互联网方面的攻击行为。尤其在重要保障时期，提升系统安全性，保障系统稳定运行。

对招标范围内 6 个等保测评三级系统开展渗透测试，以模拟黑客入侵的方式对专利代理管理系统、全国专利代理师资格考试考务系统、局门户网站、内网网站、公共服务网、全国专利管理信息平台、知识产权数据资源管理系统（升级改造后名称为：知识产权数据资源公共服务系统）、外观设计专利检索公共服务系统、公文智能流转系统、档案管理系统和“互联网+监管”简版系统等进行攻击测试，识别系统存在的安全风险，组织整改修复和复测验证，有效完善系统的安全性。

对甲方委托维护服务范围内系统，提供包括日常一体化实时安全监测分析研判、每两周一次深度态势及系统病毒防护深度分析。及时发现并清除业务系统主机存在的病毒问题及清除监测所发现的问题，完成风险跟踪处置，提升网络的主动防御能力。

2.统一访问控制服务

对甲方委托维护服务范围内系统，乙方需提供统一访问控制服务，包括开展运维账号

资源管理、流程制度设计、运维安全审计、审计数据分析等统一访问控制服务。实现统一访问控制，可以识别操作用户的身份，快速定位故障原因和责任人。

3.病毒防护服务

对甲方委托维护服务范围内所有系统的相关设备提供病毒防护服务，负责防病毒软件的授权更新（包括运维范围内所有服务器，国产台式机 77 台，X86 台式机 105 台，国产笔记本电脑 48 台）。

乙方需提供对控制台定期巡检、定期进行病毒扫描及处置，对病毒库进行定期更新，策略下发；定期进行人工分析，提供处置建议；在发生病毒事件时，处理病毒事件。

4.网络安全应急服务

对甲方委托维护服务范围内的所有系统，乙方需负责网络安全应急事件处置。

对甲方委托维护服务范围内系统，乙方需负责制订整体应急预案，定义应急事件类型和特征，明确事前、事发、事中、事后的各个过程中相关部门和有关人员的职责。协调组织完成应急演练，根据演练情况，进一步检查应急保障措施和应急预案的完整性和可行性。

发生网络安全事件时，按照应急预案执行应急响应流程，并制定针对性的技术解决方案；提供 7×24 小时现场应急响应技术支持服务，对网络安全事件开展事件调查、分析、评估、处置。对于网络安全应急事件，应急事件处置完成后，提交应急事件处置报告，对事件发生的原因进行分析，回顾事件处理过程，提出整改建议，预防类似事件的发生。

5.重要时期保障服务

在党和国家重大会议活动、知识产权宣传周、网络攻防演练、法定假日等重要敏感时期，乙方需按甲方要求提供重点保障，拟定重要时期工作计划和应急预案，提供实时监测、值班值守和应急处置等各项网络安全保障服务。完成重要时期安全保障工作，保障工作结束后形成总结汇报报告。

重要时期保障准备：重要时期保障期间，按照甲方要求完成重点保障总体工作计划及保障预案，包括业务管理、应用系统、基础环境等整体保障，做好人员、设备、资金准备。

重要时期保障实施：建立重保值班制度，确定紧急联系人，以确保系统出现问题时，及时响应处理，派驻工程师驻场。提前一周进行现场巡检及预防性维护，检查各类设备、系统运行状况。根据实际情况，进行预防性检查维护，确保应用系统和基础环境的稳定运行。

重要时期保障总结：协调组织各相关方完成重保，回顾整个总结重要时期保障过程，总结经验和不足，形成汇报报告。

6.等保测评服务

对甲方委托维护服务范围内 9 个信息化系统和内网网站（详见下表），依据网络安全等级保护最新标准要求，开展系统网络安全等级保护测评相关工作，使系统最终能够符合网络安全等级保护要求，通过安全测评，形成等级保护测评报告。

对信息系统开展等保测评，衡量信息系统的安全保护管理措施和技术防护措施是否符合等级保护基本要求，是否具备了相应的安全保护能力，完成系统定级备案，等级保护测评工作，根据测评发现的问题，乙方应形成整改方案，针对性的制定整改措施，推进网络安全防护体系不断完善，进行不涉及硬件采购的整改实施，如需硬件采购的应向甲方提出采购需求和方案，使系统最终能够符合网络安全等级保护要求，通过安全测评，形成等级保护测评报告。

表格 4 等保测评情况表

序号	系统名称	定级	等保测评 需完成时间
1	专利代理管理系统	第三级	2024 年 12 月前
2	全国专利代理师资格考试考务系统	第三级	2024 年 12 月前
3	全国专利管理信息平台	第三级	2024 年 12 月前
4	外观设计专利检索公共服务系统	第三级	2024 年 12 月前
5	知识产权数据资源公共服务系统	第三级	2024 年 12 月前
6	公共服务网	第三级	2024 年 12 月前
7	档案管理系统	第二级	2025 年 6 月前
8	公文智能交换管理系统	第二级	2025 年 6 月前
9	离退休干部工作管理信息系统	第二级	2025 年 6 月前
10	内网网站	第二级	2025 年 6 月前

7.IPv6 转换服务

对甲方委托维护服务范围内网站系统提供 IPv6 转换服务，需满足《推进互联网协议第六版(IPv6)规模部署行动计划》等政策的相关要求，满足新技术新业态的安全保护措施要求，并和网站安全监测防护相结合，对 IPv6 网站流程进行监测审计，保障网站平稳有效。

8.网站 HTTPS 安全证书

对甲方委托维护服务范围内未采用加密保护的网站，提供 SSL 通配符证书服务，加密

用户与网站间的交互访问，强化网站用户端的可信展示程度，防劫持、防篡改、防监听，实现网站的可信认证与数据安全传输，避免数据流量被劫持篡改等，提升网站安全性。

9.电子政务外网网络安全保障

对甲方电子政务外网网络安全设备进行监控、巡检、策略配置调整、权限管理、基线管理、日志采集分析等工作。主动发现安全威胁，评估安全风险，做好网络安全设备问题整改。提供网络安全设备事件处置以及重要时期安全保障服务。

（四）办公终端设备维护

1.办公终端设备维护

负责甲方局机关用户办公终端设备日常报修的及时响应，负责范围内终端设备(台式计算机、笔记本、打印机等)的系统配置、驱动安装、软件及操作系统类故障的诊断及处理，负责范围内终端设备的硬件故障分析、诊断，对重要用户提供全程高标准服务，在重要时期、巡视审计等临时需要终端的时期，提供终端支持；负责台式计算机、笔记本的硬件兼容性测试，负责台式计算机、笔记本的标准化系统制作与测试。

台式机主要型号有：世恒 DF716、世恒 KF510、世恒 ZF510、联想启天 M5900 等，约 182 台。

笔记本主要型号有：长城 UF716、联想 T400 等，约 93 台。

打印机主要型号有：光电通 OEP400DN、MP4020DN、奔图 P3305、长城 C260/A260、施乐 7100（彩色）、HP2025、HP4025、HP5200、京瓷 P4040DN/P4035DN、OKI C830、佳能 PIXMA IP110/100（彩色）等，约 193 台。

扫描仪主要型号有：光电通 OES200、HP5590 等约 12 台。

多功能一体机主要型号有：光电通 MP4020DN、联想 M7650DNF 等，约 13 台。

2.耗材及配件配发维护

负责为甲方局机关用户提供周边配件、IP 电话、打印机硒鼓墨盒等的配发维护服务。

（1）周边配件包括：有线鼠标、有线键盘、无线鼠标、无线键盘、插线板、KVM 切换器、无线网卡、扩展坞、外置光驱、打印线（1.5 米和 3 米两种规格）、网线（1.5 米、3 米和 5 米三种规格）、USB 延长线（2 米规格）。

（2）涉及 IP 电话型号：Huawei eSpace 7910、Fanvil X3SP 等。

（3）涉及硒鼓的打印机型号：光电通 OEP400DN、MP4020DN、奔图 P3305、长城 C260/A260、施乐 7100（彩色）、HP2025、HP4025、HP5200、京瓷 P4040DN/P4035DN、OKI C830、佳能 PIXMA IP110/100（彩色）等。

(4) 涉及条码打印机型号：汉印 IT4P（1 台），相应配件扫码枪：紫光 FS1650（2 把）。

3.办公终端设备硬件维修

负责甲方局机关用户办公设备维护范围内因硬件故障的无法使用的办公终端设备进行故障分析，配合甲方局机关进行资产残值评估，按照《行政事业性单位国有资产管理条例》要求，对应报废的办公终端设备提供报废鉴定服务，对于未达到报废条件的办公终端设备进行硬件维修，确保设备正常使用。

4.办公终端设备巡检清查

负责甲方用户办公终端设备的巡检清查服务，根据甲方的需求，对用户信息化办公终端设备的使用及相关信息情况进行巡检清查，做好记录。

三、全局网络安全保障服务

（一）网络安全通报、应急指导及自查迎检服务

完善健全并执行甲方网络与信息安全通报机制，将问题通报、应急处置与应急响应进行统一协同联动。提高通报预警、信息共享、事件处置等工作的及时性、有效性。

服务内容主要包括及时更新维护甲方各部门单位网络安全应急联系人名单；汇集通报网络与信息安全隐患情报，对网络安全风险提前预警；负责重要敏感时期网络安全保障任务通报工作，负责对甲方局统一网络安全监测平台发现的网络安全事件进行通报，按照中央网信办应急协调平台、网络安全专用移动 APP 等通报平台的有关要求对相关通报、答复和协调工作，包括每日通报信息的整理与确认、当日通报情况的汇报、各部门单位相关报告的接收与整理等内容；提供安全通信服务，通过通信加密系统和通信信息加密服务对通信内容进行加密，确保通信数据安全；对最新安全威胁、新闻资讯进行整理归纳，向甲方各部门单位共享。

对于甲方全局各部门单位范围内发生的网络安全事件，按照网络安全事件严重程度，提供 7×24 小时远程应急响应及技术支持服务。在发生全局性应急事件处理时，协助下属单位，按照甲方局网络安全事件应急预案等制度完成应急事件的处理。

协助甲方按照国家网信主管部门的要求，完成网络安全自查和迎检工作；协助甲方针对网信工作要点落实情况，对部分单位开展督促检查。网络安全检查方案、检查表单、检查工具等需按照信息安全国内外相关标准进行编制及提供。

（二）网络安全培训宣传服务

负责承担开展甲方对全局各部门单位的网络安全培训工作，邀请网络安全业内资深专

家开展2场网络安全培训，每场不低于3课时，需结合最新信息安全行业热点信息、典型案例以及网络安全发展趋势等主题，提高人员网络安全防范意识，提升安全防范技能以及系统管理人员工作技能。

在首都网络安全日、国家网络安全宣传周等时期，配合甲方开展全局网络安全宣传工作，负责网络安全宣传材料的设计与制作。

（三）网络安全监测平台运营服务

乙方需协助甲方运营全局统一网络安全监测平台，增强安全漏洞发现、及时处置能力，有效提升重要系统安全防护性能。乙方应负责甲方全局统一网络安全监测平台的安全运营工作，对安全事件进行日常监控、问题通报，对安全告警、可疑行为进行跟踪研判和溯源分析统计，进行安全态势的深度分析，按月度出具分析报告。协调监测平台建设供应商对平台运行状态进行定期巡检，出具巡检报告，并协调处理巡检发现的各类问题。

（四）局网络攻防演练服务

乙方需负责协调组织甲方全局各部门单位开展全局网络安全攻防演练工作，并提供技术检测、安全加固、情报收集、分析研判、应急响应、安全决策等服务，确保靶标系统和各重要网络系统安全稳定。

具体工作包括准备阶段、实施阶段及复盘阶段的工作。乙方在攻防演练活动准备阶段、实施阶段、复盘阶段三个阶段提供技术服务。

准备阶段：协助甲方制定演练技术方案，完成资产梳理和收集工作。对现有资产进行互联网暴露面探测、漏洞检测等工作。对运维服务范围内信息系统发现的问题隐患，及时完成整改加固；对甲方其他部门单位信息系统的问题隐患，整理提出安全加固建议，协助相关部门单位完成整改，并提供技术指导。

实施阶段：以驻场服务形式向甲方提供安全监测值守、应急响应处置和攻击溯源、威胁情报收集以及安全决策能力支撑服务。

复盘阶段：对演练期间出现的安全事件进行汇总，协助甲方进行复盘分析，对暴露的问题进行复测，并检查整改完成情况，协助编制总结报告，及时发现现有防护手段的缺失与防护工作中的不足之处，为后续常态化的网络安全防护措施提供优化依据。

（五）网络安全监测技术服务

乙方需提供包括安全漏洞通报服务、网站安全监测服务、联网终端安全监测服务等内容的网络安全技术服务。

具体工作包括以下内容：

(1) 安全漏洞通报服务：

依托拥有的国家信息安全漏洞共享平台（CNVD），收集、分析涉及甲方的安全漏洞，一旦发现涉及用户相关产品安全漏洞，第一时间向用户单位邮件通报，并向用户单位提供远程技术支持服务。安全漏洞通报涉及产品类型包括网上银行、手机银行、自助体验终端等，具体产品清单可由用户单位提供。漏洞通报内容包括漏洞事件、漏洞引发的威胁、评分评级、影响产品、信息来源、漏洞描述、影响范围、漏洞验证情况、通报时间等。

