

内蒙古自治区电子政务外网安全监测平台（一期）服务和网络安全检查服务
项目

公开招标文件

采购单位名称：内蒙古自治区大数据中心

采购代理机构名称：内蒙古嘉云诚招标代理有限公司

项目编号：**NMGZCS-G-F-250832**

2025年11月

目录

第一章 投标邀请

第二章 投标人须知

第三章 招标内容与技术要求

第四章 投标人应当提交的资格、资信证明文件

第五章 评标

第六章 合同与验收

第七章 投标文件格式与要求

第一章 投标邀请

内蒙古嘉云诚招标代理有限公司受 内蒙古自治区大数据中心 委托，采用公开招标方式组织采购 内蒙古自治区电子政务外网安全监测平台（一期）服务和网络安全检查服务项目 。欢迎符合资格条件的投标人参加投标。

一.项目概述

1.名称与编号

项目名称： 内蒙古自治区电子政务外网安全监测平台（一期）服务和网络安全检查服务项目

项目编号： **NMGZCS-G-F-250832**

采购计划备案号： 内政采计划[2025]32350

2.内容及划分采购包情况

采购包1：

采购包预算金额（元）：**7,440,000.00**

采购包最高限价（元）：**7,440,000.00**

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 | 内蒙古自治区电子政务外网安全监测平台（一期）服务 | 1.000 | 7,440,000.00 | 项 | 软件和信息技术服务业 | 否 | 否 | 否 | 否 |

采购包2：

采购包预算金额（元）：**666,700.00**

采购包最高限价（元）：**666,700.00**

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 | 网络安全检查服务 | 1.000 | 666,700.00 | 项 | 软件和信息技术服务业 | 否 | 否 | 否 | 否 |

二.投标人的资格要求

1.投标人应符合《中华人民共和国政府采购法》第二十二条规定的条件。

2.开标后资格审查时，投标人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

采购包2:

无

三.获取招标文件的时间、地点、方式

详见招标公告

其他要求:

无

四.招标文件售价

本次招标文件的售价为0元人民币。

五.提交投标文件截止时间、开标时间和地点

详见招标公告

六.联系方式

采购代理机构名称: 内蒙古嘉云诚招标代理有限公司

地址: 呼和浩特市赛罕区惠民街旺第嘉华27号楼1308室(赛罕区公安局十字路口西南角, 高德地图可直接搜索内蒙古嘉云诚招标代理有限公司)

邮编: 010020

联系人: 娜梅 于英 王子宜 齐淑贤 王大勇

联系电话: 0471-3289401

采购单位名称: 内蒙古自治区大数据中心

地址: 呼和浩特市赛罕区敕勒川大街6号

邮编: 010055

联系人: 纳青

联系电话: 0471-4827836

第二章 投标人须知

一.前附表

| 序号 | 条款名称 | 内容及要求 |
|----|------------------------|--|
| 1 | 划分采购包情况 | 共 2 包 |
| 2 | 采购方式 | 公开招标 |
| 3 | 开标方式 | 远程开标 |
| 4 | 评标方式 | 现场网上评标 |
| 5 | 评标方法 | 采购包1：综合评分法 采购包2：综合评分法 |
| 6 | 获取招标文件时间 | 详见招标公告 |
| 7 | 保证金缴纳截止时间（同投标文件提交截止时间） | 详见招标公告 |
| 8 | 电子投标文件递交 | 加密的电子投标文件1份，电子投标文件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。技术支持电话：400-0471-010转2键 |
| 9 | 投标文件数量 | （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”） （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。 （3）纸质投标文件（正本）0份；纸质投标文件（副本）0份。 |
| 10 | 中标人确定 | 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 | 联合体投标 | 采购包1：不接受 采购包2：不接受 |
| 12 | 采购代理机构代理费用 | 本项目收取代理服务费 代理服务费用收取对象：中标/成交供应商 代理服务费收费标准：具体收费比例按中标金额的1.5%收取（如不足一万则按一万收取） |
| 14 | 投标保证金 | 不收取保证金 |
| 15 | 电子投标文件签字、盖章要求 | 应按照第七章“投标文件格式与要求”，使用单位电子签章（CA）进行签字、加盖公章。 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投标文件。 |

| | | |
|----|----------|--|
| 17 | 投标客户端 | 投标客户端需要投标人登录“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-neimenggu.gov.cn/gp-auth-center/login?systemRegion=150001&systemRegion=150001 |
| 18 | 面向中小企业采购 | 采购包1：不属于专门面向中小企业采购。 采购包2： 属于专门面向中小企业采购，预留比例为100%。 |
| 19 | 有效投标人家数 | 采购包1：3家 采购包2：3家 |
| 20 | 中标供应商数量 | 采购包1：1名 采购包2：1名 |
| 21 | 中标候选人数量 | 采购包1：3名 采购包2：3名 |
| 22 | 报价形式 | 详见第一章，“内容及划分采购包情况”。 |
| 23 | 现场踏勘 | 采购包1：组织现场踏勘：否 采购包2：组织现场踏勘：否 |
| 24 | 兼投不兼中规则 | 本项目兼投不兼中，每个投标人最多只能被确定为1个子包的第一中标候选人。本项目按子包的顺序进行评审，依次按照评标总得分由高到低的顺序，推荐中标候选人。已获得子包一的第一中标候选人资格的，将不具有子包二的候选人推荐资格；子包二从具有中标候选人资格的投标人中，排名最高的投标供应商为第一中标候选人，排名次高的投标供应商为第二中标候选人，以此类推。 |
| 25 | 投标有效期 | 从提交投标（响应）文件的截止之日起 90 日历天 |
| 26 | 其他 | 一、供应商提供《中小企业声明函》的，按照招标文件规定的格式规范填写《声明函》。特别注意（不限于）以下几点：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。2、供应商依据“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）”确定中小企业划型。 |

二.投标须知

1.投标方式采用网上投标，流程如下：

投标人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，才可进行网上投标操作，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。

-投标人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投标的项目，点击项目的“未参与项目”按钮，进入项目投标信息页面，在右侧选择要投标的采购包，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，获取所投项目招标文件，并按照招标文件的要求制作、上传电子投标文件。

2.投标保证金

2.1投标保证金缴纳（如需缴纳保证金）

本采购项目支持“电子保函”和“虚拟子账户”两种方式收取投标保证金，同时允许投标人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 投标人选择“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，投标人需要确保在开标之前完成电子保函的开具。

2.1.2 投标人选择“虚拟子账户”方式缴纳保证金的，在进行投标信息确认后，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，并在开标时间前，缴纳至上述账号中。付款人名称必须为投标单位全称，且与其投标信息一致。

若出现账号缴纳不一致、缴纳金额与投标人须知前附表规定的金额不一致或缴纳时间超过开标时间，将导致保证金缴纳失败。投标人应认真核对账户信息，将投标保证金足额汇入以上账户，并自行承担因汇错投标保证金而产生的一切后果。投标人在转账或电汇的凭证上应按照“项目编号：***、采购包：***的投标保证金”格式注明，以便核对。

2.1.3 投标人选择以支票、汇票、本票、保函等非现金形式缴纳保证金的，投标人将相关证明材料原件扫描添加至投标文件中，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，由于投标保证金到账需要一定时间，请投标人在投标截止前及早缴纳。

2.2 投标保证金的退还

投标人在投标截止时间前放弃投标的，自所投采购包结果公告发出后5个工作日内退还，但因投标人自身原因导致无法及时退还的除外。

未中标人投标保证金，自中标通知书发出之日起5个工作日内退还；中标人投标保证金，自政府采购合同签订之日起5个工作日内退还。

2.3 有下列情形之一的，投标保证金将不予退还：

- (1) 中标后，无正当理由放弃中标资格的；
- (2) 中标后，无正当理由不与采购人签订合同的；
- (3) 在签订合同时，向采购人提出附加条件的；
- (4) 不按照招标文件要求提交履约保证金的；
- (5) 在签订合同时，投标人要求修改、补充和撤销投标文件的实质性内容的；
- (6) 投标文件中提供虚假材料的；
- (7) 与采购人、其他投标人或者采购代理机构恶意串通的；
- (8) 投标人在提交投标文件截止时间后，撤回投标文件的；
- (9) 法律法规和招标文件规定的其他情形。

3. 全流程电子化交易

各投标人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。

各投标人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。投标人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。

各投标人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（投标人无需到现场）

投标人使用“投标客户端”编制、签章、生成加密投标文件，同时生成“备用标书”，投标人自行留存，涉及“加盖公章”的内容应使用单位电子公章完成。

投标人的法定代表人或其授权代表应当按照本项目招标公告载明的时间等要求参加开标，在开标时间前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。

开标时，投标人应当使用CA证书在开始解密后30分钟内完成全部已投标采购包的投标文件在线解密，若出现系统异常情

况，工作人员可适当延长解密时长。如在开标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投标人导入“备用标书”继续开标。本项目采用电子评标，只对开标环节验证通过的电子投标文件进行评审。投标人在参加开标以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。

开标时出现下列情况的，采购人、采购代理机构应当视为投标人不再参与政府采购活动。

- (1) 投标人未在规定时间内完成电子投标文件在线解密的；
- (2) CA证书无法解密投标文件的；
- (3) 投标人自身原因造成电子投标文件未能解密的。

3.2现场网上方式（投标人需到现场）

投标人使用“投标客户端”编制、签章、生成加密投标文件，同时生成“备用标书”，由投标人自行刻录、存储，涉及“加盖公章”的内容应使用单位电子公章完成。投标人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、投标单位名称等信息。

投标人的法定代表人或其授权代表应当按照本项目招标公告载明的时间和地点参加开标。开标时，投标人应当使用CA证书完成全部已投标采购包的投标文件在线解密。如在开标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投标人导入“备用标书”继续进行。本项目采用电子评标，只对开标环节验证通过的电子投标文件进行评审。

开标时出现下列情况的，采购人、采购代理机构应当视为投标人不再参与政府采购活动。

- (1) CA证书无法解密投标文件的；
- (2) 投标人未按招标文件要求提供“备用标书”的；
- (3) 投标人自身原因造成电子投标文件未能解密的。

4.投标人可以通过“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

本招标文件依据《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《政府采购货物和服务招标投标管理办法》（财政部令第87号）及国家和自治区有关法律、法规、规章制度编制。

投标人应仔细阅读本项目信息公告及招标文件的所有内容（包括澄清或者修改），按照招标文件要求以及格式编制投标文件，并保证其真实性，否则一切后果自负。

本次公开招标项目，是以招标公告的方式邀请非特定的投标人参加投标。

2.适用范围

本招标文件仅适用于本次招标公告中所涉及的项目和内容。

3.相关费用

投标人应自行承担所有与准备、参加投标有关的费用。不论投标结果如何，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。本招标文件的采购人特指内蒙古自治区大数据中心。

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。本招标文件的采购代理机构特指内蒙古嘉云诚招标代理有限公司。

4.3“投标人”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“评标委员会”由采购人代表和评审专家组成。

4.5“中标人”是指取得与采购人签订合同资格的投标人。

5.合格的投标人

5.1符合本招标文件规定的资格要求，并按照要求提供相关证明材料。

5.2单位负责人为同一人或者存在直接控股、管理关系的不同投标人，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、检测等服务的投标人，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，并作为投标文件组成部分。

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，并在投标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投标人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投标人确定资质等级。

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投标人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，就采购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.现场踏勘

8.1招标文件规定组织踏勘现场的，采购人或者采购代理机构按招标文件规定的时间、地点组织潜在投标人踏勘项目现场。

8.2投标人自行承担踏勘现场发生的责任、风险和自身费用。

8.3采购人在踏勘现场中介绍的资料和数据等，不构成对招标文件的修改或不作为投标人编制投标文件的依据。

9.其他条款

无论中标与否，投标人递交的投标文件均不予退还。

四.招标文件的澄清或者修改

采购人或采购代理机构对已发出的招标文件进行必要的澄清或修改的，澄清或者修改的内容可能影响投标文件编制的，采购人或者采购代理机构应当在投标截止时间至少**15**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**15**日的，采购人或者采购代理机构应当顺延提交投标文件截止时间，更正公告的内容为招标文件的组成部分，投标人应自行上网查询，采购人或采购代理机构不承担投标人未及时关注相关信息的责任。

五.投标文件

1.投标文件的构成

投标文件应按照招标文件第七章“投标文件格式与要求”进行编写，可以增加附页，并作为投标文件的组成部分。

2.投标报价

2.1投标人应按照第三章“招标内容与技术要求”进行报价。投标总价中不得包含招标文件要求以外的内容，否则，在评审时不予核减。

2.2投标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 投标报价不得有选择性报价和附加条件的报价。

2.4 投标文件报价出现前后不一致的，按下列规定修正：

- (1) 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；
- (2) 大写金额和小写金额不一致的，以大写金额为准；
- (3) 单价金额小数点或者百分比有明显错位的，以开标一览表（报价表）的总价为准，并修改单价。
- (4) 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。

修正后的报价投标人应当采用书面形式，并加盖公章，或者由法定代表人或其授权的代表签字确认后产生约束力，但不得超出投标文件的范围或者改变投标文件的实质性内容，投标人不确认的，其投标无效。

2.5 投标人应在“投标客户端”对【报价部分】进行填写，“投标客户端”软件将自动根据投标人填写信息生成“开标一览表（报价表）”、“分项报价表”，若在响应文件中出现非系统生成的“开标一览表（报价表）”、“分项报价表”，且与“投标客户端”生成的“开标一览表（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. 投标有效期

3.1 投标有效期从提交投标文件的截止之日起算。投标文件中承诺的投标有效期应当不少于招标文件中载明的投标有效期。

3.2 出现特殊情况需要延长投标有效期的，采购人以书面形式通知所有投标人延长投标有效期。同意延长投标有效期的投标人少于3个的，招标人应当重新招标。投标人同意延长的，应相应延长其投标保证金的有效期，但不得要求或被允许修改或撤销其投标文件；投标人拒绝延长的，其投标失效，但投标人有权收回其投标保证金。

4. 投标文件的递交

投标人应当在投标截止时间前递交投标文件，否则视为自动放弃投标。

5. 投标文件的修改和撤回

投标人在投标截止时间前，可以对所递交的投标文件进行补充、修改或者撤回。投标人应当在投标截止时间前上传加密的最终版电子投标文件至“内蒙古自治区政府采购网-政府采购云平台”。

在提交投标截止时间后，投标人不得补充、修改、替代或者撤回其投标文件。

6. 样品

采购人、采购代理机构一般不得要求投标人提供样品，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。

6.1 招标文件规定投标人提交样品的，样品属于投标文件的组成部分。样品的生产、运输、安装、保全等一切费用由投标人自理。

6.2 开标前，投标人应将样品送达至指定地点，并按要求摆放并做好展示。若需要现场演示的，投标人应提前做好演示准备（包括演示设备）。

6.3 采购活动结束后，对于未中标投标人提供的样品，应当及时退还或者经未中标投标人同意后自行处理；对于中标投标人提供的样品，应当按照招标文件的规定进行保管、封存，并作为履约验收的参考。

六. 开标、评标、中标公告、中标通知书

1. 开标

1.1 程序

- (1) 宣布纪律；
- (2) 宣布相关人员；
- (3) 投标人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投标人名称、投标价格和招标文件规定需要宣布的其他内容（以开标一览表要求为准）；
- (4) 参加人员对开标结果进行确认；

(5) 开标结束。

1.2 疑义

投标人代表对开标过程和开标记录有疑义，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、采购代理机构对投标人代表提出的询问或者回避申请应当及时处理。

投标人对远程不见面方式过程和开标记录有疑义，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 备注说明

1.3.1 投标人不足3家的，不得开标。

1.3.2 开标时,投标人使用CA证书参与投标文件解密，投标人用于解密的CA证书应为生成、加密、上传投标文件的同一CA证书。

2. 资格审查

2.1 公开招标采购项目开标结束后，采购人或者采购代理机构应当依法对投标人的资格进行审查，以确定投标人是否具备投标资格。

2.2 资格审查中有任意一项未通过的，审查结果为未通过，未通过资格审查的投标人按无效投标处理。

2.3 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；采购人或采购代理机构应当按照查询渠道、查询时间节点、查询记录内容查询，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投标人作无效投标处理。

资格审查表

一般资格要求

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 | 审查投标人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 | 审查投标人提供的具有良好的商业信誉和健全的财务会计制度的相关材料。 |
| 3 | 有依法缴纳税收和社会保障资金的良好记录 | 审查投标人提供的依法缴纳税收和社会保障资金的相关材料。 |
| 4 | 具有履行合同所必需的设备和专业技术能力 | 审查投标人提供的具有履行合同所必需的设备和专业技术能力的证明材料。 |
| 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 | 审查投标人参加本次投标活动前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 | 开标结束后资格审查时，投标人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 | 联合体投标（若有） | 符合关于联合体投标的相关规定。 |

采购包2:

| 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 | 审查投标人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 | 审查投标人提供的具有良好的商业信誉和健全的财务会计制度的相关材料。 |
| 3 | 有依法缴纳税收和社会保障资金的良好记录 | 审查投标人提供的依法缴纳税收和社会保障资金的相关材料。 |
| 4 | 具有履行合同所必需的设备和专业技术能力 | 审查投标人提供的具有履行合同所必需的设备和专业技术能力的证明材料。 |
| 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 | 审查投标人参加本次投标活动前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 | 开标结束后资格审查时，投标人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 | 联合体投标（若有） | 符合关于联合体投标的相关规定。 |

特定资格要求

采购包1：

| | |
|----------|---------|
| 资格审查要求概况 | 评审点具体描述 |
|----------|---------|

采购包2：

| | |
|----------|---------|
| 资格审查要求概况 | 评审点具体描述 |
|----------|---------|

落实政府采购政策的资格要求

采购包1：

| | |
|----------|---------|
| 资格审查要求概况 | 评审点具体描述 |
|----------|---------|

采购包2：

| | |
|-------------------|--|
| 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中小企业采购。 | 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。） |

3.评标

详见第五章

4.中标公告

中标人确定后，采购代理机构在内蒙古自治区政府采购网上发布中标结果公告，同时将中标结果以公告形式通知未中标的投标人，中标结果公告期为1个工作日。

5.中标通知书

发布中标结果的同时，中标人可自行登录“内蒙古自治区政府采购网--政府采购云平台”打印中标通知书，中标通知书是合同的组成部分，中标通知书对采购人和中标人具有同等法律效力。

中标通知书发出后，采购人不得违法改变中标结果，中标人无正当理由不得放弃中标。

七.询问、质疑与投诉

1.询问

投标人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。投标人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 投标人认为招标文件、采购过程、中标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。

投标人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。提出质疑的投标人应当是参与所质疑项目采购活动的投标人。

潜在投标人已依法获取其可质疑的招标文件的，可以对该文件提出质疑。对招标文件提出质疑的，应当在获取招标文件或者招标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投标人的书面质疑后7个工作日内作出答复，并以书面形式通知质疑投标人和其他有关投标人，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中标结果的，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 投标人提出质疑应当提交质疑函和必要的证明材料。质疑函应当包括下列内容：

- （一）投标人的姓名或者名称、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。

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

投标人可以委托代理人进行质疑，代理人提出质疑时应当提交投标人签署的授权委托书。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 投标人提交的质疑函，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 投标邀请）。

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。

投标人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投标人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 招标内容与技术要求

一.项目概况

采购包1：为贯彻落实《关于加快推进全国政务外网安全监测平台建设工作的通知》（政务外网[2020]1号）文件要求，内蒙古自治区政务外网安全监测平台将对所辖重点网络区域进行安全监测，监测范围覆盖广域网、城域网、局域网和互联网出口、政务云等骨干网络 and 核心应用，具备数据采集、数据分析态势展现和预警通告等核心功能，形成全网监测预警、信息共享和应急联动能力，不断提升政务外网安全保障水平，为自治区数字政府行动计划、数字经济产业发展提供安全保障。按照国家相关规范和标准，自治区安全监测平台实现与国家平台、盟市系统，以及自治区相关部门的安全平台进行对接，实现安全事件、漏洞风险、威胁情报和事件处置等信息共享，形成全网综合态势，准确把握网络安全风险发生的规律、动向和趋势，建立统一高效的安全风险报告机制和情报共享机制，建立跨地区跨层级的安全监测协同联动，逐步形成覆盖全网、整体联动、协调规范的政务外网安全监测运行服务体系，保障自治区电子政务外网、政务云持续稳定运行。

