

内蒙古自治区自然资源系统网络安全监测预警与通报服务项目

竞争性磋商文件

采购单位名称：内蒙古自治区自然资源厅综合保障中心

采购代理机构名称：磐鼎工程管理有限公司

项目编号：**NMGZCS-C-F-250411**

2025年07月

目录

第一章 磋商邀请

第二章 供应商须知

第三章 采购内容与技术要求

第四章 供应商资格证明及相关文件要求

第五章 评审

第六章 合同与验收

第七章 响应文件格式与要求

第一章 磋商邀请

磐鼎工程管理有限公司 受 内蒙古自治区自然资源厅综合保障中心 委托，采用竞争性磋商方式组织采购 内蒙古自治区自然资源系统网络安全监测预警与通报服务项目 。欢迎符合资格条件的供应商前来参加。

一.项目概述

1.名称与编号

项目名称： 内蒙古自治区自然资源系统网络安全监测预警与通报服务项目

项目编号： **NMGZCS-C-F-250411**

采购计划备案号： 内政采计划[2025]16043

2.内容及划分采购包情况

采购包1：

采购包预算金额（元）：**1,750,000.00**

采购包最高限价（元）：**1,750,000.00**

报价形式： 总价

序号	标的名称	数量	标的金额（元）	计量单位	所属行业	是否核心产品	是否允许进口产品	是否属于节能产品	是否属于环境标志产品
1	内蒙古自治区自然资源系统网络安全监测预警与通报服务项目	1.00	1,750,000.00	年	软件和信息技术服务业	否	否	否	否

二.供应商的资格要求

1.供应商应符合《中华人民共和国政府采购法》第二十二条规定的条件。

2.资格审查时，供应商未被列入失信被执行人、重大税收违法失信主体、政府采购严重违法失信行为记录名单，相关信用情况通过“信用中国”网站、中国政府采购网等渠道查询。

3.落实政府采购政策需满足的资格要求：如属于专门面向中小企业采购的项目,提供货物、工程或者服务的供应商应符合享受中小企业扶持政策，并提供《中小企业声明函》。监狱企业、残疾人福利性单位视同小型、微型企业。

4.本项目的特定资格要求：

采购包1：

无

三.获取磋商文件的时间、地点、方式

详见竞争性磋商公告

其他要求：

无

四.磋商文件售价

本次磋商文件的售价为0元人民币。

五.响应文件提交的截止时间、开启时间和地点

详见竞争性磋商公告

六.联系方式

采购代理机构名称： 磐鼎工程管理有限公司

地址： 内蒙古自治区呼和浩特市玉泉区内蒙古自治区呼和浩特市玉泉区鄂尔多斯大街金宇新天地F座607、608号

邮编： 010000

联系人： 任斌、吉圆圆、王达、贾美

联系电话： 0471-6381580

采购单位名称： 内蒙古自治区自然资源厅综合保障中心

地址： 内蒙古自治区呼和浩特市赛罕区南二环路11号

邮编： 010000

联系人： 徐一凡

联系电话： 0471-4215927

第二章 供应商须知

一.前附表

序号	条款名称	内容及要求
1	划分采购包情况	共 1 包
2	采购方式	竞争性磋商
3	开启方式	远程开标
4	评审方式	现场网上评标
5	评审方法	采购包1：综合评分法
6	获取磋商文件时间	详见竞争性磋商公告
7	保证金缴纳截止时间 (同响应文件提交截止时间)	详见竞争性磋商公告
8	电子响应文件提交	在响应文件提交截止时间前上传至“内蒙古自治区政府采购网-政府采购云平台”。
9	响应文件数量	<p>(1) 加密的电子投标文件1份(需在投标截止时间前上传至“内蒙古自治区政府采购网-政府采购云平台”)</p> <p>(2) 若现场无法使用系统进行电子开评标的, 投标人须开标现场递交非加密电子版投标文件U盘(或光盘) 0份。</p> <p>(3) 纸质投标文件(正本) 0份; 纸质投标文件(副本) 0份。</p>
10	成交人确定	甲方授权评标委员会(非招标采购, 如谈判、磋商、协商、询价小组)按照采购文件规定的方式确定中标(成交) 供应商。
11	联合体响应	采购包1: 不接受
12	采购代理机构代理费用	<p>本项目收取代理服务费</p> <p>代理服务费用收取对象: 采购人</p> <p>代理服务费收费标准: 按照中标金额, 参照《内蒙古自治区建设工程招标代理服务收费指导意见》(内工建协〔2022〕34号)文件标准收取。</p>
13	磋商保证金	不收取保证金
14	电子响应文件签字、盖章要求	<p>应按照第七章“响应文件格式与要求”, 使用单位电子签章(CA)进行签字、加盖公章。</p> <p>说明: 若涉及到授权代表签字的可将文件签字页先进行签字、扫描后导入加密电子响应文件。</p>
15	投标客户端	<p>投标客户端需要供应商登录“内蒙古自治区政府采购网-政府采购云平台”自行下载。下载地址: https://www.ccgp-neimonggu.gov.cn/gp-auth-center/login?systemRegion=150001&systemRegion=150001</p>
16	面向中小企业采购	<p>采购包1:</p> <p>属于专门面向小微企业采购, 预留比例为100%。</p>
17	有效供应商家数	采购包1: 3家
18	中标供应商数量	采购包1: 1名

19	中标候选人数量	采购包1：3名
20	报价形式	详见第一章，“内容及划分采购包情况”。
21	现场考察	采购包1：组织现场踏勘：否
22	兼投兼中规则	本项目可兼投1包，本项目可兼中1包
23	其他	无

二.磋商须知

1.磋商采取网上响应方式，操作流程如下：

供应商应当在内蒙古自治区政府采购云平台申请或注册账号，完善信息后，才可进行网上响应，办理流程请登录内蒙古自治区政府采购网（<https://www.ccgp-neimenggu.gov.cn>）进行查询。

供应商登录内蒙古自治区政府采购网页面，点击“政府采购云平台”，输入用户名、密码、验证码完成登录后，点击左侧“交易执行—应标—项目应标”，在未参与项目列表中选择要响应的项目，点击项目的“未参与项目”按钮，进入项目响应信息页面，在右侧选择要响应的采购包，填写“联系人姓名”、“联系人手机号”、“联系人邮箱”等信息，点击“确认参与”按钮后，获取所响应项目磋商文件，并按照磋商文件的要求制作、上传电子响应文件。

2.磋商保证金

2.1磋商保证金缴纳（如需缴纳保证金）

本采购项目支持“电子保函”和“虚拟子账户”两种方式收取磋商保证金，同时允许供应商按照相关法律法规自主选择以支票、汇票、本票、保函等非现金形式缴纳保证金。

2.1.1供应商选择“电子保函”方式缴纳保证金的，在所投项目下采购包选择电子保函模式，跳转到内蒙古自治区金融服务平台开具电子保函，供应商需要确保在响应文件开启时间之前完成电子保函的开具。

2.1.2供应商选择“虚拟子账户”方式缴纳保证金的，在进行信息确认后，应通过“交易执行—应标—项目应标—已参与项目”，选择缴纳银行并获取对应不同采购包的缴纳金额以及虚拟子账号信息，并在响应文件开启时间前，缴纳至上述账号中。付款人名称必须为供应商全称，且与其响应信息一致。

若出现账号缴纳不一致、缴纳金额与供应商须知前附表规定的金额不一致或缴纳时间超过响应文件开启时间，将导致保证金缴纳失败。供应商应认真核对账户信息，将磋商保证金足额汇入以上账户，并自行承担因汇错磋商保证金而产生的一切后果。供应商在转账或电汇的凭证上应按照“项目编号：***、采购包：***的磋商保证金”格式注明，以便核对。

2.1.3供应商选择以支票、汇票、本票、保函等非现金形式缴纳保证金的，供应商将相关证明材料原件扫描添加至响应文件中，同时现场提供证明材料。

2.1.4缴纳保证金时间以保证金到账时间为准，由于磋商保证金到账需要一定时间，请供应商在响应文件开启时间前及早缴纳。

2.2磋商保证金的退还

2.2.1已提交响应文件的供应商，在提交最后报价之前，可以根据磋商情况退出磋商。采购人、采购代理机构应当退还退出磋商的供应商的磋商保证金。未成交供应商的磋商保证金应当在成交通知书发出后5个工作日内退还，成交供应商的磋商保证金应当在采购合同签订后5个工作日内退还。因供应商自身原因导致无法及时退还的除外。

2.2.2有下列情形之一的，磋商保证金将不予退还：

- （1）供应商在提交响应文件截止时间后撤回响应文件的；
- （2）供应商在响应文件中提供虚假材料的；
- （3）除因不可抗力或磋商文件认可的情形以外，成交供应商不与采购人签订合同的；
- （4）供应商与采购人、其他供应商或者采购代理机构恶意串通的；
- （5）本文件规定的其他情形。

3.全流程电子化交易

各供应商应当在内蒙古自治区政府采购云平台开展与本项目有关的政府采购活动。

各供应商应当在响应文件开启时间前上传加密的最终版电子响应文件至“内蒙古自治区政府采购网”，未在响应文件开启时间前上传电子响应文件的，视为自动放弃。供应商因系统问题无法上传电子响应文件时，请在工作时间及时拨打联系电话**400-0471-010**。

各供应商应当使用数字证书或者政府采购云平台生成的账号密码登录电子交易系统进行系统操作，并对其操作行为和电子签名、电子印章确认的事项承担法律责任。

3.1远程不见面方式（供应商无需到现场）

供应商使用“投标客户端”编制、签章、生成加密响应文件，同时生成“备用标书”，供应商自行留存，涉及“加盖公章”的内容应使用单位电子公章完成。

供应商的法定代表人或其授权代表应当按照本项目磋商公告载明的时间等要求参加磋商，在响应文件开启时间前**30分钟**，应当提前登录电子交易系统确认联系人姓名与联系电话。

响应文件开启时，供应商应当使用**CA证书**在开始解密后**30分钟**内完成全部已响应采购包的响应文件在线解密，若出现系统异常情况，工作人员可适当延长解密时长。如在响应文件开启过程中出现意外情况导致无法继续进行，由代理机构会同采购人决定是否允许供应商导入“备用标书”继续进行。本项目采用电子评审，只对开启环节验证通过的电子响应文件进行评审。供应商在响应文件开启前自行对使用电脑的网络环境、驱动安装、客户端安装以及**CA证书**的有效性等进行检测，保证可以正常使用。具体要求请通过“内蒙古自治区政府采购网-政采业务指南”查询相关操作手册。

响应文件开启时出现下列情况的，采购人、采购代理机构应当视为供应商不再参与政府采购活动：

- （1）供应商未在规定时间内完成电子响应文件在线解密的；
- （2）**CA证书**无法解密响应文件的；
- （3）供应商自身原因造成电子响应文件未能解密的。

3.2现场网上方式（供应商需到现场）

供应商使用“投标客户端”编制、签章、生成加密响应文件，同时生成“备用标书”，由供应商自行刻录、存储，涉及“加盖公章”的内容应使用单位电子公章完成。供应商必须保证电子存储设备能够正常读取“备用标书”，电子存储设备（**U盘或光盘**）表面、外包装上应简要载明项目编号、项目名称、供应商名称等信息。

供应商的法定代表人或其授权代表应当按照本项目磋商公告载明的时间和地点参加磋商。响应文件开启时，供应商应当使用**CA证书**完成全部已响应采购包的响应文件在线解密。如在响应文件开启过程中出现意外情况导致无法继续进行，由代理机构会同采购人决定是否允许供应商导入“备用标书”继续进行。本项目采用电子评审，只对响应文件开启环节验证通过的电子响应文件进行评审。

响应文件开启时出现下列情况的，采购人、采购代理机构应当视为供应商不再参与政府采购活动：

- （1）**CA证书**无法解密响应文件的；
- （2）供应商未按磋商文件要求提供“备用标书”的；
- （3）供应商自身原因造成电子响应文件未能解密的。

4.供应商可以通过“交易执行-应标-项目应标-已参与项目”查看有无本项目信息。

三.说明

1.总则

本磋商文件依据《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《政府采购竞争性磋商采购方式管理暂行办法》及国家和自治区有关法律、法规、规章制度编制。

供应商应仔细阅读本项目信息公告及磋商文件的所有内容（包括澄清或者修改），按照磋商文件要求以及格式编制响应文件，并保证其真实性，否则一切后果自负。

2.适用范围

本磋商文件仅适用于本次竞争性磋商公告中所涉及的项目和内容。

3.相关费用

供应商应自行承担所有与准备、参加磋商有关的费用。不论磋商结果如何，采购人或采购代理机构均无义务和责任承担相关费用。

4.各参与方

4.1“采购人”是指依法进行政府采购的国家机关、事业单位、团体组织。本磋商文件的采购人特指 内蒙古自治区自然资源厅综合保障中心。

4.2“采购代理机构”是指集中采购机构和集中采购机构以外的采购代理机构。本磋商文件的采购代理机构特指 磐鼎工程管理有限公司。

4.3“供应商”是指向采购人提供货物、工程或者服务的法人、其他组织或者自然人。

4.4“磋商小组”由采购人代表和评审专家组成。

4.5“成交供应商”是指取得与采购人签订合同资格的供应商。

5.合格的供应商

5.1符合本磋商文件规定的资格要求，并按照规定提供相关证明材料。

5.2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，不得参加同一合同项下的政府采购活动。

5.3为采购项目提供整体设计、规范编制或者项目管理、监理、检测等服务的供应商，不得再参加该采购项目的其他采购活动。

6.以联合体形式进行政府采购的，应符合以下规定：

6.1联合体各方应签订联合体协议书，明确联合体牵头人和各方权利义务，并作为响应文件组成部分。

6.2联合体各方均应当具备《中华人民共和国政府采购法》第二十二条规定的条件，并在响应文件中提供联合体各方的相关证明材料。

6.3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。

6.4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。

6.5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。

6.6联合体各方应当共同与采购人签订采购合同，就合同约定的事项对采购人承担连带责任。

6.7如要求缴纳保证金，以联合体牵头人名义缴纳，对联合体各方均具有约束力。

7.语言文字以及计量单位

7.1所有文件使用的语言文字为简体中文。专用术语使用外文的，应附有简体中文注释，否则视为无效。

7.2所有计量均采用中华人民共和国法定的计量单位。

7.3所有报价一律使用人民币，货币单位：元。

8.现场考察

8.1磋商文件规定组织现场考察的，采购人或者采购代理机构按磋商文件规定的时间、地点组织供应商考察项目现场。

8.2供应商自行承担考察现场发生的责任、风险和自身费用。

8.3采购人在考察现场介绍的资料和数据等，不构成对磋商文件的修改或不作为供应商编制响应文件的依据。

9.其他条款

无论成交与否供应商递交的响应文件均不予退还。

四.磋商文件的澄清或者修改

提交首次响应文件截止之日前，采购人、采购代理机构或者磋商小组可以对已发出的磋商文件进行必要的澄清或者修改，

澄清或者修改的内容作为磋商文件的组成部分。澄清或者修改的内容可能影响响应文件编制的，采购人、采购代理机构应当在提交首次响应文件截止时间至少5日前，在“内蒙古自治区政府采购网”上发布更正公告进行通知；不足5日的，采购人、采购代理机构应当顺延提交首次响应文件截止时间。更正公告的内容为磋商文件的组成部分，供应商应自行上网查询，采购人或采购代理机构不承担供应商未及时关注相关信息的责任。