(2) 网站安全监测服务：

依托国家网络安全监测平台，在我国公共互联网上，开展针对用户单位拥有的网站的网络安全外围性监测和预警通报，协助用户单位及时发现网站的安全事件和存在隐患。在监测发现针对用户单位网站的一般安全事件后，及时以邮件形式内向用户单位指定人员通报；监测发现较大级别以上的网络安全事件后，乙方第一时间通过电话或短信向用户单位指定人员通报，同时以邮件形式通报事件发生具体情况，并对用户单位处置这类安全事件提供一定的远程技术支持服务。

(3) 联网终端安全监测服务：

依托国家网络安全监测平台，在我国公共互联网上，针对用户单位接入互联网的计算机感染木马、蠕虫、僵尸程序等恶意程序事件进行外围性监测和预警通报，协助用户单位及时发现联网终端被恶意程序攻击的情况。在监测发现用户单位联网终端 IP 地址感染恶意程序事件后，按周（或天）汇总并以邮件形式向用户单位指定人员通报，通报内容应包括恶意程序事件的源 IP 地址、目的 IP 地址、源端口、目的端口和发生时间。

四、附件机房内 IT 设备运维清单

序号	类型	品牌	型号	数量	硬件维保截止时间
1	服务器	HP	RP7420	1	2024.6.16
2	服务器	HP	RP7410	1	2024.6.16
3	服务器	IBM	xSeries 366	4	2024.6.16
4	服务器	IBM	xSeries 336	3	2024.6.16
5	服务器	HP	DL580G7	6	2024.6.16
6	服务器	IBM	X3650 M3	3	2024.6.16
7	服务器	IBM	X3850 M2	2	2024.6.16
8	服务器	IBM	X3850 X6	2	2024.6.16
9	服务器	HPE	DL560 Gen10	4	2024.6.16
10	服务器	HPE	DL380Gen10	5	2024.6.16
11	服务器	HPE	DL380Gen8	5	2024.6.16
12	服务器	HP	DL380 GEN9	5	2024.6.16
13	服务器	HP	DL180 G6	1	2024.6.16
14	服务器	HP	HPDL580 GEN9	6	2024.6.16
15	服务器	HP	HP DL580G4	8	2024.6.16
16	服务器	联想	RD630	4	2024.6.16
17	服务器	联想	M710s	2	2024.6.16
18	服务器	联想	RD430	6	2024.6.16
19	服务器	联想	R680	2	2024.6.16
20	服务器	华为	RH2288V3	3	2024.6.16
21	服务器	擎天	DF-729	6	2025.11.10
22	服务器	Dell	PowerEDGE R940xa	4	2024.6.16
23	服务器	Dell	PowerEDGE R940	1	2024.6.16
24	服务器	Dell	R710	1	2024.6.16
25	服务器	中科曙光	A620r-G	1	2024.6.16
26	小型机	HP	RX6600	2	2024.6.16
27	刀片服务器	HP	C7000, BL680	5	2024.6.16
28	刀片服务器	HP	BL680c	1	2024.6.16
29	负载均衡	F5	BIG-IP 3400	1	2024.6.16
30	负载均衡	F5	LTM6400	2	2024.6.16
31	负载均衡	睿伟	Acteon-5208-C-6G	1	2024.6.16
32	负载均衡	F5	6400RS	2	2024.6.16
33	存储及备份	HP	HP-VA7110	1	2024.6.16
34	备份一体机	爱数	FT1220	1	2024.6.16
35	存储	同有	ACS 5000F-26R2IS11	1	2024.6.16
36	基础软件	Oracle	10/11	6	2024.6.16
37	基础软件	Tomcat	5.5/6.0/7.0/8.5/9	12	2024.6.16
38	基础软件	达梦	DM6.0.2/V8	3	2024.6.16

39	基础软件	Tongweb	5.0/7	5	2024.6.16
40	基础软件	Weblogic	11.3	2	2024.6.16
41	基础软件	mariaDB	5.5.60	2	2024.6.16
42	基础软件	apache	2.4	1	2024.6.16
43	基础软件	JDK	Jdk1.8/1.6	6	2024.6.16
44	基础软件	Mysql	5.7/8.0	7	2024.6.16
45	基础软件	sqlserver	2008	4	2024.6.16
46	基础软件	ngnix	1.14/1.15/1.17	9	2024.6.16
47	操作系统	CentOS	6.9/7.0/7.6/7.8/8.5	50	2024.6.16
48	操作系统	Windows	2003/2008/2012/2016	16	2024.6.16
49	操作系统	Suse	10/11	6	2024.6.16
50	操作系统	Ubuntu	14/16/20/22	14	2024.6.16
51	操作系统	麒麟系列	中标 5.4/银河 4.0	9	2024.6.16
52	网络设备	华为	5720-28P-LI	5	2024.6.16
53	网络设备	H3C	MSR50-40	1	2024.6.16
54	网络设备	H3C	S5120-48P-EI	2	2024.6.16
55	网络设备	H3C	S5130S-28P-EI	2	2024.6.16
56	网络设备	H3C	S5130S-28P-EI	6	2024.6.16
57	网络设备	H3C	S6800-4C	2	2024.6.16
58	网络设备	H3C	WX3024H	1	2024.6.16
59	网络设备	紫光	R3900	2	2024.6.16
60	网络设备	锐捷	RG-S6000-24T	2	2024.6.16
61	网络设备	锐捷	RG-AP820	50	2025.12.19
62	网络设备	锐捷	RG-S2910C-24GT2XS-HP	2	2025.12.19
63	网络设备	锐捷	WA5320	30	2024.6.16
64	安全设备	安恒	DAS-ABL-CH	1	2025.11.24
65	安全设备	安恒	DAS-NGFW1950	2	2025.6.6
66	安全设备	安恒	DAS-IPS295	2	2024.6.16
67	安全设备	安恒	DAS-USM1200	1	2025.12.19
68	安全设备	安恒	DAS-ABL-S2100	1	2026.8.17
69	安全设备	安恒	DAS-ABL-COS1000	1	2025.11.24
70	安全设备	思福迪	LogBaseD3890	1	2024.6.16
71	安全设备	思福迪	LogBaseA3890	1	2024.6.16
72	安全设备	绿盟	NIDS NX3	1	2024.6.16
73	安全设备	绿盟	WAF NX3	2	2024.6.16
74	安全设备	网神	Nsec-NF7000	2	2024.6.16
75	安全设备	网神	网神 Nsec NF5000	5	2024.6.16
76	安全设备	网神	SecGate3600	2	2024.6.16
77	安全设备	网神	W6150-C011	2	2024.6.16
78	安全设备	网神	SecVSS 3600	1	2024.6.16
79	安全设备	启明星辰	天玥网络安全审计系统 V6.0 GE1600ER	2	2024.6.16

80	安全设备	奇安信	网神 SecFox 运维安全管理与审计系统	1	2024.6.16
81	安全设备	榕基	RJ-iTop IIIB-128	1	2024.6.16
82	防病毒控制台		HPDL380 GEN9	2	2024.6.16
83	跳板机	联想	ThinkSystem SR590	2	2025.12.19
84	安全设备	安恒信息	DASUSM-V2.0	2	2025.11.10
85	安全设备	安恒信息	WPT-EE-H	1	2025.11.10
86	防火墙	启明星辰	USG-FWGAFT-12600G P-G014（万兆）	2	2025.11.10
87	漏洞扫描	启明星辰	TJCS-GYD-FTS2300A	1	2025.11.10
88	入侵检测	启明星辰	NT3000-ZX（千兆）	1	2025.11.10
89	日志审计	六方云	NSec-LAS3000	1	2025.11.10
90	安全设备	六方云	LinSec-P6200	1	2025.11.10
91	网络设备	信诺瑞德	ADC-3500-FT11	2	2025.11.10
92	备份一体机	爱数	FT1220	1	2025.11.10
93	入侵防御	网神	P3000-1610	1	2025.11.10
94	存储	同有	ACS 5000F-26R2IS11	1	2025.11.10
95	数据库审计	绿盟	DASNX5-HF-NDE-01	1	2025.11.10
96	交换机	清华紫光	S5600-G	2	2025.11.10
97	集中式扫描智能交换箱	神舟	B11	5	2024.6.16

附件 C：项目责任书

甲方（国家知识产权局）与乙方（XXXXXX）签订 2024 年局网络安全保障和局机关信息化系统运维服务项目合同，乙方承诺并遵守以下规定。

一、出入规定

1、严格遵守甲方有关人员、物品出入大门、治安、户籍、交通、环保、卫生等有关规定。

2、对要带走的工具、设备，乙方要提前告知甲方，并须由甲方项目负责人协助办理出门条后方可带出。

3、车辆或人员进入甲方区域内，要严格按照规定路线行驶或活动，不得随便进入与本项目无关的办公区域。

二、防火规定

1、必须做好防火工作，要有防火负责人，要建立灭火队伍，要健全防火安全责任制，要配置必要的灭火设施。

2、要明确防火通道，不得随意堵塞，不得压盖地下消防栓，并要有明显标志。

3、动用明火要向甲方防火办申请“用火证”，取得用火证后方可动用明火，必要时还需指派专人进行现场护理。

4、要对电源、电线、用电进行严格管理，严禁随意乱拉临时线，严禁使用电炉取暖。

5、一旦发生火灾要积极抢救，尽快扑灭火灾，并要保护好火灾现场，对弄虚作假破坏现场的，甲方将进行调查，并提请有关部门依法处理。

三、成品保护

1、严格控制进出场的工程物资、设备的搬运，采取铺垫保护性材料等方式保护地面。

2、不得影响其他工作人员的正常工作，要对相关设备做好管理，防止损坏；及时清理施工垃圾，严禁随意抛洒，做到工完料清。

3、经检验后的每道工序采取相应保护措施，保证下一道工序顺利进行。

4、对本项目的工作区域内实行独自管理，发生任何失误、损失、伤亡由乙

方自负；若影响到甲方，根据情节轻重追究乙方责任，并由乙方负责相应赔偿。

四、保密规定

乙方要对工作人员进行保密教育，项目相关人员应保守工作秘密，严格控制无关人员进入甲方大楼。项目相关的所有软、硬件信息资料要严格管理，严禁泄密,否则按照有关法律法规进行追究。

乙方：XXXXXX（盖章）

日期： 年 月 日

附件 D：保密承诺书

甲方（国家知识产权局）与乙方（XXXXXX）签订 2024 年局网络安全保障和局机关信息化系统运维服务项目合同，乙方承诺并遵守以下保密规定。

1 定义

保密信息：是指甲方拥有或持有的、项目活动中所披露的（或者乙方与甲方交往过程中所知悉的）符合以下条件之一的商业、经营、技术或其他信息：

（1）在甲方披露（或者乙方知悉）时标明为保密、专有（或有类似标记）的；

（2）乙方在为甲方提供服务的过程中获得的有关甲方的任何信息、数据、资料（不论是甲方提供或披露的还是乙方偶然获得的）以及因项目实施所取得的任何工作成果，均为保密信息；

（3）在保密情况下由甲方披露（或者乙方知悉）的；

（4）根据乙方合理的商业判断应理解为保密信息的；

（5）记载于保密信息传递单的；

（6）以其他书面或有形形式确认为保密信息的；或

（7）从上述信息中衍生出的信息。

“保密信息”包括但不限于：本承诺书内容；由甲方或其关联机构在本承诺书签署前或之后披露给乙方或其雇员的，任何研发设计、产品设计理念/想法、产品及其规格、数据、模型、样品、草案等技术类信息；营销要求和策略、产品计划及价格、客户名单、甲方存货情况、甲方供应商名单、甲方已经或拟购买/销售的产品或服务的价格、公司业务发展可能方向、拟进入领域、有关甲方或其客户的资信情况试用过程中出现的问题以及解决方法、试用结果、涉及经营管理的制度与流程等经营类信息；其它甲方披露的需向第三方承担保密义务的信息。无论这些信息是以书面、口头、图形、电磁还是其他任何形式披露。

2 保证

乙方就本承诺书约定的保密信息保证如下：

（1）对本承诺书和相关附件，以及乙方以各种方式获悉的保密信息进行严格保密；

(2) 乙方现行保密制度足以对保密信息进行保密；

(3) 乙方不将保密信息披露（或者促使或允许他人披露）给任何人，但因工作需要而“必须知情”的下列人员除外：乙方直接参与项目活动的高级管理人员或雇员；或者经甲方事先书面认可的、且向乙方提供专业咨询的人士；或乙方的关联机构中直接参与项目活动的高级管理人员或雇员；

(4) 乙方不将保密信息（也不会促使或允许他人将保密信息）用于项目活动目的之外的其他任何用途，包括但不限于：将此保密信息的全部或部分进行仿造、反向工程、反汇编、逆向推导；

(5) 在保密信息披露时，如甲方已明确表示保密信息不得复印、复制或储存于任何数据存储或检索系统，乙方不得复印、复制或储存保密信息；

(6) 在项目活动结束后或者经甲方要求时，乙方须把含有保密信息的所有记录或资料（无论是以书面、磁盘储存或是以其他形式保留的）交还甲方或删除，并且将促使他人将上述记录或资料交还甲方或删除；如甲方要求，乙方须向甲方书面保证已经将上述记录或资料全部归还或删除；