采购包2：自治区大数据中心负责自治区本级政府信息系统运维工作，承担自治区本级政府系统政府信息化网络与数据安全保障工作。在中心内部开展网络安全检查是一项重点工作，具有十分重要的现实意义。落实《党委（党组）网络安全工作责任制实施办法》《内蒙古自治区大数据中心网络安全工作责任制实施细则》开展网络安全检查，及时发现问题及时整改问题，感知网络安全态势，掌握中心网络安全现状。对相关处信息系统资产进行安全检查，发现安全风险、弱点和不完美的策略设置，通过系统管理合规性检查、资产梳理识别服务、安全漏洞扫描服务、渗透测试服务、数据安全风险检查、移动端APP/小程序安全检测、安全基线配置核查、APT风险检查、高危问题复测检查等，发现的安全风险和漏洞下发安全风险通报，跟进通报的风险处置情况，落实整改，形成风险处置闭环。根据发现的安全漏洞和风险进行整改加固及策略调优，完善安全防护措施。实施范围对自治区大数据中心负责运维的系统进行检查，检查系统的数量不少于60个。

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 | 合同签订后60日内具备基础监测服务能力，同时完成网络设备扩容和部署且 具备服务能力（除不具备对接条件的第三方平台或设备在具备条件后再进行对 接外），服务期从2026年2月16日到2027年2月15日。 |
| 2 | | 标的提供地点 | 采购人要求的地点 |
| 3 | | 合同履约期限 | 2026年2月16日到2027年2月15日。 |
| 4 | | 合同履约地点 | 采购人要求的地点 |
| 5 | | 验收要求 | 1期：自治区电子政务外网安全监测服务的验收,包括但不限于如下要求: (1)中标人完成项目实施并测试后,编制《项目竣工文件》。竣工文件应满足完整性、一致性和可读性等要求。(2)中标人应负责在项目验收前将全部有关产品说明书、原厂家安装手册、技术文件、资料、以及安装、测试、验收报 告等文档汇集册交付采购人。(3)验收方案由采购人最终确定,在验收时中标人准备验收测试用设备、工具、资料、人员等,采购人组织召开专家验收会议,开展相关验收工作。(4)项目验收合格后,正式开始网络安全运营服务。 |

| | | | |
|---|--|--------|--|
| 6 | | 合同支付方式 | <p>1、合同签订后，具备基础监测服务能力，同时完成网络设备扩容和部署且具备服务能力后，中标人向采购人开具合同金额30%的发票，采购人收到发票后，支付合同总额30%，达到付款条件起30日，支付合同总金额的30.00%</p> <p>2、在服务期内，服务满六个月后，根据第三方绩效评价结果达到考核标准后，中标人向采购人开具合同金额30%的发票，采购人收到发票后，支付合同总额30%，达到付款条件起30日，支付合同总金额的30.00%</p> <p>3、在服务期内，服务满十个月后，根据第三方绩效评价结果达到考核标准后，中标人向采购人开具合同金额20%的发票，采购人收到发票后，支付合同总额20%，达到付款条件起30日，支付合同总金额的20.00%</p> <p>4、在服务期满后，根据第三方绩效评价结果达到考核标准后，中标人向采购人开具合同金额20%的发票，采购人收到发票后，支付合同总额20%，达到付款条件起30日，支付合同总金额的20.00%</p> |
| 7 | | 履约保证金 | 需要缴纳履约保证金：不缴纳 |

采购包2:

| 序号 | 参数性质 | 类型 | 要求 |
|----|------|--------|--|
| 1 | | 标的提供时间 | 合同签订后一年（具体履行起始时间以合同签订为准） |
| 2 | | 标的提供地点 | 内蒙古自治区大数据中心 |
| 3 | | 合同履约期限 | 合同签订后一年（具体履行起始时间以合同签订为准） |
| 4 | | 合同履约地点 | 内蒙古自治区大数据中心 |
| 5 | | 验收要求 | <p>1期：验收标准：对12个部门的60个（不少于）系统进行安全检查并提供安全检查报告。交付标准：采购服务技术要求中的相关安全服务报告符合招标文件需求，并通过采购人组织的专家验收会交付方法：安全检查报告资料交付物为电子版和纸质版形式。</p> |
| 6 | | 合同支付方式 | <p>1、合同签订后，乙方向甲方开具合同金额40%的发票，甲方收到发票后，支付合同总额40%价款。，达到付款条件起30日，支付合同总金额的40.00%</p> <p>2、项目实施6个月后，乙方向甲方开具合同金额30%的发票，甲方收到发票后，支付合同总额30%价款。，达到付款条件起30日，支付合同总金额的30.00%</p> <p>3、项目验收合格后，乙方向甲方开具合同金额30%的发票，甲方收到发票后，支付合同总额30%价款。，达到付款条件起30日，支付合同总金额的30.00%</p> |
| 7 | | 履约保证金 | 需要缴纳履约保证金：不缴纳 |

| | | | |
|---|--|----|---|
| 8 | | 其他 | <p>知识产权归属、处理方式：投标方应在投标文件中承诺保证提供给招标方使用的货物及服务或其中的任何一部分，免受第三方提出的侵犯其知识产权的索赔或诉讼。如有任何上述指控，自行承担可能发生的一切法律责任和费用。同时，投标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。售后服务要求：提供及时、方便、有效的技术支持与售后服务，保证运维任务的顺利完成，实现各信息系统安全稳定运维，不出现重大安全事故。</p> <p>保险：招标人对保险无特定要求，若服务过程中发生任何事故，其责任由中标单位自行承担。</p> <p>保密：不得泄露用户业务数据、及设备登陆及配置信息等，供应商需签订保密协议，驻场人员需签订保密承诺书。</p> |
|---|--|----|---|

2.技术标准与要求

采购包1：

标的名称：内蒙古自治区电子政务外网安全监测平台（一期）服务

| 序号 | 参数性质 | 技术参数与性能指标 | | | | |
|---------|------|---|--------------------------|-------------|---------|----|
| | | 服务需求一览表 | | | | |
| | | 序号 | 项目名称 | 数量 | 项目内容与要求 | |
| | | 1 | 内蒙古自治区电子政务外网安全监测平台（一期）服务 | 1 | 详见后附内容 | |
| | | 备注： | | | | |
| | | 1、“服务产品和运营要求”中划“√”的表示此参数为重要技术参数，其余为一般性技术参数。投标技术参数负偏离的，评审时做不同程度扣分处理； | | | | |
| | | 2、除“服务产品和运营要求”在评审时做不同程度扣分处理外，本章的内容和要求必须全部满足； | | | | |
| | | 3.根据《中小企业划型标准规定》，本项目所属行业为“软件和信息技术服务业”。 | | | | |
| | | 供应商提供自治区电子政务外网安全监测服务，包括网络服务和安全监测服务，具体如下表所示： | | | | |
| | | 序号 | 服务项目 | 服务类型 | 数量 | 单位 |
| | | 1 | 网络服务 | 万兆网络接入服务 | 2 | 套 |
| | | | | 千兆网络接入服务 | 2 | 套 |
| | | | | 边界网络升级服务 | 72 | 套 |
| | | | | 核心网络升级服务 | 3 | 套 |
| | | 2 | 安全监测服务 | 流量采集服务(10G) | 16 | 套 |
| | | | | 流量采集服务(2G) | 4 | 套 |
| | | | | 日志采集服务 | 8 | 套 |
| | | | | 沙箱采集分析服务 | 8 | 套 |
| 云主机采集服务 | 4000 | | | 套 | | |
| 边界防护服务 | 2 | | | 套 | | |
| 行为管理服务 | 2 | | | 套 | | |

| | | |
|--|----------|----|
| | | |
| | 安全监测分析服务 | 5套 |
| | 攻击诱捕溯源服务 | 6套 |
| | 安全大数据服务 | 1套 |
| | 安全运营服务 | 1套 |

一、项目目标

为贯彻落实《关于加快推进全国政务外网安全监测平台建设工作的通知》（政务外网[2020]1号）文件要求，内蒙古自治区政务外网安全监测平台将对所辖重点网络区域进行安全监测，监测范围覆盖广域网、城域网、局域网和互联网出口、政务云等骨干网络和核心应用，具备数据采集、数据分析态势展现和预警通告等核心功能，形成全网监测预警、信息共享和应急联动能力，不断提升政务外网安全保障水平，为自治区数字政府行动计划、数字经济产业发展提供安全保障。

按照国家相关规范和标准，自治区安全监测平台实现与国家平台、盟市系统，以及自治区相关部门的安全平台进行对接，实现安全事件、漏洞风险、威胁情报和事件处置等信息共享，形成全网综合态势，准确把握网络安全风险发生的规律、动向和趋势，建立统一高效的安全风险报告机制和情报共享机制，建立跨地区跨层级的安全监测协同联动，逐步形成覆盖全网、整体联动、协调规范的政务外网安全监测运行服务体系，保障自治区电子政务外网、政务云持续稳定运行。

二、总体要求

1. 供应商提供服务的软硬件产品必须满足国家相关规范的要求，包括但不限于如下规范，如发布了最新的规范则按最新规范要求执行。

- 《信息安全技术网络安全监测基本要求与实施指南》(GB/ T 36635-2018)
- 《信息安全技术网络安全威胁信息格式规范》(GB/T 36643 -2018)
- 《国家电子政务外网安全监测体系技术规范与实施指南》(GW0203-2014)
- 《政务网络安全监测平台总体技术要求》(T/CIIA 005-2019)
- 《政务网络安全监测平台数据总线结构规范》(送审稿)

2. 供应商如果提供的相关软硬件不能满足功能和性能要求的，供应商必须按采购人要求增加软硬件或更换更高性能的产品。

3. 供应商必须确保数据安全，本次提供服务的软硬件产生的数据所有权归采购人所有，未经采购人授权同意所有数据不得查阅及做其他用途。

4. 本项目搭建的安全监测平台，采购人拥有永久使用权。

5. 本项目搭建的安全监测平台，需符合国密算法相关要求。

三、安全监测技术路线要求

需采用大数据技术、人工智能技术，加入协同联动接口，基于以全流量分析为核心，结合日志分析、威胁情报、用户和实体行为分析、失陷主机检测、图关联分析、机器学习、大数据关联分析等技术，在威胁分析、通报预警、响应处置、感知呈现、策略管理、溯源取证等方面发挥更大的作用，同时结合安全专家服务，实现安全监测的闭环管理。加强与国家、盟市和自治区相关安全部门的协同联动，最大限度提升电子政务外网安全监测智能化水平，保障网络的安全稳定运行。

四、安全监测功能要求

安全监测平台功能需求主要包括数据采集、数据分析、数据总线、展示与应用、预警通告、应急处置、威胁情报、平台运行与管理等功能。

1.数据采集

数据采集区域应覆盖：核心交换区、广域网、城域网、互联网出口等网络区域，以及政务云、托管业务区等。

数据采集内容主要包括如下：

（一）网络流量

（1）采集内容应包含常用的网络协议流量，类型包括HTTP、FTP、POP3、SMTP、DNS、SNMP、ARP等，支持对IPv4和IPv6的流量采集；

（2）对网络流量进行还原解析生成流量日志并进行采集，在发生信息安全事件时可基于流量日志进行事件回溯分析。

（二）日志

对IT设施的设备日志进行采集，包括网络设备日志、安全设备日志、主机日志、应用系统设备日志等日志类型。

（三）资产信息

对主机设备、网络设备、安全设备、应用系统设备等的资产信息进行采集。

（四）威胁情报

采集多种类型的威胁情报，包含域名类威胁情报、IP类威胁情报、文件类威胁情报、安全事件类威胁情报等类型。

（五）漏洞

对主机设备、网络设备、安全设备、应用系统设备等的漏洞信息进行采集。

（六）上下级平台交互数据

采集下级平台上报的数据，包括总体态势、告警统计、风险状况、案例、重大安全事件、报表等信息。

采集上级平台推送的数据，包括威胁情报、处置工单、案例、重大安全事件通告等信息。

2.数据分析

安全监测平台需要通过特征码匹配、关联分析、机器学习、用户与实体行为分析、威胁情报分析、数据挖掘等数据分析方法，实现对网络安全基础数据管理与挖掘分析，形成网络安全威胁的数据分析能力，提供多个维度可视化的大数据分析结果，为研判、决策、预警通报及指挥等工作提供有效支撑。

安全监测平台应提供多种态势分析：

综合态势分析：对网络的整体安全态势进行分析。

威胁态势分析：基于威胁的分析，包含对网络攻击行为和重要威胁情报的分析，包括网络扫描窃听、DDoS攻击、漏洞攻击、信息泄露、信息篡改、重要威胁情报信息等。

资产态势分析：针对网络中资产的漏洞和配置弱点进行分析。

3.数据总线

平台数据总线应参照国家相关数据标准和国家电子政务外网对接规范的要求进行建设。

数据总线主要由四部分组成：内部数据交换接口、数据采集接口、平台级联接口和外部接口。

内部数据交换接口：安全监测平台为平台内部模块之间数据的规范化交换而提供的标准接

口；

数据采集接口：安全监测平台从各种监测采集设备中收集处理后的数据进行规范化传输的接口；

平台级联接口：安全监测平台上下级平台之间进行总体态势、重大安全事件、威胁情报等数据交互的接口；

外部接口：安全监测平台通过各种外部接口与其他平台之间实现集成和数据交互。

4.展示与应用

（1）多维度展示

在态势展示页面应能够通过图形化的方式呈现各安全态势专题的情况，如GIS地图、柱状图、折线图、饼图、散点图、气泡图、雷达图、热力图、力导向图等。

（2）详细信息轨迹

在态势展示页面通过信息钻取查看安全事件的详情，可以多层钻取。

（3）自定义报表

可以基于预先定义的模板，实现各类报告数据的统计和展示，以及报表的结果输出。

（4）多种态势展示

可视化态势展示内容包括综合安全态势、攻击态势、威胁态势、资产态势等，分析结果以地图、饼图、柱图、报表等方式呈现。

5.预警通告

提供预警分级，将接收到的预警信息按照重要程度、影响范围等进行分级，进一步的预警处理。发生预警事件时，可以依照设定的流程发布信息通告。提供策略管理维护页面，协助安全分析人员进行规则和策略的开发和维护。

信息通告内容包括告警名称、告警时间、告警类型、告警级别、告警对象、所属部门、告警描述等，通告方式应支持平台告警、邮件告警、短信告警等方式。

6.应急处置

根据安全监测发现的网络攻击、重大安全隐患等情况以及相关部门通报的情况，下达网络安全事件快速处置指令，按照处置要求和规范进行事件处置。

需要将各类安全告警信息基于其安全告警等级、分级分类结果结合相应的处置策略形成处置任务，处置完成后需要进行记录和归档。

7.威胁情报

安全监测平台威胁情报应包含域名类威胁情报、IP类威胁情报、文件类威胁情报、安全事件类威胁情报等类型。

可以通过手动升级威胁情报方式，或者通过代理等安全可控方式在线更新。根据需要导入自身或者其它相关方提供的威胁情报，导入的威胁情报可以通过统一的API接口查询使用。

安全监测平台提供开放接口，以标准接口的方式来集成第三方威胁情报平台。威胁情报可以通过查询接口、邮件等方式和上级平台的威胁情报进行比对。

8.平台运行管理

（1）用户管理

具备分组的增加、删除、修改、查询及权限归属分组管理。用户管理包括用户整个生命周期的管理，对安全监测平台用户的创建、修改、删除和查询等功能。实现统一集中的用户管理，具备被管理角色的创建、编辑、删除等基本功能。

（2）数据存储

建立相应的流量数据、日志数据、告警数据、资产数据、威胁情报数据、漏洞数据、规则知识数据等数据库，能对结构化数据、半结构化数据和非结构化数据进行存储，支持文本、关键值、对象等多种数据类型的存储可伸缩的分布式数据存储架构，满足数据量持续增长需求。

（3）日志审计

用户对安全监测平台的使用等操作行为应有完整的日志记录，便于审计跟踪和分析。系统审计模块记录系统中发生的关键事件，审计内容包括用户操作审计和系统事件审计，审计操作包括审计查看、审计内容导出和审计内容统计等。

五、采集探针要求

本项目配置的采集探针包括流量探针(2G)、流量探针(10G)、日志探针、沙箱探针、软探针、蜜罐等，流量采集区域包括广域网、城域网、互联网出口、政务云等区域，采集内容包括：网络流量（HTTP、FTP、POP3、SMTP、DNS、SNMP、ARP及流量日志等）、日志（网络设备日志、安全设备日志、主机日志等）、资产信息（主机设备、网络设备、安全设备等）、威胁情报（域名类威胁情报、IP类威胁情报、文件类威胁情报、安全事件类威胁情报等）。

供应商应根据自治区电子政务外网的情况，采用最佳的采集探针部署方案，确保对三个不同地址的政务云中心所有重点区域完成数据采集，包括盟市政务外网接入区域、国家政务网对接区域、自治区城域网区域、核心交换区域、政务云业务区等。采购人可以根据政务外网各区域网络流量和资产变化情况，要求供应商调整采集探针的部署位置，以达到最佳的数据采集效果，供应商需按要求完成调整。

软探针部署在X86政务云和信创云主机上，具体部署数量按采购人约定执行，并可以根据X86政务云和信创云主机的变化，按照采购人要求，在X86云和信创云之间灵活调整软探针部署。

六、管理规范要求

按照内蒙古自治区电子政务外网安全监测平台整体架构进行编制，根据业务与管理需求制定相应的管理规范，使自治区电子政务外网安全服务更加规范化、科学化、系统化。管理规范编制如下表所示，由供应商组织完成编制，采购人可以根据实际需求增加或调整相关规范。

| 序号 | 规范名称 |
|----|-----------------------------|
| 1 | 内蒙古自治区电子政务外网安全监测平台总体框架规范 |
| 2 | 内蒙古自治区电子政务外网安全监测平台数据采集汇聚规范 |
| 3 | 内蒙古自治区电子政务外网安全监测平台数据对接与共享规范 |
| 4 | 内蒙古自治区电子政务外网安全监测平台运行管理规范 |
| 5 | 内蒙古自治区电子政务外网安全监测平台技术要求 |

七、监测平台要求

监测平台作为自治区电子政务外网的主要安全服务平台，必须按照《关于加快推进全国政务外网安全监测平台建设工作的通知》（政务外网[2020]1号）文件要求和采购人需求建设，并实现与国家平台、盟市系统以及自治区相关部门安全平台对接，提升电子政务外网安全监测预警、信息共享和应急联动处置能力。

监测平台具备基础监测，通报预警，响应处置、数据总线协同对接等以及相应的硬件支撑，实现对自治区电子政务外网数据采集、数据分析、展示与应用、平台运行管理、数据总线、

威胁情报共享等功能。

监测平台的主要功能包括但不限于如下，服务期内供应商需按照采购人要求进行功能优化调整。

（1）流量采集

流量采集子系统负责从内蒙古自治区政务外网各汇聚节点采集政务外网各重要出入口的原始流量数据，通过对采集数据的解析，提取各类用以支撑网络安全监测分析业务的数据，实现流量协议解析，流量文件还原，资产指纹采集、资产脆弱性识别等，为监测系统提供基础数据来源。

（2）资产与脆弱性识别

对内蒙古自治区政务外网关键基础设施互联网出入口、政务云边界，以及重点单位的流量分析和主动探测，形成电子政务外网资产列表，并通过网络和安全设备如防火墙、路由器、交换机等的ACL策略，建立资产互访权限关系。

（3）威胁监测与发现

将网络原始数据采用高速协议解码技术进行深度协议解析，再结合事件规则库，采用匹配技术将报文与特征规则进行匹配生成安全特征事件及相关原始报文数据，实现网络中的威胁监测与发现。