五.响应文件

1.响应文件的构成

响应文件应按照磋商文件第七章“响应文件格式与要求”进行编写，可以增加附页，并作为响应文件的组成部分。

2.报价

2.1供应商应按照磋商文件第三章“采购内容与技术要求”进行报价。报价中不得包含磋商文件要求以外的内容，否则，在评审时不予核减。

2.2报价包括本项目采购需求和投入使用、实施的所有费用，如主件、标准附件、备品备件、施工、服务、专用工具、安装、调试、检验、培训、运输、保险、税款等。

2.3报价不得有选择性报价和附有条件的报价。

2.4供应商应在“投标客户端”对【报价部分】进行填写，“投标客户端”软件将自动根据供应商填写信息在线生成“首轮报价表”、“分项报价表”，若在响应文件中出现非系统生成的“首轮报价表”、“分项报价表”，且与“投标客户端”生成的“首轮报价表”、“分项报价表”信息内容不一致，以“投标客户端”在线填写报价并生成的内容为准。

3.响应文件的递交

供应商应当在提交响应文件截止时间前递交响应文件，否则视为自动放弃。

4.响应文件的补充、修改或者撤回

供应商在提交响应文件截止时间前，可以对所提交的响应文件进行补充、修改或者撤回。供应商应当在提交响应文件截止时间前上传加密的最终版电子响应文件至“内蒙古自治区政府采购网-政府采购云平台”。在提交响应文件截止时间后，供应商不得补充、修改或者撤回其响应文件。

5.样品

5.1磋商文件规定供应商提交样品的，样品属于响应文件的组成部分。样品的生产、运输、安装、保全等一切费用由供应商自理

5.2响应文件开启前，供应商应将样品送达至指定地点，按要求摆放并做好展示。若需要现场演示的，供应商应提前做好演示准备（包括演示设备）。

5.3采购活动结束后，对于未成交供应商提供的样品，应当及时退还或者经未成交供应商同意后自行处理；对于成交供应商提供的样品，应当按照磋商文件的规定进行保管、封存，并作为履约验收的参考。

六、开启、评审、结果公告、成交通知书

1.开启

1.1程序

- （1）宣布纪律；
- （2）宣布相关人员；
- （3）供应商对已提交的加密文件进行解密，由采购人或者采购代理机构工作人员宣布供应商名称和磋商文件规定需要宣布的其他内容；
- （4）参加人员对开启情况进行确认；
- （5）开启结束。

1.2疑义

供应商代表对开启过程和开启记录有疑义，以及认为采购人、采购代理机构相关工作人员有需要回避情形的，应当场提出

询问或者回避申请。采购人、采购代理机构对供应商代表提出的询问或者回避申请应当及时处理。

供应商对远程不见面方式开启过程和记录有疑义，应在“政府采购云平台-远程开标大厅”中提出，采购代理机构应及时查看、回复。

1.3备注

开启时,供应商使用CA证书参与响应文件解密，供应商用于解密的CA证书应为生成、加密、上传响应文件的同一CA证书。

2.评审

详见第五章

3.结果公告

成交供应商确定后，采购代理机构在内蒙古自治区政府采购网上发布成交结果公告，同时将成交结果以公告形式通知未成交的供应商，成交结果公告期为1个工作日。

项目“废标”后，采购代理机构将在内蒙古自治区政府采购网上发布“废标公告”。

4.成交通知书

发布成交结果的同时，成交供应商可自行登录“内蒙古自治区政府采购网--政府采购云平台”打印成交通知书，成交通知书是合同的组成部分，成交通知书对采购人和成交供应商具有同等法律效力。

成交通知书发出后，采购人不得违法改变成交结果，供应商无正当理由不得放弃成交。

七.询问、质疑与投诉

1.询问

供应商对政府采购活动事项有疑问的，可以向采购人或采购代理机构提出询问，采购人或采购代理机构应当在3个工作日内作出答复，但答复的内容不得涉及商业秘密。供应商提出的询问超出采购人对采购代理机构委托授权范围的，采购代理机构应当告知其向采购人提出。

2.质疑

2.1供应商认为采购文件、采购过程、成交结果使自己的权益受到损害的，可以在知道或者应知其权益受到损害之日起7个工作日内，以书面形式向采购人、采购代理机构提出质疑。

供应商在法定质疑期内应当一次性提出针对同一采购程序环节的质疑。

提出质疑的供应商应当是参与所质疑项目采购活动的供应商。

潜在供应商已依法获取其可质疑的采购文件的，可以对该文件提出质疑。对采购文件提出质疑的，应当在获取采购文件或者采购文件公告期限届满之日起7个工作日内提出。

2.2采购人、采购代理机构应当在收到供应商的书面质疑后7个工作日内作出答复，并以书面形式通知质疑供应商和其他有关供应商，但答复的内容不得涉及商业秘密。

2.3询问或者质疑事项可能影响成交结果的，采购人应当暂停签订合同，已经签订合同的，应当中止履行合同。

2.4供应商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：

- （一）供应商的姓名或者名称、地址、邮编、联系人及联系电话；
- （二）质疑项目的名称、编号；
- （三）具体、明确的质疑事项和与质疑事项相关的请求；
- （四）事实依据；
- （五）必要的法律依据；
- （六）提出质疑的日期。

供应商为自然人的，应当由本人签字；供应商为法人或者其他组织的，应当由法定代表人、主要负责人，或者其授权代表签字或者盖章，并加盖公章。

供应商可以委托代理人进行质疑，代理人提出质疑时应当提交供应商签署的授权委托书。其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。

2.5 供应商提交的质疑函，应按照内蒙古自治区政府采购网中的“质疑函范本”制作。

2.6 接收质疑函的方式。为了使提出的质疑事项在规定时间内得到有效答复、处理，质疑可以由法定代表人或授权代表亲自将质疑函递交至采购人或采购代理机构，也可以通过邮寄、快递等方式提交。质疑函以邮寄、快递方式递交的，以邮寄件上的戳记日期、邮政快递件上的戳记日期和非邮政快递件上的签注日期为质疑提起日期。

接收质疑函的联系部门、联系电话、通讯地址（详见第一章）。

3. 投诉

3.1 质疑人对采购人、采购代理机构的答复不满意或者采购人、采购代理机构未在规定的时间内作出书面答复的，可以在答复期满后**15**个工作日内向财政部门提起投诉。

供应商投诉的事项不得超出已质疑事项的范围，但基于质疑答复内容提出的投诉事项除外。

3.2 投诉人投诉时，应当提交投诉书和必要的证明材料，并按照被投诉采购人、采购代理机构（以下简称被投诉人）和与投诉事项有关的供应商数量提供投诉书的副本。投诉书应当包括下列内容：

- （一）投诉人和被投诉人的姓名或者名称、通讯地址、邮编、联系人及联系电话；
- （二）质疑和质疑答复情况说明及相关证明材料；
- （三）具体、明确的投诉事项和与投诉事项相关的投诉请求；
- （四）事实依据；
- （五）法律依据；
- （六）提起投诉的日期。

投诉人为自然人的，应当由本人签字；投诉人为法人或者其他组织的，应当由法定代表人、主要负责人，或者其授权代表签字或者盖章，并加盖公章。

3.3 投诉人提交的投诉书，应严格按照内蒙古自治区政府采购网中的“投诉书范本”制作。

第三章 采购内容与技术要求

一.项目概况：

为有效提升内蒙古自治区自然资源厅在“自然资源治理体系和治理能力现代化建设”过程中的网络安全防护能力，拟采取以购买安全监测服务的方式实现全区自然资源系统网络安全监测与通报运营服务。安全监测服务通过人+制度+流程+数据+平台”，在遵守内蒙古自治区自然资源厅综合保障中心安全运维规范的前提下，通过设置专业的技术人员岗位，建立常态化、实战化、体系化的安全运行机制，全面推进可知可视、可控可管、实战闭环的网络安全运营体系建设。实现：**1、**摸清内蒙古自治区自然资源厅网络关键信息基础设施资产。**2、**综合感知内蒙古自治区自然资源厅关键信息基础设施网络安全态势。建立监测、预警、通报、处置、反馈为一体的闭环管理体系。监测范围为厅本级、厅直属单位及**14**个盟市自然资源局（含**2**个计划单列市）

二.主要商务要求、技术要求

1.主要商务要求

采购包1：

序号	参数性质	类型	要求
1		标的提供时间	合同签订之日起一年
2		标的提供地点	内蒙古自治区自然资源厅
3		合同履行期限	合同签订之日起一年
4		合同履行地点	用户指定地点，通过现场+远程方式提供服务。
5		验收要求	验收按照国家相关行业标准、竞争性磋商文件及合同约定执行。交付所有服务期内产生的记录、报告及其他规定材料，由采购人组织验收。
6		合同支付方式	1、合同签订 30 日内，我中心向中标服务商支付合同金额的 25% ，达到付款条件起 30 日，支付合同总金额的 25.00% 2、 2025 年 12 月底前，我中心向中标服务商支付合同金额的 25% ，达到付款条件起 30 日，支付合同总金额的 25.00% 3、 2026 年 1 月，我中心向中标服务商支付合同金额的 25% ，达到付款条件起 30 日，支付合同总金额的 25.00% 4、服务期满，我中心向中标服务商支付合同金额的 25% ，达到付款条件起 30 日，支付合同总金额的 25.00%
7		履约保证金	需要缴纳履约保证金：不缴纳

2.主要技术要求

采购包1：

标的名称：内蒙古自治区自然资源系统网络安全监测预警与通报服务项目

序号	参数性质	技术参数与性能指标
		采购包1： 标的名称：内蒙古自治区自然资源系统网络安全监测预警与通报服务项目 监测范围：自然资源厅本级、厅直属单位及盟市自然资源局 服务内容：详见下表

序号	服务名称	技术参数与性能指标	数量	单位
1	监测预警平台租赁	详见附表1	1	套
2	流量日志采集器租赁	详见附表2	22	台
3	远程监测服务	详见附表3	1	年
4	网站安全监测及预警	详见附表4	1	年
5	重保任务安全监测	详见附表5	30	人/天
6	漏洞扫描服务（含基线核查）	详见附表6	3	次
7	渗透测试服务	详见附表7	3	次
8	安全通告服务	详见附表8	12	次
9	应急响应服务	详见附表9	12	次
10	安全咨询规划	详见附表10	5	次
11	安全技术培训	详见附表11	2	次
12	驻场运营	详见附表12	2	人

附表1：监测预警平台租赁

序号	参数性质	技术指标项	详细服务技术参数要求
1	0	交付形式	服务工具，租赁的监测预警平台需满足软硬一体化集群部署，可水平扩展到多台设备集群。
2	0	服务工具硬件要求	服务器≥4台； 单台规格：≥2颗12核或以上CPU，主频≥2.20GHz，内存≥256GB； 系统硬盘：≥2块960G固态硬盘； 数据硬盘：≥48TB企业级SATA 3.5寸硬盘； 冗余电源，千兆电口≥4，万兆光口≥2。
3	√	服务工具处理性能	集群实时处理事件性能≥20000EPS，支持扩展到100000EPS的处理性能能力； 支持百亿级日志秒级查询。
			<p>本服务所需安全数据需通过多种方式进行采集，具体采集方式包括采用人工和机器相结合的方式，构建保护目标监测及发现能力，通过专用采集设备采集的方式针对监测范围内各单位资产信息数据分析情况进行数据采集。同时，立足于云端互联网探测与分析数据，各单位监测数据，接收第三方安全公司的监测数据、威胁情报数据等，对于采集数据进行接入和汇聚。</p> <p>本项目系统建设主要需对以下几个方面的数据采集：监测范围内各单位资产信息录入；流量采集；网站监测数据；高质量威胁情报数据；第三方系统数据接入。</p>

					<p>资产信息录入：支持通过人工录入或自动化导入、自动探测方式进行。其中自动探测可自动比对资产数据，筛选新增资产内容，供管理人员确认，从而可以对网内整体资产变化情况有效掌控，并对合法资产和非法资产进行有效稽查。</p> <p>流量采集：网络流量数据采集即通过网络传感器和流量监测设备，需通过在监测范围内各单位流量出口部署流量采集器进行流量数据实时采集监控，并通过专有接口加密方式回传至监测预警平台中，主要包括：网络流量日志数据、网络资产数据、流量日志告警数据等。监测预警平台需支持接入并管理日志采集器、流量采集器、第三方采集器的接入，支持采集网络日志、安全设备、应用中间件、服务器、终端日志等各类数据源安全日志和流量探针的流量日志，日志数据源接入点授权至少提供50个，且支持按项目实际需求扩容接入点数量。流量采集器需支持Syslog、SNMP Trap、文本日志、数据库、Netflow、WMI、HTTP、Script等采集方式；并支持数据源信息导出、数据源迁移操作。</p> <p>网站监测数据：供应商提供网站监测平台，通过SAAS服务的方式，对监测范围各单位重点网站进行7*24小时持续的可用性、安全性、内容监测，并将监测告警结果通过接口传输到平台分析。监测的数据包含如下几类：网站暗链数据、网站挂马数据、网页篡改数据、钓鱼网站数据、网站漏洞数据、网站众测数据、网站可用性数据。</p> <p>第三方互联网安全数据：依托于互联网侧第三方威胁情报中心提供的DDoS、僵尸蠕毒、APT、众测漏洞等数据，根据自然资源厅相关IP进行源/目的筛选，通过接口对接到平台分析。</p>
			4	0	数据采集

5	0	数据预处理	数据预处理是采用大数据技术通过数据的解析与富化对数据汇聚接入系统接入的结构化、半结构化、非结构化数据，进行数据的抽取、清洗、转换、加载、消重与合并、数据关联、条件比对等处理，使得数据格式相对统一、分类分级明确、标识清晰，利于数据的深度关联分析。数据预处理需支持通过图形化界面、利用正则表达式、分隔符、Key-Value、JSON等配置解析规则，支持通过界面配置操作，实现富化规则构建，包括但不限于源字段、表达式、目标字段、参数设置；
6	0	数据存储与检索	根据内蒙古自治区自然资源系统网络安全监测预警与通报服务业务需求，平台需采用高性能的分布式集群数据存储系统，核心数据存储采用分布式全文检索方式，同时支持对不同结构的数据采用不同的存储策略，支持自定义日志类型功能，支持对日志类型名称、日志类型分组、分区方式、最大保留天数、重要度等基础属性信息进行配置，达到分类存储日志、全文搜索、结构化搜索以及分析的目的。

7	√	威胁检测能力	<p>监测预警平台需具备威胁检测能力，威胁检测能力可提供关联分析、场景分析、告警管理等功能。</p> <p>关联分析：需具备关联分析引擎，关联分析引擎支持随平台集群分布式扩展，支持横向软件化部署；需支持对接入的各种日志类型数据进行关联分析、行为基线建模，包括：安全日志、网络流量日志、服务器日志、中间件日志和其他日志等。日志类型从数据采集模块实时同步。需支持接入失陷类威胁情报到本地与日志数据进行关联分析，以发现僵尸网络、勒索软件、APT事件和远控木马等威胁事件。需支持对接入平台内的资产管理数据与日志数据进行关联分析，以发现与关键资产相关的威胁事件。需支持对接入平台内的漏洞管理数据与日志数据进行关联分析，以发现与漏洞相关的威胁事件。关联规则支持根据告警扩展策略来扩展威胁告警字段，以支持不同场景下基于不同特征字段的告警分析。支持基于规则配置扩展告警属性，预置包括：网络攻击告警策略、WEB安全告警策略、主机安全告警扩展属性策略、恶意文件告警扩展属性策略、威胁情报告警扩展属性策略等扩展属性策略。</p> <p>场景分析：平台需提供场景化分析能力，场景化至少包含邮件安全、账号安全、异常访问等分析场景，可从多维度多视角进行分析并采用可视化技术进行展现，安全运营人员经过简单分析后即可判断异常事件中包含潜在威胁。平台需支持对每个场景启用/停用，可以方便的停用用户不关心的场景，以节约计算资源。</p>
---	---	--------	--