(7) 应甲方要求，乙方须就甲方根据第三方许可而披露的保密信息的任何部分与甲方签署其他有关协议；

(8) 乙方须告知并有效约束本承诺书提及的人士承担与本承诺书规定相同的保密义务并签署不低于本承诺书保护程度的书面保密承诺书或承诺。甲方要求时，乙方应向甲方提供上述承诺书或承诺的文本。如上述人士越权使用或泄露保密信息，乙方与行为人承担连带责任。

(9) 乙方保证不向本项目提供服务的乙方人员之外的其他人员（包括不为本项目提供服务的乙方人员，以及非乙方人员）披露本承诺书项下的保密信息。乙方应告知并采取必要的有效措施保证参与本承诺书项下服务项目之乙方人员履行本承诺书项下的保密义务。若乙方人员（乙方任何人员）违反本承诺书项下的保密义务或泄露本承诺书约定保密信息，视为乙方违反本承诺书，乙方应按照本承诺书约定向甲方承担全部责任。

(10) 乙方保证：在项目通过验收之日，乙方须将甲方在项目实施过程中提供的相关信息和资料全部返还给甲方；未经甲方书面同意，乙方不得擅自留存、使用、参考和拷贝。

3 陈述

3.1 保密信息包含的所有权利、产权和利益都归甲方所有。除乙方按照本承诺书规定的方式和范围使用保密信息外，乙方未被授予任何明示或默示的关于保密信息的其他权利许可。

3.2 乙方明确承认：甲方并未向乙方担保其提供的保密信息目前或将来是真实无误的。

3.3 乙方违反本承诺书可能造成甲方（包括甲方关联方）不可弥补的损失，单独的金钱损害赔偿不能提供充分的救济。因此，针对乙方的违反本承诺书或可能违反本承诺书的行为，甲方有权在实施其他可行的救济手段的同时，向任何具有管辖权的法院寻求采取禁令性救济措施。

3.4 甲方向乙方披露保密信息的行为并不构成甲方将与乙方或其他实体进行任何商业合作的承诺；如果甲乙双方意欲建立任何商业合作关系，应另行签订书面协议。

4 保密期限

乙方应按本承诺书约定对保密信息持续地承担保密义务，除非（1）甲方以书面形式明确说明其披露的特定保密信息可不再保密，或（2）保密信息已被公众从公开途径获悉。

5 违反本承诺书的责任及权利救济

5.1 如乙方违反本承诺书约定的任何一项保密义务，每次违反时，甲方可要求按下列方式（几种方式同时适用）处理：

5.1.1 乙方应立即停止并纠正违反本承诺书的行为，消除因违反本承诺书而给甲方造成的不利影响，且乙方应自行承担费用按甲方的指示采取有效的方法对保密信息进行保密。

5.1.2 乙方须向甲方支付人民币贰拾万元整（¥200,000 元）的违约金。

5.1.3 如乙方违反本承诺书行为给甲方造成损失，乙方还应赔偿甲方因此遭受的全部损失，在此所称的甲方损失包括但不限于：甲方直接和间接损失、甲方因调查乙方违约并向其主张权利而支出的调查费、误工费、交通费、律师费、诉讼费以及其他因此而支出的全部合理费用。

5.1.4 乙方因违反本承诺书约定、披露保密信息而获得的全部收益，均归甲方所有。

5.2 以上处理并不影响甲方同时根据本承诺书或有关法律采取其他救济措施的权利。

乙方：XXXXXX（盖章）

日期： 年 月 日

附件 E：分包意向协议

第五章 附件——投标文件格式

第一部分 开标一览表及资格证明文件

- 1、开标一览表；
 - 2、法人或者非法人组织的营业执照等证明文件复印件（须加盖本单位公章）或自然人的身份证明复印件；法定代表人身份证明书；
 - 3、法定代表人授权书（自然人投标的无需提供）；
 - 4、投标人具有良好的商业信誉和健全的财务会计制度的证明文件；
 - 5、投标保证金缴纳凭证复印件或投标担保函；
 - 6、符合要求的依法缴纳税收和社会保障资金记录；
 - 7、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；
 - 8、投标人具有履行合同所必需的设备和专业技术能力的承诺函；
 - 9、中小企业声明函；
 - 10、分包意向协议（如有）；
 - 11、投标须知前附表要求的其他资格证明文件。
- 如投标须知前附表中规定其不作为资格要求，请勿装订在投标文件第一部分。

1、开标一览表

项目名称：

招标编号：

报价单位：人民币元

序号	投标总价	合同履行 期限	投标保证金	投标 声明
1	小写：_____元 大写：_____			

投标人（盖公章）：_____

法定代表人或委托代理人（签字或签章）：_____

日期：_____

注：1、此表应按投标人须知的规定装订密封。

2、此表中，投标总价应和投标分项报价表的总价相一致。

2、法人或者非法人组织的营业执照等证明文件或自然人的身份证明

说明：

- 1.提供有效的营业执照等证明文件复印件，复印件上应加盖本单位公章。
- 2.投标人为自然人的，应提供身份证明的复印件。
- 3.联合体投标应提供联合体各方满足以上要求的证明文件。

法定代表人身份证明书

致（采购代理机构名称）：

_____（姓名、性别、年龄、身份证号码）在我单位任_____（董事长、总经理等）职务，是我单位的法定代表人。

特此证明。

投标人（盖公章）：_____

详细通讯地址：_____

邮 政 编 码：_____

传 真：_____

电 话：_____

注：自然人投标的无需提供。联合体投标联合体各方均需提供。

3、法定代表人授权委托书

本授权书声明：注册于（国家或地区的名称）的（投标人）的在下面签字的（法人代表姓名、职务）代表我单位授权在下面签字的（被授权人的姓名）为我单位的合法代理人，就（项目名称）投标，以我单位名义处理一切与之有关的事务。

本授权书于_____年_____月_____日生效至本项目结束，特此声明。

投标人（盖公章）：_____

法定代表人（签字或签章）：_____

身份证号码：_____

委托代理人（签字或签章）：_____

身份证号码：_____

详细通讯地址：_____

邮 政 编 码：_____

传 真：_____

电 话：_____

注 1：请提供法定代表人及授权代表身份证复印件并加盖公章。

注 2：自然人投标的或法定代表人投标的无需提供。

注 3：联合体投标各方均需提供。

4、投标人具有良好的商业信誉和健全的财务会计制度的证明文件

会计师事务所出具的上一年度财务审计报告或银行出具的说明投标人商业信誉或结算情况等事项的证明文件。

说明：

- 1、投标人在投标文件中，必须提供本单位上年度经会计师事务所出具的审计报告复印件并加盖本单位公章。
- 2、如投标人无法提供上年度审计报告，则需提供银行出具的证明文件。银行证明文件可提供原件；也可提供银行在投标截止时间前三个月内开具证明文件的复印件，复印件正反面均需要提供。若提供的是复印件，招标采购单位保留审核原件的权利。
- 3、成立时间距离投标截止时间不足三个月的投标人可出具承诺良好的商业信誉和健全的财务会计制度（格式自拟）。
- 4、银行出具的证明文件应能说明该投标人与银行之间业务往来正常，企业信誉良好等。
- 5、如果是联合体投标，联合体各方均需提供上述证明。

5、投标保证金缴纳凭证复印件或投标担保函

投标人可将本项目投标保证金支付的汇款凭证、支票、汇票或保证金收据（如有）的复印件作为缴纳凭证装订在本部分，复印件上应加盖本单位公章；使用银行保函等其他投标担保函的，应将担保函正本，装订在本部分正本中；如采用政府采购信用担保形式的，应使用以下格式，将原件装订在本部分正本中。

政府采购投标担保函（项目用）

编号：

_____（采购人或采购代理机构）：

鉴于_____（以下简称“投标人”）拟参加编号为_____的_____项目（以下简称“本项目”）投标，根据本项目招标文件，供应商参加投标时应向你方交纳投标保证金，且可以投标担保函的形式交纳投标保证金。应供应商的申请，我方以保证的方式向你方提供如下投标保证金担保：

一、保证责任的情形及保证金额

（一）在投标人出现下列情形之一时，我方承担保证责任：

1. 中标后投标人无正当理由不与采购人或者采购代理机构签订《政府采购合同》；
2. 招标文件规定的投标人应当缴纳保证金的其他情形。

（二）我方承担保证责任的最高金额为人民币_____元（大写_____），即本项目的投标保证金金额。

二、保证的方式及保证期间

我方保证的方式为：连带责任保证。

我方的保证期间为：自本保函生效之日起_____个月止。

三、承担保证责任的程序

1. 你方要求我方承担保证责任的，应在本保函保证期间内向我方发出书面索赔通知。索赔通知应写明要求索赔的金额，支付款项应到达的账号，并附有证明投标人发生我方应承担保证责任情形的事实材料。

2. 我方在收到索赔通知及相关证明材料后，在_____个工作日内进行审查，符合应承担保证责任情形的，我方应按照你方的要求代投标人向你方支付投标保证金。

四、保证责任的终止

1. 保证期间届满你方未向我方书面主张保证责任的，自保证期间届满次日起，我方保证责任自动终止。

2. 我方按照本保函向你贵方履行了保证责任后，自我方向你贵方支付款项（支付款项从我方账户划出）之日起，保证责任终止。

3. 按照法律法规的规定或出现我方保证责任终止的其它情形的，我方在本保函项下的保证责任亦终止。

五、免责条款

1. 依照法律规定或你方与投标人的另行约定，全部或者部分免除投标人投标保证金义务时，我方亦免除相应的保证责任。

2. 因你方原因致使投标人发生本保函第一条第（一）款约定情形的，我方不承担保证

责任。

3. 因不可抗力造成投标人发生本保函第一条约定情形的，我方不承担保证责任。

4. 你方或其他有权机关对招标文件进行任何澄清或修改，加重我方保证责任的，我方对加重部分不承担保证责任，但该澄清或修改经我方事先书面同意的除外。

六、争议的解决

因本保函发生的纠纷，由你我双方协商解决，协商不成的，通过诉讼程序解决，诉讼管辖地法院为_____法院。

七、保函的生效

本保函自我方加盖公章之日起生效。

保证人：（公章）

年 月 日

6、依法缴纳税收和社会保障资金的记录

说明：1.按照规定提供复印件。

2.复印件上应加盖本单位公章。

3.如果是联合体投标，联合体各方均需提供上述证明。

7、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：中招国际招标有限公司

我公司在参加本次政府采购活动前 3 年内，在经营活动中没有重大违法记录，特此声明。

投标人（盖公章）：_____

法定代表人或委托代理人（签字或签章）：_____

日期：_____

说明：

- 1、投标人应按照相关法规规定如实作出说明。
- 2、按照招标文件的规定加盖公章（自然人投标的无需盖章，需要签字）。
- 3、如果是联合体投标，联合体各方均需提供上述证明。

8、投标人具有履行合同所必需的设备和专业技术能力的承诺函

致：中招国际招标有限公司

我公司具有履行合同所必需的设备和专业技术能力，特此承诺。

投标人（盖公章）：_____

法定代表人或委托代理人（签字或签章）：_____

日期：_____

说明：1.投标人应按照相关法规规定如实作出说明。

2.按照招标文件的规定加盖公章（自然人投标的无需盖章，需要签字）。

3.如果是联合体投标，联合体各方均需提供上述证明。

9 中小企业声明函（如本项目专门面向中小企业，或专门面向中小企业预留份额项目，或与中小企业以联合体形式参加投标人须提供）

9-1 中小企业声明函

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，服务全部由符合政策要求的中小企业承接（或者：工程的施工单位全部为符合政策要求的中小企业）。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（采购文件中明确的所属行业）行业；承接（承建）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，属于（中型企业、小型企业、微型企业）；
2. （标的名称），属于（采购文件中明确的所属行业）行业；承接（承建）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，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1：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2：请在本表中填写前附表中写明的中小企业行业类别。

注3：承接企业如为监狱企业或残疾人福利性单位的，视同为小型、微型企业，请填写此声明函，并需要出具相应的声明函和证明文件（格式后附）。

9-2 监狱企业声明函

本单位郑重声明，本单位在参加（采购人名称）的（招标项目名称）项目采购活动提供以下监狱企业承接的服务（或监狱企业承担的工程、或制造的货物），具体情况如下：（按照实际情况勾选或填空）

（1）☐ （监狱企业名称）属于监狱企业，后附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。

（2）☐ （监狱企业名称）属于监狱企业并作为联合体一方，其提供协议合同金额占到共同投标协议合同总金额的比例为_____。后附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。

（3）☐ （监狱企业名称）属于监狱企业并作为分包方，其提供协议合同金额占到分包意向协议合同总金额的比例为_____。后附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。

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：

9-3 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服务（由本单位承担工程/制造的货物），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：