（4）异常行为分析

通过将内蒙古自治区政务外网关键基础设施，以及相关系统行为、业务行为与机器学习相结合，学习并构建日常网络行为模型，以客观对象的行为视角来主动发现异常网络行为，从海量的网络行为记录中挖掘、监测、分析潜在的安全风险数据，通过对全量流量、DNS 审计数据、HTTP 审计数据等，进行全流量分析，利用流行的UEBA技术、行为分析技术等建立各类流量模型，结合威胁情报库、IP地址库挖掘业务、主机访问异常等各种异常行为事件进行实时行为分析。

（5）用户管理

在自治区政务外网安全运营服务的日常管理实现多级账户权限控制，及针对角色的责任划分对应角色类型，分成外部专家组角色、管理员角色、涉事单位角色、涉事单位子账号角色等，具体可根据采购人的需要进行优化调整。

（6）资产管理

资产管理包括业务资产和未知资产，未知资产部分数据可以转移添加至相关单位，转化为该单位已知资产数据。资产管理需要实现应用系统、终端、业务系统责任人实名管理，资产归属单位管理，资产安全状态识别等。

（7）事件分析

实现自治区电子政务外网整体安全情况分析 & 异常情况告警，及时对数据进行事件分析及处置，以多种分析方式来覆盖分析全部数据，包括网络异常行为发现分析方式、流量异常智能发现方式、恶意代码分析方式等。

（8）威胁情报

面对新威胁能够及时进行威胁情报的预警、查验、加固，自治区安全监测平台的威胁情报数据来源于监测平台、对接的第三方威胁情报平台、人工录入等多方数据来源途径，并且支持通过平台、邮件、短信等多种方式发布威胁情报预警信息。

（9）通报预警消息发送

通报预警系统是通过智能事件关联分析，实时不间断地对所有日志、事件流进行分析，提

供丰富的可视化事件分析视图。同时，支持通过邮件、短信方式进行预警到事发单位、事发单位责任人和处置专家，持续提醒相关人员进行快速跟踪处置。

（10）全局指挥

通过安全监测平台提供的各项指标的统计和展示，包括首页展示、资产概览、隐患事件概览、安全应急事件概览、安全态势感知、访问非工作网站统计、抵御外部攻击统计、安全事件处置统计等，实现有效地全局指挥。安全监测平台可以分配独立的账号和权限，供相关人员随时登录平台查阅电子政务外网安全总体态势情况。

（11）应急响应管理

根据安全监测发现的网络攻击、重大安全隐患等情况以及相关部门通报的情况，下达网络安全事件快速处置指令，指令接收部门按照处置要求和规范进行事件处置，及时消除影响和危害，并及时建档、归档并入库。

（12）安全隐患处置

实现感知政务外网存在的安全风险隐患，及时进行隐患处置和隐患闭环管理。通过主动加被动的形式，结合脆弱性指纹信息，快速聚焦应用系统存在的脆弱性情况，包括漏洞、明文传输、弱密码、风险端口/应用等。

（13）协同处置

通过全流程的可视化安全事件应急指挥管理和工单流转，实现协同处置。工单流转机制包括隐患处理流程、应急事件处置流程等，实现初步处理、指派专家、安全处理、复核归档、总结归档等全流程协同处置。

（14）归档留存

通过工单生成、事件/隐患初判、事件/隐患核判、初步处理，以及完全处理完成后，所有环节中产生的日志，将统一、完整归档。归档后管理员和各单位可以通过后台界面看到权限范围内的归档日志，归档日志内容应包括ID、工单类型、事件/隐患相关情况，以及创建时间、事发单位、责任人和配套附件等。

（15）平台数据总线

必须按照《政务网络安全监测平台数据总线结构规范》(送审稿)的要求以及采购人的实际需求，如发布了最新的规范则按最新规范要求执行，完成与国家平台、盟市系统、自治区相关部门安全平台对接，完成远程知识库、威胁情报库、漏洞库、通知公告库等的对接，按采购人要求完成相关接口开发、对接和共享。

如果国家或自治区相关部门要求新的对接或数据共享需求，服务期内必须按照采购人的要求完成相关第三方安全平台或设备的接口开发、对接和共享。

数据总线在政务网络安全监测平台中需要实现功能包括但不限于如下：

- 1) 内部各功能模块之间的数据交互；
- 2) 与国家、盟市监测系统的数据格式标准化，实现数据级联对接；
- 3) 根据各部门的需求，实现与自治区相关部门安全平台对接，数据共享；
- 4) 接入安全服务商、CVE、CNCERT、CNVD、Google Virustotal等第三方威胁

情报。

八、安全大数据中心定制开发要求

安全大数据中心提供对自治区电子政务外网网络安全相关数据进行统一采集、处理、分析和存储的能力。安全大数据中心依托大数据技术提供采集和汇聚各类网络安全数据的能力，以及数据解析和数据映射等数据泛化能力，同时大数据中心提供关联分析、行为分析、用户实体

行为分析和可视化分析的能力来支撑上层威胁感知与监测、安全监测、预警和处置等安全业务系统。

安全大数据中心实现的功能包括但不限于如下：

1.数据集成

提供数据采集和解析，数据采集功能主要实现汇聚自治区电子政务外网网络与安全基础设施信息采集层、安全监测、预警与处置系统以及其他网络安全设备的数据。

支持各类IT和安全相关设备、系统和平台，来自于不同设备的多源日志数据，包括主机操作系统、防火墙、WAF、蜜罐等输出日志格式各异，需要支持syslog、snmp trap、webapi和终端代理等多种接入方式，满足不同场景下的不同类型的日志采集需求。支持汇集数据来自于多个业务系统、多种数据形态，安全数据接入能够针对异构的数据源，集成各类数据，能对数据采集任务的状态进行监控，数据标准化之后的结果日志数据包含富化后的数据、资产、情报等信息。

支持非结构化日志的采集、过滤、缓存、中转分发和调度，并提供数据格式转换、数据解析、数据清洗、数据增强等数据泛化能力。同时数据采集子系统为业务提供消息队列服务，提供缓存共享，支持用户进行数据订阅。

2.关联分析

提供针对流式数据的复杂事件处理能力，支持对多源日志进行关联分析，提升自治区政务外网安全事件发现准确性。支持多类型源数据融合处理分析，并提供可视化关联分析建模的工具，通过可视化拖拽和参数配置的方式构建关联分析和建模任务，加速数据从原始状态到高价值状态的转化。

建模模型包括但不限于以下模型：

下载异常分析：FTP下载模型、服务器外连下载模型、服务器外发文件模型、服务器外发数据模型；

网站访问异常：Webshell访问模型、CC攻击模型、渗透攻击模型；

外连IP模型：SSH服务地域模型、RDP服务地域模型、服务器开发端口模型；

服务器被访问模型：包括SSH服务访问模型、RDP服务访问模型、TELNET登录IP模型；

数据库模型：数据库登录用户模型、数据库登录地址模型、数据库用户访问数据量模型、数据库访问频率模型。

3.可视化安全开发

包含批流画布（可视化建模画布）和搜索工具，并具备安全编排自动化响应（SOAR）能力，能够集成各类协助处置的IT资源和设备，如防火墙、EDR等，实现安全策略下发及设备联动处置。

4.日志检索

实现对于自治区电子政务外网海量的日志数据、告警信息和安全事件的快速检索查询。支持按照数据资料的内容而不是结构化特征来实现信息的检索，能提供快捷的非结构化数据管理工具和强大的数据查询手段，快速、方便地查到所需信息。

5.全流量留存检索

根据特定策略，对重点自治区电子政务外网网络原始流量进行全流量存储、标注、检索和分析，支持对相关的网络安全事件进行回溯。

6.安全多租户

提供统一、可视化的多租户资源管理服务，支持细粒度（数据存储、计算和分析）的资源分配、调度和管理，支持租户配额管理和扩缩容，租户独立管理自有的数据、权限（功能权限，资源权限和数据权限）、用户、角色，实现不同部门间资源隔离，支持多租户服务的SLA，抢占式调度，高优先级任务抢占低优先级任务，租户间可通过数据共享来实现数据交换。

7.大数据存储和计算

安全大数据中心为上层各子系统和安全业务提供存储和计算资源，包括离线分析引擎、分布式搜索引擎、分布式消息队列、流式计算引擎和日志中心等，具备快速日志检索和展示等功能。

8.大数据平台管理

提供大数据管理能力，为内蒙古自治区政务外网安全运营服务中心和相关管理人员提供灵活方便的平台管理功能，支持自定义组件组合，提供可视化的集群性能监控、用户管理、权限控制、日志监控、系统诊断优化等管理功能。

九、现网网络和安全系统利旧要求

（1）安全监测平台需和现网系统、设备联动

供应商需将安全监测平台与现网站点监测预警系统和态势感知系统的日志、漏洞、告警等数据通过syslog、REST API等方式对接，安全数据汇聚到安全监测平台进行统一分析和展示。实现安全监测平台与现网的防火墙、WAF等安全设备通过REST API等方式对接，安全设备产生的各类数据汇聚至安全监测平台，实现监测平台和安全设备的联动处置。

通过和上网行为管理设备联动，冻结用户上网账号，从而针对用户实现一键断网。在发现政务云上的用户网站遭受攻击、篡改等紧急情况下，安全运营服务人员需要及时汇报电子政务外网主管以及网站所属单位的管理人员，由所属单位管理人员操作网站下线，安全运营服务人员应配合进行紧急处置，以及加固整改。

（2）电子政务外网安全统一管理和运营运维

安全监测平台建设完成以后，将现网已有的站点监测预警系统和态势感知系统纳入安全监测体系，供应商需对自治区电子政务外网的所有安全系统和安全设备进行统一管理和运行维护，现网已有系统功能保持不变，通过平台之间接口对接，实现各类数据的统一汇总分析和态势展示，形成政务外网完整统一的安全保障体系。

十、安全运营服务要求

（一）安全运营服务内容要求

安全运营服务基本工作包括但不限于如下，服务过程中应根据采购人的需要优化调整。

1.资产识别与梳理

资产管理服务提供资产识别、录入以及资产全生命周期的追踪管理，为用户清晰掌握单位资产信息，减少僵尸资产以及安全暴露面。包括资产全面梳理录入、明确核心资产、探测资产变更、维护资产台账等。

2.脆弱性评估与管理

对于脆弱性评估与管理需要按照脆弱性识别、评估、重要性排序、跟踪处置、价值展示的顺序进行整体管理，确定处置方案，进行漏洞加固等。

3.威胁管理

综合运用安全专家经验和威胁情报知识库，对不同安全设备的安全日志、流量进行关联，并通过资深安全专家对安全威胁的专业分析及定位，实现精准检测网络和主机中的有效安全告

警/威胁。同时，安全专家团队对识别到的威胁进行主动响应，采取措施降低威胁可能造成的影响，协助闭环处置安全事件，并且通过对安全威胁的趋势分析，提供长期的安全规划及改进建议。

4.安全问题处置

需要对安全问题的管理明确响应处置流程，并通过固定流程完成相应的处置工作，包括应急预案制定、入侵影响抑制、入侵威胁清除、入侵原因分析等。

5.人工研判

运营服务人员需要基于安全监测平台的自动化分析结果，针对中、高危风险进行二次人工分析研判，形成精确结论，避免误报。

6.策略管理

针对安全策略、白名单、误告警等进行持续优化管理，进行策略调优、策略定期管理、误判优化等。

7.安全通告

结合威胁情报，安全运营专家排查是否对用户资产造成威胁并通知用户，协助及时进行安全加固。

8.安全巡检

定期针对安全设备健康状态进行一次安全巡检，包括设备运行状态、安全设备的授权情况和序列号的有效期、规则库有效期等。

9.流程优化

根据运营阶段的实际执行情况，在已有的运营流程上，进行优化改进，去除实际执行中不合适的部分，新增实际执行中新发现的、值得固化下来的部分，由采购人进行审核，审核通过后进行更新发布。

10.渗透测试

信息系统在正常运行前提下，模拟黑客攻击行为通过远程或本地方式对信息系统进行非破坏性的入侵测试，查找针对应用程序的各种漏洞，发现在系统复杂结构中的最脆弱链路并针对安全隐患提出解决办法，保证信息系统安全。

11.应急演练

安全运营服务人员，使用安全监测和服务工具，演练模拟信息安全攻击事件，通过演练锻炼人员的实际处理能力，检验人员对网络安全事件、应急处理相关制度掌握情况，验证应急处置方案的有效性与可行性，根据可能面临的主要风险和系统特点，检验应急处理流程及突发安全事件的处理能力。

12.工作汇报

基于全面的资产识别与梳理工作，结合安全监测平台对安全态势的分析与统计结果，定期对电子政务外网的综合安全现状进行评估，每天、每周、每月、每季度、每年进行安全监测运营成果的工作汇报，报告内容包括但不限于工作成果、遗留问题、加固建议等。

（二）安全服务合规性要求

安全服务商必须在等保、关保、密保、风评等方面落实法律法规的符合性，保障安全监测平台和电子政务外网各类信息系统合法、合规。

1、需按照《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019）等相关等保2.0规范进行平台建设和提供服务，实现物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全和安全管理，构建可信、可控、可管的安全体系。

2、根据中国国家标准化管理委员会《信息安全技术关键信息基础设施边界确定方法》征求意见稿、国家互联网信息办公室《关键信息基础设施安全保护条例（征求意见稿）》等的要求，确定电子政务外网关键网络设施和信息系统，识别出关键信息基础设施边界，采取技术措施，监测、记录网络运行状态、网络安全事件。

3、按照《中华人民共和国密码法》、《信息安全技术信息系统密码应用基本要求》（GB/T 39786-2021）、《商用密码应用安全性评估管理办法（试行）》等的要求，安全监测平台需是满足国密算法要求的产品，在访问控制、身份鉴别、通信完整性等方面均需符合密码应用要求，同时依托电子政务外网现有的密码基础设施，与现网密码系统集成。

4、根据《信息安全技术信息安全风险评估规范》（GB/T 20984-2007）、《信息安全技术信息安全风险评估实施指南》（GB/T 31509-2015）等相关规范和要求，服务商需加强电子政务外网的风险评估和风险管理，开展信息安全风险评估工作，包括资产评估、威胁评估、脆弱性评估、现有安全措施评估、风险计算和分析、风险决策和安全建议等评估内容。

（三）安全运营服务人员要求

供应商配置驻场服务人员不少于15人，与厂商远程支撑技术人员不少于5人，负责自治区电子政务外网安全监测平台（含原有态势感知系统、站点监测预警系统，以及相关网络安全设备）的安全运营服务。提供7×24小时驻场服务，7×24小时应急响应服务。提供厂商高级安全技术专家7×24小时远程技术支撑，远程无法解决的问题需到现场处理。

安全运营服务人员具体配置及要求如下：

| 序号 | 类别 | 职责 | 组长 (人数) | 组员 (人数) | 人员要求 |
|----|----|---------|------------|------------|---|
| 1 | | 安全运营经理 | 1 | | 具备人力资源和社会保障部颁发的计算机技术与软件专业技术资格高级证书，且具备CISP证书，具备网络安全运营服务管理经验5年以上。 |
| 2 | | 安全运营监测组 | 1 | 5 | 组长：具备人力资源和社会保障部颁发的计算机技术与软件专业技术资格高级证书，具备网络安全服务经验3年以上。 组员：至少2人具备人力资源和社会保障部颁发的计算机技术与软件专业技术资格证书，或具备CISP、CISAW其中1个证书。 |

服务商

| | | | | | |
|---|--------|------------|---|---|---|
| 3 | 驻场人员 | 安全运营处置执行组 | 1 | 5 | 组长：具备人力资源和社会保障部颁发的计算机技术与软件专业技术资格证书，具备网络安全服务经验3年以上。 组员：至少2人具备人力资源和社会保障部颁发的计算机技术与软件专业技术资格证书，或具备CISP、CISAW其中1个证书。 |
| 4 | | 安全运营安全审核组 | 1 | 1 | 组长：具备人力资源和社会保障部颁发的计算机技术与软件专业技术资格证书，具备同类网络安全审核经验3年以上。 组员：具备人力资源和社会保障部颁发的计算机技术与软件专业技术资格证书，具备同类网络安全审核经验2年以上。 |
| 5 | 厂商服务人员 | 安全运营远程技术人员 | 1 | 4 | 组长：资深安全专家，具备网络安全行业工作经验8年以上，具备丰富的攻防实战、渗透测试、应急响应等经验。 组员：高级安全专家，具备网络安全行业工作经验5年以上，具备丰富的攻防实战、渗透测试、应急响应等经验。 |

（四）弱口令专项排查服务

投标人应按照按采购人约定执行弱口令专项排查服务，具体内容要求如下：

| 序号 | 服务名称 | 服务内容 |
|----|-----------|---|
| 1 | 弱口令专项排查服务 | 针对全区电子政务外网指定系统（或网段）开展弱口令专项排查工作，输出《弱口令专项排查》报告（一年一次，排查范围由采购人安排） |

十一、自治区核心路由器扩容要求

自治区电子政务外网连接盟市和城域网的3台核心路由器，供应商需对3台核心路由器进行扩容，每台各扩容1块24端口万兆板卡及光模块，并按照采购人要求，按需完成相关链路和设备接入的集成工作。具体扩容地址按采购人约定执行。

十二、边界路由器部署要求

自治区各厅局部门共有72台边界路由器需要部署，供应商需按照采购人的要求，完成边界路由器的部署，以及提供相关光纤、网线、光模块等配套材料，完成边界网络设备部署的集成工作。具体部署地址按采购人约定执行。

十三、服务产品和运营要求

供应商提供的所有软硬件产品或服务期内需提供质保服务。

1.万兆接入交换机

| 序号 | 重要性 | 指标项 | 指标要求 |
|----|-----|--------|---|
| 1 | √ | 产品 | 国产品牌产品；配置数量≥2台。 |
| 2 | √ | 主要性能参数 | 交换容量≥4.5Tbps，包转发率≥1600Mpps，10GE光接口≥48个，40GE光接口≥6个，具备IPv6，配置满足需求的光模块，冗余电源。 |
| 3 | 0 | 三层功能 | 支持IP报文分片重组 |
| 4 | 0 | 安全性 | 支持微分段 |
| 5 | 0 | 配置和维护 | 支持Telemetry，支持VxLAN OAM：VxLAN ping，VxLAN tracer，支持IPCA。 |
| 6 | 0 | 流量分析 | 支持Netstream |

2.千兆接入交换机

| 序号 | 重要性 | 指标项 | 指标要求 |
|----|-----|--------|--|
| 1 | √ | 产品 | 国产品牌产品；配置数量≥2台。 |
| 2 | √ | 主要性能参数 | 交换容量≥600Gbps，包转发率≥250Mpps，千兆以太网电口≥48个，10GE光接口≥4个，具备IPv6，配置满足需求的光模块，冗余电源。 |
| 3 | 0 | 二层 | 支持MAC地址≥128K，支持ARP表项≥128K。 |
| 4 | 0 | 三层 | 支持IPv4路由表≥512K，支持IPv6路由表≥64K。 |
| 5 | 0 | VxLAN | 支持VxLAN功能，支持VxLAN二层网关、三层网关，支持BGP EVPN，实现自动建立隧道。 |
| 6 | 0 | 可靠性 | 支持真实业务流实时检测技术，实时检测网络故障。 |

3.边界路由器

| 序号 | 重要性 | 指标项 | 指标要求 |
|----|-----|--------|---|
| 1 | √ | 产品 | 国产品牌产品；配置数量≥72台。 |
| 2 | √ | 主要性能参数 | 交换容量≥80Tbps，包转发率≥12500Mpps，整机业务载板插槽≥6个，配置双主控，GE光电自适应口≥10个，配置≥2个千兆单模光模块，≥2个千兆多模光模块，≥6个千兆电模块，冗余电源，支持MPLS VPN功能，支持NAT转换功能，支持OSPF、BGP等主流协议，支持扩展2个以上10GE光口，具备IPv6。 |
| 3 | 0 | 芯片 | 设备CPU为国产芯片，提供第三方测试报告。 |

| | | | |
|---|---|-------|--|
| 4 | 0 | 接口类型 | 设备支持50GE/25GE/10GE/GE/FE/CPOS/E1等接口类型 |
| 5 | 0 | 协议与功能 | IPv4路由表容量≥12M,IPv6路由表容量≥10M; IPv4转发表容量≥4M,IPv6转发表容量≥2M; |
| 6 | 0 | 业务保障 | 设备支持Flex网络硬切片，提供第三方测试报告。 |