8	√	响应处置能力	<p>监测预警平台需具备相应处置能力，相应处置可提供事件调查、攻击者分析、攻击链分析等功能。</p> <p>事件调查：提供对威胁事件的调查分析能力，安全运营人员可以对需要调查的威胁事件创建任务，将所有与调查问题相关的告警、日志、漏洞、弱口令、配置弱点、文本和图片信息都添加至任务中。通过时间线展示、标注等功能回溯并记录威胁事件的发展过程和相关影响，借助日志检索功能不断的扩展其他的日志线索，丰富该威胁事件相关证据。平台具备完整的攻击链分析能力，在数据完备的情况下可以还原整个攻击过程。</p> <p>攻击者分析：服务支持基于攻击者视角对告警进行归纳分析，能够提供更直观、目的性更强的告警信息，可快速定位攻击者IP、攻击类型、攻击链阶段、危害等级，同时用户能够通过攻击者详情查看攻击行为、受害者影响范围情况，快速定位问题，进行处置。</p> <p>攻击链分析：支持基于已经发生的事件、告警，作为分析线索，从网络攻击阶段的角度出发，追踪溯源网络攻击的目标、源头、方法、手段等，最终站在攻击者角度，把攻击分为侦查跟踪、武器构建、载荷投递、漏洞利用、安装植入、命令控制、命令达成7个阶段，提供完整的溯源攻击链，进行攻击画像以可视化的方法将攻击链整个过程进行描述，用于刻画IP间的攻击关系及攻击链各阶段IP对象间的关系。可描述攻击者、受害者。</p>
---	---	--------	---

9	0	<p>风险预警能力</p> <p>监测预警平台需具备风险预警能力，风险预警能力可提供资产管理、脆弱性管理、资产风险评估、威胁预警等功能</p> <p>资产管理：1) 资产发现：可支持通过网络流量被动发现资产信息、支持通过脆弱性发现资产信息，资产信息至少包含：IP地址、操作系统、主机名、物理地址、服务信息等。可支持配置资产探查探针等进行主动资产发现。可最大限度的支持与现有安全设备对接实现资产信息的同步，安全设备包括服务器管理系统、终端管理系统、网站监测系统等2) 资产管理：需具备完善的资产管理功能，能够建立资产信息、资产分组信息，可录入以下类型资产：主机设备、网站、终端办公主机、网络设备、安全设备、应用系统等。</p> <p>脆弱性管理：支持通过同品牌流量日志采集器采集漏洞，弱口令信息。平台可对漏扫设备进行集中管理，可下发漏洞扫描任务和弱口令扫描任务，收集扫描结果，并可同步第三方配置核查系统的配置核查扫描任务，建立完整、持续的脆弱性发现和管理手段。支持针对扫描后的漏洞结果自动关联漏洞知识库信息，提供定期的数据更新并获取最新漏洞解决方案，协助完成漏洞闭环处置。</p> <p>资产风险评估：支持对资产风险值的自定义计算，计算范围包括威胁告警及脆弱性的危害等级、时间范围、处置状态等维度。支持对风险计算周期进行配置。</p> <p>威胁预警：当业界发生重大、热点安全事件时，支持导入厂商提供的威胁预警包，可快速检测并展示此威胁事件对用户内网安全的影响，包括展示影响的风险资产数、受攻击资产数、失陷资产数及影响面趋势图；支持展示该事件的关键点信息如首次出现、大面积爆发、有效控制、威胁缓解等里程碑节点；支持该事件影响面分布、受攻击资产列表和风险资产列表。</p>
---	---	--

10	√	持续监测能力	<p>监测预警平台需具备持续监测能力，持续监测能力提供态势可视化、仪表板、报表等功能。</p> <p>态势可视化：支持从外部威胁、内部威胁、攻击者、资产、脆弱性、风险、威胁预警、安全运营、资产外连等维度可视化展示态势。支持从综合风险值、风险资产数量、威胁数量、脆弱性数量和日志接入量等多个维度展示综合安全情况。支持统计服务器、网络设备、数据库服务器、中间件服务器、存储设备、应用服务器的资产和日志接入情况，动态展示被保护IP网段情况，安全运营支持统计规则（威胁情报、关联规则、漏洞知识库）运营、威胁检测（威胁、脆弱性）和处置情况，支持统计安全运维人员在平台上的运营情况（处理威胁数量、使用平台时长、常用功能等）。支持可视化呈现内网中是否存在威胁告警，威胁是否在内网网络中蔓延，能够聚焦于核心资产网段，提供对攻击者维度和受害者维度的攻击情况分析，对威胁类型、等级和趋势等进行统计呈现。支持发现内网中的攻击者，以帮助快速定位内网威胁的根源。</p> <p>仪表板：监测预警平台需具有多种仪表板，在系统部署后就能够使用多维度的监控能力。自定义仪表板在视图管理中通过可视化建模工具制作统计图，让视图间的组合更为灵活。同时还可以将自定义仪表板分享给其他用户，增加协同的效率。</p> <p>统计报表：视图支持11种以上的可视化分析图形，如散点图、柱状图、地图等，能够满足对不同维度的数据进行可视化分析。</p>
----	---	--------	---

11	0	安全系统支撑能力	<p>知识库支撑：支持知识库管理，内置漏洞知识库、IP地址定位知识库、ATT&CK 知识库、应用识别知识库、事件日志ID知识库。</p> <p>权限管理：可针对各个用户的数据访问权限和功能使用权限进行自定义配置，基于各种授权模型对平台内不同的账号（可映射到不同的身份）进行权限划分（授权），并对授权进行持续的分析、监控和优化。</p> <p>系统审计：支持系统审计，包含系统运行日志和操作日志，记录并支持查询最近30天的日志数据。</p>
12	0	威胁情报能力	<p>平台具备丰富的威胁情报供给能力，平台内置本地威胁情报并具备实时升级能力，运营人员配合厂商的云端威胁情报分析平台进行进一步的分析，了解攻击者背景信息，以及攻击者的相关网络资源和历史攻击行为，并进行深入追踪。同时，本地威胁情报也应用在数据关联分析和威胁溯源场景中，给用户快速补充攻击者上下文信息，提升威胁分析和溯源效率。</p> <p>支持本地威胁情报的检索，检索类型支持域名、URL、IP地址、文件MD5值；威胁情报内容支持IOC、攻击链阶段、ID、置信度、类型描述、定向攻击、风险等级、恶意家族、发布时间、攻击事件/团伙、影响平台、情报当前状态、威胁描述等</p> <p>投标企业或厂商自身应具备威胁情报收集能力，为用户提供安全运营威胁情报的数据服务，具备威胁情报系统的计算机软件著作权登记证书。</p>
13	0	行为异常检测	<p>支持行为异常检测，预置行为基线模型，威胁类型包括但不限于账号异常、进程异常、Web应用异常、进程异常、数据库应用异常、用户操作数据库异常、用户传输文件异常、用户登录行为异常、用户访问应用系统异常、用户收发邮件异常、账号异常。</p> <p>支持类VISIO的图形化方式自定义行为基线模型，包括日志行为基线和统计行为基线；基线检测对象支持个体和群体，支持对基线学习周期、学习频率、基线更新策略、基线降噪方式进行灵活定义。</p>

14	0	通报预警	支持将重大安全问题以通报和预警方式通知给内部或外部单位，通知方式支持短信、邮件、即时通讯等；可支持自定义通报和预警模板，包括年份、编号、事件等级、标题、红头标题、副标题等内容；支持查看通报和预警的发送接收流程；支持预警引入威胁预警信息
----	---	------	---

附表2：流量日志采集器租赁

序号	参数性质	技术指标项	详细服务技术参数要求
1	0	交付形式	流量日志采集器作为服务工具，全部由供应商提供，软硬一体化设备，由供应商负责设备的安装、调试、上线、策略配置、日常特征库、软件版本的升级工作。
2	√	服务工具处理性能	租赁的流量日志采集器，其中厅本级要求在网络流量采集、威胁数据采集和日志上报功能情况下混合流（模拟企业级网络真实场景流量）吞吐量 $\geq 3\text{Gbps}$ 探针1台；其他单位要求在网络流量采集、威胁数据采集和日志上报功能情况下混合流（模拟企业级网络真实场景流量）吞吐量 $\geq 1\text{Gbps}$ 探针20台，监测范围内各单位溜溜日志采集器接口标准配置 ≥ 6 个10/100/1000M自适应千兆电口， ≥ 2 个接口扩展板卡插槽，供应商需根据实际接入环境进行光口或者电口的扩展。提供部署互联网全流量威胁检测探针1台作为远程监测服务工具，工具以租赁的形式提供，要求流量处理能力 $\geq 2\text{Gbps}$ ，接口配置不少于6个千兆电口，4个万兆光口。
3	0	流量采集	采集过滤条件支持但不限于源地址、目的地址、服务、流量采样比、时间等；支持离线采集，可通过手动PCAP导入或FTP等协议批量上传导入等方式对离线流量进行采集支持空载荷过滤，支持对采集的流量的上下行载荷长度设置；
4	0	流量识别与解析	支持精准识别通讯类、语音类、视频类、更新类、下载类、邮件类、金融类、理财类等多类别的应用识别，应用识别库3000+。支持VXLAN、GRE、VLAN、MPLS的流量接入与解析，支持Oracle、MySQL、MSSQL、PostgreSQL、MongoDB、DB2等数据库行为的解析；

5	0	文件还原	支持还原多种文件传输协议，包括：邮件（SMTP、POP3、IMAP、webmail）、Web（HTTP）、FTP、SMB、TFTP等；
6	0	威胁检测	<p>系统具备全面的间谍软件检测能力，可检测常见的病毒蠕虫、僵尸网络、黑市工具、勒索软件、挖矿木马、远控木马等；</p> <p>系统具备全面的漏洞检测能力，可检测常见的溢出攻击、跨站脚本、SQL注入、拒绝服务、跨站请求伪造、目录遍历等；</p> <p>系统支持Flood攻击检测，包括SYN Flood、ICMP Flood、UDP Flood和IP Flood；支持应；</p> <p>系统需具备攻击检测能力的扩展功能，支持自定义恶意文件、自定义漏洞、自定义间谍软件、自定义威胁情报；</p> <p>系统本地需具备攻击告警的过滤能力，能够针对IP地址或端口对攻击告警进行过滤</p>
7	0	数据外发	通信模式支持但不限于KAFKA、ZMQ、SYSLOG等协议，需支持多路外发，并支持外发多地址的负载均衡处理，传输模式支持加密、压缩、以及认证，认证包括但不限于kerberos认证、LDAP认证。
8	0	SSL旁路解密	支持基于SSL协议的SMTPS、POP3S、IMAPS、HTTPS流量进行解密，可添加基于源目的地址及端口的过滤条件。（提供证明文件，并加盖投标企业公章）
9	0	流量及样本取证	支持威胁告警的相关pcap数据留存，支持本地下载及外发，外发通信协议包括但不限于KAFKA、FTP、SFTP等
10	0	兼容性要求	要求与本项目中安全监测平台为同一品牌。

附表3：远程监测服务

序号	参数性质	技术指标项	详细服务技术参数要求
1	0	服务形式	服务需在约定地点部署全流量威胁检测探针1台作为服务工具，工具以租赁的形式提供，设备要求流量处理能力 $\geq 2\text{Gbps}$ ，接口配置不少于6个千兆电口，4个万兆光口，同时要求后端有安全团队专人专岗开展7x24小时持续保障。

2	√	服务工具 功能要求	<p>1. 流量采集：支持网络协议、文件协议、数据库协议、离线流量、会话流量、自定义协议的采集</p> <p>2.威胁情报：支持基于流量实时IOC匹配功能，设备具备主流的IOC，情报总量大于350万条。</p> <p>3.WEB攻击检测：支持检测针对WEB应用的攻击，如SQL注入、XSS、系统配置、跨站请求伪造CSRF攻击检测、目录遍历、弱口令、权限绕过、信息泄露、文件包含、文件写入攻击、挖矿等检测（提供截图证明）。</p> <p>4.Webshell攻击检测：支持基于工具特征的WEBSHELL检测，能通过系统调用、系统配置、文件的操作来及时发现威胁；5.网络攻击检测：支持多种攻击检测，如：SQL注入、XSS、信息泄露、间谍软件、协议异常、网络欺骗、黑市工具、代码执行、挖矿等（提供功能截图）</p> <p>6.情报查询：支持与云端威胁情报中心联动，可对受害IP、攻击IP、IOC/规则ID、文件MD5进行一键搜索，查看基本信息、开源情报、相关样本、可视化分析、域名解析、注册信息、关联域名、数字证书等。（提供功能截图）</p> <p>7.行为分析：支持告警的深度行为分析，行为包括DNS解析行为、TCP/UDP交互行为、WEB访问行为、传输文件行为。</p> <p>8.挖矿检测：支持比特币、以太坊、比特币等二十余种币种的检测，</p> <p>9.HTTPS威胁检测：支持旁路HTTPS解密、威胁检测（提供功能截图）</p> <p>10.检测能力：具备AI隧道检测、非TCP完整流、畸形包检测、数据包完整性检测、碎片重组检测、编码绕过检测、高级逃逸 AET 检测等防逃逸检测能力。</p> <p>11.检测能力扩展：支持根据攻击载荷自定义漏洞检测规则，可自定义载荷检测位置、检测字段、匹配方式（文本匹配/正则匹配）等</p>
---	---	--------------	---

3	0	服务内容	<p>1. 设备管理和维护：设备运行监控、规则情报等实时升级、设备异常实时响应等；</p> <p>2. 威胁监测：全量告警7x24H实时监测；</p> <p>3. 事件管理：威胁事件分析、协助客户完成事件闭环；</p> <p>4. 服务支持：安全专家实时在线，对客户关于威胁及服务问题提供支持。</p> <p>5. 服务交付物：</p> <p>《远程监测服务安全事件报告》</p> <p>《远程监测服务周报》</p> <p>《远程监测服务月报》</p>
---	---	------	--

附表4：网站安全监测及预警

序号	参数性质	技术指标项	详细服务技术参数要求
1	0	交付形式	通过SaaS平台作为服务工具，用户端无需部署任何软硬件，对监测范围内各单位重要互联网资产进行监测，服务工具提供至少27个IP或域名的安全监测授权
2	0	监测及预警频率	提供7*24小时远程监测及5*8小时本地驻场监测服务，出现安全事件，实时进行预警,及时将监控信息反馈至指定接口人。提供问题处置建议和咨询；提供重大活动运营支撑服务。
3	0	网站漏洞监测	<p>对发现网站存在的SQL注入、XSS跨站脚本、目录遍历、文件包含、备份文件、敏感文件等漏洞，检测内容覆盖WASC分类的多种Web应用漏洞和OWASP TOP10网站漏洞进行管理；定期跟踪漏洞的修复情况从而使网站的漏洞得以快速修复，降低网站被入侵的风险。</p> <p>利用POC对目标网页进行WEB漏扫，发现SQL注入漏洞、命令注入、CRLF注入、LDAP注入、XSS跨站脚本漏洞、路径遍历漏洞、URL跳转漏洞、文件包含漏洞、应用程序漏洞、文件上传漏洞、等安全漏洞问题</p> <p>对mysql、redis、ftp、ssh等弱口令进行监测支持针对常见漏洞进行程序自动化验证，并可将自动验证漏洞生成安全告警</p> <p>支持针对行业漏洞情报进行同步预警，展示最新漏洞情报关联的资产信息</p>