10、分包意向协议（如需要格式自拟）

注 1：如本项目面向中小企业采购预留份额，采用分包意向协议方式须提供；

注 2：接受分包合同的中小企业与分包企业之间不存在直接控股、管理关系。

注 3：其他注意事项请见投标人须知 1.4 部分相关内容。

11、投标须知前附表要求的其他资格证明文件

说明：1.应提供投标须知前附表要求的其他资格证明文件。

2.复印件上应加盖本单位公章（自然人投标的无需盖章，需要签字）。

3.如果是联合体投标，联合体各方需提供的满足招标文件要求的其他资格证明文件。

第二部分 商务及技术文件

- 1、投标书
- 2、投标分项报价表
- 3、服务需求偏离表
- 4、商务条款偏离表
- 5、缴纳招标代理费承诺书
- 6、投标人商务符合性承诺函
- 7、投标人关联单位的说明（格式自拟）
- 8、联合体协议（如需要格式自拟）
- 9、评审所需要的其他商务文件
- 10、评审所需要的技术文件
- 11、简历格式
- 12、投标须知前附表要求的其他文件

1、投标书

致：中招国际招标有限公司

根据贵方为（项目名称）项目的投标邀请（招标编号），签字代表（姓名、职务）经正式授权并代表投标人（投标人名称、地址）提交下述文件正本____份、副本____份及电子文档____份，以_____形式出具的金额为人民币_____元的投标保证金。

据此，签字代表宣布同意如下：

- （1）本投标有效期为自投标截止之日起_____个自然日。
- （2）投标人已详细审查全部招标文件，包括所有补充通知（如果有的话）。我们完全理解并同意放弃对这方面有不明、误解的权力。
- （3）根据投标人须知第 1 条规定，我方承诺，我方不是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，我方不是采购代理机构的附属机构。
- （4）在规定的开标时间后，投标人保证遵守招标文件中有关保证金的规定。
- （5）按照招标文件的规定，在中标后向贵方一次性支付招标代理费。
- （6）投标人同意提供按照贵方可能要求的与其投标有关的一切数据或资料，完全理解贵方不一定接受最低价的投标或收到的任何投标。
- （7）投标人将按招标文件的规定履行合同责任和义务。

与本投标有关的一切正式往来信函请寄：

地址_____ 传真_____

电话_____ 电子函件_____

法定代表人或委托代理人（签字或签章）：_____

投标人名称（盖公章）_____

投标人开户银行（全称）_____

投标人银行帐号_____

日期_____

2、投标分项报价表

项目名称：

招标编号：

报价单位：人民币元

序号	服务名称	服务内容	数量	服务期限	报价	备注
1						
2						
3						
4						
5						
...						
总价：						

投标人（盖公章）：_____

法定代表人或委托代理人（签字或签章）：_____

日期：_____

注：1.如果投标人认为需要，每种服务及其伴随的货物和工程填写一份本表。

2.如果按单价计算的结果与总价不一致，以单价为准修正总价。

3.如果不提供详细分项报价将视为没有实质性响应招标文件。

4.上述各项的详细分项报价，可另页描述。

5.如果开标一览表（报价表）内容与本表内容和合计金额不一致的，以开标一览表（报价表）内容为准。

3、服务需求偏离表

项目名称：

招标编号：

序号	招标文件条款号	招标要求	投标响应	偏离	说明

投标人（盖章）：_____

法定代表人或委托代理人（签字或签章）：_____

日期：_____

4、商务条款偏离表

项目名称：

招标编号：

序号	招标文件条款号	招标文件的商务条款	投标文件的商务条款	说明

投标人（盖公章）：_____

法定代表人或委托代理人（签字或签章）：_____

日期：_____

5、缴纳招标代理费承诺书

致：中招国际招标有限公司

我们在贵公司组织的_____项目招标中若获得中标资格（招标文件编号：_____），我们保证在领取中标通知书的同时按招标文件的规定，以支票、电汇等形式，向贵公司一次性支付应由我们缴纳的招标代理服务费用。

特此承诺！

投标人名称：_____

地址：_____

电话：_____ 传真：_____

电子邮件：_____ 邮编：_____

承诺方授权代表签字：_____（承诺方盖章）

承诺日期：_____

6、投标人商务符合性承诺函

我公司在此郑重承诺：未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；投标过程中不存在向采购人提供、给予任何有价值的物品，试图影响其正常决策行为。

投标人名称（盖章）：

日 期：

7、投标人关联单位的说明

(格式自拟)

说明：投标人应当如实披露与本单位存在下列关联关系的单位名称：

- (1) 与投标人单位负责人为同一人的其他单位；
- (2) (2) 与投标人存在直接控股、管理关系的其他单位；
- (3) 如无关联单位可不提供此说明。

8、联合体协议（如需要格式自拟）

注 1：如本项目面向中小企业采购预留份额，采用联合体形式参加投标须提供；

注 2：联合体中的中小企业与联合体中的其他企业之间不存在直接控股、管理关系。

注 3：其他注意事项请见投标人须知 1.5 部分相关内容。

9、评审所需要的其他商务文件

10、评审所需要的技术文件

11、简历格式

个人简历

项目名称：

招标编号：

姓名		年龄		专业	
职称		职务		拟在本项目 担任职务	
毕业学校		学位学历		毕业时间	
相关技术 资格证书				入职时间	
工作业绩					
时间	同类项目名 称	担任何职	合同金额(万元)	客户联系人	联系电话

注：表中所列职称、学位学历、相关技术资格证书均必须附加盖投标人公章的复印件。

投标人名称（加盖公章）：_____

法定代表人或其授权代理人（签字或签章）：_____

日期：_____

12、投标须知前附表要求的其他文件

第六章 评标办法

评标办法

为规范评标工作程序，切实做好本项目招标评标工作，特制定本评标标准和方法。

一、评标依据

1. 《中华人民共和国政府采购法》《中华人民共和国政府采购法实施条例》
2. 《政府采购货物和服务招标投标管理办法》（财政部令第 87 号）

二、评标原则

1. 坚持公平、公正、科学、择优的原则；
2. 通过评标，推荐能实质上响应招标文件，确能履行合同且经评审综合评分最高者为中标候选人。

三、评标委员会

评标活动依法成立评标委员会，评标委员会在开标前组建，评标委员会由 5 位以上专家和采购人代表组成。

四、评标标准和方法

- 1、本项目评标采用综合评分法。
- 2、评标委员会依据评标方法和标准对投标文件进行评审，任何其他的外部证据均不作为评标的依据。
- 3、各评委独立评分。
- 4、评标委员会根据本办法组织评标，并依此推荐排名位于前三名的投标人为中标候选人。综合得分最高并通过评标委员会资格后审的投标人为推荐中标供应商。

五、评审时需考虑的其他因素

1. 根据《关于进一步加大政府采购支持中小企业力度的通知》（财库〔2022〕19 号）、《政府采购促进中小企业发展管理办法》（财库〔2020〕46 号），对满足价格扣除条件且在投标文件中提交了《中小企业声明函》的投标人，小微企业报价给予 10 % 的扣除，用扣除后的价格参与评审。专门面向中小企业采购或预留份额的情况不适用。

2. 根据《财政部 司法部关于政府采购支持监狱企业发展有关问题的通知》（财库〔2014〕68 号）和《三部门联合发布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，在投标文件中提交了《残疾人福利性单

位声明函》或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的企业视同小型、微型企业，其报价部分按第 1 条的比例扣除后参与评审。对于同时属于小微企业、监狱企业或残疾人福利性单位的，不重复进行投标报价扣除。

3.大中型企业与小微企业组成联合体或者允许大中型企业向一家或者多家小微企业分包的采购项目，对于联合协议或者分包意向协议约定小微企业的合同份额占到总金额 30%以上的，对联合体或者大中型企业的报价给与 4% 的扣除，用扣除后的价格参加评审。组成联合体或者接受分包的小微企业与联合体内其他企业、分包企业之间存在直接控股、管理关系的，不享受价格扣除优惠政策。

联合体各方均为小型、微型企业和监狱企业的，联合体视同为小型、微型企业和监狱企业。

3.采购人采购的服务伴随的货物如属于节能产品、环境标志产品品目清单范围内，且投标人所投产品具有有效期内的产品认证证书，在评标时予以优先采购，具体优惠措施为：在技术部分打分项中加 1 分，投标人须提供相关证明文件。

投标人所投产品列入无线局域网产品清单，应提供相关证明，在评标时予以优先采购，具体优惠措施为：在技术部分打分项中加 1 分，投标人须提供相关证明文件。

评标采用百分制，满分为 100 分。

资格审查表

投标人名称	审查项目												结论
	以招标文件规定的方式获取招标文件	在中华人民共和国境内注册	营业执照等证明	法定代表人授权书	具有良好的商业信誉和健全的财务会计制度的证明文件	纳税和社保记录	无重大违法记录声明	具有履行合同所必需的设备和专业技术能力的承诺函	信用记录	中小企业声明函	分包协议（如有）	投标须知前附表中要求的其他资格要求	

符合性审查表

审查事项		投标人名称	投标人名称	投标人名称
招标文件要求	条款号			
符合联合体规定	1.5			
满足投标人的关联性要求	1.6			
未参与其他服务	1.7			
报价未超过预算或最高限价	2.3			
满足投标范围的完整性要求	8			
未包含价格调整要求	11.3			
保证金符合要求	12.4			
投标有效期满足要求	13.1			
符合强制采购节能产品及信息安全产品要求	20.3			
签署和盖章符合要求	22.2			
未发现串通投标	22.2			
报价说明可以接受	22.2			
无采购人不能接受的附加条件	22.2			
结论				

详细评分表

序号	类别	评审因素	评审标准
1	商务部分 (20分)	资质要求 (4分)	<p>供应商具备以下资质： 供应商具备 ISO20000 服务管理体系认证、ISO27001 信息安全管理体系认证证书，提供以上每项有效期内的资质认证证明，得 2 分，总分 4 分。 需提供证书复印件并加盖公章，未提供或提供不全的不得分。</p>
		系统运维服务经验 (6分)	<p>供应商具备系统运维服务经验，自 2021 年 1 月 1 日起至投标截止日，供应商承担过“公共服务类”、“数据服务类”、“综合行政办公类”、“政务服务类”相关信息化系统的运维或服务经验，每提供一个类别的合同案例得 2 分，最多得 6 分，不提供不得分。 需提供合同首页、金额页、服务内容页、签章页复印件并加盖公章，未提供或提供不全的，不得分。 注：本评分项以供应商提供合同案例覆盖的系统运维服务类别计分，同一类别的多项合同案例不重复计分。</p>
		安全运维服务经验 (8分)	<p>供应商具备安全运维服务经验，自 2021 年 1 月 1 日起至投标截止日，供应商承担过“网络安全攻防演练服务”、“网络安全应急服务”、“网络安全等保测评服务”、“网络安全防护服务”的服务案例，每提供一个类别的合同案例得 2 分，最多得 8 分，不提供不得分。 需提供合同首页、金额页、服务内容页、签章页复印件并加盖公章，未提供或提供不全的不得分。 注：本评分项以合同案例覆盖的安全运维服务类别计分，同一类别的多项合同案例不重复计分。</p>
		办公终端设备维护服务经验 (2分)	<p>供应商具备办公终端设备运维服务经验，自 2021 年 1 月 1 日起至投标截止日，供应商承担过办公终端设备运维服务案例，每提供一个合同案例得 1 分，本项最高得 2 分。 需提供合同首页、金额页、服务内容页、签章页复印件并加盖公章，未提供或提供不全的不得分。</p>
2	技术及服务部分 (70分)	对服务内容 及标准的满足情况 (26分)	<p>【招标文件第七章采购需求】中加“★”的关键指标有 16 项，加“#”的重要指标有 26 项。 加“★”的为关键指标，投标人需针对每项关键指标提供承诺函，不满足任一项，将导致废标； 加“#”的为重要指标，每满足其中 1 项，得 1 分，满足全部要求得 26 分。</p>
		项目理解 (5分)	<p>①供应商对本项目现有信息化系统、基础环境、终端环境、网络安全等现状情况，理解全面、深入，对现状的评估和分析完整、准确、透彻，完全符合项目现状，得 5 分； ②供应商对本项目现有信息化系统、基础环境、终端环境、网络安全等现状情况理解较全面，对现状的评估和分析较</p>

			<p>完整、较准确，基本符合项目现状，得 3 分；</p> <p>③供应商对本项目现有信息化系统、基础环境、终端环境、网络安全等现状情况，理解不全面，不符合项目现状，得 1 分。</p> <p>④未提供相关内容，得 0 分。</p>
		服务方案编制 (7 分)	<p>①服务方案详细，能完全实现服务要求和指标，有针对性，符合本项目实际特点，可实施性强，有清晰、操作性强的服务流程和手册，得 7 分；</p> <p>②服务方案完整，实现关键指标和部分重要指标，针对性一般，基本符合本项目实际特点，可实施性较强，服务流程和手册较清楚，得 5 分；</p> <p>③服务方案基本完整，一定程度可实现关键指标和部分重要指标，针对性一般，可实施性较差，有部分服务流程和手册，得 3 分；</p> <p>④服务方案较差，较难实现关键指标和部分重要指标，针对性和可实施性差，无服务流程和手册，得 1 分；</p> <p>⑤未提供服务方案，得 0 分。</p>
		IT 设备备品、备件方案编制 (3 分)	<p>供应商需制定 IT 设备备品备件方案，详细阐述备品备件的安排计划和保障措施，以满足采购人运维需求。</p> <p>①方案全面、科学、合理、可行，得 3 分；</p> <p>②方案较全面，能够基本满足项目要求，得 2 分；</p> <p>③方案不全面、不合理或不能满足项目要求或未提供管理方案，得 0 分。</p>
		驻场服务团队人员数量保障 (9 分)	<p>①供应商承诺在服务地点能提供驻场维护服务人员总数不少于 37 人，其中应用系统维护人员不少于 11 人，基础环境维护人员不少于 6 人，终端环境运维人员不少于 4 人，网络安全保障人员不少于 16 人，并提供驻场服务团队人员的近 6 个月内任意 1 个月的社保证明，得 6 分；</p> <p>②仅提供驻场维护人员总人数不少于 37 人承诺函的，得 3 分。</p> <p>③其他情况，得 0 分。</p>
		驻场服务团队人员能力保障 (15 分)	<p>①除前述要求驻场维护人员外，供应商能够在采购人北京办公地点派驻 4 人项目管理团队，得 3 分；</p> <p>②除前述要求驻场维护人员外，供应商能够在采购人北京办公地点派驻 2 人项目管理团队，得 1 分；</p> <p>③其他情况，得 0 分。</p> <p>需提供驻场管理团队人员的近 6 个月内任意 1 个月的社保证明。</p> <p>①驻场人员每提供一份信息系统项目管理师（高级）证书，得 2 分，本项最高得 4 分；</p> <p>②驻场人员每提供一份系统集成项目管理工程师（中级）证书，得 1 分；本项最高得 3 分；</p> <p>③驻场人员每提供一份软件设计师（中级）证书，得 1 分，本项最高得 3 分；</p>