4.核心路由器板卡

| 序号 | 重要性 | 指标项 | 指标要求 |
|----|-----|--------|--|
| 1 | √ | 产品 | 国产品牌产品；配置数量≥3块。 |
| 2 | √ | 主要性能参数 | 现有自治区电子政务外网核心交换区域的3台核心路由器各扩容1块24端口万兆板卡，单块配置万兆单模光模块≥18个，万兆多模光模块≥6个。 |

5.流量探针(10G)

| 序号 | 重要性 | 技术指标 | 技术参数及性能指标 |
|----|-----|--------|---|
| 1 | √ | 产品 | 国产品牌产品；具有公安部公布的“计算机信息系统安全专用产品销售许可证”。配置数量≥16台。 |
| 2 | √ | 性能规格 | 处理性能≥10Gbps，≥2U，内存≥32G，数据盘≥960GB SSD，千兆电口≥8，千兆光口≥8，万兆光口≥4，具备IPV6，配置满足需求的光模块，冗余电源。通过网络流量镜像对用户到业务资产、业务的访问关系进行识别，基于捕捉到的网络流量对内部进行攻击识别、违规行为检测与异常行为识别，旁路部署方式对全流量信息进行采集。 |
| 3 | 0 | 部署模式 | 旁路部署，支持探针接入多个镜像口，每个接口相互独立且不影响。 |
| 4 | 0 | 资产发现 | 具备主动发送少量探测报文，发现潜在的服务器（影子资产）以及学习服务器的基础信息，如：操作系统、开放的端口号等。 |
| 5 | 0 | 基础检测功能 | 具备报文检测引擎,可实现IP碎片重组、TCP流重组、应用层协议识别与解析等；具备多种的入侵攻击模式或恶意URL监测模式，可完成模式匹配并生成事件，可提取URL记录和域名记录。 |
| 6 | 0 | 网站攻击检测 | 支持SQL注入、XSS攻击、网页木马、网站扫描、WEBSHELL、跨站请求伪造、系统命令注入、文件包含攻击、目录遍历攻击、信息泄露攻击、Web整站系统漏洞等网站攻击检测。 |
| 7 | 0 | 敏感信息检测 | 支持敏感数据泄密功能检测能力，可自定义敏感信息，支持根据文件类型和敏感关键字进行信息过滤。 |

| | | | |
|----|---|----------|--|
| 8 | 0 | 漏洞利用攻击检测 | 支持Database漏洞攻击、DNS漏洞攻击、FTP漏洞攻击、Mail漏洞攻击、Net work Device 、Scan漏洞攻击、System漏洞攻击、Telnet漏洞攻击、Tftp漏洞攻击、Web漏洞攻击等服务漏洞攻击检测。 |
| 9 | 0 | 异常流量检测 | 支持标准端口运行非标准协议，非标准端口运行标准协议的异常流量检测，端口类型包括3389、53、80/8080、21、69、443、25、110、143、22等。 |
| 10 | 0 | 僵尸网络行为检测 | 支持HTTP未知站点下载可执行文件、浏览最近30天注册域名、浏览恶意动态域名、访问随机算法生成域名、暴力破解攻击、反弹连接、IRC通信等僵尸网络行为检测。 |
| 11 | 0 | 违规访问检测 | 支持IP，IP组，服务，端口，访问时间等定义访问策略，主动建立针对性的业务和应用访问逻辑规则，包括白名单和黑名单方式。 |
| 12 | 0 | 沙箱对接 | 支持将流量还原的文件发送至沙箱分析，可支持第三方沙箱对接。 |
| 13 | 0 | 特征库 | 内置URL库、IPS漏洞特征识别库、应用识别库、WEB应用防护识别库、僵尸网络识别库、实时漏洞分析识别库、恶意链接库、白名单库。 |

6.流量探针(2G)

| 序号 | 重要性 | 技术指标 | 技术参数及性能指标 |
|----|-----|--------|--|
| 1 | √ | 产品 | 国产品牌产品；具有公安部公布的“计算机信息系统安全专用产品销售许可证”。配置数量≥4台。 |
| 2 | √ | 性能规格 | 处理性能≥2Gbps，≥2U，内存≥8G，数据盘≥480GB SSD，千兆电口≥6，万兆光口≥4，具备IPV6，配置满足需求的光模块，冗余电源。通过网络流量镜像对用户到业务资产、业务的访问关系进行识别，基于捕捉到的网络流量对内部进行攻击识别、违规行为检测与异常行为识别，旁路部署方式对全流量信息进行采集。 |
| 3 | 0 | 部署模式 | 旁路部署，支持探针接入多个镜像口，每个接口相互独立且不影响； |
| 4 | 0 | 资产发现 | 具备主动发送少量探测报文，发现潜在的服务器（影子资产）以及学习服务器的基础信息，如：操作系统、开放的端口号等； |
| 5 | 0 | 基础检测功能 | 具备报文检测引擎,可实现IP碎片重组、TCP流重组、应用层协议识别与解析等；具备多种的入侵攻击模式或恶意UR监测模式，可完成模式匹配并生成事件，可提取URL记录和域名记录； |

| | | | |
|----|---|----------|---|
| 6 | 0 | 网站攻击检测 | 支持SQL注入、XSS攻击、网页木马、网站扫描、WEB SHELL、跨站请求伪造、系统命令注入、文件包含攻击、目录遍历攻击、信息泄露攻击、Web整站系统漏洞等网站攻击检测； |
| 7 | 0 | 敏感信息检测 | 支持敏感数据泄密功能检测能力，可自定义敏感信息，支持根据文件类型和敏感关键字进行信息过滤； |
| 8 | 0 | 漏洞利用攻击检测 | 支持Database漏洞攻击、DNS漏洞攻击、FTP漏洞攻击、Mail漏洞攻击、Net work Device、Scan漏洞攻击、System漏洞攻击、Telnet漏洞攻击、Tftp漏洞攻击、Web漏洞攻击等服务漏洞攻击检测； |
| 9 | 0 | 异常流量检测 | 支持标准端口运行非标准协议，非标准端口运行标准协议的异常流量检测，端口类型包括3389、53、80/8080、21、69、443、25、110、143、22等； |
| 10 | 0 | 僵尸网络行为检测 | 支持HTTP未知站点下载可执行文件、浏览最近30天注册域名、浏览恶意动态域名、访问随机算法生成域名、暴力破解攻击、反弹连接、IRC通信等僵尸网络行为检测； |
| 11 | 0 | 违规访问检测 | 支持IP，IP组，服务，端口，访问时间等定义访问策略，主动建立针对性的业务和应用访问逻辑规则，包括白名单和黑名单方式； |
| 12 | 0 | 沙箱对接 | 支持将流量还原的文件发送至沙箱分析，可支持第三方沙箱对接； |
| 13 | 0 | 特征库 | 内置URL库、IPS漏洞特征识别库、应用识别库、WEB应用防护识别库、僵尸网络识别库、实时漏洞分析识别库、恶意链接库、白名单库； |

7.日志探针

| 序号 | 重要性 | 技术指标 | 技术参数及性能指标 |
|----|-----|------|--|
| 1 | √ | 产品 | 国产品牌产品；具有公安部公布的“计算机信息系统安全专用产品销售许可证”。配置数量≥8台。 |
| 2 | √ | 性能规格 | 支持多端口采集，≥2U，内存≥32G，硬盘≥4T S A T A × 2，冗余电源，主机和资产审计≥500个，千兆电口≥4个，万兆光口≥2个，配置满足需求的光模块，具备IPV 6，平均每秒处理日志数（eps）性能：4000。 |

| | | | |
|----|---|-------|---|
| 3 | 0 | 日志采集 | 支持主动、被动相结合的数据采集方式，支持通过Agent采集日志数据，支持通过syslog、SNMP Trap、JDBC、WMI、webservice、FTP、文件\文件夹读取、Kafka等多种方式完成日志收集； |
| 4 | 0 | | 支持接入TLS加密方式的日志，支持对日志传输状态、最近同步时间进行监控，可统计每个日志源的今日传输量和传输总量； |
| 5 | 0 | 日志标准化 | 支持通过正则、分隔符、json、xml的可视方式进行自定义规则解析，支持对解析结果字段的新增、合并、映射； |
| 6 | 0 | 日志过滤 | 支持对每个日志源设置过滤条件规则，自动过滤无用日志，满足根据实际业务需求减少采集对象发送到核心服务器的安全事件数，减少对网络带宽和数据库存储空间占用； |
| 7 | 0 | 日志转发 | 支持对单个/多个日志源批量转发，支持定时转发，可通过syslog和kafka方式转发到第三方平台，并且支持转发原始日志和已解析日志的两种日志； |
| 8 | 0 | 日志存储 | 支持日志文件备份到外置存储节点，支持NFS、NAS、ISCSI三种存储方式，并可查看外置存储容量、状态等信息。支持以FTP方式将日志数据备份至外部存储空间，支持备份数据的恢复和查询； |
| 9 | 0 | 全文检索 | 支持通配符、范围搜索、字段等多种输入方式、搜索框模糊搜索、相关语段进行语法搜索；可根据时间、严重等级等进行组合查询；可根据具体设备、来源/目的所属、IP地址、特征ID、URL进行具体条件搜索；支持可设置定时刷新频率，根据刷新时间显示实时接入日志事件； |
| 10 | 0 | | 支持解码小工具，按照不同的解码方式解码成不同的目标内容，编码格式包括base64、Unicode、GBK、HEX、UTF-8等； |
| 11 | 0 | 日志分析 | 支持自定义审计规则与关联规则，支持网站攻击、漏洞利用、C&C通信、暴力破解、拒绝服务、主机脆弱性、主机异常、恶意软件、账号异常、权限异常、侦查探测等内置关联分析规则，内置关联分析规则数量达到350条以上； |
| 12 | 0 | 资产管理 | 支持对IPv4/ipv6对象的自动发现功能，对自动发现的设备可以修改、删除或转为资产 |

| | | | |
|----|---|------|--|
| 13 | 0 | 日志告警 | 支持告警事件归并、告警确认和告警归档，支持基于频率、频次、时间的设定条件； |
| 14 | 0 | | 日志进行归一化操作后，对日志等级进行映射，根据不同日志源统计不同等级下的日志数量； |
| 15 | 0 | 系统管理 | 提供管理员账号创建、修改、删除，并可针对创建的管理员进行权限设置；支持IP免登录，IP免认证直接进入平台；支持只允许某些IP登录平台；支持页面权限配置和资产范围配置，用于管理账号权限，满足用户三权分立的需求；支持usb-key认证； |

8.沙箱探针

| 序号 | 重要性 | 技术指标 | 技术参数及性能指标 |
|----|-----|--------|--|
| 1 | √ | 产品 | 国产品牌产品；具有公安部公布的“计算机信息系统安全专用产品销售许可证”。配置数量≥8台。 |
| 2 | √ | 性能规格 | 虚拟沙箱数量≥10个，静态文件检测数量≥100万个/天，动态文件检测数量≥1万个/天，千兆电口≥4个，内存≥64G，硬盘≥2T，≥2U，具备IPV6，冗余电源。通过对HTTP、SMTP、POP3、SMB、IMAP、FTP等协议传输过程中的文件进行还原，对提取的文件进行多病毒引擎扫描、安全漏洞检测、虚拟环境执行等静态和动态分析。在沙箱虚拟环境执行过程中监测进程内存操作、注册表操作、网络通讯、系统变更、API调用等行为特征，结合风险行为规则来为未知文件进行评分，根据评分阈值确定文件的风险等级，并给出详细的分析报告和运行截图，为分析人员提供依据，并支持将沙箱分析结果上报安全监测平台进行关联分析； |
| 3 | 0 | 文件处理 | 支持但不限于Office文档、WPS、PDF、HTML、JS、ZIP、7Z、RAR、CMD、PE、APK等60种以上文件类型检测，且支持自定义文件类型 |
| 4 | 0 | | 支持压缩包检测，支持5层以上解压，可对压缩包内的文件进行独立检测； |
| 5 | 0 | | 支持文件检测告警日志上传功能，能够将检测告警日志发送给第三方Syslog服务器； |
| 6 | 0 | 静态特征检测 | 具备独立的文件内容分析特征库分析引擎，支持对Office文件、PE文件等文件内容进行检测，发现漏洞利用、木马、蠕虫、病毒、黑客工具等恶意代码； |
| 7 | 0 | | 具备独立的文件HASH库检测引擎，支持对文件的MD5 HASH进行检测，发现已知的恶意文件，同时文件HASH库支持100万个以上已知恶意文件MD5特征； |

| | | | |
|----|---|--------|--|
| 8 | 0 | 动态行为检测 | 具备杀软检测、CVE、沙箱检测、YARA检测、机器学习、威胁情报检测等综合检测能力，且每种检测能力可独立输出检测结果； |
| 9 | 0 | | 沙箱引擎的虚拟机系统支持常见操作系统模板，且支持在不重启系统情况下的实时切换沙箱模版； |
| 10 | 0 | | 支持200种以上反沙箱逃逸检测规则，可检测特种木马睡眠、虚拟机探测等反沙箱逃逸行为； |
| 11 | 0 | | 支持反病毒检测功能，针对特种木马的反病毒检测技术进行检测和处理； |
| 12 | 0 | 机器学习检测 | 支持机器学习模型，检测PE、office、PDF等格式文件； |
| 13 | 0 | | 支持通过机器算法对恶意样本分类，分类方式至少包含病毒木马、后门、蠕虫、广告等； |
| 14 | 0 | 配置管理 | 支持自定义配置检测流程来提升检测效率，包含但不限于配置进入沙箱的文件类型、发现威胁后进入沙箱、未发现进入沙箱和始终进入沙箱； |
| 15 | 0 | 设备联动 | 支持与安全监测平台联动，把恶意文件检测结果推送到平台进行了联合分析并展示，提升平台未知威胁检测能力； |

9.软探针

| 序号 | 重要性 | 指标功能 | 规格要求 |
|----|-----|---------|--|
| 1 | √ | 产品 | 国产品牌产品；具有公安部公布的“计算机信息系统安全专用产品销售许可证”。配置数量≥4000套。 |
| 2 | √ | 性能规格 | 轻量化Agent方式部署在虚拟化服务器操作系统主机上，负责采集服务器虚拟主机安全数据，上报给安全监测平台，同时具备云内威胁检测、资产梳理、漏洞检测能力，具备IPV6； |
| 3 | √ | 低资源开销 | 支持软件形态极简安装部署，客户端常态下占用内存不超过50MB，CPU不影响平台运行，磁盘不超过200MB；自动降低agent的工作优先级，释放资源给业务系统； |
| 4 | 0 | 架构稳定 | Agent采用业务零侵害架构，具备极低的资源开销，结合自调节的网络负载和自守护安全的无驱架构，以业务稳定运行为优先；采用无驱架构，终端兼容性高，不蓝屏；Agent终端安全自守护机制，防恶意关闭或Kill行为； |
| 5 | 0 | 网络负载自调节 | 自调节数据传输内容，在网络高负载情况下只上报核心数据到中心端；差分数据传输机制，增量差异数据传输，降低数据重复上报量； |

| | | | |
|----|---|--------|---|
| 6 | 0 | 云主机 | 支持采集云主机的资产信息，显示主机详细的资产指纹信息，包括进程、账号、端口、应用软件、数据库和Web资产等 |
| 7 | 0 | 主机基本信息 | 支持主机基本信息清点，如操作系统、硬件配置、网卡信息、磁盘等信息，至少 包括：主机名、操作系统、内核版本、系统启动时间、生产商、设备型号、序列号等 |
| 8 | 0 | 进程信息 | 支持进程信息清点，包括：进程名、进程状态、进程路径等 |
| 9 | 0 | 主机账号 | 支持主机账号资产清点，包括：用户名、账号状态、账号主目录等 |
| 10 | 0 | 端口信息 | 支持端口信息清点，包括：端口号、进程名、绑定IP、协议等 |
| 11 | 0 | 应用软件 | 支持应用软件信息清点，包括应用名、版本号、配置文件路径、二进制路径、运行用户、关联进程等 |
| 12 | 0 | 数据库资产 | 支持数据库资产清点，包括：数据量类型、版本、运行用户、配置文件路径、日志文件路径等 |
| 13 | 0 | WEB资产 | 支持WEB站点资产清点、WEB服务资产清点、WEB应用资产清点、WEB框架资产清点等； |
| 14 | 0 | 管理可视化 | 采用B/S架构的管理控制中心，具备主机安全可视，主机统一管理，统一威胁检测响应，病毒防御，日志记录与查询等功能； |
| 15 | 0 | 系统管理 | 支持对已安装Agent的主机按需分组管理，按照主机IP、核心程度、操作系统、运行状态、事件标签、主机名称等多个方式进行筛选管理； |

10.防火墙

| 序号 | 重要性 | 指标项 | 指标要求 |
|----|-----|--------|--|
| 1 | √ | 产品 | 国产品牌产品；配置数量≥2台。 |
| 2 | √ | 性能规格 | CPU为国产芯片，网络层吞吐量≥9.5Gbps，应用层吞吐量≥1Gbps，并发连接数≥220万，新建连接数≥10万，≥2U，内存≥8GB，硬盘≥64GB SSD，冗余电源，千兆电口≥6，千兆光口≥4，配置满足需求的光模块，具备IPv6； |
| 3 | 0 | 系统功能 | 产品支持透明传输、路由转发模式部署，提供包过滤、地址转换、状态检测等 网络层访问控制功能，提供应用类型控制、应用关键内容控制等应用层控制功能，提供拒绝服务攻击、恶意代码防护、应用攻击防护等功能 |
| 4 | 0 | 访问控制策略 | 产品支持多维度安全策略设置，可基于时间、用户、应用、IP、域名等内容进行安全策略设置。 |

| | | | |
|----|---|---------|--|
| 5 | 0 | 应用控制 | 产品内置应用特征识别库，支持不少于 2500 种应用规则，支持对游戏、下载工具、IM聊天工具、视频软件、股票软件等类型应用进行检测与控制。 |
| 6 | 0 | DDoS防御 | 产品具备至少对ARP Flood、ICMP Flood、SYN Flood、DNS Flood、UDPFlood等泛洪类攻击防护的能力，并支持IP地址扫描和端口扫描攻击防护。 |
| 7 | 0 | 入侵防御 | 产品具备入侵防御检测引擎，支持对各类漏洞利用攻击进行检测与防护。 |
| 8 | 0 | Web应用防御 | 产品具备Web应用攻击检测引擎，支持文件包含攻击、抵御注入式攻击（包含SQL注入、系统命令注入）、信息泄露攻击、跨站脚本（XSS）、网站扫描、WEBSHELL后门攻击、跨站请求伪造、目录遍历攻击、WEB整站系统漏洞等应用层攻击行为。 |
| 9 | 0 | 对象智能识别 | 产品支持服务器自动侦测功能，采用双向流量检测技术识别网络中的服务器对象。 |
| 10 | 0 | 安全策略管理 | 产品支持在单条安全策略中可同时启用入侵防御、防病毒、URL过滤、文件过滤、Web应用防护等安全功能，简化安全策略部署。 |
| 11 | 0 | 双机部署 | 产品支持主主和主备两种双机部署方式。 |