4	0	网站黑链监测	使用模拟浏览器，爬虫UA等多种技术发现网站黑链，支持图片暗链的检测，支持全站对于潜在在页面深处的第三方黄赌毒广告类链接进行监测并告警，可定位源代码黑链的位置和内容。黑词样本数 5700+ ， 2021 年检测黑链告警事件 543W+ 支持配置监测频率，支持任务并发量配置，支持用户自定义黑词
5	0	违规内容监测	结合海量词库及人工识别，通过机器学习手段，提供敏感词发现的技术手段，支持全站监测，可定位敏感词位置和内容。 支持配置监测频率，支持任务并发量配置，支持用户自定义敏感词，支持网页附件内容检测
6	0	可用性监测	WEB 服务可用性监测需确保电信、联通和移动都具备监测点；支持网站故障原因定位，不限于： ：响应连接被重置、连接超时、 http 状态码、连接被拒绝等； 支持 get/head/post 三种方式对 HTTP/HTTPS 服务进行监控，监控频率支持自定义。支持添加域名时识别 IP 协议栈情况，并且根据识别结果分别配置 IPv4 和 IPv6 的监测节点 支持 HTTP/HTTPS 多线路监测 支持自定义监测节点，在高级配置中，设置异常节点阈值和超时阈值 支持 A 记录更改监测，网站 A 记录解析变更时可进行告警，告警支持短信/邮件方式 支持 禁PING 是否告警的选择，在高级配置中，配置每次 PING 间隔时间和执行检测次数的异常值
7	0	信息泄露监测	支持身份证、手机号码、 ip 地址等信息泄露监测并告警
8	0	内容变更（篡改）监测	页面发生变更即产生告警，变更类型包括外链、黑词、 body 标签为空等
9	0	网站挂马监测	采用特征分析技术对网站进行木马检测分析，实现快速、准确的发现和定位网页木马，确保用户在第一时间发现感染的木马并及时消除。对木马威胁进行报警、通知、处置管理
10	0	告警短信、邮件通知	支持短信、邮件将通知发给网站负责人

11	0	周期性报告	支持日报、周报、月报、季报的生成； 支持自定义周期性报告内容，包括自定义报告覆盖的资产、告警类型等
----	---	-------	--

附表5：重保任务安全监测

序号	参数性质	技术指标项	详细服务技术参数要求
1	0	交付形式	<p>特殊时期，提前做好资源的分配准备工作，保障时期加强系统主动监控和测试，实时掌握安全防护状态。发现事件、事故等情况后，应一边向内蒙古自治区自然资源综合保障中心主管部门进行报告，一边进行处理。处理过程中，应首先确保系统畅通，然后进行恢复和优化，处理完后需撰写相关保障报告。</p> <p>重保任务安全监控为7×24远程监控、现场监控、驻场服务。</p>
2	√	服务要求	<p>在服务期内，重大节假日（包括元旦、春节、清明、劳动、端午、中秋和国庆）、重大政治活动、特殊时期或重大变更，需要对自然资源业务专网安全系统进行重点保障时，供应商需在驻场安全运营工程师之外，再指派2-3名专业安全工程师提供针对性服务，通过多种方式实时发现网络和信息系统中的攻击事件，面向系统业务特点，以大数据和安全专家结合的方式，以威胁狩猎的分析方法，针对特定系统的特定攻击进行分析挖掘，重点发现未知类型攻击，为事件响应和处置提供参考依据。</p> <p>供应商需具备重保任务组织保障能力并提供充分全面的保障资源，制定充分的保障计划，从人力资源和防护设备方面建立充分的保障准备，以公司级整体资源能力协同监测范围内各单位应对重要敏感时期所面临的安全风险。</p>

3	0	情报支撑	<p>（1）威胁情报</p> <p>供应商需具备提供多源情报API聚合、可视化关联分析等关键性威胁情报运营能力，可针对重保任务安全监测报警提供高质量的上下文信息，供以对报警数据的研判、筛除误报并确定事件优先级，从海量报警中筛选出真正需要响应处理的部分。</p> <p>（2）漏洞情报</p> <p>供应商需具备漏洞情报能力，具备对多种渠道获取到的原始漏洞信息进行联合分析研判及脱敏加工，形成深层次的行业漏洞情报，及时通过邮件、平台、API等多种方式进行推送，确保漏洞情报的有效性和及时性。</p>
4	0	服务工具支撑	<p>在重保工作中，仅靠安全服务的支撑和人员能力的输出无法实现实时监测，也无法高效应对网络安全事件，而单纯的设备堆叠也无法体现安全产品本身的优势，故将人与产品相结合才能更好的发挥各自的作用，综合重保工作中的关键点和防护场景，在重保服务中供应商可借助各单位已有的监测、防护等安全产品进行，如果防护需要，需具备提供相关安全防护产品的能力。</p>

附表6：漏洞扫描服务（含基线核查）

序号	参数性质	技术指标项	详细服务技术参数要求
1	0	交付形式	<p>根据已有的安全漏洞知识库，模拟黑客攻击方法，检测网络协议、网络服务、网络设备、应用系统、服务器、交换机、防火墙等各种信息资产所存在的安全隐患和漏洞。对识别出的可能被入侵者利用非法进入网络或者非法获取信息资产的漏洞或脆弱性进行记录，通报到监测范围内各单位安全管理人员，及时完善安全策略，降低安全风险，含现场服务1次，远程服务2次。</p>
2	0	服务工具	<p>服务工具需采用漏洞扫描系统和开源漏洞扫描工具相结合，开展漏洞扫描工作，对扫描结果进行交叉比对，以提升漏洞扫描的准确性，服务工具中的漏洞扫描系统采取租赁的方式或供应商可自备具有自主知识产权的漏洞扫描系统</p>

3	√	服务内容	<p>1) 系统安全扫描</p> <p>供应商需针对传统的操作系统、网络设备、防火墙、远程服务等系统层漏洞进行渗透性测试。测试系统补丁更新情况、网络设备漏洞情况、远程服务端口开放等情况进行综合评估，在系统漏洞发现前期提供安全隐患评估报告，指导系统管理员提前进行漏洞修复，预防黑客攻击事件。</p> <p>2) Web安全</p> <p>供应商需基于OWASP TOP10（开放式Web应用程序安全项目10项最严重的Web应用程序安全风险列表）WEB安全标准，针对SQL注入、XSS跨站脚本、信息泄露、网络爬虫、目录遍历等Web攻击方式进行模拟黑客渗透攻击评估，包括Web安全隐患，预知Web安全漏洞，告知管理员修复Web漏洞。</p> <p>3) 数据库安全</p> <p>供应商需针对数据库，包括Oracle、MySQL、SQL Server、DB2、Sybase、Postgres等常见数据库进行漏洞检测，并提供登录扫描功能，全面发现数据库漏洞信息。</p> <p>4) 弱口令探测</p> <p>供应商需针对账户和密码相同、密码相对比较简单、默认密码等问题进行自动探测，测试口令是否存在弱口令现象。</p> <p>5) 配置基线核查</p> <p>供应商需针对操作系统、数据库、网络设备等系统的配置进行核查，检查配置是否符合标准。</p>
4	0	服务要求	<p>扫描结束后，供应商负责人需确认被扫描业务运行无异常；</p> <p>扫描完成后下载原始扫描报告，并且将扫描器上的数据删除。</p> <p>扫描结束后，3-5个工作日内提交安全扫描报告以及安全加固建议。</p>

附表7：渗透测试服务

序号	参数性质	技术指标项	详细服务技术参数要求
----	------	-------	------------

			<p>在重要时期前对监测范围内各单位面向公众提供的服务应用和内部重要服务器开展渗透测试服务，模拟黑客攻击，在内蒙古自治区自然资源综合保障中心的授权和监督下对应用、系统和网络进行非破坏性质的攻击性测试，发现系统中存在的安全隐患，提出解决问题的建议措施。修复完成后，对发现的安全隐患进行复测。含现场服务1次，远程服务2次。</p>
		交付形式	<p>系统层安全渗透测试</p> <p>系统安全脆弱点测试包括但不限于如下内容：</p> <p>口令猜解：针对操作系统、数据库等应用的口令登录安全进行测试，利用自动化工具，并通过使用密码字典文件，大量尝试登录单位内部的系统，进而找出存在空口令、弱口令的系统账号。该测试存在一定的安全风险，因为当系统设备启用密码登录安全策略时，大量的尝试会造成账号锁定，导致拒绝服务攻击发生，故执行相关操作时需特别当心。</p> <p>溢出测试：当无法直接利用帐户口令登陆系统时，也会采用系统溢出的方法直接获得系统控制权限，此方法有时会导致系统死机或从新启动，但不会导致系统数据丢失，如出现死机等故障，只要将系统从新启动并开启原有服务即可。</p> <p>敏感信息泄露：敏感信息的泄露会使系统存在于风险当中，如开启了不需要的服务、服务端口不恰当的对非授权区域开放、DNS区域传送机制未合理配置、特定系统服务（如telnet、SSH、FTP等）旗标未修改屏蔽等，此类敏感信息的不合理控制，会给攻击者的信息收集以及系统攻击工作带来极大便利，因此，在本服务测试中供应商应针对此类信息进行重点排查。</p> <p>系统安全管理：严格管理系统账户、有效控制系统服务，优化系统的安全配置，启用系统必要的安全控制措施，避免系统发生故障或遭受攻击。</p> <p>系统漏洞：针对业务系统所需要的系统服务进行优化管理和配置。</p> <p>系统访问控制和审计：对系统进行有效访问控制和日志审计。</p> <p>采用以下方法获得主机系统的安全弱点，服务中</p>

		2	√	<p>可以根据实际情况适当采纳：</p> <p>工具扫描：通过评估工具对主机、应用程序和数据库进行扫描。扫描评估主要是根据已有的安全漏洞知识库，模拟黑客的攻击方法，检测网络协议、网络服务、网络设备、应用系统等各主机设备所存在的安全隐患和漏洞。</p> <p>漏洞扫描：主要依靠带有安全漏洞知识库的网络安全扫描工具对信息资产进行基于网络层面安全扫描，其特点是能对被评估目标进行覆盖面广泛的安全漏洞查找，并且评估环境与被评估对象在线运行的环境完全一致，能较真实地反映主机系统、网络设备、应用系统所存在的网络安全问题。</p> <p>安全基线分析：依据对主机平台的标准化的安全审计列表（安全基线），检查和分析主机系统平台存在的安全问题。专家评估与工具扫描相结合，可以完成许多工具所无法完成的事情，从而得出全面的、客观的评估结果。</p> <p>专家评估是根据最新的安全检查核对表内容，逐项检查系统的各项配置和运行状态。核对表内容根据最新漏洞发现、不同的系统和运行环境、以及专家的经验知识而制定，它主要包括有以下几个方面：</p> <p>安全配置检查：系统管理和维护的正常配置，合理配置，及优化配置。例如系统目录权限，账号管理策略，文件系统配置，进程通信管理等。</p> <p>安全机制检查：安全机制的使用和正常配置，合理配置，及优化配置。例如日志及审计、备份与恢复，签名与校验，加密与通信，特殊授权及访问控制等。</p> <p>入侵追查及事后取证：检查与发现系统入侵，攻击或其它危害，尽可能追查及取证。例如日志被毁坏篡改或删除，计费数据被删除，遭受DOS攻击，系统被监听，控制或安装后门等。</p>

		3	0	服务内容	<p>WEB中间件渗透测试</p> <p>针对WEB常见的软件，例如APACHE、IIS、TO MCAT中间件等各类应用软件中常用到的软件，自身存在一些由于版本较低或配置不当所造成的安全隐患和漏洞，作为渗透测试的一些主要内容和方向。</p> <p>缓冲区溢出：由于应用服务版本过低所造成的应用自身的安全漏洞。</p> <p>路径和参数安全：由于对应用配置不足够所造成的路径和参数泄露。</p> <p>测试和帮助页面：由于应用配置不足所造成的测试和帮助页面显示。</p> <p>账号和口令：由于应用配置和测试导致无用账号或口令简单。</p>
					<p>WEB应用渗透测试</p> <p>针对WEB常见的应用，重点是由于应用软件在设计和开发的过程中，由于安全设计不足和开发不规范所造成的隐患和漏洞，主要包括如下几类：</p> <p>信息收集</p> <p>域名及IP信息收集：收集被测试网站的域名、二级域名、ip地址、对应的C段IP地址等信息；</p> <p>系统信息收集：WEB运行平台的操作系统信息、数据库信息；</p> <p>中间件信息收集：WEB应用的中间件信息，如A pache、Tomcat、weblogic等；</p> <p>信息系统开发框架信息：收集web应用开发框架的信息，如Struts2；</p> <p>CMS信息收集：探测并收集web应用的应用类型、版本等；</p> <p>其他信息：其他必要的渗透测试信息，如第三方组件等。</p> <p>身份验证</p> <p>在未加密的网络链上传递身份验证凭据或身份验证 cookie，这会引起凭据捕获或会话攻击；</p> <p>利用弱密码和账户策略，这会引起未经授权的访问；</p>

					<p>将个性化与身份验证混合起来。</p> <p>授权</p> <p>使用越权角色和账户；</p> <p>没有提供足够的角色粒度；</p> <p>没有将系统资源限制于特定的应用程序身份。</p> <p>输入和数据验证</p> <p>完全依赖于客户端验证；</p> <p>使用 deny 方法而非 allow 来筛选输入；</p> <p>将未经验证的数据写出到 Web 页；</p> <p>利用未经验证的输入来生成 SQL 查询；</p> <p>使用不安全的数据访问编码技术，这可能增加 SQL 注入引起的威胁；</p> <p>使用输入文件名、URL 或用户名进行安全决策。</p> <p>配置管理</p> <p>以明文存储配置机密信息，例如，连接字符串和服务帐户证书；</p> <p>没有保护应用程序配置管理的外观，包括管理界面；</p> <p>使用越权进程帐户和服务帐户。</p> <p>敏感数据</p> <p>在不需要存储机密信息时保存它们；</p> <p>在代码中存储机密信息；</p> <p>以明文形式存储机密信息；</p> <p>在网络上以明文形式传递敏感数据。</p> <p>会话管理</p> <p>在未加密信道上传递会话标识符；</p> <p>延长会话的生存期；</p> <p>不安全的会话状态存储；</p> <p>会话标识符位于查询字符串中。</p> <p>加密</p> <p>使用自定义加密方法；</p> <p>使用错误的算法或者长度太短的密钥；</p> <p>没有保护密钥；</p> <p>对于延长的时间周期使用同一个密钥。</p>
			4	0	