			<p>④驻场人员每提供一份网络工程师（中级）证书，得 1 分，本项最高得 3 分；</p> <p>⑤驻场人员每提供一份由中国信息安全测评中心颁发的注册信息安全专业人员（CISP）证书，得 0.5 分，本项最高得 2 分；</p> <p>需提供符合上述要求的职称证书复印件并加盖公章，未提供或提供不全的不得分。</p>
		项目经理能力保障（5分）	<p>供应商需派出两名项目经理，要求具备：</p> <p>（1）与本项目相同或类似领域项目管理工作 8 年及以上经验；</p> <p>（2）注册信息安全专业人员(CISP)证书；</p> <p>（3）具有副高级（含）以上专业技术任职资格或同等资质（包括取得副研究员（含）、高级工程师（含）以上职称）。完全满足此要求，得 5 分；只有一名项目经理满足此要求，得 3 分；其他情况得 0 分。</p> <p>需提供符合上述要求的职称证书复印件及工作履历说明并加盖公章，未提供或提供不全的不得分。</p> <p>需提供项目经理近 6 个月内任意 1 个月的社保证明（投保单位要与供应商主体完全一致）。</p>
3	价格评分（10分）	公式计算	<p>满足招标文件要求且投标价格最低的投标报价为评标基准价，其价格分为满分。其他投标人的价格分统一按照下列公式计算：投标报价得分=(评标基准价 / 投标报价)×10%×100。</p>

注：1. 所有打分分值小数位按四舍五入保留两位计算。

2. 评标方法中对业绩状况的要求以独立法人单位为考核对象。如投标人下属分公司为非独立法人单位，则分公司的业绩可计入投标人的业绩中；如投标人下属子公司为独立法人单位，则子公司的业绩不可计入投标人的业绩中。

第七章 采购需求

国家知识产权局 2024 年局网络安全
保障和局机关信息化系统运维服务
项目采购需求

一、总体要求

（一）服务内容及期限

中标方应整体承接采购人信息化系统运行维护和网络安全保障工作。保障采购人有关信息化基础设施及应用系统的高效、安全、稳定运行，为采购人履行政府职能，对社会公众服务提供信息化基础性保障。

服务内容包括两部分：局机关信息化运行维护保障服务、全局网络安全保障服务。

1.局机关信息化运行维护保障服务：包括采购人委托维护范围内系统的基础环境运维、数据专线保障、应用系统运维、网络安全保障相关服务以及办公终端设备维护服务。

（1）基础环境运维：对服务器、网络设备、安全设备等硬件设备开展定期巡检、日常维护及故障处理，提供不低于原功能性能的设备备件及配件，根据现场紧急状况提供备机；对操作系统、数据库、中间件等软件进行版本升级、日常维护及故障处理，保障系统软件正常运行；提供内外网各一条连接局蓟门桥办公区至老干部活动中心的10M专线链路，保障链路的正常通信使用及网络安全。提供知识产权数据资源公共服务系统运行所需云平台租用，并负责公有云产品日常运行维护，保障系统运行环境安全。

（2）应用系统运维：对应用系统故障提供热线电话、远程在线诊断和故障排除、现场响应等支持服务；提供每月预防性现场巡检服务；对系统基础资源进行监控和管理，及时掌握系统资源现状、运行状态、配置信息、可用性等信息；重要敏感时期按需提供现场值守服务；提供系统整合、优化方案建议并配合实施，提供用户咨询等服务。

（3）局机关信息化网络安全保障：中标方需对运维范围内系统开展网络安全技术防护、统一访问控制、病毒防护、网络安全应急处置、重要时期保障、等保测评、IPv6转换、网站HTTPS安全证书、电子政务外网网络安全保障等服务，保障相关系统的可靠、稳定、安全运行。

（4）办公终端设备维护服务：中标方需提供采购人局机关用户使用的台式计算机、便携式计算机、打印机、传真机等办公终端设备的现场维护和维修；负责鼠标、键盘等配件，打印机硒鼓、墨盒等耗材及IP电话等的配发及维护。

2.全局网络安全保障服务：中标方需面向采购人全局范围内，提供网络安全通报、

应急、检查、培训及宣传等服务；负责网络安全监测平台运营、网络攻防演练、网络安全监测技术等服务。

3.项目整体服务期限为：2024 年 6 月 17 日至 2025 年 6 月 16 日。

（二）服务管理要求

中标方作为技术总责方及项目管理方应坚持用户利益第一的原则，在采购人的管理、监督下开展日常运维工作，整体负责相关信息化系统的可用性、安全性，以及业务的连续性和稳定性保障。为采购人知识产权行政管理相关业务开展、履行政府职能、对社会公众提供服务等提供有力支撑。作为技术总责方及项目管理方，其主要职责目标应包括：

1.标准运维管理体系

按 ISO20000 标准建立规范的运维管理体系，建立结构合理、标准统一、层次清晰的运维服务队伍，持续优化维护管理流程和工作规范。

（1）工作规范管理要求

中标方应根据采购人的运维服务及网络安全相关管理制度要求，持续优化运维保障、应急处置等各类相关制度、规范及技术标准，并贯彻实施。遵循流程和规范组织运维工作，保障各应用系统的稳定正常运行。

（2）流程制度管理

中标方应对流程制度进行管理，包括故障响应、故障处理、故障处理过程管控以及日常巡检，日常资源申请等流程。在重要节假日前，提供相应的应急保障预案和巡检报告，并进行归档。

（3）服务过程管理

中标方应对服务过程进行标准化管理，以确保提高运维服务质量，降低服务成本，降低因 IT 服务中断所导致的业务风险。包括：服务级别管理、配置管理、变更管理、发布管理、事件管理、问题管理等。

（4）系统底数台账管理

中标方需负责详细清理盘点采购人委托维护范围内信息化系统的基本情况，包括：各系统的信息化资产、应用架构、机房部署、网络拓扑结构、等级保护、安全防护情况等，按照采购人要求，建立系统底数台账并及时更新。

2.运维服务

(1) 整体技术运维

负责信息化系统的可用性、安全性、稳定性及业务的连续性保障，确保各项运维服务保障工作有效落实和顺利开展。

(2) 运维需求及知识管理

负责接收用户服务保障要求，分派服务保障任务，跟踪服务保障过程；收集用户运维服务需求信息，接收和反馈用户投诉并报告采购人等；负责建立系统运维保障知识库，有效做好系统各类运维知识收集、管理、使用和共享发布。

(3) 运行状态监控

负责全方位监控系统基础环境和业务应用运行状态，及时发现并上报服务保障异常和业务运行风险情况，定期分析系统使用情况，根据采购人要求开展系统下线评估。

(4) 系统变更优化

负责根据用户需求开展业务系统的缺陷处理、变更和优化。

(5) 运维安全管理

承担系统运维安全保密责任，严格遵守系统运维保密要求，确保运维中的系统安全、数据安全、人员安全。负责严格落实运维请示报告制度，系统相关信息未经采购人允许，不得对外披露。

(6) 应急处置

负责按照采购人需求制定信息化系统重大突发事件应急预案，并报采购人备案。按照预案中关于运维事件分类和等级的要求，第一时间发现、受理各类系统运维事件并进行处置，及时按照有关规定进行分类分级上报和跟踪协调，在规定时限内完成应急事件处理。

(7) 特殊时期保障服务

在特殊时期，如巡视、审计等，提供可靠的终端支持以及配套的网络环境保障，并根据采购人要求增加巡检频次。

(8) 人员要求

在整体服务期间，供应商需提供总数不少于 41 人的服务团队，其中驻场服务人员不少于 37 人（含两名项目经理），项目管理团队不少于 4 人。项目管理团队需在北京办公地点驻场，并负责本项目中的信息化台账、账户、网络接入、资源调配等管

理运营协调工作，网络安全通报、应急、演练、检查、宣传、培训等管理工作，以及办公设备管理、资产管理、软件正版化等工作，并需要保持团队稳定性。

★未经采购人同意，项目经理和项目核心技术人员不做变更。

（三）服务指标要求

中标方应按照采购人对运维服务及网络安全保障服务的总体要求，负责运维服务质量相关的程序、计划、报告的编制或生成。中标方应规范运维服务质量管理，加强运维服务质量管理的有效性，为采购人提供高质量的运维服务，保障相关业务系统的平稳开展。

根据 ISO20000 服务管理体系、ITSS 运维系列标准（国家标准）、制定以下具体要求：

表格 1 服务指标明细表

服务内容	服务指标说明	服务指标	指标重要度
机房内 IT 设备巡检	日常巡检	不低于 2 次/天	#
	深度巡检	不低于 1 次/月	
应用系统巡检	日常巡检	核心系统不低于 1 次/天；其他系统不低于 2 次/周	#
	深度巡检	不低于 1 次/月	
应用系统故障处理	应用系统故障事件	30 分钟内响应，5×9 小时现场服务，7×24 小时电话咨询服务	★
	核心系统	2 小时解决，每 2 小时向采购人汇报故障处理进展情况，故障处理完毕后向采购人提供处理报告	★
	重要系统	4 小时解决，每 2 小时向采购人汇报故障处理进展情况，故障处理完毕后向采购人提供处理报告	★
	一般系统	6 小时解决，每 2 小时向采购人汇报故障处理进展情况，故障处理完毕后向采购人提供处理报告	★
系统非计划中断发生次数	在约定的服务时间内，发生系统非计划中断的次数	≤3 次	★
集中监控	现场集中监控服务	提供 7×24 小时现场集中监控服务，在 30 分钟内对监控告警作出响应	#
机房内设备备品/备件/备机服务	负责维保中涉及的机房内设备的备品备件的提供、部署或	7×24 小时机房内设备全天候备件服务，包括设备重要部件、常用机型易损配件等	#

服务内容	服务指标说明	服务指标	指标重要度
	更换服务		
办公终端设备维护驻场服务	工作日工作时间提供驻场服务	工作日 5×8 小时	★
办公终端运维事件处理	事件响应时长和解决率	30 分钟响应并到达现场，事件平均 2 小时解决，且全年事件解决率不低于 90%	★
网络安全应急响应服务	网络安全事件应急处理	7×24 小时电话支持，5 分钟内响应，工作时间提供 5×9 小时驻场应急支持服务，非工作时间 2 小时内到场。	★
网络安全监测服务	提供日常网络安全监测、分析研判及配合处置服务	7×24 小时电话支持，30 分钟内响应，工作时间提供 5×9 小时驻场服务，非工作时间 2 小时内到场	#
网络攻防演练服务	提供网络攻防演练期间防守相关工作	7×24 小时现场值守，10 分钟内响应支持服务	★
服务报告	需提供系统运维服务周报、月报、季报、年报，记录系统运行、资源使用、故障处置、巡检情况和维护记录等，按月提供统一监测平台运行统计分析报告，对于重大故障或安全事件，提交专项处置报告。	保证服务文档的可读性、标准化和有效性，以及文档数据的准确性。 服务报告频次： 周报为次周 1 个工作日内提交； 月报为次月 5 个工作日内提交；季报为次季 10 个工作日内提交；年报为次年 20 个工作日内提交；故障或安全事件处置报告为事件解决后 5 个工作日内提交；重保、等保测评、攻防演练等专项报告为活动结束后 10 个工作日内提交。	#
	需提供重要敏感时期安全保障情况报告、网络安全等级保护测评报告、攻防演练专项报告等。		

备注：1. ★为关键指标，中标方需完全满足的服务指标；#为重要指标。

二、局机关信息化运行维护保障服务内容

局机关信息化运行维护保障服务：包括基础环境运维、数据专线保障、应用系统运维、局机关信息化网络安全保障、办公终端设备维护服务等。具体情况详见下表：

表格 2 局机关信息化系统及基础环境维护服务范围清单

序号	系统名称	上线时间	系统级别	应用系统服务期限	软硬件服务期限	链路服务期限
1	全国专利管理信息平台	2011 年	重要	9 个月	9 个月	无
2	专利代理管理系统	2011 年	重要	9 个月	9 个月	无