11.行为管理

| 序号 | 重要性 | 指标项 | 指标要求 |
|----|-----|-----------|--|
| 1 | √ | 产品 | 国产品牌产品；具有公安部公布的“计算机信息系统安全专用产品销售许可证”。配置数量≥2台。 |
| 2 | √ | 配置要求 | 网络层吞吐量≥10Gbps，带宽性能≥1G，万兆以太网光接口≥2，千兆以太网光接口≥2，千兆以太网电接口≥6，配置满足需求的光模块，具备IPV6，冗余电源。 |
| 3 | 0 | 管理界面 | 支持SSL加密WEB方式、SSH命令行方式管理设备； |
| 4 | 0 | IPsec VPN | 具有IPSec VPN远程加密访问和连接的模块，并能提供IPSec VPN客户端授权远程接入访问； |
| 5 | 0 | 上网故障排除系统 | 支持开启直通后，流量控制模块依然生效，避免全部数据直通导致线路流量过大； |
| 6 | 0 | 流控通道可视化 | 能够实时看到各级流控通道的状态：包括所属线路、瞬时速率、通道占用比例、用户数、保证带宽、最大带宽、优先级，启用状态等。 |
| 7 | 0 | 应用流控 | 支持基于应用类型、网站类型和文件类型划分与分配带宽； |
| 8 | 0 | 动态流控 | 支持在设置流量策略后，根据整体线路或者某流量通道内的空闲情况，自动启用和停止使用流量控制策略，以提升带宽的高使用率；空闲值可自定义。 |

| | | | |
|----|---|------------|--|
| 9 | 0 | 邮件审计 | 支持审计用户外发 Email 邮件的正文及附件；能审计用户使用邮件客户端外发 SSL 加密邮件的邮件内容； |
| 10 | 0 | 文件外发 审计 | 支持审计用户通过 HTTP 、 FTP 、 Email 当方式外发的文件内容；能对加密文件外发行为识别并记录； |
| 11 | 0 | 应用细分 控制 | 能够对常见应用进行细分控制，如：登录、浏览、发微博、上传附件等。能够对常见网络应用的上传动作进行细分控制； |

12.监测平台

| 序号 | 重要性 | 技术指标 | 技术参数及性能指标 |
|----|-----|------------|---|
| 1 | √ | 产品 | 国产品牌产品；具有公安部公布的“计算机信息系统安全专用产品销售许可证”。配置数量≥5台。 |
| 2 | √ | 主要性能 参数 | <p>CPU≥2颗，单颗≥16核，主频≥2.3HZ，内存≥256GB，可用存储容量≥50TB，冗余电源，千兆电口≥6个，万兆光口≥2个，配置满足需求的光模块，每天不少于40000万条日志处理能力，具备IPV6。具备基础监测，通报预警，响应处置、数据总线协同对接等功能以及相应的硬件支撑，实现对自治区电子政务外网数据采集、数据分析、展示与应用、平台运行管理、数据总线、威胁情报共享等功能。</p> <p>具备流量采集、资产与脆弱性识别、威胁监测与发现、异常行为分析功能，以流量采集为基础，重点采集电子政务外网核心区域流量，基于海量流量数据，通过机器学习、数据关联分析、用户与实体行为分析、动态文件威胁鉴定、威胁情报分析等多种检测技术，实现电子政务外网各类攻击威胁的安全监测。</p> <p>具备用户管理、资产管理、威胁情报、通报预警、事件分析功能，为电子政务外网整体安全提供统一管理的通报、预警，针对事件能及时作出相应动作，对收集到的通报预警消息，通过安全通讯方式，集中收集安全事件进行处理，从而实现针对电子政务外网的安全事件的集中通报预警。</p> <p>具备全局指挥、应急响应管理、安全隐患处置、协同处置、归档留存功能，达到更好的管理通报预警消息，使得每个有效的预警消息能够得到处置，使得系统自动发现的告警消息能得到及时有效的闭环。</p> <p>具备数据总线协同对接功能，用于打通各个不同的安全平台实现数据的互联互通，实现上下级平台或第三方平台接入，实现各个安全平台之间数据上报、共享、预警通报、协同处置及数据展示查询等功能。</p> |

| | | | |
|----|---|------------|---|
| 3 | √ | 对接要求 | 按照国家规范以及采购人的要求，实现与中央级平台、盟市系统、自治区各部门的第三方安全平台对接、数据共享。 按照采购人的要求与自治区电子政务外网网安全系统和安全设备对接实现联动。 |
| 4 | √ | 对接标准 | 完成内蒙古自治区电子政务外网安全监测平台技术规范标准的制定，制定电子政务外网安全监测平台与上下级平台、其他第三方平台、其他安全设备等对接标准规范。 |
| 5 | 0 | 全网安全态势可视 | 支持不同安全视角展示15个以上独立的大屏展示功能，包括全网安全态势感知大屏、资产态势大屏等，支持实时告警、大屏轮播，可自定义播放顺序。 |
| 6 | 0 | 分支权限管理 | 支持自定义下属机构管理权限，下属管理员具备独立的管理页面，且只能管理和查看所属下属单位的业务和终端资产的安全信息且具备完整的功能展示。 |
| 7 | 0 | 资产全生命周期管理 | 支持资产多级分支管理，可至15级分支，支持资产全生命周期自动管理，包括资产自动发现、多级资产、资产入库审核、资产离线风险识别、资产退库、资产数据更新，责任人管理机制等。 |
| 8 | 0 | 资产发现 | 支持通过主动发送微量包的扫描方式探测潜在的影子资产以及学习服务器的基础信息，资产指纹信息包括资产类型、端口、操作系统、mac地址、主机名等。 |
| 9 | 0 | 弱密码检测 | 弱密码检测技术基于机器学习提取登录成功的特征，支持自定义WEB登录规则，可设置判定成功规则、判定失败规则。 |
| 10 | 0 | 漏洞分析 | 支持流量实时识别漏洞分析，漏洞分析类型包含配置错误漏洞、OpenSSH漏洞、OpenLDAP等操作系统、数据库、Web应用等，页面上展示业务脆弱性风险分布、漏洞类型分析、漏洞态势与危害和处置建议，并导出脆弱性感知报告。 |
| 11 | 0 | Webshell检测 | 具备基于AI的webshell通信流量检测，可检出加密的通信流量，具备webshell规则检测，且覆盖webshell整个攻击阶段检测，包括上传点探测、上传下载、通信等。 |
| 12 | 0 | 事后异常行为检测 | 具备元数据行为分析引擎httpflow、dnsflow、adflow、icmpflow、maillflow等,通过异常行为分析，结合各类机器学习算法完成未知威胁检测。包括：内网穿透、代理、远控、隧道、反弹shell等事后检测场景。 |

| | | | |
|----|---|-------------|--|
| 13 | 0 | 挖矿专项检测 | 支持挖矿专项检测页面，具备挖矿攻击事前、事中和事后全链路的检测分析能力，综合运用威胁情报、IPS特征规则和行为关联分析技术，如检测发现文件传输阶段的异常，对挖矿早期的准备动作即告警。 |
| 14 | 0 | 威胁情报关联分析 | 具备情报源200个以上，DNS信誉库2000万以上。具备企业级域名信誉库、URL分类库。支持威胁情报关联分析，内置威胁情报数量不少于150万。 |
| 15 | 0 | 第三方日志关联分析可视 | 支持日志关联分析结果的可视化展示，包括数据分布、安全事件趋势图、关联规则告警趋势图、接入设备概况等，可提供每一台设备专项分析的页面，通过设备专项页面对每一台设备安全情况深度专业化分析。 |
| 16 | 0 | 日志检索 | 支持安全检测日志、审计日志、第三方日志存储；日志类型包括漏洞利用攻击、网站攻击、僵尸网络、业务弱点、DOS攻击、邮件安全、文件安全、网络流量、DNS、HTTP、用户、数据库、文件审计、POP3、SMTP、IMAP、LDAP、FTP、Telnet等。 |
| 17 | 0 | 主机行为分析 | 资产行为分析，对这些对象进行持续的学习和行为画像构建，以基线画像的形式检测异于基线的异常行为作为入口点，结合以降维、聚类、决策树为主的计算处理模型发现异常用户/资产行为。 |
| 18 | 0 | 实战攻防中心 | 具备实战化攻防中心，支持备战阶段的对外服务器外网暴露面分析、内网服务器暴露面梳理。实战阶段的实时攻击分析，实时展示受害者IP、攻击者IP、XFF、攻击结果、攻击次数、事件类型、威胁等级、联动响应、状态码、确定性等级等。具备实战阶段的全过程可视溯源分析、总结阶段的值守报告等全过程流程。 |
| 19 | 0 | 威胁情报共享 | 支持云端与本地威胁情报共享，实时收集同步攻击者IP，并详细展示情报列表，包括IOC、区域、来源、更新时间、剩余封锁时间、状态、操作等，并可对本地威胁情报及云端威胁情报联动防火墙实现自动封锁。 |
| 20 | 0 | 溯源中心 | 支持自动化溯源，可自动化复现受害者从最开始的遭受攻击到权限维持各个阶段的黑客行为，包括攻击入口溯源。支持基于可视化的形式展示威胁的影响面，通过大数据分析和关联检索技术，能够直观的看到失陷主机的威胁影响面，同时基于列表模式展示攻击、违规访问、风险访问、可疑行为、正常访问等详细信息。 |

13.蜜罐

| 序号 | 重要性 | 指标项 | 指标要求 |
|----|-----|-----|------|
|----|-----|-----|------|

| | | | |
|---|---|-------|--|
| 1 | √ | 产品 | 国产品牌产品；具有公安部公布的“计算机信息系统安全专用产品销售许可证”。配置数量≥6台。 |
| 2 | √ | 配置要求 | 沙箱数≥4，伪装代理≥12，千兆电口≥2。基于欺骗防御理念，采用攻击溯源技术，实现内部高级攻击者的诱捕分析，保护核心应用及数据安全。在攻击者视角及攻击路径上，通过业务仿真、诱饵设置等方式进行攻击捕获和行为监控分析，并对攻击者设备指纹及各类属性信息进行自动化反向溯源，精准感知内部安全风险，防御APT、高级攻击渗透等攻击行为。 |
| 3 | 0 | 设备要求 | 具备防止攻击逃逸，支持主流操作系统环境，系统稳定可靠，无需额外存储设备即可运行，系统采用B/S设计架构，用户可以通过浏览器远程方便的对产品进行管理。 |
| 4 | 0 | 地址识别 | 支持并识别攻击者IP地址，可自定义配置攻击者IP获取方式（包括ipv4地址和ipv6地址） |
| 5 | 0 | 漏洞自定义 | 支持Web漏洞自定义服务，可以自定义添加PHP/ASP/JSP等不同语言的漏洞类型 |
| 6 | 0 | 文件诱饵 | 支持文件诱饵，当黑客访问word/excel/ppt文件时，捕获感知信息。 |
| 7 | 0 | 身份定位 | 支持分析黑客的身份信息和设备指纹信息，包括IP地址、地理位置、网络身份、设备指纹、操作系统、浏览器等，支持黑客身份信息自定义配置。 |

14.安全大数据中心

安全大数据中心软件功能必须全部满足。

安全大数据中心软件需同时适配X86和信创环境，供应商需要提供安全大数据中心软件部署的服务器和接入交换机，以及安全大数据中心软件部署所需的配套软件。

服务器数量配置≥8台，单台配置要求如下：配置2颗CPU，单颗CPU核数≥20核，主频≥2.5GHz，内存≥384G，硬盘≥12×8TB SATA+2×480G SSD+2×3.2T NVME SSD，千兆电口≥2个，万兆光口≥6个，配置满足需求的光模块，RAID卡支持Raid 0/1/5/6/10，冗余电源。

万兆交换机数量配置≥2台，单台配置要求如下：交换容量≥4.5Tbps，包转发率≥1600Mpps，万兆光口≥48个，配置满足需求的光模块，具备IPV6，冗余电源。

千兆交换机数量配置≥2台，单台配置要求如下：交换容量≥600Gbps，包转发率≥250Mpps，千兆电口≥48个，万兆光口≥4个，配置满足需求的光模块，具备IPV6，冗余电源。

安全大数据中心需要实现的功能包括但不限于如下表所列功能模块，供应商应在开发、部署和运营过程中可以按照采购人的要求进行优化和调整。

| 序号 | 功能 | 子模块 | 功能描述 |
|----|----|-----|------|
|----|----|-----|------|

| | | | |
|----|---------|----------|---|
| 1 | 数据采集 | 数据采集 | 通过syslog、kafka等多种方式对流量数据、安全设备告警数据、终端系统日志、应用日志、漏扫数据等多种数据源进行采集。 |
| 2 | 数据治理 | 数据治理 | 通过可视化配置的方式对采集到的多种来源的数据进行数据治理，包括：数据过滤、数据解析、数据标准化、富化、添加标签等。 |
| 3 | 基础平台 | 基础平台 | 基于Hadoop、Spark、Flink、ES等的分布式处理框架，提供具备弹性扩展能力和数据高可靠冗余存储的大数据基础平台。通过集群的方式弹性扩展平台规模，满足PB级别数据处理。 |
| 4 | 待处理问题分布 | 待处理问题分布 | 对待处理的安全事件、告警、威胁、资产脆弱性等数据做统计与展示。 |
| 5 | 资产风险分布 | 资产风险分布 | 对资产数量和安全状态进行统计与展示，包括：服务器的数量、终端的数量；及存在严重风险/中危/低危的资产数量。 |
| 6 | 安全事件分析 | 安全事件分析 | 对安全事件的严重级别、处置状态进行统计与展示，包括发生安全事件最多的资产、命中热点事件的资产等。 |
| 7 | 威胁概览 | 威胁概览 | 对近期威胁情况进行统计，包括：已处理和待处理的威胁数量；近期的外部攻击趋势展现，外部发起攻击数量最多的攻击者。 |
| 8 | 脆弱性概览 | 脆弱性概览 | 按照时间周期对资产脆弱性进行统计，包括：发现了多少漏洞、修复了多少漏洞、存在待处理漏洞的数量，资产脆弱性的趋势，以及修复最差的资产和责任人、修复排行最好的资产和责任人。 |
| 9 | 大屏展示 | 综合安全态势大屏 | 大屏展示综合安全态势，包括资产态势、脆弱性态势、网络攻击态势、安全事件态势、外连态势、横向威胁态势、设备运行态势；页面跳转到对应态势大屏，并具备大屏告警能力。 |
| 10 | | 资产脆弱性可视 | 大屏展示资产态势，包括服务器操作系统分布、服务器开放服务、最新资产动态、最近变动资产。 |
| 11 | | 安全事件可视 | 大屏展示安全事件态势，包括安全事件、事件等级分布、安全事件态势、安全事件、威胁面最大的事件、事件类型、风险业务/终端。 |
| | 大屏展示 | | |

| | | | |
|----|--------------|--------------|---|
| 12 | | 外部攻击态势 | 地球3D模式展示网络攻击态势，包括攻击次数、遭受攻击资产组、攻击源地址、攻击源IP、攻击手段排行、遭受攻击服务器排行；境外、境内切换。 |
| 13 | | 安全运营大屏 | 大屏展示安全事件处置流程、应急响应流程状态。 |
| 14 | | 平台运行状态监控大屏 | 对接入大数据平台的数据源的类型和数据量进行统计、模型的数量和运行状态进行监控、平台的资源消耗进行监控。 |
| 15 | 应急预案演练 | 应急预案管理 | 内置应急预案文档，基于单位情况修改应急预案流程，实现应急预案电子化。 |
| 16 | | 应急预案演练 | 对应急预案流程进行灵活编排与演练观摩，包括：启用应急演练、事件定级与预警、响应进展监测、处置、评估总结。 |
| 17 | 基于流量的威胁检测 | 基于流量的威胁检测 | 对探针采集的网络流量进行威胁检测，包括：外部攻击检测、文件威胁检测、邮件威胁检测、外连分析、横向威胁分析、威胁影响面分析等。 |
| 18 | 基于多源数据关联分析检测 | 基于多源数据关联分析检测 | 对流量数据、防火墙设备、WAF设备、IPS等安全设备的告警数据、资产数据、漏洞数据等进行综合分析检测，安全信息和事件管理分析的总览展示，包括数据分布、安全事件状态分布、安全事件趋势图、安全事件、关联规则告警趋势、关联规则告警、日志传输趋势等。 |
| 19 | 威胁定性 | 威胁定性 | 通过可视化配置界面的方式对各类安全风险进行定性、能够灵活配置鉴定是威胁还是安全事件。 |
| 20 | 告警消减 | 告警消减 | 通过攻击场景关联、攻击阶段的关联、拓扑结构、白名单等多种方式进行告警数量消减，将海量无效告警进行消减，挑选真实有效告警。 |
| 21 | 资产录入 | 资产录入 | 资产信息的新增、删除、编辑、导入、查看等操作，并能对多种资产数据的对接。 |
| 22 | 资产识别 | 资产识别 | 可通过流量发现服务器、终端、路由器等各类资产，资产属性包括：操作系统、开放的服务与端口；且可通过kafka、syslog等方式灵活对接各类设备识别到的资产数据。 |

| | | | |
|----|----------|----------|---|
| 23 | 业务资产 | 业务资产 | 服务器、终端、网络设备、安全设备等资产进行分类，可定义IP地址、所属分支、主机名、责任人、责任人邮箱、所属业务、操作系统、服务与端口等信息，并基于流量识别操作系统、开放的服务与端口。 |
| 24 | 终端资产 | 终端资产 | 终端资产分类，可定义终端/ip组、主机名、用户名、用户邮箱等信息，并基于流量自动识别终端。 |
| 25 | 安全域资产 | 安全域资产 | 安全域分类资产，可定义安全域名称、安全域属性、责任人、责任人邮箱、IP范围、备注等信息，并导入导出csv配置文件。 |
| 26 | 分支资产 | 分支资产 | 分支分类资产，可定义分支名称、责任人、责任人邮箱、设备、地理位置地图，地图可选择在线地图、离线地址或本地导入地图。 |
| 27 | 资产风险关联 | 资产风险关联 | 能够对资产、漏洞、弱口令、配置风险、安全事件等数据进行关联，直观展示资产的风险情况；可直接通过资产信息逐级进行查看资产存在的漏洞、弱口令、配置风险、安全事件等信息。 |
| 28 | 资产拓扑 | 资产拓扑 | 网络拓扑图的自定义编辑，各类型网络和安全设备的图元拖拽组合生成拓扑，实现所画及所得的拓扑编辑效果。 |
| 29 | 资产生命周期管理 | 资产生命周期管理 | 从资产入网的识别、入网审核、正常运转、退库等全流程的管理跟踪。 |
| 30 | 事件管理 | 事件告警 | 通过短信或邮件等方式进行安全事件的告警 |
| 31 | | 事件统计 | 对告警的分布、状态、严重性、类型进行统计和分析。 |
| 32 | | 处置响应流程编排 | 通过拖拽方式自定义编排威胁的响应处置流程，能够按照配置好的剧本进行威胁的响应。 |
| 33 | | 事件处置 | 通过流程、自动化处置等方式提升安全运营的管理水平和闭环的效率和效果。 |
| 34 | | 联动响应 | 提供开放式的RESTFUL API对接各类安全产品或设备进行安全事件的分析研判、处置、溯源分析；联动防火墙、EDR等各类安全产品。 |
| 35 | 威胁管理 | 威胁告警 | 通过短信或邮件等方式进行威胁的告警。 |
| 36 | | 威胁响应流程编排 | 通过拖拽方式自定义编排威胁的响应处置流程，支撑流程的灵活配置。 |
| 37 | | 事件处置 | 通过流程、自动化分析研判、自动化处置等方式来提升安全运营的管理水平和威胁闭环的效率和效果。 |