			<p>参数管理</p> <p>没有验证所有的输入参数这使系统的应用程序容易受到拒绝服务攻击和代码注入攻击，包括 SQL 注入和 XSS。</p> <p>未加密的 cookie 中包含敏感数据。攻击者可以在客户端更改 cookie 数据，或者当它在网络上传递时进行捕获和更改。</p> <p>查询字符串和表单域中包含敏感数据。很容易在客户端更改查询字符串和表单域。</p> <p>异常管理</p> <p>没有验证所有的输入参数；</p> <p>显示给客户端的信息太多。</p> <p>审核与记录</p> <p>没有审核失败的登录；</p> <p>没有保护审核文件；</p> <p>没有跨应用程序层和服务器进行审核。</p>
5	0	服务要求	<p>供应商需根据渗透测试工作开展情况，出具详细的测试报告，重点描述测试发现的问题、严重程度，同时在报告中提供对安全漏洞及问题的整改建议，同时配合内蒙古自治区自然资源综合保障中心或者第三方安全服务公司一起讨论具体加固实施办法，规避安全整改风险，协助进行安全加固工作修复漏洞，降低安全风险。</p> <p>在实施完整改工作后，根据渗透测试报告及整改报告进行复测（回归测试），以确认先前的安全漏洞得以有效的修复，同时没有引入新的安全漏洞，确保整改工作达到预期目标。</p>
6	0	服务工具要求	<p>工具须为自动化渗透系统，具备项目管理、指纹管理、插件管理、信息收集、漏洞探测、权限维持-GTShell、权限维持-GTWebshell、权限维持-GTSession、渗透辅助-口令爆破、渗透辅助-目录扫描、渗透辅助-漏洞利用、系统管理、报告管理等功能。</p>

附表8：安全通告服务

序号	参数性质	技术指标项	详细服务技术参数要求
----	------	-------	------------

1	0	交付形式	<p>提供多种方式的安全通告和通报方式，平时按月提供通告服务，紧急情况随时进行通告，并对未按期完成安全整改的单位进行通报。</p> <p>邮件通告：通过邮件的形式定期为内蒙古自治区自然资源厅提供新的安全事件、漏洞、病毒以及后门等的信息，并提供相应的解决方案与建议。</p> <p>电话通告：通过电话的形式为内蒙古自治区自然资源厅提供紧急的安全事件漏洞、病毒以及后门等的信息，并提供解决方案与建议。</p> <p>现场交流：对于特别紧急的情况，通过现场交流的形式为内蒙古自治区自然资源厅提供新的安全事件、漏洞、病毒以及后门等的信息，并提供解决方案与建议。</p>
2	0	服务要求	<p>供应商需持续关注安全技术的发展和新型漏洞情况，并根据信息系统中的信息资产情况提供相应的安全信息通告，包括厂商安全通告、Windows平台安全通告、紧急事件安全通告、重要安全问题通告等，以提高监测范围内各单位的安全防范意识，预先处理安全隐患。</p>

3	0	通告内容	<p>1)安全热点资讯</p> <p>供应商应提供安全热点资讯服务，安全热点资讯属于定期推送分享服务，主要通过“安全事件”、“权威发布和安全趋势”和“安全快讯”多个专栏向用户分享网络攻击事件分析、黑客组织攻击行为分析、软硬件漏洞技术分析、病毒或恶意代码等有害程序事件和技术原理分析、安全技术研究报告，以及一些安全新闻或事件动态。旨在让用户持续了解和熟悉最新的攻击技术、漏洞技术、安全研究以及行业内安全新闻和资讯动态。</p> <p>2)高危漏洞预警</p> <p>高危漏洞预警属于实时预警通告服务，供应商依据全面的攻防能力和强大的漏洞验证能力，在第一时间向用户发布高危漏洞预警，向用户通告漏洞的危害程度，风险等级，影响范围（如涉及的软件及版本情况），处置建议等信息。便于用户及时掌握高风险级别漏洞信息，及时修复并应对外部威胁。</p> <p>3）月度漏洞统计</p> <p>供应商应提供月度漏洞统计服务，月度漏洞统计属于定期推送服务，数据来源于CNVD站点漏洞月报统计数据。主要向用户呈现月度内漏洞统计信息，包含漏洞危害，漏洞影响软硬件及其版本，漏洞级别、漏洞类型、漏洞受关注度情况、漏洞发展趋势。旨在为用户对自有信息化资产的漏洞管理提供重要参考。</p> <p>4）威胁情报解读</p> <p>供应商应提供威胁情报解读服务，威胁情报解读属于定期推送分享服务，供应商需具备对APT攻击的研究以及企业内部安全事件研究的能力，定期分享APT攻击行为和事件情报、攻击团伙情报、恶意代码和漏洞利用情报，攻击团伙活跃态势情报，为保障自然资源信息基础设施和数据提供最有价值的情报信息。</p>
4	0	其他要求	<p>供应商需提供多种方式的安全通告和通报方式，平时按月提供通告服务，紧急情况随时进行通告，并对未按期完成安全整改的单位进行通报。</p>

附表9：应急响应服务

序号	参数性质	技术指标项	详细服务技术参数要求
1	0	交付形式	<p>安全事件告警信息主要有2种产生方式，一是为安排5×8小时的现场值守服务，对信息系统进行日常巡检、监控和运维，当发现安全事件、事故后及时进行告警；二是由内蒙古自治区自然资源综合保障中心直接发出的告警信息。</p> <p>供应商需采用以下4种具体的应急处理方式。</p> <p>一是紧急热线。当安全事件发生的时候，监测范围内各单位可以通过7×24小时热线电话，向服务经理或安全专家进行咨询，服务经理会及时根据情况协调后台资源进行解答，安全专家将会从保护内蒙古自治区自然资源厅利益和技术可实现角度为用户提供满意的答复。</p> <p>二是远程支持。在主机或网络发生安全事件时，工程师将应监测范围内各单位要求第一时间通过电话或网络远程解决安全问题，支持的内容包括：解答安全问题、分析安全日志、远程优化或入侵追踪等。</p> <p>三是现场支持。如果热线支持与远程支持均不能够解决安全问题或紧急安全事件，在接到报警通知并确认需要上门服务后，技术支持人员按照内蒙古自治区自然资源综合保障中心要求的故障处理时限要求，尽快赶到现场，查找事件原因，提出解决方案，修复故障，恢复系统正常运行。现场支持的内容包括入侵分析、安全隐患排除和安全紧急修复等。</p> <p>四是事后服务。在解决问题、恢复用户系统正常运行后，供应商提供应急响应处理报告，详细描述发现现象、处理过程和处置结果，并提出整改建议。</p>

2	0	服务要求	<p>供应商需无条件提供应急支撑工具（检测类、处置类、扫描类等），提供7×24的应急支持服务，建立健全安全事件应急工作机制，提高应对突发安全事件的组织指挥能力和应急处置能力，保证应急响应工作迅速、高效、有序地进行，确保监测范围内各单位业务系统妥善应对各类事件。</p> <p>根据实际和自有维护经验，事先建立完备的应急响应预案，维护团队和安全专家24小时处于待命状态，一旦发现安全系统故障、可疑黑客入侵活动，或者接到我单位的警报通知，将在距离事发现场较短时间内立即赶往事发现场，按照操作规程针对设备事故进行紧急处理，对事件进行实时地阻断、反击入侵行为，彻底清除入侵行为对内蒙古自治区自然资源厅信息系统造成的影响，同时修补存在的安全漏洞，恢复系统的正常运营，最大程度的减小因为安全事件、事故造成的损失。</p>
3	0	其他要求	<p>1) 供应商应向服务对象提供完备的网络安全事件处理报告；</p> <p>2) 供应商应向服务对象提供网络安全方面的措施和建议；</p>

附表10：安全咨询规划

序号	参数性质	技术指标项	详细服务技术参数要求
1	0	安全咨询规划	<p>监测范围内各单位工作人员可以直接联系供应商，进行信息安全方面的咨询等服务，供应商有责任努力解决工作人员提出的咨询问题。服务范围包括：基础信息安全规划、安全方案设计、安全管理咨询、等级保护建设、系统维护或技术发展等方面，输出相关资讯报告或解决方案</p>

附表11：安全技术培训

序号	参数性质	技术指标项	详细服务技术参数要求
			<p>1.培训对象：</p> <p>培训对象主要包括监测范围内各单位主管信息化主要领导及一般工作人员、技术人员及安全管理人员，可视情况与用户就培训对象在合同中具体明确</p> <p>2.培训方式：</p>

1	0	安全技术培 训	<p>1. 集中培训。2) 现场辅导。3) 技术交流。为了提高培训的效果，每次培训，服务供应商应针对参加培训人员进行考核，考核的方式以调差问卷或书面考试为主，以验证受训人员是否真正掌握。</p> <p>3.培训内容： 培训课程需分为以下几类： 基本培训类： 1) 网络安全基础知识； 2) 网络安全意识与法律法规。 服务工具类： 讲述服务工具的基本概念和原理、产品结构、产品功能、操作使用及日常排错等。 服务工具类主要对监测预警平台及流量日志采集器、网站安全监测、漏洞隐患监测、安全态势分析、漏洞扫描、渗透测试相关工具，以技术人员及安全管理人员为对象，对工具功能操作进行培训。 安全服务类： 主要以技术人员及安全管理人员为对象，对服务中的安全加固流程、措施手段以及发生安全事件第一时间应急响应的安全措施等进行培训。</p> <p>4.培训输出： 服务供应商应根据实际的培训情况输出具体培训内容PPT和相关培训资料等。</p> <p>5.培训师资： 服务供应商培训讲师需选用在网络安全行业从业至少5年以上，具备丰富的网络安全知识及经验，具备相关网络安全相关认证证书的人员进行培训。</p> <p>6. 培训次数 服务期内不少于2次</p>
---	---	------------	---

附表12：驻场运营

序号	参数性质	技术指标项	详细服务技术参数要求
----	------	-------	------------

1	√	驻场运营	<p>提供驻场运营人员≥ 2人。安全运营人员具有网络安全工作3年以上经验，需具有《注册信息安全专业人员（CISP）》，提供证书复印件。</p> <p>驻场运营服务内容包括：服务期内由驻场运维服务人员提供网络安全事件监测及预警、漏洞隐患监测及预警、日常安全事件分析、安全态势分析、安全加固支持服务，并按要求进行报告输出，包括：</p> <p>《安全监测运营日报》，每天一次</p> <p>《安全监测运营周报》，每周一次</p> <p>《安全监测运营月度综合分析报告》，每月度一次</p> <p>《安全监测运营季度综合分析报告》，每季度一次</p> <p>《安全监测运营年度综合分析报告》，服务周期内一次</p> <p>《网站安全监测预警与处置分析报告》，按需</p> <p>《网络安全事件分析与处置报告》，按需</p> <p>《漏洞隐患监测及预警处置与分析报告》，按需</p> <p>《日常安全事件分析与处置报告》，按需</p> <p>《安全态势分析报告》，按需</p> <p>《重保任务安全监测日报/总结报告》，重保期间</p> <p>《监测预警通报服务安全通告》，每月1次；</p> <p>《漏洞扫描报告》，每季度一次</p> <p>《渗透测试报告》，每季度一次</p> <p>《安全加固处置建议》，每季度一次</p> <p>《应急响应处置与分析报告》，每月一次，不少于9次</p> <p>《远程监测服务安全事件报告》，按需</p> <p>《远程监测服务周报》，每周一次</p> <p>《远程监测服务月报》，每月一次</p> <p>驻场服务人员与远程支撑技术人员需一起完成上述工作，共同提供相关报告。</p>
---	---	------	---

2	√	<p>网络安全事件监测及预警</p> <p>交付形式：通过监测预警平台进行现场监控，驻场服务，发现安全事件实时进行预警并协助进行处置</p> <p>服务内容：驻场服务工程师对监测范围内各单位自然资源业务网进行网络安全事件监测及预警，具体内容包括但不限于：</p> <p>（A）网络监控内容主要包括数据流异常分析和黑客入侵监控。</p> <p>（B）主机监控内容主要包括重要服务器系统信息监控、服务器重要文件监控和重要服务器网络连接。</p> <p>（C）数据库监控内容主要包括对核心数据库的异常操作进行监控。</p> <p>（D）网络设备监控内容主要包括核心网络设备的日志告警信息。</p> <p>（E）安全设备监控内容主要包括重要安全设备的安全事件和入侵报警等信息。</p> <p>服务要求：1）以网络流量、告警日志为基础，结合先进的威胁情报检测能力、丰富的关联规则、强大的机器学习检测三位一体。在产生威胁后，进行验证分析，为各级用户提供真实可靠的威胁情况分析，提供解决方案协助各单位及时进行处理。一线运营人员通告安全事件时根据内蒙古自治区自然资源厅综合保障中心的要求，完成《事件通告报告》，报告内容应包括但不仅限于：漏洞描述、告警分析、影响范围、处置建议等内容。同时将事件记录到《事件通报处置汇总表》，最终体现在日常的运营日报、周报中。</p> <p>2）根据监测范围内各单位提供的互联网、政务外网重要资产名单，基于云监测和流量日志采集器进行漏洞分析和流量安全分析，安全运营工程师对安全监测和流量分析，按照不同的业务提供漏洞验证和流量分析，分析以后输出《安全监测报告》和《流量分析报告》。</p>
---	---	--

		3	√	漏洞隐患监测及预警	<p>通过专业的工具，依据OWASP TOP10进行标准化漏洞人工验证，并给出安全加固建议报告。工具需要具备IPv4、Ipv6网络协议接入方式，具备系统扫描、基线配置核查、口令猜解、Web扫描和数据库扫描功能。安全评估工具须为商业正版化软件，所形成的漏洞报告支持导入到监测预警平台进行关联分析。</p> <p>漏洞隐患监测包括但不限于SQL注入漏洞、XSS漏洞、参数污染、JAVA漏洞、文件包含漏洞、URL跳转漏洞、Nginx任意文件执行漏洞、SVN/CVS文件泄漏漏洞、Padding Oracle漏洞、目录遍历漏洞、DNS漏洞、Flash安全配置缺陷、Mysql弱口令及远程溢出、FTP弱口令及远程溢出库、WordPress漏洞库、Web漏洞集（CMS、BBS等）、缓冲区溢出等漏洞审核或验证工作，确保漏洞的准确性，对漏洞进行详情解释和处置建议，最终输出《漏洞验证报告》。</p>
		4	√	日常安全事件分析	<p>由驻场服务人员现场完成，针对重大安全事件必要时需由远程安全专家介入与现场服务人员共同完成</p> <p>针对在日常网络安全监测中发现的较大安全影响的网络安全事件，协助进行安全事件处置，配合进行网络安全事件的判定，配合收集和提供相关的处置工具，协助相关单位共同对安全事件进行抑制，降低安全事件可能造成的影响程度。最终输出《日常安全事件分析及处置报告》</p>
		5	√	安全态势分析	<p>由驻场服务人员现场完成，安全态势分析服务包括，通过持续的安全运营收集安全事件的分布情况、分类情况、损失情况，威胁情报等，对当前阶段威胁风险进行预警，并结合威胁狩猎手段，主动发现未知风险，协助进行排查。</p> <p>每周现场安全运营人员进行全网流量安全态势分析，主要涉及分析Web安全、系统安全、数据库安全、威胁情报等重点内容，并对态势分析形成专业《流量分析报告》。</p>
					针对渗透测试、漏洞扫描和安全检查过程中发现
		6	√	安全加固支持服务	<p>针对各种安全隐患，提出整改建议。监测范围内各单位完成安全隐患整改后，进行复测，检查隐患是否消除。</p>