序号	系统名称	上线时间	系统级别	应用系统服务期限	软硬件服务期限	链路服务期限
3	全国专利代理师资格考试考务系统	2009 年	核心	9 个月	9 个月	无
4	知识产权数据资源公共服务系统	2023 年	重要	7.5 个月	无	无
5	公文智能交换管理系统	2022 年	重要	12 个月	12 个月	无
6	离退休干部工作管理信息系统	2009 年	一般	12 个月	12 个月	无
7	老干部活动中心信息化项目	2018 年	一般	无	12 个月	12 个月
8	外观设计专利检索公共服务系统	2023 年	一般	12 个月	12 个月	无
9	档案管理系统	2022 年	重要	12 个月	12 个月	无
10	公共服务网	2020 年	核心	12 个月	12 个月	无

重点备注：

- 1.中标方需提供内外网各一条连接采购人北京蓟门桥办公区至老干部活动中心的市内 10M 专线链路（上表序号 7），并保障链路网络安全。
- 2.知识产权数据资源公共服务系统所需环境在公有云服务中提供。
- 3.硬件未出保设备需提供日常运行维护服务，电子政务外网提供沟通协调服务。

（一）基础环境运维服务

1.制度流程管理

对属于招标范围内的 PC 服务器及小型机、存储、数据库、中间件、网络、安全相关的流程制度进行管理，包括故障响应、故障处理、故障处理过程管控以及日常巡检，日常资源申请等日常流程。执行故障响应流程，对范围内故障来源进行分析，满足各设备的故障响应条件和机制。执行故障处理流程，分为一般故障处理和重要故障处理流程，并形成相应的汇报机制。执行故障处理管控流程，形成对故障处理流程的执行规范，形成在流程执行过程中文档的存放及更新机制。执行日常巡检类流程，提供相应设备的巡检手册，包含标准、流程及记录模板。执行检查流程，提供设备的健康检查手册，包含标准、流程及记录模板等。执行深度巡检类流程，在重要节假日前，提供相应的应急保障预案和巡检报告，并进行归档。

2.硬件设备管理

PC 服务器和小型机日常巡检

工作日对 PC 服务器和小型机进行现场巡检、非工作时间通过监控平台处理告警信息。在特殊时期、巡视审计等时期根据采购人要求增加巡检频次。

PC 服务器和小型机深度巡检

对 PC 服务器和小型机进行现场深度巡检、预防性维护，以满足服务器的运行要求。

PC 服务器和小型机重要保障服务

重大节假日和特殊时期按要求对 PC 服务器和小型机提供保障服务。

网络设备日常巡检

通过集中监控平台、人工现场巡检等方式对网络设备硬件状态进行监控。在特殊时期、巡视审计等时期根据采购人要求增加巡检频次。

网络设备深度巡检

对网络设备进行现场深度巡检、预防性维护，以满足网络设备的运行要求。

网络设备重要保障服务

重大节假日和特殊时期按要求对网络设备提供保障服务。

安全设备日常巡检

对安全设备进行现场巡检，以满足安全设备的日常运行要求。在特殊时期、巡视审计等时期根据采购人要求增加巡检频次。

安全设备深度巡检

对安全设备进行现场深度巡检、预防性维护，以满足安全设备的运行要求。

安全设备重要保障服务

重大节假日和特殊时期按要求对安全设备提供保障服务。

存储设备和备份系统日常巡检

现场巡检，通过监控平台监控存储设备和备份系统运行情况。在特殊时期、巡视审计等时期根据采购人要求增加巡检频次。

存储设备和备份系统深度巡检

对存储设备和备份系统进行现场深度巡检、预防性维护，以满足存储设备和备份系统的运行要求。

存储设备和备份系统重要保障服务

重大节假日和特殊时期对存储设备和备份系统进行现场保障和健康检查，对监控

平台中的重要报警进行实时响应。

3.基础软件管理

产品软件日常巡检

对操作系统、数据库、中间件等产品软件进行日常巡检。在特殊时期，如巡视审计等时期，根据采购人要求增加巡检频次。

服务器类产品软件补丁服务

按照采购人的补丁测试流程完成补丁测试评估报告，制定保障方案，在获得采购人认可的前提下，按照实施方案组织补丁安装实施工作。

#4.故障处理

对采购人范围内的 PC 服务器及小型机、存储、备份、操作系统、数据库、中间件、网络设备、安全设备等发生的故障进行处理。对相关的故障信息进行沟通，记录故障发生时间和其他相关信息，进行故障初步分析，对故障的影响做出评估，按照故障处理流程，协调完成故障处理工作，管理和记录相关信息，对结果进行审核和汇报。

#5.维保服务

提供基础软硬件维保服务，包括服务器、操作系统、数据库、中间件、存储设备、网络设备和安全设备等。服务内容包括进行预防性维护服务，现场设备巡检；在规定的时限内排除硬件故障，进行备件备机等更换；提供操作系统、数据库、中间件的高可用性能优化服务；提供设备升级服务、产品升级在内的产品服务；提供网络设备监控和性能检测分析服务；提供安全设备策略调整优化技术支持服务。在采购人实施重大项目，如网络改造、系统切换、系统升级、机房搬迁或机房停电等时，需要中标方配合或协助时，提供运维支撑服务。

6.资源管理

对属于招标范围内的 PC 服务器及小型机、存储、备份、数据库、中间件等基础应用维护的资源进行管理，对相应的流程制度进行改进等。提供资源使用规划，执行资源回收、优化及调整，审核资源分配相关操作。

运维资料管理，按照采购人要求收集并审核运维相关的资料，包括收集网络安全系统配置信息、关联关系、基础数据、资源分配、权限管理等信息。

对属于招标范围内的硬件设备、基础软件、网络信息、安全信息及 VPN 配置信息进行管理，配置管理流程包括创建配置管理数据库，维护配置数据以及定期对配置

信息进行检查和审核。制定合理的配置信息如：硬件基本信息、运行状态、软件版本号、操作系统，通过这些信息真实的反映出管理对象的技术指标和应用情况。保证数据的准确性、可靠性和有效性。按需给采购人提供配置数据。

#7.数据专线保障

提供内外网各一条连接采购人北京蓟门桥办公区至老干部活动中心的市内 10M 专线链路，保障链路的正常通信使用。

#8.公有云平台租用

为知识产权数据资源公共服务系统提供满足等级保护测评要求三级的公有云租用；并提供公有云产品日常运行维护，保障系统运行环境安全，服务内容包括共有云产品配置、日常巡检、故障处理、应急处置、漏洞修复、补丁升级、病毒查杀、核心数据备份、IPv6 转换服务、短信服务等。公有云产品及规格主要参数详见下表：

表格 3 公有云产品及规格明细表

序号	产品名称	参数及配置	数量
1	负载均衡	提供负载均衡服务	3
2	IPv6 服务	提供 IPv6/IPv4 转换服务	1
3	云服务器	4 核 8GiB, 40GiB, 数据盘 SSD: 64GiB	4
		2 核 8GiB, 40GiB, 数据盘 SSD: 64GiB	4
		2 核 4GiB, 40GiB, 数据盘 SSD: 64GiB	2
4	云数据库 MySQL	MySQL8.0, 高可用版, 4 核 8G, 40GB	1
5	文件存储	通用型 (50T)	1
6	弹性公网 IP	支持 BGP 线路	14
7	共享带宽	800M	1
8	主机安全	企业版	10
9	Web 应用防火墙	黑白名单个数: 20 个, 单域名 CC 防护规则个数: 5 个, 子域名数量: 10 个, 一级域名数: 1 个	1
10	云堡垒机	存储空间不小于 500G, 管理节点数量: 20	1
11	日志审计	存储空间不小于 500G, 支持日志源数量: 20	1
12	云防火墙	4 核/16G; 120G, 吞吐量: 2Gbps	2
13	数据库审计	合规性管理功能, 实现合规报告	1
14	SSL 证书	域名型 (DV) 通配符 SSL 证书	1
15	虚拟私有网络	专有网络 VPC	1
16	短信服务		1

（二）应用系统运维服务

1.系统相关情况简介

（1）全国专利管理信息平台

全国专利管理信息平台为支撑我局与地方局之间业务交流所需的管理信息平台，涵盖了法律规章及与知识产权相关文件公告、规划与计划管理、地方管理工作评价等业务内容，方便各地方知识产权局更快、更及时的获取相关数据；满足部分地方局对于数据特殊化的需求；提高专利管理工作效率。

（2）专利代理管理系统

专利代理管理系统主要实现了代理机构、代理人基本信息、管理信息的电子化，管理流程的电子化；实现电子审批及相关系统自动获得代理机构、代理人的相关信息，为实现智能化代理审查提供数据基础；建立更丰富数据指标的代理机构和代理人的评价体系；最终达到专利审批与代理专利代理管理的业务充分融合。

（3）全国专利代理师资格考试考务系统

全国专利代理师资格考试网上考务管理信息系统，以考务管理中心为平台，对各考点知识产权局的考务工作实行统一管理、全面规划，为考务管理工作提供便利服务，对社会公众提供考试网上报名和成绩查询等服务。

（4）知识产权数据资源公共服务系统

知识产权数据资源公共服务系统是支撑国家知识产权局知识产权信息公共服务工作重要的信息系统。该系统为社会公众，知识产权公共服务节点网点单位，确有知识产权数据需求，且具备知识产权数据加工处理和分析利用能力的服务机构和创新主体等提供知识产权数据服务。实现对国家知识产权局拥有的各类数据的统一管理，工作人员可以对数据资源进行全面、及时的掌握；可根据区域/地方常态化以及个性化的数据请求，高效快捷的调配全局甚至全行业的专利数据资源；实现对常态化数据的定期分发，对个性化数据请求的及时分发。

本系统以我局原来的知识产权数据资源管理系统（下称“国数系统”）为基础，迁移了原专利数据服务试验系统的用户数据，优化了原国数系统的功能，国数系统升级优化为现在的知识产权数据资源公共服务系统，同时下线了原专利数据服务试验系统，提升了信息化资源利用效率，节约财政资金、增强网络安全防护能力、改善用户体验。

(5) 公文智能交换管理系统

公文智能交换管理系统是一套包含软硬件的机要文件管理系统，该系统利用条码和自动化识别技术，实现对机要文件和信件的信息化管理，从而动态、准确、全面的掌握与共享查询文件和信件的流转状态信息。该系统包括文件登记、业务管理、交换员自助、语音短信提醒等功能。

(6) 离退休干部工作管理信息系统

离退休干部工作管理信息系统主要功能为实现离退休干部工作人员各类信息资源的共享，该系统以离退休人员基本数据为基础，与有关功能模块中的特殊信息相结合，实现多种检索应用和综合统计功能。该系统实现离退休干部部各项工作的一体化、垂直化管理的目标，达到部门内部的无纸化办公要求。

(7) 中国外观设计检索公共服务系统

中国外观设计检索公共服务系统利用“基于内容的图像检索技术”，实现外观设计专利图像内容的检索，并与基于全文检索技术的文字检索功能结合，建立一套全新的检索模式。该检索系统依据一定的规则，对外观设计专利的图形图像进行自动识别和基本判断，保留可作为对比文件的设计，过滤掉绝大多数没有价值的设计，把有价值的检出对象缩小到最小范围。用户范围涉及：地方局、代办处、保护中心、快速维权中心、省级知识产权公共服务机构、地市级综合性知识产权公共服务机构、TISC 机构、高校国家知识产权信息服务中心、国家知识产权信息公共服务网点，以及有需要的创新主体等。

(8) 档案管理系统

档案管理系统主要实现电子档案接收采集、归档编目、检索利用、鉴定统计、档案编研等档案业务管理功能；实现对已有文件资料信息资源的科学整合、集中管理、长久保存、有效利用、安全共享，保障电子档案的真实性、完整性、有效性和可用性。

(9) 公共服务网

公共服务网整合了局内现有知识产权公共服务资源平台，实现了专利、商标、地理标志、集成电路布图设计的申请、缴费、信息查询、检索及数据下载等服务“一网通办”，实现了全国知识产权公共服务机构一体化查询，为全国的创新创业主体和社会公众提供了便捷、高效的知识产权公共服务。实现了国务院客户端小程序、中国科学院知识服务平台等 120 余个外部网站链接公共服务网，实现公共服务网在副省级以

上知识产权管理部门网站链接的全覆盖。公共服务网主要包括网上办事、信息服务、行政许可、在线公益课堂、公共服务机构查询、服务事项通知以及地方特色等栏目。

2.服务过程管理

(1) 服务级别管理

中标方应与采购人就服务内容和指标达成协议，中标方按照双方达成的协议提供服务，应定期测量所提供的服务是否满足服务级别协议，并制定和实施服务改进计划，提高服务质量，保证系统运行的稳定性、可靠性。

(2) 服务报告管理

中标方需按照采购人规定按时提供运维服务报告，服务报告分为定期和不定期，不定期的服务报告应根据相应事项规定的时限出具，定期服务报告按周期分为周报、月报、季报、年报。服务报告的范围包括但不限于运维周报、月报、季报、年报，记录系统故障情况、巡检情况和维护记录、重大事件处理报告等。服务报告的内容包括但不限于：