| | | | |
|--|----|-------|--|
| | | | |
| | 38 | 联动响应 | 通过RESTFUL API的方式对接第三方设备进行响应闭环，如防火墙、EDR等。 |
| | 39 | 脆弱性管理 | 对接漏扫、EDR、流量探针等多种数据来源中的漏洞数据，通过图形化的配置界面对漏洞数据进行提取和标准化，最终实现对多种来源的数据进行整合与校验，形成完整和准确的漏洞数据。 |
| | 40 | | 对从漏洞发现、漏洞分析研判、漏洞通报、漏洞修复、漏洞修复验证等多个环节进行全流程的跟踪，实现漏洞全生命周期管理。 |
| | 41 | | 对接和提取漏扫、EDR、流量探针等多种数据来源中的弱口令数据，通过图形化的配置界面对弱口令数据进行提取和标准化，最终实现对多种来源的数据进行整合与校验，形成完整和准确的弱口令数据。 |
| | 42 | | 对弱口令发现、弱口令分析研判、弱口令修复、弱口令验证等多个环节进行全流程的跟踪，实现弱口令全生命周期管理。 |
| | 43 | | 对接和提取漏扫、EDR等多种数据来源中的配置风险数据，通过图形化的配置界面对配置基线风险数据进行提取和标准化，最终实现对多种来源的数据进行整合与校验，形成完整和准确的配置风险数据。 |
| | 44 | | 对基线配置风险的发现、基线配置风险的分析研判、基线配置风险的修复、基线配置风险消除的验证等多个环节进行全流程的跟踪，实现基线配置 风险全生命周期管理。 |
| | 45 | | 通过拖拽方式自定义威胁检测模型，实现无代码的建模。 |
| | 46 | | 第三方算法模型导入与运行，编码实现的检测模型。 |
| | 47 | | 导入用户自定义函数的方式，实现检测算子的定制个性化需求。 |
| | 48 | | 对模型进行在线调试功能，可以在页面测试规则的运行结果。 |
| | | | |

| | | | |
|----|--------------|--------------|---|
| 49 | 批流画布建模工具 | 批流画布工具 | 对模型进行指标监控，包括但不限于：模型持续运行时间、待处理数据量、输入数据量、输出数据量、异常数据量。 |
| 50 | | | 对模型进行异常监控、包括能查看异常原因，异常数据。 |
| 51 | | | 多种字段比较运算符，包括但不限于=、!=、>、>=、Contain、Exist、Not Exist、Like、Rlike、Match、in、正则表达式等。 |
| 52 | | | ANSI SQL语法对数据进行多维分析、数据透视、数据筛选等，且能够对任意字段进行组合查询；常规的统计分析函数，至少包括Count、Sum、Avg、Max、Min等。 |
| 53 | | | 提供基础模板、统计类模板、时序类模板。基础模版与或非过滤关系；统计类模板计数不去重（having count）、计数去重（having count(distinct))、求和（having sum）；时序模板(follow by)；并且多个模板组合。 |
| 54 | | | 对模型运行状态进行监控、资源使用情况进行监控。 |
| 55 | SOAR自动编排响应工具 | SOAR自动编排响应工具 | 通过的拖拽方式灵活自定义编排威胁的响应处置流程。 |
| 56 | | | 通过SOAR编排实现同网络安全设备的联动，包括防火墙、EDR等进行联动，实现对威胁的快速响应与处置。 |
| 57 | | | 通过SOAR编排实现威胁的自动化分析研判、响应处置。 |
| 58 | | | 提供自动化处置的剧本，能够在部分安全场景下实现自动化或半自动化的对威胁进处置。 |
| 59 | SPL检索工具 | SPL检索工具 | 管道式SPL语句，字段过滤（filter）、聚合(agg)、排序(sort)、分页(page)、高亮(highlight)。 |
| 60 | | | 界面可视化简易筛选、交互式字段筛选。 |
| 61 | | | 对检索结果数据以柱状图直观展示，体现数据趋势。 |
| 62 | 自定义BI | 自定义BI | 通过拖拽式的自定义BI方式配置仪表盘。 |
| 63 | | | 自定义BI的数据源ES、mpp类数据库。 |

| | | | |
|----|---------|---------------|--|
| 64 | 流程自定义工具 | 安全运营流程自定义 | 可通过安全运营工具，创建安全运营流程用以辅助日常安全运营工作，如：资源申请、公文下发等。 |
| 65 | | 安全运营流程节点自定义 | 可对新增或已有的安全运营流程各个节点进行新增、删减、顺序调整等操作，匹配安全运营流程节点中各个组织、责任人的加签、处置、跳转等场景。 |
| 66 | | 安全流程节点公共字段自定义 | 可对各安全运营流程节点的公共字段（内容）进行调整，如：名称、内容、通知放、抄送方、附件添加、建议、评价等，满足各流程节点的推动所需的相关信息。 |
| 67 | 基础管理 | 用户管理 | 对系统用户进行权限分离、满足三权的管理要求。 |
| 68 | | 设备管理 | 对接入平台的网络安全设备进行管理，以及免密认证登陆。 |
| 69 | | 黑白名单 | 平台对告警黑白名单设置，包括按照源IP、目的IP、模型ID、生效时间等参数进行配置。 |
| 70 | 等级保护 | 等级保护管理 | 对等级保护建设整改过程中系统定级、差距分析、备案、整改、测评过程中产生的文档结论进行统计归档，并使用可视化的统一界面进行展现与管理。 |
| 71 | | 等保报告查询 | 基于年份、系统名称，报告名称等不同条件检索等保建设过程中的文档报告。 |
| 72 | | 文档知识库 | 导入内部法律、内部制度、外部法律、外部制度等文档知识。 |
| 73 | | 合规自检 | 业务合规基线检查，管控业务安全，实时监测等保差距项和高风险项，避免策略变更导致不合规，有效满足不定期抽查和复测场景。 |
| 74 | 运维管理 | RestAPI接口 | 平台通过RESTful API接口对平台数据资源的“开放”与“共享”，第三方平台可获取受监控IP组、资产信息、风险业务与终端、漏洞详情、弱密码和明文传输等信息。 |
| 75 | | Kafka接口 | 平台通过kafka将产生的安全事件发送给其他平台，第三方平台可获取受监控威胁等级，IP组，安全事件，漏洞详情，风险业务及终端，攻击类型 等。 |

15.安全运营服务

根据国家的相关法律法规要求，以及自治区电子政务外网的安全运营实际需求，供应商需提供的安全运营服务包括但不限于如下，在服务过程中需按照采购人的要求优化调整。

以下安全运营服务必须全部满足。

| 序号 | 项目 | 子项 | 服务内容描述 |
|----|---------|-----------|---|
| 1 | 资产识别与梳理 | 资产发现与识别 | 需要摸清政务外网各类资产状况，借助资产梳理工具对用户资产进行全面发现和深度识别，并在后续服务过程中触发资产变更等相关服务流程，确保资产信息的准确性和全面性。 |
| | | 资产信息梳理与管理 | 结合安全工具发现的资产信息，首次进行服务范围内资产的全面梳理（梳理的信息包含支撑业务系统运转的操作系统、数据库、中间件、应用系统的版本，类型，IP地址；应用开放协议和端口；应用系统管理方式、资产的重要性以及网络拓扑等），并将信息录入到安全监测平台中进行管理；当资产发生变更时，对变更信息确认与更新。 |
| 2 | 安全现状评估 | 脆弱性评估 | 系统与Web漏洞扫描：对操作系统、数据库、常见应用/协议、Web通用漏洞与常规漏洞进行漏洞扫描。 |
| | | | 弱口令扫描：实现信息化资产不同应用弱口令猜解检测。 |
| | | | 基线配置核查：检查支撑信息化业务的主机操作系统、数据库、中间件的基线配置情况，确保达到相应的安全防护要求。检查项包含但不限于帐号和口令管理、认证、授权策略、网络与服务、进程和启动、文件系统权限、访问控制等配置情况。 |
| | | 病毒类事件评估 | 勒索病毒事件分析：分析判断主机是否感染了勒索病毒；是否已感染勒索病毒文件；根据已发生的漏洞攻击行为分析判断是否存在勒索病毒攻击等。 |
| | | | 挖矿病毒事件分析：分析是否感染了挖矿病毒/木马；是否处于挖矿状态；根据已发生的漏洞攻击行为分析判断是否存在以植入挖矿木马为目的的漏洞攻击等。 |
| | | | 蠕虫病毒事件：确认文件是否被感染，定位失陷的代码并进行修复。 |
| | | 攻击行为评估 | 针对漏洞利用攻击行为、Webshell上传行为、Web系统目录遍历攻击行为、SQL注入攻击行为、信息泄露攻击行为、口令暴力破解攻击行为、僵尸网络攻击行为、系统命令注入攻击行为及僵尸网络攻击行为进行分析评估，判断攻击行为是否成功以及业务风险点。 |

| | | | | | |
|--|--|---|------|---|--|
| | | | | 失陷类事件 评估 | <p>失陷主机分析：对失陷主机进行分析研判（如后门脚本类事件），并给出修复建议。</p> <p>潜伏威胁分析：分析主机的非法外联威胁行为，判断是否存在潜伏威胁，并给出解决建议。含：对外攻击、APT C&C通道、隐藏外联通道等外联威胁行为。</p> |
| | | 3 | 问题处置 | 脆弱性问题 处置 病毒类事件 处置 入侵攻击行 为处置 失陷类事件 处置 | <p>针对内网脆弱性进行分析研判，并给出修复建议。</p> <p>针对病毒类事件，使用病毒处置工具进行查杀，确保主机安全。</p> <p>针对分析研判确认的入侵行为，给出策略调整建议。</p> <p>针对勒索、挖矿类事件，主导处置工作，提供溯源服务；定位恶意文件路径并提供查杀指导；并分析有无异常进程与服务，发现异常进行通告。</p> <p>针对后门脚本类事件，主导处置工作，对感染主机进行全面后门脚本查杀，并提供溯源服务。</p> <p>针对隐藏通信通道、可疑外发行为，给出修复建议，提供溯源服务。配合定位异常进程以及恶意文件，提供查杀建议。</p> |
| | | 4 | 漏洞管理 | 漏洞分析与 管理 弱口令分析 与管理 最新漏洞预 警与响应 | <p>漏洞扫描与验证：针对资产的系统漏洞和Web漏洞进行全量扫描，并针对发现的漏洞进行验证，验证漏洞在已有的安全体系发生的风险及分析发生后可造成的危害。</p> <p>漏洞修复优先级排序与通告：基于漏洞扫描结果、资产重要性及漏洞的威胁情报，对漏洞进行重要性排序，确定修复的优先级。</p> <p>漏洞落地性处置建议：对漏洞进行分类并书写漏洞分类处置方案，并跟踪修复情况。</p> <p>漏洞复测与状态追踪：对修复的漏洞进行复测，制定漏洞闭环服务报告。</p> <p>实现信息化资产不同应用弱口令猜解检测，有针对性的进行内网弱口令检测，跟踪修复状态。</p> <p>资产指纹信息梳理：梳理信息化资产详情（含操作系统、中间件、数据库、应用框架，开发语言等指纹信息）并将梳理的信息录入安全监测平台。</p> <p>最新漏洞预警与排查：最新漏洞与详细资产信息进行匹配，对最新漏洞进行预警与排查。预警信息中包含最新漏洞信息、影响资产范围。</p> |

| | | | |
|---|------|-----------|--|
| 5 | 威胁管理 | 漏洞协助处置 | 最新漏洞处置指导：一旦确认漏洞影响范围后，提供专业的处置建议，处置建议包含两部分，补丁方案以及临时规避措施。 |
| | | | 最新漏洞复测与状态跟踪：对最新漏洞建立状态追踪机制，跟踪修复状态。 |
| | | | 制定处置方案：根据实际业务场景需求，制定可行的漏洞处置方案。 |
| | | | 处置方案验证：根据漏洞处置方案，在测试环境中开展漏洞处置方案验证工作，观察处置方案对测试环境产生的影响，并提供最优修复方案建议。 |
| | | | 漏洞处置实施：对漏洞进行处置工作，并验证漏洞是否依然存在以及配合验证业务影响程度。 |
| | | | |
| | 威胁管理 | 威胁分析与通告 | 结合大数据分析提供安全事件发现服务：将海量安全数据脱敏，包括漏洞信息、共享威胁情报、异常流量、攻击日志、病毒日志等数据，经由大数据处理平台使用多种数据分析算法模型进行数据归因关联分析，实时监测网络安全状态,发现各类安全事件。 |
| | | | 实时监测网络安全状态，对攻击事件自动化生成工单,及时进行分析与预警。 |
| | | | 实时监测网络安全状态，对病毒事件自动化生成工单,及时进行分析与预警。病毒类型包含勒索型、流行病毒、挖矿型、蠕虫型、外发DOS型、C&C访问型、文件感染型、木马型等。 |
| | | | 针对每一类威胁，进行深度分析验证，分析判断是否存在其他可疑主机。 |
| | | 流行威胁通告与排查 | 结合威胁情报，排查是否对用户资产造成威胁并通知用户，协助及时进行安全加固。 |
| | | 主动分析与响应 | 主动分析病毒类的安全事件：针对业务资产使用病毒处置工具进行病毒查杀。 |
| | | | 主动分析攻击类的安全事件：通过攻击日志分析，发现持续性攻击，立即采取行动实时对抗，提供攻击类安全事件的处置建议。 |
| | | | 主动分析漏洞利用类的安全事件并验证该漏洞是否利用成功，提供工具协助处置。 |
| | | | 主动分析失陷类的安全事件并协助用户处置，并提供溯源服务。 |
| | | | 策略调配：新增资产、业务变更策略调优服务，业务变更时策略随业务变化而同步更新。 |
| | | | |

| | | | | | | | |
|--|--|--|--|-----------------------|------------------------|---|---|
| | | | | | 策略管理 | 策略定期管理：对安全策略进行统一管理工作，确保安全策略始终处于最优水平，针对威胁能起到最好的防护效果。 | |
| | | | | | | 策略调整：根据安全事件分析的结果以及处置方式，按需对安全策略进行调整工作。 | |
| | | | | | 持续攻击对抗 | 通过攻击日志分析，发现持续性攻击，立即采取行动实时对抗。 | |
| | | | | | | 通过全网大数据分析，发现有攻击行为，立即采取行动封锁。 | |
| | | | | 6 | 事件管理 | 事件分析与处置 | 对系统上报的安全事件进行及时响应。 |
| | | | | | | | 实时针对异常流量分析、攻击日志和病毒日志分析，经过海量数据脱敏、聚合发现安全事件。 |
| | | | | | | | 针对分析得到的勒索病毒、挖矿病毒、篡改事件、webshell、僵尸网络等安全事件，通过工具和方法对恶意文件、代码进行清除，快速恢复业务，消除或减轻影响。 |
| | | | | | | 应急响应 | 入侵影响抑制：通过事件检测分析，提供抑制手段，降低入侵影响，协助快速恢复业务。 |
| | | | | | | | 入侵威胁清除：排查攻击路径，恶意文件清除。 |
| | | | | | | | 入侵原因分析：还原攻击路径，分析入侵事件原因。 |
| | | | | | | | 加固建议指导：结合现有安全防御体系，进行安全加固、提供整改建议、防止再次入侵。 |
| | | | | | | 7 | 运营可视 |
| | | | | 展示所有事件监测结果、防御过程和防御结果。 | | | |
| | | | | 展示所有服务内容、流程和事件处理进展。 | | | |
| | | | | 定期安全运营汇报 | 定期总结阶段性安全运营情况，并进行总结汇报。 | | |
| | | | | | | 渗透测试方案 | 信息系统在正常运行前提下，模拟黑客攻击行为通过远程或本地方式对信息系统进行非破坏性的入侵测试，查找针对应用程序的各种漏洞，发现在系统复杂结构中的最脆弱链路并针对安全隐患提出解决办法，保证信息系统安全。应根据重要业务系统结构，设计针对性的渗透测试方案，包括渗透方法和流程、渗透测试风险评估和控制方案、渗透测试采用的检测工具、渗透测试所面临的主要风险及相应的风险规避措施等。 |
| | | | | | | | |

| | | | |
|---|------|----------|--|
| 8 | 渗透测试 | 渗透测试内容 | <p>每次在政务云上筛选不少于10个的平台/应用进行渗透测试。平台/应用由服务商评估筛选，采购人可以根据需要选择某个平台/应用。</p> <p>通过模拟黑客攻击行为通过本地或远程方式对目标对象进行非破坏性的入侵测试。</p> <p>渗透测试应包括以下的漏洞：WEB应用系统渗透、主机操作系统渗透、数据库系统渗透等；</p> <p>渗透测试内容包括身份验证类、会话管理类、访问控制类、输入处理类、信息泄露类、第三方应用类等；</p> <p>渗透测试应使用不同技术手段发现不同维度的漏洞，并进行验证，形成记录和报告；</p> <p>渗透测试具备以目标业务系统为跳板进行横向渗透，发掘更深层次的漏洞并展现漏洞被利用后的危害。</p> |
| | | 应急演练 | <p>使用安全工具，演练模拟信息安全攻击事件，通过演练锻炼人员的实际处理能力，检验人员对网络安全事件、攻击对抗、应急处理相关制度掌握情况，验证应急处置方案的有效性与可行性，根据可能面临的主要风险和系统特点，检验应急处理流程及突发安全事件的处理能力。</p> |
| 9 | 报告输出 | 安全监测运营报告 | <p>《电子政务外网安全监测运营日报》，每天一次；</p> <p>《电子政务外网安全监测运营周报》，每周一次；</p> <p>《电子政务外网安全监测运营月度综合分析报告》，每月度一次；</p> <p>《电子政务外网安全监测运营季度综合分析报告》，每季度一次；</p> <p>《电子政务外网安全监测运营年度综合分析报告》，每年度一次；</p> <p>《电子政务外网重保安全监测报告》，重保期间；</p> <p>《电子政务外网事件分析与处置报告》，按需；</p> <p>《电子政务外网安全通告》，按需；</p> <p>《电子政务外网资产清单》，按需；</p> <p>《电子政务外网漏洞扫描报告》，每季度一次；</p> <p>《电子政务外网基线评估报告》，每季度一次；</p> <p>《电子政务外网渗透测试报告》，每半年一次；</p> <p>《电子政务外网应急演练报告》，每年一次；</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> |

| | | | |
|----|--------|--------|--|
| 10 | 安全测评服务 | 安全测评服务 | <p>一、在合同签订后组织第三方有资质单位对以下系统开展一次等保测评服务、一次密评服务：</p> <p>1、内蒙古自治区政务云密码服务平台</p> <p>2、云上北疆系统</p> <p>3、内蒙古自治区政务云（广电节点）云平台</p> <p>4、内蒙古自治区政务云（联通节点）云平台</p> <p>二、在服务期内组织第三方有资质单位对以下系统开展一次风险评估服务：</p> <p>1、内蒙古自治区政务云密码服务平台</p> <p>2、云上北疆系统</p> <p>3、内蒙古自治区政务云（广电节点）云平台</p> <p>4、内蒙古自治区政务云（联通节点）云平台</p> <p>三、在服务期内对安全监测平台开展一次等保测评服务、一次风险评估服务。</p> <p>四、配合政务云上的信息系统用户提供等保测评和安全风险评估相关材料。</p> <p>以上服务均由服务商负责完成。</p> |
| 11 | 工具要求 | 工具要求 | <p>提供安全漏洞扫描器工具、等级保护合规性检查工具。</p> <p>安全漏洞扫描器工具：扫描对象包含主流网络设备、操作系统、数据库、中间件等，快速发现网络和系统存在的漏洞风险隐患，及时处置。安全漏洞扫描器工具需具备7天内完成自治区电子政务外网和三个政务云中心承载业务系统的漏洞扫描能力。</p> <p>等级保护合规性检查工具：以等级保护2.0的安全要求为依据，自动化检测业务系统的合规情况，快速定位差距项和高风险项，提供清晰的整改指引，实现安全合规。</p> |
| 12 | 培训服务 | 培训服务 | <p>供应商应提供不少于45人天的现场安全技术和管理培训课程，相关培训课程可以在项目实施时根据实际需求由采购人灵活安排。</p> |

保密承诺要求：

1、在参与该项目采购活动过程中，投标人应对本项目有关技术资料、商业秘密及相关信息保密。

2、投标人中标后，应当与采购人签订保密协议，严格按照采购人的要求，不得以任何方式向任何其他组织或个人泄露、转让、许可使用、交换、赠与项目相关信息和资料等。中标人违反保密协议，一经查出，采购人有权追究其相应责任，有权要求中标人赔偿因此所造成的全部损失。