打“★”号条款为实质性条款，若有任何一条偏离或不满足则导致响应无效。

第四章 供应商应当提交的资格、资信证明文件

供应商应提交证明其有资格参加磋商和成交后有能力履行合同的相关文件，并作为其响应文件的一部分，所有文件必须真实可靠、不得伪造，否则将按相关规定予以处罚。

一、法人或者其他组织的营业执照等证明文件，自然人的身份证明。法人包括企业法人、机关法人、事业单位法人和社会团体法人；其他组织主要包括合伙企业、非企业专业服务机构、个体工商户、农村承包经营户；自然人是指具有完全民事行为能力、能够承担民事责任和义务的公民。如供应商是企业（包括合伙企业），要提供在市场监督管理部门注册的有效“企业法人营业执照”或“营业执照”；如供应商是事业单位，要提供有效的“事业单位法人证书”；供应商是非企业专业服务机构，如律师事务所、会计师事务所，要提供有效的执业许可证等证明文件；如供应商是个体工商户，要提供有效的“个体工商户营业执照”；如供应商是自然人，要提供有效的自然人身份证明。

分公司不是独立法人，不具备政府采购法第二十二条规定的供应商应当具备独立承担民事责任能力的条件。分公司经总公司授权，可以以分公司的名义参加政府采购活动，但其民事责任由总公司承担。

二、财务状况报告，依法缴纳税收和社会保障资金的相关材料（详见资格审查表）

三、具备履行合同所必需的设备和专业技术能力的证明材料。

四、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。

五、按照磋商文件要求，供应商应当提交的其他资格、资信证明文件。

第五章 评审

一.评审要求

1.评审方法

磋商小组采用综合评分法对提交最后报价的供应商的响应文件和最后报价进行综合评分。综合评分法，是指响应文件满足磋商文件全部实质性要求且按评审因素的量化指标评审得分最高的供应商为成交候选供应商的评审方法。

2.评审原则

2.1磋商小组成员应当遵循客观、公正、审慎的原则，根据磋商文件规定的评审程序、评审方法和评审标准进行独立评审。

2.2具体评审事项由磋商小组负责，并按磋商文件规定的办法进行评审。

3.磋商小组

由采购人代表和评审专家两部分共3人组成，其中由评审专家库产生的评审专家2人，由采购人派出的采购人代表1人。技术复杂、专业性强的采购项目，评审专家中应当包含1名法律专家。

3.1磋商小组由采购人代表和评审专家共3人以上单数组成，其中评审专家人数不得少于磋商小组成员总数的2/3。

3.2磋商小组成员有下列情形之一的，应当回避：

（1）参加政府采购活动前3年内,与供应商存在劳动关系,或者担任过供应商的董事、监事,或者是供应商的控股股东或实际控制人；

（2）与供应商的法定代表人或者负责人有夫妻、直系血亲、三代以内旁系血亲或者近姻亲关系；

（3）与供应商有其他可能影响政府采购活动公平、公正进行的关系；

3.3磋商小组负责具体评审事务，并独立履行下列职责：

（1）对响应文件的有效性、完整性和响应程度进行审查；

（2）要求供应商对响应文件有关事项作出澄清、说明或更正；

（3）磋商小组所有成员应当集中与单一供应商分别进行磋商；

（4）对响应文件进行比较和评价；

（5）确定成交候选人名单，以及根据采购人委托直接确定成交供应商；

（6）向采购人、采购代理机构或者有关部门报告评审中发现的违法行为；

（7）法律法规规定的其他职责。

4.澄清

磋商小组在对响应文件的有效性、完整性和响应程度进行审查时，可以要求供应商对响应文件中含义不明确、同类问题表述不一致或者有明显文字和计算错误的内容等作出必要的澄清、说明或者更正。供应商的澄清、说明或者更正不得超出响应文件的范围或者改变响应文件的实质性内容。

磋商小组要求供应商澄清、说明或者更正响应文件应当以书面形式作出。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，应当附法定代表人授权书。供应商为自然人的，应当由本人签字并附身份证明。

4.1磋商小组不接受供应商主动提出的澄清、说明或更正。

4.2磋商小组对供应商提交的澄清、说明或更正有疑问的，可以要求供应商进一步澄清、说明或更正。

5.有下列情形之一的，属于恶意串通，并追究法律责任：

（1）供应商直接或者间接从采购人或者采购代理机构处获得其他供应商的相关情况并修改其响应文件；

（2）供应商按照采购人或者采购代理机构的授意撤换、修改响应文件；

- (3) 供应商之间协商报价、技术方案等响应文件的实质性内容；
- (4) 属于同一集团、协会、商会等组织成员的供应商按照该组织要求协同参加政府采购活动；
- (5) 供应商之间事先约定由某一特定供应商成交；
- (6) 供应商之间商定部分供应商放弃参加政府采购活动或者放弃成交；
- (7) 供应商与采购人或者采购代理机构之间、供应商相互之间，为谋求特定供应商成交或者排斥其他供应商的其他串通行为。

6. 响应无效的情形

- (1) 供应商未按照磋商文件要求提交磋商保证金的，响应无效；
- (2) 在提交响应文件截止时间后递交响应文件的，响应无效；
- (3) 未实质性响应磋商文件的，响应无效；
- (4) 法律、法规和磋商文件规定的其他无效情形。

7. 终止的情形

出现下列情形之一的，采购人或者采购代理机构应当终止竞争性磋商采购活动，发布公告并说明原因，重新开展采购活动：

- (1) 因情况变化，不再符合规定的竞争性磋商采购方式适用情形的；
- (2) 出现影响采购公正的违法、违规行为的；
- (3) 除《政府采购竞争性磋商采购方式管理暂行办法》及其补充通知规定的情形外，在采购过程中符合要求的供应商或者报价未超过采购预算的供应商不足3家的。
- (4) 法律、法规以及磋商文件规定的其他情形。

8. 成交

评审结束后，磋商小组根据采购人书面授权直接确定成交供应商或者由采购人从评审报告提出的成交候选供应商中按顺序确定成交供应商。

二. 落实政府采购政策

1. 节约能源、保护环境

采购的产品属于品目清单范围的，将依据国家确定的认证机构出具的、处于有效期之内的节能产品、环境标志产品认证证书，对获得证书的产品实施政府优先采购或强制采购，具体按照本磋商文件相关要求执行。

2. 促进中小企业发展

2.1 采购人在政府采购活动中应当通过加强采购需求管理，落实预留采购份额、价格评审优惠、优先采购等措施，提高中小企业在政府采购中的份额，支持中小企业发展。

2.2 《政府采购促进中小企业发展管理办法》所称中小企业，是指在中华人民共和国境内依法设立，依据国务院批准的中小企业划分标准确定的中型企业、小型企业和微型企业，但与大企业的负责人为同一人，或者与大企业存在直接控股、管理关系的除外。符合中小企业划分标准的个体工商户，在政府采购活动中视同中小企业。

2.3 在政府采购活动中，供应商提供的货物、工程或者服务符合下列情形的，享受《政府采购促进中小企业发展管理办法》规定的中小企业扶持政策：

- (1) 在货物采购项目中，货物由中小企业制造，即货物由中小企业生产且使用该中小企业商号或者注册商标；
- (2) 在工程采购项目中，工程由中小企业承建，即工程施工单位为中小企业；
- (3) 在服务采购项目中，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。

在货物采购项目中，供应商提供的货物既有中小企业制造货物，也有大型企业制造货物的，不享受《政府采购促进中小企业发展管理办法》规定的中小企业扶持政策。

以联合体形式参加政府采购活动，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。

2.4依照《政府采购促进中小企业发展管理办法》《关于政府采购支持监狱企业发展有关问题的通知》和《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》的规定，凡符合要求的小型、微型企业、监狱企业或残疾人福利性单位，按照以下比例给予相应的价格扣除：【相应的价格扣除磋商】

2.5在政府采购活动中，提供货物、工程或者服务符合享受中小企业扶持政策的，供应商应提供《中小企业声明函》；属于监狱企业的，应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；属于残疾人福利性单位的，应提供《残疾人福利性单位声明函》。供应商应当按照《中小企业声明函》《残疾人福利性单位声明函》规定格式提供（格式附后，不可修改），未按规定提供的，不得享受相关中小企业扶持政策。

供应商应当对提供材料的真实性负责，若有虚假，将追究其法律责任。

三.评审程序

1.资格审查

1.1磋商小组依据法律法规和磋商文件的规定，对响应文件中的资格证明文件等进行审查，以确定供应商是否具备响应资格。

1.2资格审查中有任意一项未通过的，审查结果为未通过，未通过资格审查的供应商按无效响应处理。

1.3信用记录查询

查询渠道：通过“信用中国”网站(www.creditchina.gov.cn)和“中国政府采购网”（www.ccgp.gov.cn）进行查询；

查询截止时点：本项目资格审查时查询；

查询记录：对列入失信被执行人、重大税收违法失信主体、政府采购严重违法失信行为记录名单、信用报告进行查询；

磋商小组应当按照查询渠道、查询时间节点、查询记录内容进行查询，并存档。对信用记录查询结果中显示被列入失信被执行人、重大税收违法失信主体、政府采购严重违法失信行为记录名单的供应商将被拒绝参与政府采购活动。

资格审查表

采购包1：

序号	资格审查要求概况	评审点具体描述
1	具有独立承担民事责任的能力	审查供应商营业执照等证明文件或者身份证明。
2	具有良好的商业信誉和健全的财务会计制度	供应商提供2023年度或2024年度经审计部门审计的财务审计报告（财务审计报告包括“四表一注”，即资产负债表、利润表、现金流量表、所有者权益变动表及其附注（所有者权益无变动的可不提供该表）或基本开户银行出具的近一年内资信证明或健全的财务会计制度承诺
3	有依法缴纳税收和社会保障资金的良好记录	1.提供递交投标文件截止之日前一年内（至少一个月）的良好缴纳税收的相关凭据。（以税务机关提供的纳税凭据或银行入账单为准） 2.提供递交投标文件截止之日前一年内（至少一个月）缴纳社会保险的凭证。（以专用收据或社会保险缴纳清单为准）或出具“参加采购活动前依法缴纳税收和社会保障资金承诺书。注：其他组织和自然人也需要提供缴纳税收的凭据和缴纳社保的凭据。依法免税或不需要缴纳社会保障资金的投标人，应提供相应文件证明其依法免税或不需要缴纳社会保障资金

4	具有履行合同所必须的设备和专业技术能力	审查供应商提供的具有履行合同所必需的设备和专业技术能力的书面声明。
5	参加采购活动前3年内，在经营活动中没有重大违法记录	审查供应商参加本次采购活动前3年内在经营活动中没有重大违法记录的书面声明。
6	信用记录	资格审查时，供应商未被列入失信被执行人、税收违法黑名单、政府采购严重违法失信行为记录名单。
7	联合体响应（若有）	符合关于联合体响应的相关规定。

采购包1：

资格审查要求概况	评审点具体描述
----------	---------

采购包1：

资格审查要求概况	评审点具体描述
本采购包属于专门面向小微企业采购。	提供《中小企业声明函》，残疾人福利性单位提供《残疾人福利性单位声明函》，监狱企业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。（如供应商以联合体形式参加本采购包的，联合体各方均应当符合本采购包专门面向的企业类型；如供应商合同分包的，分包意向协议中分包意向供应商应当符合本采购包专门面向的企业类型。）

2.符合性审查

2.1磋商小组依据磋商文件的规定，从响应文件的有效性、完整性和对磋商文件的响应程度进行审查，以确定是否对磋商文件的实质性要求作出响应。

2.2符合性审查中有任何一项未通过的，评审结果为未通过，未通过符合性审查的供应商按无效响应处理。

符合性审查表

采购包1：

序号	符合审查要求概况	评审点具体描述
1	投标及保证金缴纳情况	按要求进行网上投标、进行保证金缴纳。（审查汇款凭证）
2	投标报价	投标报价（包括分项报价，投标总报价）只能有一个有效报价且不超过采购预算或最高限价，投标报价不得缺项、漏项。
3	投标文件规范性、符合性	响应文件的签署、盖章、涂改、删除、插字、公章使用等符合磋商文件要求；响应文件文件的格式、文字、目录等符合磋商文件要求或对投标无实质性影响。
4	主要商务条款	审查供应商出具的“满足主要商务条款的承诺书”，且进行盖章。
5	技术部分实质性内容	1.明确所投标的的产品品牌、规格型号或服务内容或工程量； 2.响应文件应当对磋商文件提出的要求和条件作出明确响应并满足磋商文件全部实质性要求。
6	其他要求	磋商文件要求的其他无效投标情形；围标、串标和法律法规规定的其它无效投标条款。

3.磋商

磋商小组所有成员应当集中与单一供应商分别进行磋商，并给予所有参加磋商的供应商平等的磋商机会。

在磋商过程中，磋商小组可以根据磋商文件和磋商情况实质性变动采购需求中的技术、服务要求以及合同草案条款，但不得变动磋商文件中的其他内容。实质性变动的内容，须经采购人代表确认。

对磋商文件作出的实质性变动是磋商文件的有效组成部分，磋商小组应当及时通过政府采购云平台同时通知所有参加磋商的供应商。

供应商应当按照磋商文件的变动情况和磋商小组的要求重新提交响应文件，并由其法定代表人或授权代表签字或者加盖公章。由授权代表签字的，应当附法定代表人授权书。供应商为自然人的，应当由本人签字并附身份证明。

4.最后报价

磋商结束后，磋商小组应当要求所有实质性响应的供应商在规定时间内提交最后报价。最后报价是供应商响应文件的有效组成部分。

已提交响应文件的供应商，在提交最后报价之前，可以根据磋商情况退出磋商。

未在最终轮次规定时间内进行响应的，视为不再参与该政府采购活动。

5.政府采购政策功能落实

依据《政府采购促进中小企业发展管理办法》等规定，对符合条件的小微企业、监狱企业或残疾人福利性单位给予价格扣除。

6.综合评分

由磋商小组采用综合评分法对提交最后报价的供应商的响应文件和最后报价进行综合评分（得分四舍五入保留两位小数）。

采购包1:

采购包1:

评审因素		评审标准		
分值构成		技术部分 80.00 分 商务部分 10.00 分 报价得分 10.00 分		
评审因素分类	评审项	详细描述	分值	客观/主观
	响应文件对竞争性磋商文件技术需求的响应程度	对竞争性磋商文件技术参数和要求的响应程度，标记“√”项完全满足得 15 分，有一项负偏离扣 1 分，扣完为止。	15.00	客观

技术评审	服务方案	<p>供应商结合本项目的特点，提供包括但不限于以下方案，需进行详细阐述: 1.对本次服务目标的理解; 2.对本次服务的重点、难点进行全面分析总结概述; 3.对本项目拟派服务团队配置的说明; 4.服务过程中的数据安全风险识别; 5.服务风险规避措施。以上5项内容，整体最多得20分;每缺一项扣4分，每存在一种瑕疵扣0.5分，扣完为止。(本项所指“瑕疵”的种类包括: 内容不完整或缺少关键点; 非专门针对本项目或不适用本项目特性、套用其他项目内容;存在逻辑漏洞、科学原理或常识错误;不利于本项目实施、现有技术条件下无法实现等情形)</p>	20.00	主观
	现状及需求的理解	<p>根据投标人对整体现状及用户需求分析理解进行综合评审。整体最多得5分;未提供不得分，每存在一种瑕疵扣1分，扣完为止。(本项所指“瑕疵”的种类包括: 内容不完整或缺少关键点;非专门针对本项目或不适用本项目特性、套用其他项目内容;存在逻辑漏洞、科学原理或常识错误;不利于本项目实施、现有技术条件下无法实现等情形)</p>	5.00	主观
	技术方案设计	<p>投标人需根据本项目的特点进行整体规划方案设计，1、方案整体规划合理、设计编制规范、内容完整可行、符合项目特点、针对性强、落地且符合用户需求; 2、投标人结合项目要求，提出完善的安全运营服务方案，涵盖安全评估、渗透测试、资产发现服务等方面，服务描述全面、科学合理、可落地; 3、根据各投标人的实施方案进行综合评审: 方案包括但不限于安全运营项目组人员架构设计、管理计划、项目实施进度计划、工具部署计划。以上3项内容，整体最多得12分;每缺一项扣4分，每存在一种瑕疵扣1分，扣完为止。(本项所指“瑕疵”的种类包括: 内容不完整或缺少关键点;非专门针对本项目或不适用本项目特性、套用其他项目内容;存在逻辑漏洞、科学原理或常识错误;不利于本项目实施、现有技术条件下无法实现等情形)</p>	12.00	主观