信息化系统整体运维工作情况；

信息化系统运行使用情况；

信息化系统运维服务情况；

对运行使用情况和运维服务情况的回顾与改进分析；

专项工作的专项报告。

中标方在提供服务期间需能够按照采购人需求调整运维服务报告内容。

(3) 事件管理

事件管理着重管理的是对事件的响应速度和尽快恢复业务运作的的能力。事件管理负责对事件进行查明和记录、分类和初步支持、调查和分析、解决和恢复，其目标是在尽可能短的时间内恢复业务系统的正常运转，同时记录事件并为其提供其他流程的支持。事件流程建设的目标为：规范生产事件管理工作流程，保证生产系统安全、稳定、高效运行。允许预先定义事件的分类（严重等级、影响程度、紧急程度的分类）和优先级信息。事件可以和问题、变更、配置等相互关联。

(4) 问题管理

问题管理的目标是将由业务系统错误引起的事件和问题对业务的影响减少到最低程度；查明事件或问题产生的根本原因，制定解决方案和防止事件再次发生的预防

措施；实施主动问题管理，在事件发生之前发现和解决可能导致事件产生的问题。从问题申报、归类、分派、处理到最后结束，所有的过程均在问题管理中进行了严格合理的定义。其间所涉及到的各类人员：如最终用户、维护人员、二线支持人员和专家组、管理层等，都会在指定的范围和规范化的框架和流程下进行日常工作。从而保证问题处理的所有环节有条不紊，并具有最优效率。提供问题的分类（严重等级、影响程度、紧急程度的分类）和优先级。对已经找到根本原因但暂时无法根本解决的，通过独立的已知错误管理流程进行管理，要求提供临时解决方案。对于已经找到根本原因且有解决方案的问题，可以提交知识条目给知识管理。

问题审计：能够记录数据变化前后的修改人、时间进行记录保证数据的安全性。

中标方应构建运维服务知识库，实现知识的积累，便于查询和更新。知识库应使参与事件处理的所有人员可访问，帮助提高故障的一线解决率，帮助解决已知错误故障，有效减少故障恢复时间。知识库和知识管理流程应按规范管理，具有对知识条目进行规范管理的流程（创建，审核，发布，撤回等）；知识条目可按产品、用户群、业务领域、地点等进行分类，知识可设定维护责任人。

（5）变更管理

变更管理是指为在最短的时间内，安全、准确地完成各业务系统的任一方面的变更而对其进行控制的服务管理流程。其目标主要是为了保证对变更的有效控制，确保在实施过程中使用标准的方法和步骤，准确高效地完成变更任务，减少由于变更引起的影响业务效率的突发事件，降低可能带来的负面效应。提供变更的分类和优先级。

能够提供大量的字段记录变更的详细信息如：实施日期、相应资源、请求人、实施者、实施计划等。

提供变更风险评估功能，可以基于配置管理数据库提供的数据库模型进行影响模拟分析。

变更审计：能够记录数据变化前后的修改人、时间进行记录保证数据的安全性。

（6）配置管理

中标方需为采购人建立维护服务档案，记录所有设备系统配置、维护记录等信息。中标方应定期进行配置审核，维护配置信息完整性、准确性。每个配置项的配置信息应包括：

唯一性标识；

配置项类型；
配置项描述；
与其它配置项的关系；
状态。

配置项应受控，配置项的变更应可追溯和可审计。配置项在进行相关的变更发布后，配置项应及时更新。

(7) 发布管理

发布管理的目的在于全盘了解 IT 服务的过程，并确保考虑到发布的所有方面，包括技术和非技术方面。适用于：

发布大型或关键硬件
发布主要软件
打包或成批的系列变更

通过发布成功率提高和业务中断率降低，从而改进服务的质量，降低使用非法、存在缺陷或未经授权软件的几率。

3.应用系统维护

中标方需保障应用系统的稳定运行，完成应用系统维护工作，维护工作包括但不限于以下内容：

(1) 日常例行维护

定期对应用系统进行预防性日常巡检，做好巡检记录，发现问题及时处理或上报。在特殊时期，如巡视审计等时期，根据采购人要求增加巡检频次。

通过自动化监控工具，包括但不限于集中监控系统，监控系统和设备的运行状况，及时发现潜在隐患及故障等。

按采购人要求定期执行系统数据备份操作，并定期检查备份执行情况，做好记录。

负责日常故障导致的应用程序安装部署。运行环境变更和迁移导致的应用系统重新安装和部署不在本合同规定的工作范围内。

对具备演练条件的系统按照采购人的要求，配合采购人完成容灾演练。

重大节假日和特殊时期按要求对应用系统提供重点保障服务。

(2) 事件及故障处理

按照采购人的工作流程处理用户关于应用系统的报修。对用户报修故障进行记录

并跟踪，并将处理情况和结果反馈采购人。

应用系统故障的处理。对应用系统发生的故障，进行故障定位并协调跟踪处理，处理过程要遵循相应的服务流程规范执行，重大故障要按照故障上报制度及流程上报处理，管理和记录相关信息，对结果进行审核和汇报。

按照采购人的流程，实施应用系统的重大操作，如停启系统等。

按采购人要求，从应用系统层面评估防病毒软件或操作系统补丁对应用系统可用性的影响；在发生病毒事件时，从应用系统层面配合采购人处理病毒事件。

（3）咨询及答疑

为用户提供应用软件使用咨询，对在应用系统软件使用过程中出现的有关使用方面的疑问进行解答、培训、咨询。

#（4）应用数据维护

根据用户要求，进行应用数据维护工作。数据维护的工作包括：

按要求进行业务数据的提取和统计。

按要求提供系统使用情况的统计数据。

按要求提供关于系统信息的统计数据。

按要求进行批量及个别数据的修正。

#（5）数据更新服务

中标方需负责对知识产权数据资源公共服务系统涉及的数据资源（约 83 种），按照采购人要求的更新周期，制定更新计划，协调数据产品提供方、按照数据资源规范要求，完成数据资源核查、数据资源包组织、数据资源上传更新以及过档数据资源回收工作；及时监管数据资源上传、下载情况，处理数据资源上传、下载问题，维护并更新常见问题处理，分析统计数据资源上传、下载情况，并定期形成服务报告。

#（6）系统完善及优化

中标方应负责维护范围内系统应用程序的 BUG 修复。对在用户使用过程中发现的系统 BUG 进行修改，并进行应用程序发布。按采购人要求提供应用系统的优化建议，必要时形成优化方案技术文档。

（7）项目配合

项目配合工作是指在项目开展的各个时期以采购人项目组为主，从有利于项目正

常进展的角度，进行的一系列协助工作。主要包括以下内容：

采购人在实施重大项目，如系统切换、系统升级、服务器虚拟化系统迁移、机房搬迁或设备搬迁等时，需要中标方配合或协助，中标方积极响应及时指派资深系统人员现场协助及指导，提供现场技术支持和后续维护保障工作。必要时，形成技术方案建议等文档。

按照采购人要求及流程提供应用系统下线服务。

按照采购人要求，对其职能范围内中办专网、中纪委专线、党委督查专网、电子政务内网、电子政务外网等网络进行相关配置或协调工作。

（三）局机关信息化网络安全保障服务

#1.网络安全云端及主机防护服务

针对采购人 5 个局机关重要互联网业务系统（域名）部署云端安全防护，包括全国专利代理师资格考试考务系统、公共服务网、全国专利管理信息平台、知识产权数据资源公共服务系统、外观设计专利检索公共服务系统等，对系统进行 Web 攻击防护，拦截互联网方面的攻击行为。尤其在重要保障时期，提升系统安全性，保障系统稳定运行。

对招标范围内 6 个等保测评三级系统开展渗透测试，以模拟黑客入侵的方式对专利代理管理系统、全国专利代理师资格考试考务系统、局门户网站、内网网站、公共服务网、全国专利管理信息平台、知识产权数据资源管理系统（升级改造后名称为：知识产权数据资源公共服务系统）、外观设计专利检索公共服务系统、公文智能流转系统、档案管理系统和“互联网+监管”简版系统等进行攻击测试，识别系统存在的安全风险，组织整改修复和复测验证，有效完善系统的安全性。

对采购人委托维护服务范围内系统，提供包括日常一体化实时安全监测分析研判、每两周一次深度态势及系统病毒防护深度分析。及时发现并清除业务系统主机存在的病毒问题及清除监测所发现的问题，完成风险跟踪处置，提升网络的主动防御能力。

#2.统一访问控制服务

对采购人委托维护服务范围内系统，中标方需提供统一访问控制服务，包括开展运维账号资源管理、流程制度设计、运维安全审计、审计数据分析等统一访问控制服务。实现统一访问控制，可以识别操作用户的身份，快速定位故障原因和责任人。

3.病毒防护服务

★对采购人委托维护服务范围内所有系统的相关设备提供病毒防护服务，负责防病毒软件的授权更新（包括运维范围内所有服务器，国产台式机 77 台，X86 台式机 105 台，国产笔记本电脑 48 台）。

中标方需提供对控制台定期巡检、定期进行病毒扫描及处置，对病毒库进行定期更新，策略下发；定期进行人工分析，提供处置建议；在发生病毒事件时，处理病毒事件。

4.网络安全应急服务

★对采购人委托维护服务范围内的所有系统，中标方需负责网络安全应急事件处置。

对采购人委托维护服务范围内系统，中标方需负责制订整体应急预案，定义应急事件类型和特征，明确事前、事发、事中、事后的各个过程中相关部门和有关人员的职责。协调组织完成应急演练，根据演练情况，进一步检查应急保障措施和应急预案的完整性和可行性。

发生网络安全事件时，按照应急预案执行应急响应流程，并制定针对性的技术解决方案；提供 7×24 小时现场应急响应技术支持服务，对网络安全事件开展事件调查、分析、评估、处置。对于网络安全应急事件，应急事件处置完成后，提交应急事件处置报告，对事件发生的原因进行分析，回顾事件处理过程，提出整改建议，预防类似事件的发生。

5.重要时期保障服务

★在党和国家重大会议活动、知识产权宣传周、网络攻防演练、法定假日等重要敏感时期，中标方需按采购人要求提供重点保障，拟定重要时期工作计划和应急预案，提供实时监测、值班值守和应急处置等各项网络安全保障服务。完成重要时期安全保障工作，保障工作结束后形成总结汇报报告。

重要时期保障准备：重要时期保障期间，按照采购人要求完成重点保障总体工作计划及保障预案，包括业务管理、应用系统、基础环境等整体保障，做好人员、设备、资金准备。

重要时期保障实施：建立重保值班制度，确定紧急联系人，以确保系统出现问题时，及时响应处理，派驻工程师驻场。提前一周进行现场巡检及预防性维护，检查各

类设备、系统运行状况。根据实际情况，进行预防性检查维护，确保应用系统和基础环境的稳定运行。

重要时期保障总结：协调组织各相关方完成重保，回顾整个总结重要时期保障过程，总结经验和不足，形成汇报报告。

6.等保测评服务

★对采购人委托维护服务范围内 9 个信息化系统和内网网站（详见下表），依据网络安全等级保护最新标准要求，开展系统网络安全等级保护测评相关工作，使系统最终能够符合网络安全等级保护要求，通过安全测评，形成等级保护测评报告。

对信息系统开展等保测评，衡量信息系统的安全保护管理措施和技术防护措施是否符合等级保护基本要求，是否具备了相应的安全保护能力，完成系统定级备案，等级保护测评工作，根据测评发现的问题，中标方应形成整改方案，针对性的制定整改措施，推进网络安全防护体系不断完善，进行不涉及硬件采购的整改实施，如需硬件采购的应向采购人提出采购需求和方案，使系统最终能够符合网络安全等级保护要求，通过安全测评，形成等级保护测评报告。

表格 4 等保测评情况表

序号	系统名称	定级	等保测评需完成时间
1	专利代理管理系统	第三级	2024 年 12 月前
2	全国专利代理师资格考试考务系统	第三级	2024 年 12 月前
3	全国专利管理信息平台	第三级	2024 年 12 月前
4	外观设计专利检索公共服务系统	第三级	2024 年 12 月前
5	知识产权数据资源公共服务系统	第三级	2024 年 12 月前
6	公共服务网	第三级	2024 年 12 月前
7	档案管理系统	第二级	2025 年 6 月前
8	公文智能交换管理系统	第二级	2025 年 6 月前
9	离退休干部工作管理信息系统	第二级	2025 年 6 月前
10	内网网站	第二级	2025 年 6 月前

#7.IPv6 转换服务

对采购人委托维护服务范围内网站系统提供 IPv6 转换服务，需满足《推进互联

网协议第六版(IPv6)规模部署行动计划》等政策的相关要求，满足新技术新业态的安全保护措施要求，并和网站安全监测防护相结合，对 IPv6 网站流程进行监测审计，保障网站平稳有效。

#8.网站 HTTPS 安全证书

对采购人委托维护服务范围内未采用加密保护的网站,提供 SSL 通配符证书服务,加密用户与网站间的交互访问,强化网站用户端的可信展示程度,防劫持、防篡改、防监听,实现网站的可信认证与数据安全传输,避免数据流量被劫持篡改等,提升网站安全性。

#9.电子政务外网网络安全保障

对采购人电子政务外网网络安全设备进行监控、巡检、策略配置调整、权限管理、基线管理、日志采集分析等工作。主动发现安全威胁,评估安全风险,做好网络安全设备问题整改。提供网络安全设备事件处置以及重要时期安全保障服务。