售后服务要求：

1、服务质量要求

| | | |
|-------------------------------------|--|---|
| | | <p>在服务期内，投标人应对服务产品提供质保服务，对出现故障的设备免费进行现场维修、更换，更换的设备或部件必须是全新同型设备或备件且不收取任何费用，对本次项目范围内软件的修改、完善、补丁更新以及版本升级，在服务期内提供不收取任何费用。</p> <p>2、技术服务体系</p> <p>投标人必须有统一、完善的技术支持服务体系，要求能够为自治区电子政务外网安全监测提供高效的技术支持服务。投标人应在售后服务工作材料中详细介绍其技术支持服务体系和服务能力。</p> <p>3、技术运营服务质量</p> <p>投标人应向采购人提供7×24小时安全运营服务及远程技术支撑，对发生的问题必须立即做出实质性响应，提出故障解决方案。按采购人要求，安排专业技术人员进行故障处置，恢复相关系统正常运行。投标人需列明承诺的服务响应时间、故障解决时间等。</p> |
| 打“★”号条款为实质性条款，若有任何一条负偏离或不满足则导致响应无效。 | | |

采购包2：

标的名称：网络安全检查服务

| 序号 | 参数性质 | 技术参数与性能指标 |
|----|------|---|
| 1 | ★ | 总体目标： 内蒙古自治区大数据中心运维的自治区本级政府信息系统进行全面网络与数据安全检查，主要包括系统管理合规性检查、资产梳理识别、安全漏洞扫描、渗透测试、数据安全风险检查、移动端APP/小程序安全检测、安全基线配置核查、APT风险检查、高危问题复测检查服务等。 |
| 2 | ★ | 服务人员： 提供检查人员高级安全服务工程师1名，中级安全服务工程师4名，服务期1年。 |
| 3 | ★ | 实施范围： 对自治区大数据中心负责运维的系统进行检查，即数据资源服务处、信息技术服务一至十一处，检查系统的数量不少于60个。 |
| 4 | ★ | 服务工具要求： 依据服务内容，提供相关网络与数据安全检查工具。 |
| | | <p>服务内容：</p> <p>1.系统管理合规性检查</p> <p>聚焦于对自治区大数据中心负责运维的系统，全面核查系统是否严格遵循《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国密码法》以及《信息安全技术 网络安全等级保护基本要求》《信息安全技术 信息系统密码应用基本要求》等一系列相关法律法规和标准规范，落实等级保护备案与测评、商用密码应用安全性评估、网络安全管理领导、机构组织、相关人员、相关制度建设等工作。交付物包括但不限于：《系统管理合规性检查报告》。</p> <p>2.资产梳理识别服务</p> <p>对自治区大数据中心负责运维的系统进行资产梳理识别服务；在甲方人员在配合下，服务人员采用实地检查、问询和工具探查扫描的方式调查统计信息系统所涉及资产，填写相关资产调研表，并对信息资产IP地址、端口和服务等进行探测识别。交付物包括但不限于：《资产梳理识别服务报告》。</p> |

3.安全漏洞扫描服务

对自治区大数据中心负责运维系统的相关服务器、网络设备、安全设备、数据库、中间件等通过专业漏洞扫描工具并结合人工核验的方式进行漏洞扫描，对漏洞提供修复建议。交付物包括但不限于：《漏洞扫描报告》。

4.渗透测试服务

在获取责任单位或处室授权的前提下，对自治区大数据中心负责运维系统进行受控的、非破坏性的渗透测试，查找存在的安全隐患。渗透测试内容要求涵盖：身份验证类，如用户注册、登录、密码修改和重置、验证码绕过、用户锁定等漏洞；会话管理类：如cookie重放攻击、会话令牌分析、会话令牌泄露、会话固定攻击、跨站请求伪造等；访问控制类：如功能滥用、垂直权限提升、水平权限提升等；输入处理类，如SQL注入、文件上传、任意文件下载、XML注入、目录穿越、SSRF、本地文件包含、远程文件包含、远程代码执行、反射型跨站脚本、存储型跨站脚本、DOM-based跨站脚本、服务端URL重定向等；信息泄露类：如error code、stack traces、敏感信息等；第三方应用类，如中间件等。交付物包括但不限于：《渗透测试报告》。

5.数据安全风险检查

依据《数据安全法》要求，规范自治区大数据中心负责运维系统数据安全防护、数据保护工作。针对具有收集、使用、重要数据功能的业务系统，完成数据存储、数据备份、数据流相关风险检查。交付物包括但不限于：《数据安全风险检查报告》。

6.移动端APP/小程序安全检测

对自治区大数据中心负责运维的系统中存在的移动端，如移动端APP、小程序进行安全检测。内容包含但不限于程序机密性检测：检查代码混淆、DEX保护监测、SO保护监测、程序签名检测等安全问题。组件安全检测：扫描代码组件的Activity、Broadcast Receiver、service、Content Provider存在的安全漏洞。数据及业务安全检测：检测APP是否存在数据安全问题，用户账号密码泄漏等风险。交付物包括但不限于：《移动APP/小程序安全检测报告》。

7.安全基线配置核查

根据相关标准和规范，对自治区大数据中心负责运维系统相关网络设备、安全设备、服务器操作系统、数据库、中间件等进行抽样安全配置核查，识别出现有安全配置与普适性规范或行业规范的安全配置要求之间的差距，并提供相关加固建议。在服务过程中除已知、未知的漏洞外，对自治区大数据中心负责运维的系统范围内安全防护设备策略的弱点或策略上的缺陷进行核查，提供策略加固建议。服务交付物包括但不限于：《基线配置与安全配置策略核查报告》。

8.APT风险检查

基于全流量分析识别技术，旁路采集、分析系统网络流量，通过威胁情报系统检测APT威胁，通过回溯分析数据包特征、异常网络行为，发现潜伏已久的APT攻击。交付物包括但不限于：《APT风险检查报告》。

9.高危问题复测检查

| | | |
|-------------------------------------|--|---|
| | | 针对以上各项检查服务中发现的高危问题，在自治区大数据中心要求的高危问题整改修复时间后的一周内，安排专业人员依据之前检查的详细记录与报告，对整改情况进行全面复测。服务交付物包括但不限于：《高危问题复测检查报告》。 |
| 打“★”号条款为实质性条款，若有任何一条负偏离或不满足则导致响应无效。 | | |

第四章 投标人应当提交的资格、资信证明文件

投标人应提交证明其有资格参加投标和中标后有能力履行合同的相关文件，并作为其投标文件的一部分，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。如投标人是企业（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”；如投标人是事业单位，要提供有效的“事业单位法人证书”；投标人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；如投标人是个体工商户，要提供有效的“个体工商户营业执照”；如投标人是自然人，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投标人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、按照招标文件要求，投标人应当提交的其他资格、资信证明文件。

第五章 评标

一.评标要求

1.评标方法

详见须知前附表

2.评标原则

2.1评标活动遵循客观、公正、审慎的原则，以招标文件和投标文件为评标的基本依据，并按照招标文件规定的评标方法和评标标准进行评标。

2.2具体评标事项由评标委员会负责，并按招标文件规定的办法进行评审。

2.3合格投标人不足三家的，不得评标。

3.评标委员会

由采购人代表和评审专家两部分共7人组成，其中由评审专家库产生的评审专家5人，由采购人派出的采购人代表2人。

3.1评标委员会由采购人代表和评审专家组成，成员人数应当为5人及以上单数，其中评审专家不得少于成员总数的三分之二。

3.2评标委员会成员有下列情形之一的，应当回避：

（1）参加采购活动前3年内,与投标人存在劳动关系,或者担任投标人的董事、监事,或者是投标人的控股股东或实际控制人；

（2）与投标人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）与投标人有其他可能影响政府采购活动公平、公正进行的关系。

3.3评标委员会负责具体评标事务，并独立履行下列职责：

（1）审查、评价投标文件是否符合招标文件的商务、技术等实质性要求；

（2）要求投标人对投标文件有关事项作出澄清或者说明；

（3）对投标文件进行比较和评价；

（4）确定中标候选人名单，以及根据采购人委托直接确定中标人；

（5）向采购人、采购代理机构或者有关部门报告评标中发现的违法行为；

（6）法律法规规定的其他职责。

4.澄清

对于投标文件中含义不明确、同类问题表述不一致或者有明显文字和计算错误的内容，评标委员会应当以书面形式要求投标人作出必要的澄清、说明或者补正。

投标人的澄清、说明或者补正应当采用书面形式，并加盖公章，或者由法定代表人或其授权的代表签字。投标人的澄清、说明或者补正不得超出投标文件的范围或者改变投标文件的实质性内容。

4.1评标委员会不接受投标人主动提出的澄清、说明或补正。

4.2评标委员会对投标人提交的澄清、说明或补正有疑问的，可以要求投标人进一步澄清、说明或补正。

5.有下列情形之一的，视为投标人串通投标，其投标无效：

（1）不同投标人的投标文件由同一单位或者个人编制，包括但不限于不同投标人上传的投标文件项目内部识别码一致的情形；

（2）不同投标人委托同一单位或者个人办理投标事宜；

（3）不同投标人的投标文件载明的项目管理成员或者联系人员为同一人；

（4）不同投标人的投标文件异常一致或者投标报价呈规律性差异；

(5) 不同投标人的投标文件相互混装;

(6) 不同投标人的投标保证金从同一单位或个人的账户转出;

6.有下列情形之一的,属于恶意串通投标,其投标无效,并追究法律责任:

(1) 投标人直接或者间接从采购人或者采购代理机构处获得其他投标人的相关情况并修改其投标文件;

(2) 投标人按照采购人或者采购代理机构的授意撤换、修改投标文件;

(3) 投标人之间协商报价、技术方案等投标文件的实质性内容;

(4) 属于同一集团、协会、商会等组织成员的投标人按照该组织要求协同参加政府采购活动;

(5) 投标人之间事先约定由某一特定投标人中标、成交;

(6) 投标人之间商定部分投标人放弃参加政府采购活动或者放弃中标、成交;

(7) 投标人与采购人或者采购代理机构之间、投标人相互之间,为谋求特定投标人中标、成交或者排斥其他投标人的其他串通行为。

7.投标无效的情形

投标人存在下列情况之一的,投标无效:

(1) 未按照招标文件的规定提交投标保证金的;

(2) 投标文件未按招标文件要求签署、盖章的;

(3) 不具备招标文件中规定的资格要求的;

(4) 报价超过招标文件中规定的预算金额或者最高限价的;

(5) 投标文件含有采购人不能接受的附加条件的;

(6) 法律、法规和招标文件规定的其他无效情形。

8.废标的情形

出现下列情形之一的,应予以废标。

(1) 符合专业条件的投标人或者对招标文件作实质响应的投标人不足3家;或参与竞争的核心产品品牌不足3个的;

(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的;

(4) 因重大变故,采购任务取消的;

9.定标

评标委员会按照招标文件确定的评标方法、步骤、标准,对投标文件进行评审。评标结束后,评标委员会根据采购人委托直接确定中标人或者由采购人在评标报告确定的中标候选人名单中按顺序确定中标人。

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,具体按照本招标文件相关要求执行。

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,投标人提供的货物、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，投标人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：

采购包1：

| 序号 | 评审内容 | 适用情形 | 扣除比例 | 具体标准和要求 | 关联投标（响应）文件格式文件 |
|----|-----------------------|------------------|--------|---|----------------|
| 1 | 小型、微型企业，监狱企业，残疾人福利性单位 | 非联合体或联合体各方均为小微企业 | 20.00% | 1、对小、微企业报价给予相应比例的扣除。 2、监狱企业视同小型、微型企业，评审中价格扣除按照小、微企业的扣除比例执行。 3、残疾人福利性单位提供本单位制造的货物、承担的工程或服务，或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），视同小型、微型企业，按小微企业的扣除比例执行。 | 开标一览表 分项报价表 |

采购包2：

| 序号 | 评审内容 | 适用情形 | 扣除比例 | 具体标准和要求 | 关联投标（响应）文件格式文件 |
|----|------|------|------|---------|----------------|
| 无 | | | | | |

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，投标人应提供《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》。投标人应当按照《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。

投标人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.评标程序

1.符合性审查

1.1依据招标文件的规定，从投标文件的有效性、完整性和对招标文件的响应程度进行审查，以确定是否满足招标文件的实质性要求。

1.2符合性审查中有任意一项未通过的，审查结果为未通过。投标人未通过符合性审查的，投标无效。

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 | 投标文件的签署、盖章、涂改、删除、插字、公章使用等符合招标文件要求；投标文件文件的格式、文字、目录等符合招标文件要求或对投标无实质性影响。 |
| 4 | 主要商务条款 | 审查投标人出具的“满足主要商务条款的承诺”，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.投标文件应当对招标文件提出的要求和条件作出明确响应并满足招标文件全部实质性要求。 |
| 6 | 其他要求 | 招标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。 |

采购包2：

| 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 | 投标文件的签署、盖章、涂改、删除、插字、公章使用等符合招标文件要求；投标文件文件的格式、文字、目录等符合招标文件要求或对投标无实质性影响。 |
| 4 | 主要商务条款 | 审查投标人出具的“满足主要商务条款的承诺”，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.投标文件应当对招标文件提出的要求和条件作出明确响应并满足招标文件全部实质性要求。 |
| 6 | 其他要求 | 招标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。 |

2.投标报价审查

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，有可能影响产品质量或者不能诚信履约的，应当要求其在评标现场合理的时间内提供书面说明，必要时提交相关证明材料；投标人不能证明其报价合理性的，评标委员会应当将其作为无效投标处理。

3.政府采购政策功能落实

对于小型、微型企业、监狱企业或残疾人福利性单位给予价格扣除。

4.相同品牌审查

采用最低评标价法的采购项目，提供相同品牌产品的不同投标人参加同一合同项下投标的，以其中通过资格审查、符合性审查且报价最低的参加评标；报价相同的，由采购人或者采购人委托评标委员会按照招标文件规定的方式确定一个参加评标的投标人，招标文件未规定的采取随机抽取方式确定，其他投标无效。

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

多家投标人提供的核心产品品牌相同的，按上述规定处理。

5.详细评审

采购包1:

采购包1:

| 评审内容 | | 评审标准 | | | |
|--------|------|--|----|-------|----------------|
| 分值构成 | | 技术部分 82.00 分 商务部分 8.00 分 报价得分 10.00 分 | | | |
| 评审因素分类 | 评审内容 | 具体标准和要求 | 分值 | 客观/主观 | 关联投标（响应）文件格式文件 |

| | | | | | |
|--|------|--|---------|----|--|
| | 满足程度 | 根据投标服务与招标文件要求的满足程度进行评价：“服务产品和运营要求”章节，“√”表示重要技术参数，重要技术参数全部满足，得10分，有一项不满足，本项得0分；在此基础上，“0”为一般性技术参数，每有一项不满足扣0.5分，扣完为止。 | 10.0000 | 客观 | 封面 目录 投标人（供应商）应提交的相关证明 投标人业绩情况表 投标人基本情况表 具备履行合同所必需设备和专业技术能力的声明函 主要商务要求承诺书 具有良好的商业信誉和健全的财务会计制度的相关材料 技术偏离表 具有独立承担民事责任的能力证明文件 联合体协议 项目实施方案、质量保证及售后服务承诺 投标人承诺函 依法缴纳税收和社会保障资金的良好记录的相关材料 项目组成人员一览表 中小企业声明函 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 缴纳投标保证金证明材料 其他材料 法定代表人授权委托书 监狱企业证明文件 残疾人福利性单位声明函 |
| | | | | | |

| | | | | |
|------|--|--------|----|--|
| 项目经理 | 项目经理需同时具有人力资源和社会保障部颁发的计算机技术与软件专业技术资格高级证书的得2分。 注：需提供人员证书的扫描件，不提供不得分。 | 2.0000 | 客观 | 封面 目录 投标人（供应商）应提交的相关证明 投标人业绩情况表 投标人基本情况表 具备履行合同所必需设备和专业技术能力的声明函 主要商务要求承诺书 具有良好的商业信誉和健全的财务会计制度的相关材料 技术偏离表 具有独立承担民事责任的能力证明文件 联合体协议 项目实施方案、质量保证及售后服务承诺 投标人承诺函 依法缴纳税收和社会保障资金的良好记录的相关材料 项目组成人员一览表 中小企业声明函 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 缴纳投标保证金证明材料 其他材料 法定代表人授权委托书 监狱企业证明文件 残疾人福利性单位声明函 |
|------|--|--------|----|--|

| | | | | |
|--------|---|---------------|----|--|
| 项目实施团队 | <p>项目实施团队具有人力资源和社会保障部颁发的计算机技术与软件专业技术资格中级以上证书的，每提供一人得0.5分，最高得 4.5分。</p> <p>注：需提供人员证书的扫描件，1人1证计分，如1人多证，只计1次分数，不提供不得分。</p> | 4.5000 | 客观 | 封面 目录 投标人（供应商）应提交的相关证明 投标人业绩情况表 投标人基本情况表 具备履行合同所必需设备和专业技术能力的声明函 主要商务要求承诺书 具有良好的商业信誉和健全的财务会计制度的相关材料 技术偏离表 具有独立承担民事责任的能力证明文件 联合体协议 项目实施方案、质量保证及售后服务承诺 投标人承诺函 依法缴纳税收和社会保障资金的良好记录的相关材料 项目组成人员一览表 中小企业声明函 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 缴纳投标保证金证明材料 其他材料 法定代表人授权委托书 监狱企业证明文件 残疾人福利性单位声明函 |
|--------|---|---------------|----|--|

| | | | | | |
|-------------|--------------|--|----------------|-----------|--|
| <p>技术评审</p> | <p>服务方案1</p> | <p>根据投标人针对本项目提供的服务方案1进行评审：①项目总体实施方案；②提出与国家平台、盟市系统等单位对接方案；③与现网安全系统和安全设备对接方案等。本项最多得12分，其中每小项最多得4分；每小项内容每存在一处缺陷的扣1分，扣完为止。不提供不得分。（注：缺陷是指非专门针对本项目、不适用项目实际情形、内容不完整、缺少关键节点，只有简单描述无实质性内容、套用其它项目方案、内容前后矛盾、涉及的规范及标准错误、地点区域错误、不利于项目实施。）</p> | <p>12.0000</p> | <p>主观</p> | <p>封面 目录 投标人（供应商）应提交的相关证明 投标人业绩情况表 投标人基本情况表 具备履行合同所必需设备和专业技术能力的声明函 主要商务要求承诺书 具有良好的商业信誉和健全的财务会计制度的相关材料 技术偏离表 具有独立承担民事责任的能力证明文件 联合体协议 项目实施方案、质量保证及售后服务承诺 投标人承诺函 依法缴纳税收和社会保障资金的良好记录的相关材料 项目组成人员一览表 中小企业声明函 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 缴纳投标保证金证明材料 其他材料 法定代表人授权委托书 监狱企业证明文件 残疾人福利性单位声明函</p> |
|-------------|--------------|--|----------------|-----------|--|

| | | | | |
|-------|---|---------|----|--|
| 服务方案2 | 根据投标人针对本项目提供的服务方案2进行评审：①采集探针部署服务方案；②安全系统及设备运行维护方案；③弱口令专项排查服务方案。本项最多得12分，其中每小项最多得4分；每小项内容每存在一处缺陷的扣1分，扣完为止。不提供不得分。（注：缺陷是指非专门针对本项目、不适用项目实际情形、内容不完整、缺少关键节点，只有简单描述无实质性内容、套用其它项目方案、内容前后矛盾、涉及的规范及标准错误、地点区域错误、不利于项目实施。） | 12.0000 | 主观 | 封面 目录 投标人（供应商）应提交的相关证明 投标人业绩情况表 投标人基本情况表 具备履行合同所必需设备和专业技术能力的声明函 主要商务要求承诺书 具有良好的商业信誉和健全的财务会计制度的相关材料 技术偏离表 具有独立承担民事责任的能力证明文件 联合体协议 项目实施方案、质量保证及售后服务承诺 投标人承诺函 依法缴纳税收和社会保障资金的良好记录的相关材料 项目组成人员一览表 中小企业声明函 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 缴纳投标保证金证明材料 其他材料 法定代表人授权委托书 监狱企业证明文件 残疾人福利性单位声明函 |
|-------|---|---------|----|--|