售后服务方案	根据投标人提供的售后服务方案(包括但不限于质保期、人员安排及能力、售后服务响应时间、解决故障时间、故障处理过程中的替代品措施、售后维护、应急保障、服务承诺)整体最多得5分;未提供不得分,每存在一种瑕疵扣1分,扣完为止。(本项所指“瑕疵”的种类包括:内容不完整或缺少关键点;非专门针对本项目或不适用本项目特性、套用其他项目内容;存在逻辑漏洞、科学原理或常识错误;不利于本项目实施、现有技术条件下无法实现等情形)	5.00	主观
应急响应方案	根据投标人的应急响应方案详细、科学程度综合比较,应急响应方案详细、科学程度高。整体最多得3分;未提供不得分,每存在一种瑕疵扣0.5分,扣完为止。(本项所指“瑕疵”的种类包括:内容不完整或缺少关键点;非专门针对本项目或不适用本项目特性、套用其他项目内容;存在逻辑漏洞、科学原理或常识错误;不利于本项目实施、现有技术条件下无法实现等情形)	3.00	主观
项目管理方案	投标人针对本次项目要求交付时间及服务内容进行项目管理方案设计,方案设计覆盖全面合理,包括但不限于:项目组织协调管理、项目安全保密管理、项目验收管理等方面进行设计。整体最多得5分;未提供不得分,每存在一种瑕疵扣1分,扣完为止。(本项所指“瑕疵”的种类包括:内容不完整或缺少关键点;非专门针对本项目或不适用本项目特性、套用其他项目内容;存在逻辑漏洞、科学原理或常识错误;不利于本项目实施、现有技术条件下无法实现等情形)	5.00	主观
保密保障措施	根据投标人:1、保密管理 2、保密措施 3、保密制度 以上3项内容,整体最多得12分;每缺一项扣4分,每存在一种瑕疵扣1分,扣完为止。(本项所指“瑕疵”的种类包括:内容不完整或缺少关键点;非专门针对本项目或不适用本项目特性、套用其他项目内容;存在逻辑漏洞、科学原理或常识错误;不利于本项目实施、现有技术条件下无法实现等情形)	12.00	主观

	实施方案	根据产品特点提供具有先进、可行、安全、合理及针对性的安装调试方案进行综合评分。整体最多得3分;未提供不得分,每存在一种瑕疵扣0.5分,扣完为止。(本项所指“瑕疵”的种类包括:内容不完整或缺少关键点;非专门针对本项目或不适用本项目特性、套用其他项目内容;存在逻辑漏洞、科学原理或常识错误;不利于本项目实施、现有技术条件下无法实现等情形)	3.00	主观
商务评审	类似业绩	提供(2022年至投标截止时间)类似业绩,每提供一个业绩得2分,最多得10分(以合同或中标通知书复印件为标准,未提供或提供不全的不得分)。	10.00	客观
价格分	价格分	$F1$ 指价格项评审因素得分=(评标基准价/投标报价) $\times 100 \times$ 价格项评审因素所占的权重(注: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。)最低报价不是中标的唯一依据。因落实政府采购政策进行价格调整的,以调整后的价格计算评标基准价和投标报价。	10.00	客观

价格扣除

序号	情形	适用对象	比例	说明
无				

7.汇总、排序

磋商小组根据综合评分情况,按照评审得分由高到低顺序推荐3名以上成交候选供应商,并编写评审报告。符合《政府采购竞争性磋商采购方式管理暂行办法》相关规定的,可以推荐2家成交候选供应商。评审得分相同的,按照最后报价由低到高的顺序推荐。评审得分且最后报价相同的,按照技术指标优劣顺序推荐。

第六章 合同与验收

一.合同

1.合同要求

1.1采购人应当自中标（成交）通知书发出之日起**30**日内，按照招标（磋商、谈判）文件或询价通知书和中标（成交）供应商投标（响应）文件的规定，与中标（成交）供应商签订书面合同。所签订的合同不得对招标（磋商、谈判）文件或询价通知书确定的事项作实质性修改。采购人、供应商不得提出任何不合理的要求作为签订合同的条件。

1.2政府采购合同应当包括采购人与中标（成交）供应商的名称和住所、标的、数量、质量、价款或者报酬、履行期限及地点和方式、验收要求、违约责任、解决争议的方法等内容。

1.3采购人与中标（成交）供应商应当根据合同的约定依法履行合同义务。政府采购合同的履行、违约责任和解决争议的方法等适用《中华人民共和国民法典》。政府采购合同的双方当事人不得擅自变更、中止或者终止合同。

1.4采购人应当自政府采购合同签订之日起**2**个工作日内，将政府采购合同在内蒙古自治区政府采购网（<https://www.ccgp-neimenggu.gov.cn/>）公告，但政府采购合同中涉及国家秘密、商业秘密的内容除外。

1.5采购人应当自政府采购合同签订之日起**7**个工作日内，将合同副本向同级财政部门 and 有关部门备案。

2.合同格式及内容

政府采购合同

(货物类合同参考文本)

合同编号:

甲方:*** (填写采购单位名称)

地址:*** (填写详细地址)

乙方:*** (填写中标、成交供应商名称)

地址:*** (填写详细地址)

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》《中华人民共和国民法典》等相关法律法规、规范性文件以及 _____ 项目(填写项目名称) _____ (填写政府采购项目编号)的中标(成交)结果、招标(磋商、谈判)文件或询价通知书、投标(响应)文件等文件的相关内容,甲乙双方经平等协商,就如下合同条款达成一致意见。

一、甲方向乙方采购的货物基本情况

(一)根据招标(磋商、谈判)文件或询价通知书及中标(成交)结果公告,甲方所采购的货物、服务(如有)基本情况如下: _____。

(二)货物名称、数量、规格型号、生产厂家、品牌、单价、与货物相关的服务等详细内容,见合同附件-货物清单。

二、乙方交付货物的时间及地点

(一)交付时间: _____

(二)交付地点: _____ (填写详细地址)

(三)交付货物的名称及数量: _____

(四)乙方交付货物代表及联系电话: _____ (填写姓名和联系电话)

(五)甲方接收货物代表及联系电话: _____ (填写姓名和联系电话)

注:货物为多批次交付的,应详细列明每批次交付的内容、数量、交付时间、交付地点等。

三、乙方交付货物的质量

(一)乙方交付的货物应同时满足:1.符合国家法律法规和规范性文件对货物的质量要求;2.符合甲方招标(磋商、谈判)文件或询价通知书对货物的质量要求;3.符合乙方在投标(响应)文件中或磋商、谈判过程中对货物质量作出的书面承诺、声明或保证。上述质量要求作为甲方对乙方货物质量的验收依据。

(二)乙方应根据国家法律法规和规范性文件的规定、招标(磋商、谈判)文件或询价通知书的相关要求、投标(响应)文件及乙方承诺、声明或保证,向甲方提供相应的货物质量证明文件。

四、乙方交付货物的包装及标识

(一)乙方交付货物的包装和标识应同时满足:1.符合国家法律法规和规范性文件对产品包装及标识的要求;2.符合甲方招标(磋商、谈判)文件或询价通知书对货物包装及标识的要求;3.符合乙方在投标(响应)文件中对货物包装及标识作出的承诺、声明或保证;4.符合绿色环保、运输及安全性等要求。

(二)货物的包装费用由乙方承担。

五、货物的运输要求

(一)运输方式及运输线路: _____。

(二)运输、保险及其他相关费用由乙方承担。

六、甲方对货物的验收

(一)乙方将货物送达至甲方指定的地点,应及时通知甲方。在甲方收到到货通知并在货物到达指定地点后 _____ 日

内，由甲乙双方及第三方（如有）对货物的数量、规格型号、生产厂家、品牌、外观进行验收，在条件允许的情况下，可以同步对货物质量进行初步验收，甲乙双方应签署书面验收记录，作为本项目的履行文件留存。

（二）在甲方收到货物_____日内，如发现质量问题，甲方应在_____日内向乙方提出书面异议，甲方逾期提出的，视为乙方所交付的货物质量符合合同的约定。乙方在收到甲方关于质量问题的书面异议后，应当在_____日内负责解决处理。

（三）乙方提交的货物数量、规格型号及质量不符合本合同要求的，甲方应在验收记录中作出明确记载，保留相关的证据，并有权拒绝接受货物，解除合同且不承担任何法律责任。

七、合同金额

在乙方提供完全符合合同要求的货物的前提下，本合同总金额为_____元（小写）_____（大写）

八、付款时间、金额及条件

（一）付款时间及付款金额：_____

（二）付款条件：_____

（三）乙方账户信息

乙方名称：_____

开户银行：_____

银行账号：_____

九、货物质量保证及售后服务

招标（磋商、谈判）文件或询价通知书对货物质量保证期及售后服务作出明确要求的，适用招标（磋商、谈判）文件或询价通知书对保证期和售后服务的规定，如乙方在投标（响应）文件及磋商、谈判过程中对货物质量保证期和售后服务作出更优的承诺、声明或保证的，适用乙方的承诺、声明或保证。

十、知识产权

乙方保证其提供的货物的全部及部分，均不存在任何侵犯第三方知识产权的情形。否则，乙方应向甲方承担违约责任及赔偿由此给甲方造成的名誉及经济损失。

十一、违约条款

（一）甲方没有正当理由逾期支付合同款项的，每延期一日，甲方应按照逾期支付金额_____的_____承担违约责任。延期达到_____日，乙方有权解除合同，并要求甲方赔偿由此造成的经济损失。

（二）甲方存在其他违反本合同的行为，应承担相应的违约责任（注：可以根据情况进行细化）；违约金不足以赔偿乙方损失的，乙方有权要求甲方赔偿由此造成的经济损失。

（三）乙方逾期交付货物的，每延期一日，乙方应按照合同总金额的_____承担违约责任。延期达到_____日，甲方有权解除合同，拒付延期部分货物的相应货款，并要求乙方赔偿甲方的经济损失。

（四）乙方交付的货物不符合质量约定或乙方未履行相应的质量保证责任及售后服务义务、或存在侵权行为的，甲方有权退货，并要求乙方支付合同总金额_____%的违约金，违约金不足以赔偿甲方损失的，甲方有权要求乙方赔偿经济损失。

（五）乙方在参与本项目采购活动过程中，如存在提供虚假承诺、证明、串通投标等违法违规行为，除承担相应的行政责任外，甲方有权解除合同，并要求乙方承担合同总金额_____%的违约金，违约金不足以赔偿甲方损失的，甲方有权要求乙方赔偿经济损失。

（六）乙方存在其他违反本合同的行为，应承担相应的违约责任（注：可以根据情况进行细化）；违约金不足以赔偿甲方损失的，甲方有权要求乙方赔偿经济损失。

十二、不可抗力

因不可抗力致使一方不能及时或完全履行合同的，应及时通知另一方，双方互不承担责任，并在_____天内提供有关不可抗力的相关证明。合同未履行部分是否继续履行、如何履行等问题，双方协商解决。

十三、争议的解决方式

合同发生纠纷时，双方应协商解决，协商不成，可以采用下列方式解决：

（一）提交_____仲裁委员会仲裁。

（二）向_____人民法院起诉。

十四、合同保存

合同文本一式_____份，采购单位、中标（成交）供应商、采购代理机构、_____各执一份。合同文本保存期限为从采购结束之日起至少保存十五年。

十五、合同附件

本合同所附下列文件是构成本合同不可分割的组成部分，其内容与本合同具有同等的法律效力：

- 1、货物清单（双方应盖章确认）
- 2、乙方出具的报价单（函）
- 3、中标（成交）结果公告及中标（成交）通知书
- 4、甲方招标（磋商、谈判）文件或询价通知书
- 5、乙方投标（响应）文件
- 6、甲乙双方商定的其他文件

十六、双方约定的其他条款

_____。

十七、本合同未尽事宜，由双方另行签订补充协议，补充协议是本合同的组成部分。

十八、本合同由甲乙双方盖章生效。

甲方名称：（章）

甲方法定代表人或负责人：（签字）

年 月 日

乙方名称：（章）

乙方法定代表人或负责人：（签字）

年 月 日

政府采购合同

（服务类合同参考文本）

合同编号：

甲方：***（填写采购单位名称）

地址：***（填写详细地址）

乙方：***（填写中标、成交供应商名称）

地址：***（填写详细地址）

甲乙双方根据《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》《中华人民共和国民法典》等相关法律法规、规范性文件以及_____项目（填写项目名称）_____（填写政府采购项目编号）的中标（成交）结果、招标（磋商、谈判）文件、投标（响应）文件等文件的相关内容，经平等自愿协商一致，就如下合同条款达成一致意见。

一、乙方向甲方提供的服务内容

（一）根据招标（磋商、谈判）文件及中标（成交）结果公告，乙方向甲方提供的服务、货物（如有）内容如下：_____

_____。

（二）服务项目名称、服务具体内容、服务方式、服务要求、服务成果及与之相关的货物等详细内容，见合同附件—服务清单。

二、乙方服务成果的交付时间、地点

（一）服务期限：_____

（二）服务成果的交付时间和交付要求（如有）：_____

（三）服务地点：_____（填写详细地址）

（四）乙方代表及联系电话：_____（填写姓名和联系电话）

（五）甲方代表及联系电话：_____（填写姓名和联系电话）

注：服务成果分阶段交付的，应分别列明各阶段的交付时间、交付内容。

三、乙方提供服务成果的质量

（一）乙方提供的服务应同时满足：**1.**符合国家法律法规和规范性文件对服务质量的要求；**2.**符合甲方招标（磋商、谈判）文件对服务的质量要求；**3.**符合乙方在投标（响应）文件中或磋商、谈判过程中对服务质量作出的书面承诺、声明或保证。上述质量要求作为甲方对乙方服务质量的验收依据。

（二）乙方应根据国家法律法规和规范性文件的规定、招标（磋商、谈判）文件的相关要求、投标（响应）文件及乙方承诺、声明或保证，向甲方提供相应的服务质量证明文件。

四、乙方服务成果的交付方式及载体

乙方交付服务成果方式及载体应符合国家法律法规和规范性文件的要求，并符合甲方招标（磋商、谈判）文件的要求、乙方在投标（响应）文件中对服务成果交付方式及载体作出的承诺。

五、甲方对乙方服务的监督

甲方对乙方提供的服务有权进行监督，当乙方服务质量、服务内容不符合约定时，甲方有权要求乙方及时整改，对乙方拒不改正或整改不到位的，甲方有权随时解除合同，并根据具体情况扣除部分或全部服务费用。

六、合同金额

在乙方提供完全符合合同要求的服务的前提下，本合同总金额为_____元（小写）_____（大写）。

七、付款时间及条件

（一）付款时间：_____

(二) 付款条件: _____

(三) 乙方账户信息

乙方名称: _____

开户银行: _____

银行账号: _____

八、知识产权

乙方应保证其提供的服务及服务成果的全部及部分, 均不存在侵犯第三方知识产权的情形, 其服务成果的所有权由甲方享有。否则, 乙方应向甲方承担违约责任及赔偿由此给甲方造成的名誉及经济损失。