(四) 办公终端设备维护

#1.办公终端设备维护

负责采购人局机关用户办公终端设备日常报修的及时响应,负责范围内终端设备(台式计算机、笔记本、打印机等)的系统配置、驱动安装、软件及操作系统类故障的诊断及处理,负责范围内终端设备的硬件故障分析、诊断,对重要用户提供全程高标准服务,在重要时期、巡视审计等临时需要终端的时期,提供终端支持;负责台式计算机、笔记本的硬件兼容性测试,负责台式计算机、笔记本的标准化系统制作与测试。

台式机主要型号有:世恒 DF716、世恒 KF510、世恒 ZF510、联想启天 M5900 等,约 182 台。

笔记本主要型号有:长城 UF716、联想 T400 等,约 93 台。

打印机主要型号有:光电通 OEP400DN、MP4020DN、奔图 P3305、长城 C260/A260、施乐 7100(彩色)、HP2025、HP4025、HP5200、京瓷 P4040DN/P4035DN、OKI C830、佳能 PIXMA IP110/100(彩色)等,约 193 台。

扫描仪主要型号有:光电通 OES200、HP5590 等约 12 台。

多功能一体机主要型号有:光电通 MP4020DN、联想 M7650DNF 等,约 13 台。

#2.耗材及配件配发维护

负责为采购人局机关用户提供周边配件、IP 电话、打印机硒鼓墨盒等的配发维护服务。

(1) 周边配件包括：有线鼠标、有线键盘、无线鼠标、无线键盘、插线板、KVM 切换器、无线网卡、扩展坞、外置光驱、打印线（1.5 米和 3 米两种规格）、网线（1.5 米、3 米和 5 米三种规格）、USB 延长线（2 米规格）。

(2) 涉及 IP 电话型号：Huawei eSpace 7910、Fanvil X3SP 等。

(3) 涉及硒鼓的打印机型号：光电通 OEP400DN、MP4020DN、奔图 P3305、长城 C260/A260、施乐 7100(彩色)、HP2025、HP4025、HP5200、京瓷 P4040DN/P4035DN、OKI C830、佳能 PIXMA IP110/100（彩色）等。

(4) 涉及条码打印机型号：汉印 IT4P（1 台），相应配件扫码枪：紫光 FS1650（2 把）。

#3.办公终端设备硬件维修

负责采购人局机关用户办公设备维护范围内因硬件故障的无法使用的办公终端设备进行故障分析，配合采购人局机关进行资产残值评估，按照《行政事业性单位国有资产管理条例》要求，对应报废的办公终端设备提供报废鉴定服务，对于未达到报废条件的办公终端设备进行硬件维修，确保设备正常使用。

4.办公终端设备巡检清查

负责采购人用户办公终端设备的巡检清查服务，根据采购人的需求，对用户信息化办公终端设备的使用及相关信息情况进行巡检清查，做好记录。

三、全局网络安全保障服务

#（一）网络安全通报、应急指导及自查迎检服务

完善健全并执行采购人网络与信息安全通报机制，将问题通报、应急处置与应急响应进行统一协同联动。提高通报预警、信息共享、事件处置等工作的及时性、有效性。

服务内容主要包括及时更新维护采购人各部门单位网络安全应急联系人名单；汇集通报网络与信息安全隐患情报，对网络安全风险提前预警；负责重要敏感时期网络安全保障任务通报工作，负责对采购人局统一网络安全监测平台发现的网络安全事件

具体工作包括准备阶段、实施阶段及复盘阶段的工作。中标方在攻防演练活动准备阶段、实施阶段、复盘阶段三个阶段提供技术服务。

准备阶段：协助采购人制定演练技术方案，完成资产梳理和收集工作。对现有资产进行互联网暴露面探测、漏洞检测等工作。对运维服务范围内信息系统发现的问题隐患，及时完成整改加固；对采购人其他部门单位信息系统的问题隐患，整理提出安全加固建议，协助相关部门单位完成整改，并提供技术指导。

实施阶段：以驻场服务形式向采购人提供安全监测值守、应急响应处置和攻击溯源、威胁情报收集以及安全决策能力支撑服务。

复盘阶段：对演练期间出现的安全事件进行汇总，协助采购人进行复盘分析，对暴露的问题进行复测，并检查整改完成情况，协助编制总结报告，及时发现现有防护手段的缺失与防护工作中的不足之处，为后续常态化的网络安全防护措施提供优化依据。

（五）网络安全监测技术服务

★中标方需提供包括安全漏洞通报服务、网站安全监测服务、联网终端安全监测服务等内容的网络安全监测技术服务。

具体工作包括以下内容：

（1）安全漏洞通报服务：

依托拥有的国家信息安全漏洞共享平台（CNVD），收集、分析涉及采购人的安全漏洞，一旦发现涉及用户相关产品安全漏洞，第一时间向用户单位邮件通报，并向用户单位提供远程技术支持服务。安全漏洞通报涉及产品类型包括网上银行、手机银行、自助体验终端等，具体产品清单可由用户单位提供。漏洞通报内容包括漏洞事件、漏洞引发的威胁、评分评级、影响产品、信息来源、漏洞描述、影响范围、漏洞验证情况、通报时间等。

（2）网站安全监测服务：

依托国家网络安全监测平台，在我国公共互联网上，开展针对用户单位拥有的网站的网络安全外围性监测和预警通报，协助用户单位及时发现网站的安全事件和存在隐患。在监测发现针对用户单位网站的一般安全事件后，及时以邮件形式内向用户单位指定人员通报；监测发现较大级别以上的网络安全事件后，供应商第一时间通过电话或短信向用户单位指定人员通报，同时以邮件形式通报事件发生具体情况，并对用

户单位处置这类安全事件提供一定的远程技术支持服务。

(3) 联网终端安全监测服务：

依托国家网络安全监测平台，在我国公共互联网上，针对用户单位接入互联网的计算机感染木马、蠕虫、僵尸程序等恶意程序事件进行外围性监测和预警通报，协助用户单位及时发现联网终端被恶意程序攻击的情况。在监测发现用户单位联网终端 IP 地址感染恶意程序事件后，按周（或天）汇总并以邮件形式向用户单位指定人员通报，通报内容应包括恶意程序事件的源 IP 地址、目的 IP 地址、源端口、目的端口和发生时间。

附件：机房内 IT 设备运维清单

序号	类型	品牌	型号	数量	硬件维保截止时间
1	服务器	HP	RP7420	1	2024.6.16
2	服务器	HP	RP7410	1	2024.6.16
3	服务器	IBM	xSeries 366	4	2024.6.16
4	服务器	IBM	xSeries 336	3	2024.6.16
5	服务器	HP	DL580G7	6	2024.6.16
6	服务器	IBM	X3650 M3	3	2024.6.16
7	服务器	IBM	X3850 M2	2	2024.6.16
8	服务器	IBM	X3850 X6	2	2024.6.16
9	服务器	HPE	DL560 Gen10	4	2024.6.16
10	服务器	HPE	DL380Gen10	5	2024.6.16
11	服务器	HPE	DL380Gen8	5	2024.6.16
12	服务器	HP	DL380 GEN9	5	2024.6.16
13	服务器	HP	DL180 G6	1	2024.6.16
14	服务器	HP	HPDL580 GEN9	6	2024.6.16
15	服务器	HP	HP DL580G4	8	2024.6.16
16	服务器	联想	RD630	4	2024.6.16
17	服务器	联想	M710s	2	2024.6.16
18	服务器	联想	RD430	6	2024.6.16
19	服务器	联想	R680	2	2024.6.16
20	服务器	华为	RH2288V3	3	2024.6.16
21	服务器	擎天	DF-729	6	2025.11.10
22	服务器	Dell	PowerEDGE R940xa	4	2024.6.16
23	服务器	Dell	PowerEDGE R940	1	2024.6.16
24	服务器	Dell	R710	1	2024.6.16
25	服务器	中科曙光	A620r-G	1	2024.6.16
26	小型机	HP	RX6600	2	2024.6.16
27	刀片服务器	HP	C7000, BL680	5	2024.6.16
28	刀片服务器	HP	BL680c	1	2024.6.16
29	负载均衡	F5	BIG-IP 3400	1	2024.6.16

30	负载均衡	F5	LTM6400	2	2024.6.16
31	负载均衡	睿伟	Acteon-5208-C-6G	1	2024.6.16
32	负载均衡	F5	6400RS	2	2024.6.16
33	存储及备份	HP	HP-VA7110	1	2024.6.16
34	备份一体机	爱数	FT1220	1	2024.6.16
35	存储	同有	ACS 5000F-26R2IS11	1	2024.6.16
36	基础软件	Oracle	10/11	6	2024.6.16
37	基础软件	Tomcat	5.5/6.0/7.0/8.5/9	12	2024.6.16
38	基础软件	达梦	DM6.0.2/V8	3	2024.6.16
39	基础软件	Tongweb	5.0/7	5	2024.6.16
40	基础软件	Weblogic	11.3	2	2024.6.16
41	基础软件	mariaDB	5.5.60	2	2024.6.16
42	基础软件	apache	2.4	1	2024.6.16
43	基础软件	JDK	Jdk1.8/1.6	6	2024.6.16
44	基础软件	Mysql	5.7/8.0	7	2024.6.16
45	基础软件	sqlserver	2008	4	2024.6.16
46	基础软件	ngnix	1.14/1.15/1.17	9	2024.6.16
47	操作系统	CentOS	6.9/7.0/7.6/7.8/8.5	50	2024.6.16
48	操作系统	Windows	2003/2008/2012/2016	16	2024.6.16
49	操作系统	Suse	10/11	6	2024.6.16
50	操作系统	Ubuntu	14/16/20/22	14	2024.6.16
51	操作系统	麒麟系列	中标 5.4/银河 4.0	9	2024.6.16
52	网络设备	华为	5720-28P-LI	5	2024.6.16
53	网络设备	H3C	MSR50-40	1	2024.6.16
54	网络设备	H3C	S5120-48P-EI	2	2024.6.16
55	网络设备	H3C	S5130S-28P-EI	2	2024.6.16
56	网络设备	H3C	S5130S-28P-EI	6	2024.6.16
57	网络设备	H3C	S6800-4C	2	2024.6.16
58	网络设备	H3C	WX3024H	1	2024.6.16
59	网络设备	紫光	R3900	2	2024.6.16
60	网络设备	锐捷	RG-S6000-24T	2	2024.6.16
61	网络设备	锐捷	RG-AP820	50	2025.12.19
62	网络设备	锐捷	RG-S2910C-24GT2XS-	2	2025.12.19

			HP		
63	网络设备	锐捷	WA5320	30	2024.6.16
64	安全设备	安恒	DAS-ABL-CH	1	2025.11.24
65	安全设备	安恒	DAS-NGFW1950	2	2025.6.6
66	安全设备	安恒	DAS-IPS295	2	2024.6.16
67	安全设备	安恒	DAS-USM1200	1	2025.12.19
68	安全设备	安恒	DAS-ABL-S2100	1	2026.8.17
69	安全设备	安恒	DAS-ABL-COS1000	1	2025.11.24
70	安全设备	思福迪	LogBaseD3890	1	2024.6.16
71	安全设备	思福迪	LogBaseA3890	1	2024.6.16
72	安全设备	绿盟	NIDS NX3	1	2024.6.16
73	安全设备	绿盟	WAF NX3	2	2024.6.16
74	安全设备	网神	Nsec-NF7000	2	2024.6.16
75	安全设备	网神	网神 Nsec NF5000	5	2024.6.16
76	安全设备	网神	SecGate3600	2	2024.6.16
77	安全设备	网神	W6150-C011	2	2024.6.16
78	安全设备	网神	SecVSS 3600	1	2024.6.16
79	安全设备	启明星辰	天玥网络安全审计系统 V6.0 GE1600ER	2	2024.6.16
80	安全设备	奇安信	网神 SecFox 运维安全管理与审计系统	1	2024.6.16
81	安全设备	榕基	RJ-iTop IIIB-128	1	2024.6.16
82	防病毒控制台		HPDL380 GEN9	2	2024.6.16
83	跳板机	联想	ThinkSystem SR590	2	2025.12.19
84	安全设备	安恒信息	DASUSM-V2.0	2	2025.11.10
85	安全设备	安恒信息	WPT-EE-H	1	2025.11.10
86	防火墙	启明星辰	USG-FWGAFT-12600G P-G014（万兆）	2	2025.11.10
87	漏洞扫描	启明星辰	TJCS-GYD-FTS2300A	1	2025.11.10
88	入侵检测	启明星辰	NT3000-ZX（千兆）	1	2025.11.10
89	日志审计	六方云	NSec-LAS3000	1	2025.11.10
90	安全设备	六方云	LinSec-P6200	1	2025.11.10

91	网络设备	信诺瑞德	ADC-3500-FT11	2	2025.11.10
92	备份一体机	爱数	FT1220	1	2025.11.10
93	入侵防御	网神	P3000-1610	1	2025.11.10
94	存储	同有	ACS 5000F-26R2IS11	1	2025.11.10
95	数据库审计	绿盟	DASNX5-HF-NDE-01	1	2025.11.10
96	交换机	清华紫光	S5600-G	2	2025.11.10
97	集中式扫描 智能交换箱	神舟	B11	5	2024.6.16