| | | | | |
|--------|--|---------|----|--|
| 运营服务方案 | <p>1.需根据本项目的特点，围绕构建7×24小时持续、主动、闭环的安全运营体系为目标，提出针对政务外网资产、漏洞、威胁、事件等要素的运营服务方案1，包括但不限于①运营阶段设计；②安全运营服务内容；③安全运营流程；④安全运营组织建设。本项最多得14分，其中每小项最多得3.5分；每小项内容每存在一处缺陷的扣1分，扣完为止。不提供不得分。（注：缺陷是指非专门针对本项目、不适用项目实际情形、内容不完整、缺少关键节点，只有简单描述无实质性内容、套用其它项目方案、内容前后矛盾、涉及的规范及标准错误、地点区域错误、不利于项目实施。）</p> <p>） 2.根据投标人针对本项目提供的运营服务方案2进行评审：①安全评估方案；②渗透测试方案；③应急演练方案；④培训方案。本项最多得14分，其中每小项最多得3.5分；每小项内容每存在一处缺陷的扣1分，扣完为止。不提供不得分。（注：缺陷是指非专门针对本项目、不适用项目实际情形、内容不完整、缺少关键节点，只有简单描述无实质性内容、套用其它项目方案、内容前后矛盾、涉及的规范及标准错误、地点区域错误、不利于项目实施。）</p> | 28.0000 | 主观 | 封面 目录 投标人（供应商）应提交的相关证明 投标人业绩情况表 投标人基本情况表 具备履行合同所必需设备和专业技术能力的声明函 主要商务要求承诺书 具有良好的商业信誉和健全的财务会计制度的相关材料 技术偏离表 具有独立承担民事责任的能力证明文件 联合体协议 项目实施方案、质量保证及售后服务承诺 投标人承诺函 依法缴纳税收和社会保障资金的良好记录的相关材料 项目组成人员一览表 中小企业声明函 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 缴纳投标保证金证明材料 其他材料 法定代表人授权委托书 监狱企业证明文件 残疾人福利性单位声明函 |
|--------|--|---------|----|--|

| | | | | |
|--------------------|---|---------|----|--|
| 服务水平协议SLA和售后服务承诺方案 | 根据投标人针对本项目提供的提出服务水平协议SLA和售后服务承诺进行评审：①安全事件；②安全威胁；③安全漏洞等。本项最多得10.5分，其中每小项最多得3.5分；每小项内容每存在一处缺陷的扣1分，扣完为止。不提供不得分。（注：缺陷是指非专门针对本项目、不适用项目实际情形、内容不完整、缺少关键节点、套用其它项目方案、内容前后矛盾、涉及的规范及标准错误、不利于项目实施。） | 10.5000 | 主观 | 封面 目录 投标人（供应商）应提交的相关证明 投标人业绩情况表 投标人基本情况表 具备履行合同所必需设备和专业技术能力的声明函 主要商务要求承诺书 具有良好的商业信誉和健全的财务会计制度的相关材料 技术偏离表 具有独立承担民事责任的能力证明文件 联合体协议 项目实施方案、质量保证及售后服务承诺 投标人承诺函 依法缴纳税收和社会保障资金的良好记录的相关材料 项目组成人员一览表 中小企业声明函 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 缴纳投标保证金证明材料 其他材料 法定代表人授权委托书 监狱企业证明文件 残疾人福利性单位声明函 |
|--------------------|---|---------|----|--|

| | | | | | |
|--|------|---|--------|----|--|
| | 保密方案 | <p>根据投标人针对本项目提供的保密方案进行评审：①保密制度；②保密管理及措施。本项最多得3分，其中每小项最多得1.5分；每小项内容每存在一处缺陷的扣0.5分，扣完为止。不提供不得分。（注：缺陷是指非专门针对本项目、不适用项目实际情形、内容不完整、缺少关键节点，只有简单描述无实质性内容、套用其它项目方案、内容前后矛盾、涉及的规范及标准错误、地点区域错误、不利于项目实施。）</p> | 3.0000 | 主观 | <p>封面 目录 投标人（供应商）应提交的相关证明 投标人业绩情况表 投标人基本情况表 具备履行合同所必需设备和专业技术能力的声明函 主要商务要求承诺书 具有良好的商业信誉和健全的财务会计制度的相关材料 技术偏离表 具有独立承担民事责任的能力证明文件 联合体协议 项目实施方案、质量保证及售后服务承诺 投标人承诺函 依法缴纳税收和社会保障资金的良好记录的相关材料 项目组成人员一览表 中小企业声明函 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 缴纳投标保证金证明材料 其他材料 法定代表人授权委托书 监狱企业证明文件 残疾人福利性单位声明函</p> |
| | | | | | |

| | | | | | |
|------|----|--|--------|----|--|
| 商务评审 | 业绩 | <p>投标人自2021年11月起至投标文件递交截止时间止，承接过的同类项目业绩，每提供一个同类项目合同得2分，最多得8分。（注：合同至少包含合同首页、合同服务内容所在页、盖章页等。）</p> | 8.0000 | 客观 | 封面 目录 投标人（供应商）应提交的相关证明 投标人业绩情况表 投标人基本情况表 具备履行合同所必需设备和专业技术能力的声明函 主要商务要求承诺书 具有良好的商业信誉和健全的财务会计制度的相关材料 技术偏离表 具有独立承担民事责任的能力证明文件 联合体协议 项目实施方案、质量保证及售后服务承诺 投标人承诺函 依法缴纳税收和社会保障资金的良好记录的相关材料 项目组成人员一览表 中小企业声明函 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 缴纳投标保证金证明材料 其他材料 法定代表人授权委托书 监狱企业证明文件 残疾人福利性单位声明函 |
|------|----|--|--------|----|--|

| | | | | | |
|-----|-----|--|---------|----|----------------|
| 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）×100×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。 | 10.0000 | 客观 | 分项报价表 开标一览表 |
|-----|-----|--|---------|----|----------------|

价格扣除

| 序号 | 价格扣除评审内容 | 适用情形 | 扣除比例（C1） | 具体标准和要求 | 关联投标（响应）文件格式文件 |
|----|-----------------------|------------------|----------|---|----------------|
| 1 | 小型、微型企业，监狱企业，残疾人福利性单位 | 非联合体或联合体各方均为小微企业 | 20.00% | 1、对小、微企业报价给予相应比例的扣除。2、监狱企业视同小型、微型企业，评审中价格扣除按照小、微企业的扣除比例执行。3、残疾人福利性单位提供本单位制造的货物、承担的工程或服务，或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），视同小型、微型企业，按小微企业的扣除比例执行。 | 分项报价表 开标一览表 |

采购包2：

采购包2：

| 评审内容 | | 评审标准 | | | |
|--------|------|---|----|-------|----------------|
| 分值构成 | | 技术部分 65.00 分 商务部分 25.00 分 报价得分 10.00 分 | | | |
| 评审因素分类 | 评审内容 | 具体标准和要求 | 分值 | 客观/主观 | 关联投标（响应）文件格式文件 |

| | | | | | |
|--|------|---|---------|----|--|
| | 服务方案 | 服务方案符合项目需求且方案详细、实用、可行，方案内容应包含:1.服务实施计划;2.管理合规性检查服务方案; 3.资产梳理识别方案;4.安全漏洞扫描服务方案;5.渗透测试服务方案;6.数据安全风险检查服务方案;7.移动端APP/小程序安全检测服务方案 8.安全基线配置核查服务方案;9.APT风险检查服务方案; 10 . 高危问题复测检查服务方案。本项最多得30分，其中每小项最多得3分；每小项内容每存在一处缺陷的扣1分，扣完为止。不提供不得分。（注：缺陷是指非专门针对本项目、不适用项目实际情形、内容不完整、缺少关键节点，只有简单描述无实质性内容、套用其它项目方案、内容前后矛盾、涉及的规范及标准错误、地点区域错误、不利于项目实施。） | 30.0000 | 主观 | 封面 目录 投标人（供应商）应提交的相关证明 投标人业绩情况表 投标人基本情况表 具备履行合同所必需设备和专业技术能力的声明函 主要商务要求承诺书 具有良好的商业信誉和健全的财务会计制度的相关材料 技术偏离表 具有独立承担民事责任的能力证明文件 联合体协议 项目实施方案、质量保证及售后服务承诺 投标人承诺函 依法缴纳税收和社会保障资金的良好记录的相关材料 项目组成人员一览表 中小企业声明函 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 缴纳投标保证金证明材料 其他材料 法定代表人授权委托书 监狱企业证明文件 残疾人福利性单位声明函 |
| | | | | | |

| | | | | |
|------------------|--|---------------|-----------|--|
| <p>进度及质量控制措施</p> | <p>进度及质量控制符合项目需求且方案详细、实用、可行，方案内容包含:1.服务质量保障措施;2.进度保障措施。本项最多得5分，其中每小项最多得2.5分；每小项内容每存在一处缺陷的扣1分，扣完为止。不提供不得分。（注：缺陷是指非专门针对本项目、不适用项目实际情形、内容不完整、缺少关键节点，只有简单描述无实质性内容、套用其它项目方案、内容前后矛盾、涉及的规范及标准错误、地点区域错误、不利于项目实施。）</p> | <p>5.0000</p> | <p>主观</p> | <p>封面 目录 投标人（供应商）应提交的相关证明 投标人业绩情况表 投标人基本情况表 具备履行合同所必需设备和专业技术能力的声明函 主要商务要求承诺书 具有良好的商业信誉和健全的财务会计制度的相关材料 技术偏离表 具有独立承担民事责任的能力证明文件 联合体协议 项目实施方案、质量保证及售后服务承诺 投标人承诺函 依法缴纳税收和社会保障资金的良好记录的相关材料 项目组成人员一览表 中小企业声明函 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 缴纳投标保证金证明材料 其他材料 法定代表人授权委托书 监狱企业证明文件 残疾人福利性单位声明函</p> |
|------------------|--|---------------|-----------|--|

| | | | | | |
|-------------|---------------|--|---------------|-----------|--|
| <p>技术评审</p> | <p>人员组织方案</p> | <p>项目人员组织方案符合项目需求且方案详细、实用、可行，方案内容包含1.人员组织安排方案及人员组织架构;2.岗位职责及岗位分工。本项最多得4分，其中每小项最多得2分；每小项内容每存在一处缺陷的扣1分，扣完为止。不提供不得分。（注：缺陷是指非专门针对本项目、不适用项目实际情形、内容不完整、缺少关键节点，只有简单描述无实质性内容、套用其它项目方案、内容前后矛盾、涉及的规范及标准错误、地点区域错误、不利于项目实施。）</p> | <p>4.0000</p> | <p>主观</p> | <p>封面 目录 投标人（供应商）应提交的相关证明 投标人业绩情况表 投标人基本情况表 具备履行合同所必需设备和专业技术能力的声明函 主要商务要求承诺书 具有良好的商业信誉和健全的财务会计制度的相关材料 技术偏离表 具有独立承担民事责任的能力证明文件 联合体协议 项目实施方案、质量保证及售后服务承诺 投标人承诺函 依法缴纳税收和社会保障资金的良好记录的相关材料 项目组成人员一览表 中小企业声明函 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 缴纳投标保证金证明材料 其他材料 法定代表人授权委托书 监狱企业证明文件 残疾人福利性单位声明函</p> |
|-------------|---------------|--|---------------|-----------|--|

| | | | | |
|------|--|---------|----|--|
| 测评工具 | 1、投标人提供具有相关安全检查工具，包括漏洞扫描类、攻击溯源类、信息安全漏洞预警类、数据安全类、数据风险评估类，满分得10分，每缺少一项扣2分，扣完为止。(需提供采购发票或软件著作权证书，不提供不得分)。 | 10.0000 | 主观 | 封面 目录 投标人（供应商）应提交的相关证明 投标人业绩情况表 投标人基本情况表 具备履行合同所必需设备和专业技术能力的声明函 主要商务要求承诺书 具有良好的商业信誉和健全的财务会计制度的相关材料 技术偏离表 具有独立承担民事责任的能力证明文件 联合体协议 项目实施方案、质量保证及售后服务承诺 投标人承诺函 依法缴纳税收和社会保障资金的良好记录的相关材料 项目组成人员一览表 中小企业声明函 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 缴纳投标保证金证明材料 其他材料 法定代表人授权委托书 监狱企业证明文件 残疾人福利性单位声明函 |
|------|--|---------|----|--|

| | | | | |
|----------|---|---------|----|--|
| 安全应急服务方案 | <p>应急服务方案符合项目需求且方案详细、实用、可行，方案内容包括：1.定期预防性安全检查方案;2.故障分析及处理方案;3.应急人员组织方案4.应急演练服务方案;5.重要时期安全保障服务方案。本项最多得10分，其中每小项最多得2分；每小项内容每存在一处缺陷的扣1分，扣完为止。不提供不得分。（注：缺陷是指非专门针对本项目、不适用项目实际情形、内容不完整、缺少关键节点，只有简单描述无实质性内容、套用其它项目方案、内容前后矛盾、涉及的规范及标准错误、地点区域错误、不利于项目实施。）</p> | 10.0000 | 主观 | 封面 目录 投标人（供应商）应提交的相关证明 投标人业绩情况表 投标人基本情况表 具备履行合同所必需设备和专业技术能力的声明函 主要商务要求承诺书 具有良好的商业信誉和健全的财务会计制度的相关材料 技术偏离表 具有独立承担民事责任的能力证明文件 联合体协议 项目实施方案、质量保证及售后服务承诺 投标人承诺函 依法缴纳税收和社会保障资金的良好记录的相关材料 项目组成人员一览表 中小企业声明函 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 缴纳投标保证金证明材料 其他材料 法定代表人授权委托书 监狱企业证明文件 残疾人福利性单位声明函 |
|----------|---|---------|----|--|

| | | | | | |
|--|------|--|--------|----|--|
| | 服务承诺 | 服务承诺内容应符合项目需求且方案详细、实用、可行，方案内容包含:1.安全技术培训服务方案及承诺:2.项目履行过程中保密承诺(人员保密实施过程保密、资料保密)。本项最多得6分，其中每小项最多得3分；每小项内容每存在一处缺陷的扣1分，扣完为止。不提供不得分。（注：缺陷是指非专门针对本项目、不适用项目实际情形、内容不完整、缺少关键节点，只有简单描述无实质性内容、套用其它项目方案、内容前后矛盾、涉及的规范及标准错误、地点区域错误、不利于项目实施。） | 6.0000 | 主观 | 封面 目录 投标人（供应商）应提交的相关证明 投标人业绩情况表 投标人基本情况表 具备履行合同所必需设备和专业技术能力的声明函 主要商务要求承诺书 具有良好的商业信誉和健全的财务会计制度的相关材料 技术偏离表 具有独立承担民事责任的能力证明文件 联合体协议 项目实施方案、质量保证及售后服务承诺 投标人承诺函 依法缴纳税收和社会保障资金的良好记录的相关材料 项目组成人员一览表 中小企业声明函 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 缴纳投标保证金证明材料 其他材料 法定代表人授权委托书 监狱企业证明文件 残疾人福利性单位声明函 |
| | | | | | |

| | | | | | |
|------|--------|---|---------|----|--|
| | 类似项目业绩 | 供应商近三年(2021年1月1日至今，以合同签订时间为准)每提供一份类似项目业绩的得1分，本项最多得10分。附:业绩的证明材料中标通知书、合同协议书(未组织招标的项目可不提供中标通知书)，资料不齐全或未提供不得分，日期以合同签订时间为准，合同须能体现采购内容，盖章签署日期完整，否则不得分。 | 10.0000 | 客观 | 封面 目录 投标人（供应商）应提交的相关证明 投标人业绩情况表 投标人基本情况表 具备履行合同所必需设备和专业技术能力的声明函 主要商务要求承诺书 具有良好的商业信誉和健全的财务会计制度的相关材料 技术偏离表 具有独立承担民事责任的能力证明文件 联合体协议 项目实施方案、质量保证及售后服务承诺 投标人承诺函 依法缴纳税收和社会保障资金的良好记录的相关材料 项目组成人员一览表 中小企业声明函 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 缴纳投标保证金证明材料 其他材料 法定代表人授权委托书 监狱企业证明文件 残疾人福利性单位声明函 |
| 商务评审 | | | | | |

| | | | | |
|--------|---|---------|----|---|
| 项目组织人员 | <p>1.拟派项目经理资格条件: ①具有网络安全专业副高级及以上职称证书, 得7分。本未提供不得分。注: 需提供人员证书扫描件及近一年内任意一个月投标人为其缴纳社保的证明材料, 未提供的不得分。 2.安全检查服务团队成员具有信息系统项目管理师、信息安全工程师、网络工程师、软件测评师, 每提供1种职称证书得2分, 满分8分, 未提供不得分。注: 需提供人员证书扫描件及近一年内任意一个月投标人为其缴纳社保的证明材料, 未提供的不得分。</p> | 15.0000 | 客观 | <p>封面</p> <p>目录</p> <p>投标人(供应商)应提交的相关证明</p> <p>投标人业绩情况表</p> <p>投标人基本情况表</p> <p>具备履行合同所必需设备和专业技术能力的声明函</p> <p>主要商务要求承诺书</p> <p>具有良好的商业信誉和健全的财务会计制度的相关材料</p> <p>技术偏离表</p> <p>具有独立承担民事责任的能力证明文件</p> <p>联合体协议</p> <p>项目实施方案、质量保证及售后服务承诺</p> <p>投标人承诺函</p> <p>依法缴纳税收和社会保障资金的良好记录的相关材料</p> <p>项目组成人员一览表</p> <p>中小企业声明函</p> <p>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</p> <p>缴纳投标保证金证明材料</p> <p>其他材料</p> <p>法定代表人授权委托书</p> <p>监狱企业证明文件</p> <p>残疾人福利性单位声明函</p> |
|--------|---|---------|----|---|

| | | | | | |
|-----|-----|--|---------|----|----------------|
| 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）×100×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。 | 10.0000 | 客观 | 分项报价表 开标一览表 |
|-----|-----|--|---------|----|----------------|

价格扣除

| 序号 | 价格扣除评审内容 | 适用情形 | 扣除比例（C1） | 具体标准和要求 | 关联投标（响应）文件格式文件 |
|----|----------|------|----------|---------|----------------|
| 无 | | | | | |

6.汇总、排序

最低评标价法：评标结果按投标报价由低到高顺序排列。投标报价相同的并列。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排名第一的中标候选人。

综合评分法：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。得分且投标报价相同的并列。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排名第一的中标候选人。

7.确定中标人

采购人或者评标委员会按照中标候选人名单顺序确定中标人。中标候选人并列的，按采购人授权评标委员会按照评审原则直接确定中标（成交）人。规定的方式确定中标人。招标文件未规定的，采取随机抽取的方式确定。

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. 合同内容及格式

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 service 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, 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
- 详见附件: 投标人(供应商)应提交的相关证明
- 详见附件: 投标人业绩情况表
- 详见附件: 投标人基本情况表
- 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: 主要商务要求承诺书
- 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: 技术偏离表
- 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: 联合体协议
- 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: 投标人承诺函
- 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: 项目组成人员一览表
- 详见附件: 中小企业声明函
- 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: 缴纳投标保证金证明材料
- 详见附件: 其他材料
- 详见附件: 法定代表人授权委托书
- 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

报价分册:

- 详见附件: 分项报价表
- 详见附件: 开标一览表

采购包2:

通用分册:

- 详见附件: 封面
- 详见附件: 目录
- 详见附件: 投标人(供应商)应提交的相关证明
- 详见附件: 投标人业绩情况表
- 详见附件: 投标人基本情况表
- 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: 主要商务要求承诺书
- 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: 技术偏离表

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：联合体协议

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：投标人承诺函

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：项目组成人员一览表

详见附件：中小企业声明函

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：缴纳投标保证金证明材料

详见附件：其他材料

详见附件：法定代表人授权委托书

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

报价分册：

详见附件：分项报价表

详见附件：开标一览表