九、违约条款

(一) 甲方没有正当理由逾期支付合同款项的, 每延期一日, 甲方应按照逾期支付金额_____的_____承担违约责任。延期达到_____日, 乙方有权解除合同, 并要求甲方赔偿由此造成的经济损失。

(二) 甲方存在其他违反本合同的行为, 应承担相应的违约责任(注: 可以根据情况进行细化); 违约金不足以赔偿乙方损失的, 乙方有权要求甲方赔偿由此造成的经济损失。

(三) 乙方逾期提供服务成果的, 每延期一日, 乙方应按照合同总金额的_____承担违约责任。延期达到_____日, 甲方有权解除合同, 拒付延期部分的相应服务款项, 并要求乙方赔偿甲方的经济损失。

(四) 乙方交付的服务不符合质量要求, 或其服务成果存在侵权行为的, 甲方有权解除合同, 并要求乙方支付合同总金额_____ %的违约金, 违约金不足以赔偿甲方损失的, 甲方有权要求乙方赔偿经济损失。

(五) 乙方在参与本项目采购活动过程中, 如存在提供虚假承诺、证明、串通投标等违法违规行为, 除承担相应的行政责任外, 甲方有权解除合同, 并要求乙方承担合同总金额_____ %的违约金, 违约金不足以赔偿甲方损失的, 甲方有权要求乙方赔偿经济损失。

(六) 乙方存在其他违反本合同的行为, 应承担相应的违约责任(注: 可以根据情况进行细化); 违约金不足以赔偿甲方损失的, 甲方有权要求乙方赔偿经济损失。

十、不可抗力

因不可抗力致使一方不能及时或完全履行合同的, 应及时通知另一方, 双方互不承担责任, 并在_____天内提供有关不可抗力相关证明。合同未履行部分是否继续履行、如何履行等问题, 由双方协商解决。

十一、争议的解决方式

合同发生纠纷时, 双方应协商解决, 协商不成, 可以采用下列方式解决:

(一) 提交_____仲裁委员会仲裁。

(二) 向_____人民法院起诉。

十二、合同保存

合同文本一式_____份, 采购单位、中标(成交)供应商、采购代理机构、_____各执一份。合同文本保存期限为从采购结束之日起至少保存十五年。

十三、合同附件

本合同所附下列文件是构成本合同不可分割的部分, 与本合同具有同等法律效力:

- 1、服务清单(双方应盖章确认)
- 2、乙方出具的报价单(函)
- 3、中标(成交)结果公告及中标(成交)通知书
- 4、甲方招标(磋商、谈判)文件
- 5、乙方投标(响应)文件
- 6、甲乙双方商定的其他文件

十四、双方约定的其他事宜

_____。
十五、合同未尽事宜，双方另行签订补充协议，补充协议是合同的组成部分。

十六、本合同由甲乙双方盖章生效。

甲方名称：（章）

甲方法定代表人或负责人：（签字）

年 月 日

乙方名称：（章）

乙方法定代表人或负责人：（签字）

年 月 日

政府采购合同

(工程类合同参考文本)

合同编号:

甲方:*** (填写采购单位名称)

地址:*** (填写详细地址)

乙方:*** (填写中标、成交供应商名称)

地址:*** (填写详细地址)

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》《中华人民共和国民法典》等相关法律法规、规范性文件以及_____项目(填写项目名称)_____填写政府采购项目编号)的成交结果、磋商(谈判)文件、响应文件等文件的相关内容,甲乙双方经平等协商,就如下合同条款达成一致意见。

一、工程项目的的基本情况

(一)根据磋商(谈判)文件及成交结果公告,乙方向甲方提供的工程项目及设施设备(如有)、服务(如有)基本情况如下:_____。

(二)工程项目的名称、建设地点、工程技术规范及要求、工程量等具体内容,乙方提供的材料及设备名称、规格型号、品牌、单价、产地以及与工程、材料、设施设备相关的服务等详细内容,见合同附件一工程清单

二、工程建设计划及相应的工期要求

_____。

注:如工程建设分阶段,应详细列明各阶段工程建设内容及工期要求。

三、工程质量要求

(一)乙方建设工程应同时满足:1.符合国家法律法规和规范性文件对工程的质量要求;2.符合甲方磋商(谈判)文件对工程的质量要求;3.符合乙方在响应文件中或磋商、谈判过程中对工程质量作出的书面承诺、声明或保证。上述工程质量要求作为甲方对乙方工程质量的验收依据

(二)乙方应根据国家法律法规和规范性文件的规定、磋商(谈判)文件的相关要求、响应文件及乙方承诺、声明或保证,向甲方提供相应的工程质量满足要求的证明文件。

四、对工程验收的约定

(一)甲乙双方对工程建设过程中的各阶段验收、总验收及乙方提供的材料设备验收的条件和时间约定如下:

_____。

注:根据项目具体情况填写。

(二)如乙方未通过甲方组织的各阶段验收,甲方有权要求乙方在限定期限内整改,如整改不合格,甲方有权追究乙方违约责任,解除合同并要求乙方赔偿经济损失。

五、合同金额

在乙方提供完全符合合同要求的工程、材料、设施设备、服务的前提下,本合同总金额为_____元(小写)_____ (大写)。

六、付款时间及条件

(一)付款时间:_____

(二)付款条件:_____

(三)乙方账户信息

乙方名称:_____

开户银行：_____

银行账号：_____

七、甲方对乙方工程的监督

甲方及甲方委派的代表有权对乙方工程、材料及设施设备、服务等质量及管理进行监督，当乙方工程质量、材料及设施设备、服务内容不符合约定时，甲方及授权代表有权要求乙方及时整改，对乙方拒不改正或整改不到位的，甲方有权随时解除合同，并根据具体情况扣除部分或全部工程费用。

八、质量保证及售后服务

磋商（谈判）文件对工程质量保证期、材料设施设备质保期和售后、服务质量作出明确要求的，适用磋商（谈判）文件对工程质量保证期及材料设施设备质保期和售后、服务质量的规定，如乙方在响应文件及磋商（谈判）过程中对工程质量保证期及设施设备质保期和售后、服务质量作出更优的承诺、声明或保证的，适用乙方的承诺、声明或保证。

九、违约条款

（一）甲方没有正当理由逾期支付合同款项的，每延期一日，甲方应按照逾期支付金额_____的_____承担违约责任。延期达到_____日，乙方有权解除合同，并要求甲方赔偿由此造成的经济损失。

（二）甲方存在其他违反本合同的行为，应承担相应的违约责任（注：可以根据情况进行细化）；违约金不足以赔偿乙方损失的，乙方有权要求甲方赔偿由此造成的经济损失。

（三）乙方逾期交付工程的，每延期一日，乙方应按照合同总金额的_____承担违约责任。延期达到_____日，甲方有权解除合同，拒付延期部分的相应工程款，并要求乙方赔偿甲方经济损失。

（四）乙方交付的工程及设施设备、服务质量不符合质量规定或乙方未履行相应的工程质量保证期及设施设备质保期和售后、服务义务的，甲方有权拒付相应的工程款，并要求乙方支付合同总金额_____%的违约金。违约金不足以赔偿损失的，甲方有权要求乙方赔偿经济损失。

（五）乙方在参与本项目采购活动过程中，如存在提供虚假承诺、证明、串通投标等违法违规行为，除承担相应的行政责任外，甲方有权解除合同，并要求乙方承担合同总金额_____%的违约金，违约金不足以赔偿甲方损失的，甲方有权要求乙方赔偿经济损失。

（六）乙方存在其他违反本合同的行为，应承担相应的违约责任（可以根据情况进行细化）；违约金不足以赔偿甲方损失的，甲方有权要求乙方赔偿经济损失。

十、不可抗力条款

因不可抗力致使一方不能及时或完全履行合同的，应及时通知另一方，双方互不承担责任，并在_____天内提供有关不可抗力相关证明。合同未履行部分是否继续履行、如何履行等问题，由双方协商解决。

十一、争议的解决方式

合同发生纠纷时，双方应协商解决，协商不成，可以采用下列方式_____解决：

（一）提交_____仲裁委员会仲裁。

（二）向_____人民法院起诉。

十二、合同保存

合同文本一式_____份，采购单位、中标（成交）供应商、采购代理机构、_____各执一份。合同文本保存期限为从采购结束之日起至少保存十五年。

十三、合同附件

本合同所附下列文件是构成本合同不可分割的部分，与本合同具有同等法律效力：

- 1.工程清单（双方应盖章确认）
- 2.乙方出具的报价单（函）
- 3.成交结果公告及成交通知书
- 4.甲方磋商（谈判）文件

5.乙方响应文件

6.甲乙双方商定的其他文件

十四、双方约定的其他事宜

_____。

十五、本合同未尽事宜，双方另行签订补充协议，补充协议是合同的组成部分。

十六、本合同由甲乙双方盖章生效。

甲方名称：（章）

甲方法定代表人或负责人：（签字）

年 月 日

乙方名称：（章）

乙方法定代表人或负责人：（签字）

年 月 日

二.验收

严格按照采购合同开展履约验收。采购人或者采购代理机构应当成立验收小组，按照采购合同的约定对投标人履约情况进行验收。验收时，应当按照采购合同的约定对每一项技术、服务、安全标准的履约情况进行确认。验收结束后，应当出具验收书（参考格式附后），列明各项标准的验收情况及项目总体评价，由验收双方共同签署。验收结果应当与采购合同约定的资金支付及履约保证金返还条件挂钩。履约验收的各项资料应当存档备查。

政府采购货物履约验收书

（参考格式）

项目名称	
项目编号	
采购人	
使用人	
供应商	
验收依据	<p>1.政府采购合同（合同名称及编号）</p> <p>2.中标（成交）公告或中标（成交）通知书</p> <p>3.招标（磋商、谈判）文件或询价通知书</p> <p>4.投标（响应）文件</p> <p>5.供应商的承诺、声明或保证（如有）</p> <p>注：验收依据可根据项目具体情况适当增加</p>
供应商对履约情况的总结及提供的相关证明材料	<p>注：供应商根据采购合同的约定，对履约情况（包括但不限于采购合同中约定的货物数量、货物规格型号、生产厂家、交货时间、交货地点、验收情况、货物质量、售后服务等）进行总结，并提供相应的履约证明材料作为附件。</p>
采购人（使用人）对履约情况的确认	<p>注：采购人或使用人根据采购合同约定，对供应商履约情况进行逐一确认。</p>
验收人员名单及组成	<p>1. 采购人代表：</p> <p>2. 采购代理机构代表：</p> <p>3. 第三方专业机构代表及专家：</p> <p>4. 其他供应商代表：</p>
验收评价及结论	<p>评价：</p> <p>结论：<input type="checkbox"/>通过 <input type="checkbox"/>不通过，具体说明：</p>
验收人员签字	年 月 日
采购人确认意见（注：采购人委托代理机构验收时适用）	<p><input type="checkbox"/>同意验收结论。</p> <p><input type="checkbox"/>不同意验收结论。具体说明：</p> <p>年 月 日</p>
备注	

采购人代表签字：

年 月 日

供应商代表签字：

年 月 日

政府采购服务履约验收书

(参考格式)

项目名称	
项目编号	
采购人	
使用人	
供应商	
验收依据	<p>1.政府采购合同（合同名称及编号）</p> <p>2.中标（成交）公告或中标（成交）通知书</p> <p>3.招标（磋商、谈判）文件或询价通知书</p> <p>4.投标（响应）文件</p> <p>5.供应商的承诺、声明或保证（如有）</p> <p>注：验收依据可根据项目具体情况适当增加</p>
供应商对履约情况的总结及提供的相关证明材料	<p>注：供应商根据采购合同的约定，对履约情况（包括但不限于采购合同中约定的服务内容、服务要求、服务质量、人员配置、服务成果、服务成果的交付等）进行总结，并提供相应的履约证明材料作为附件。</p>
采购人（使用人）对履约情况的确认	<p>注：采购人或使用人根据采购合同约定，对供应商履约情况进行逐一确认。</p>
验收人员名单及组成	<p>1. 采购人代表：</p> <p>2. 采购代理机构代表：</p> <p>3. 第三方专业机构代表及专家：</p> <p>4. 其他供应商代表：</p>
验收评价及结论	<p>评价：</p> <p>结论：<input type="checkbox"/>通过 <input type="checkbox"/>不通过，具体说明：</p>
验收人员签字	年 月 日
采购人确认意见（注：采购人委托代理机构验收时适用）	<p><input type="checkbox"/>同意验收结论。</p> <p><input type="checkbox"/>不同意验收结论。具体说明：</p> <p>年 月 日</p>
备注	

采购人代表签字：

年 月 日

供应商代表签字：

年 月 日

政府采购工程履约验收书

(参考格式)

项目名称	
项目编号	
采购人	
使用人	
供应商	
验收依据	1.政府采购合同（合同名称及编号） 2.成交公告及成交通知书 3.磋商、谈判文件 4.响应文件 5.供应商的承诺及保证（如有） 6.国家关于工程建设的相关法律法规及规范性文件 注：验收依据可根据项目具体情况适当增加
供应商对履约情况的总结及提供的相关证明材料	注：供应商根据采购合同的约定，对履约情况（包括但不限于采购合同中约定的工程内容、工程质量、工程进度、工程各阶段验收、安全管理、材料及设施设备等进行总结，并提供相应的履约证明材料作为附件。
采购人（使用人）对履约情况的确认	注：采购人或使用人根据采购合同约定，对供应商履约情况进行逐一确认。
验收人员名单及组成	1. 采购人代表： 2. 采购代理机构代表： 3. 第三方专业机构代表及专家： 4. 其他供应商代表：
验收评价及结论	评价： 结论： <input type="checkbox"/> 通过 <input type="checkbox"/> 不通过，具体说明：
验收人员签字	年 月 日
采购人确认意见（注：采购人委托代理机构验收时适用）	<input type="checkbox"/> 同意验收结论。 <input type="checkbox"/> 不同意验收结论。具体说明： 年 月 日
备注	

采购人代表签字：

年 月 日

供应商代表签字：

年 月 日

第七章 响应文件格式与要求

采购包1:

通用分册:

详见附件: 封面

详见附件: 目录

资格符合分册:

详见附件: 缴纳投标保证金证明材料

详见附件: 投标人(供应商)应提交的相关证明

详见附件: 法定代表人授权委托书

详见附件: 参加政府采购活动前三年内在经营活动中没有重大违法记录的书面声明

详见附件: 依法缴纳税收和社会保障资金的良好记录的相关材料

详见附件: 具有良好的商业信誉和健全的财务会计制度的相关材料

详见附件: 具备履行合同所必需设备和专业技术能力的声明函

详见附件: 投标人基本情况表

详见附件: 联合体协议

详见附件: 投标人承诺函

详见附件: 中小企业声明函

详见附件: 具有独立承担民事责任的能力证明文件

详见附件: 监狱企业证明文件

详见附件: 残疾人福利性单位声明函

技术商务分册:

详见附件: 技术偏离表

详见附件: 投标人业绩情况表

详见附件: 项目组成人员一览表

详见附件: 项目实施方案、质量保证及售后服务承诺

详见附件: 主要商务要求承诺书

详见附件: 其他材料

报价分册:

详见附件: 分项报价表

详见附件: 开标一览表