城市网络安全运营中心服务项目（一期）

公开招标文件

采购单位名称：呼和浩特市大数据管理局

采购代理机构名称：呼和浩特市政府采购中心

项目编号：150101-HSZC-GK-20260129

2026年10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

呼和浩特市政府采购中心 受 呼和浩特市大数据管理局 委托，采用公开招标方式组织采购 城市网络安全运营中心服务项目（一期） 。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： 城市网络安全运营中心服务项目（一期）

项目编号： 150101-HSZC-GK-20260129

采购计划备案号： 呼政采计划[2026]06156

2.内容及划分采购包情况

采购包1：安全运营服务

采购包预算金额（元）：4,831,700.00

采购包最高限价（元）：4,831,700.00

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	安全运营服务	1.00	4,831,700.00	项	软件和信息技术服务业	否	否	否	否

3.是否涉及本国产品

采购包1：

序号	采购品目名称	标的名称	产品名称
不涉及			

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：安全运营服务

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： 呼和浩特市政府采购中心

地址： 内蒙古自治区呼和浩特市新城区呼和浩特市丁香路2号

邮编： 010000

联系人： 呼市政府采购中心

联系电话： 0471-4669338

采购单位名称： 呼和浩特市大数据管理局

地址： 呼市新城区新华东街1号市党政机关办公大楼

邮编： 010000

联系人： 白燕飞

联系电话： 19719714371

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 1 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
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
12	采购代理机构代理费用	本项目不收取代理服务费
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。
19	有效投标人家数	采购包1：3家
20	中标供应商数量	采购包1：1名
21	中标候选供应商数量	采购包1：3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
24	兼投不兼中规则	本项目可兼投1包，本项目可兼中1包
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	无

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，同时在开标时提供证明材料。

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时，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时，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呼和浩特市大数据管理局。

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呼和浩特市政府采购中心。

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：安全运营服务

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	具有履行合同所必须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：安全运营服务

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

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

本项目采购城市网络安全运营中心服务，城市网络安全运营中心服务围绕"云网端网络安全＋政务云数据安全＋第三方安全服务"的总体框架，构建集约化、智能化的城市级网络安全运营体系。

二.主要商务要求、技术要求

1.主要商务要求

采购包1：安全运营服务

序号	参数性质	类型	要求
1		标的提供时间	合同签订之日起30日内提供服务
2		标的提供地点	呼和浩特市
3		合同履约期限	签订合同后一年
4		合同履约地点	呼和浩特市
5		验收要求	投标人需在合同签订后15个工作日提交并通过初步验收申请，服务期自初步验收合格之日起计算。若因投标人自身原因未能在规定时限内完成上述工作，由此产生的一切额外费用及损失均由投标人自行承担（含上一期安全服务延期费用）。
6		合同支付方式	1、1期：支付比例40%，供应商须在合同签订后15个工作日内完成所有软硬件设备的供货及上架安装，并经采购人初步验收合格后，采购人在收到供应商开具的发票之日起15个工作日内支付；，达到付款条件起15日内，支付合同总金额的40.00% 2、2 期：支付比例60%，服务期满后，采购人收到供应商发票之日起15个工作日内支付服务费。，达到付款条件起15日内，支付合同总金额的60.00%
7		履约保证金	需要缴纳履约保证金：不缴纳

2.技术标准与要求

采购包1：安全运营服务

标的名称：安全运营服务

序号	参数性质	技术参数与性能指标
		一、采购内容 本项目采购城市网络安全运营中心服务，城市网络安全运营中心服务围绕"云网端网络安全＋政务云数据安全＋第三方安全服务"的总体框架，构建集约化、智能化的城市级网络安全运营体系。城市网络安全运营中心服务包括网络安全运营服务、数据安全运营服务、安全运营专业技术服务、安全运营人员驻场服务、机柜租用服务。网络安全运营服务提供城市网络安全运营平台服务、云网安全采集对接防护服务、主机安全运营平台服务；数据安全运营服务提供数据安全运营平台服务、数据安全采集监测防护服务；安全运营专业技术服务提供应急演练服务、网络安全意识培训服务、IT资产梳理服务、安全配置核查服务、互联网暴露面梳理服务、漏洞管理服务、渗透测试服务、数据安全

风险评估服务、安全策略梳理服务、蜜罐诱捕服务、安全巡检服务、7*24小时安全监测服务等12项专业技术服务，机柜租用服务提供服务所需软硬件部署支撑保障服务。本项目开展城市网络安全运营中心服务，构建城市网络安全运营中心核心基础框架，补齐市本级政务云网在监测感知、数据防护、策略管控等方面的短板，实现市本级政务云网安全态势"一图统览"，保障市本级政务系统安全稳定运行。

二、服务要求

★（一）投标人需在合同签订后15个工作日提交并通过初步验收申请，服务期自初步验收合格之日起计算。若因投标人自身原因未能在规定时限内完成上述工作，由此产生的一切额外费用及损失均由投标人自行承担（含上一期安全服务延期费用）。（投标人须提供承诺函并加盖公章）

★（二）本项目服务所需的软硬件服务工具应符合安全可靠要求，硬件设备核心部件采用国产化芯片，业务应用系统应具备适配国产主流技术架构的能力。（投标人须提供承诺函并加盖公章）

（三）投标人应结合本项目网络安全运营、平台建设、安全服务落地、数据安全防护等实际建设内容，提供完整、贴合本项目的重难点分析及专项应对解决方案。包括项目建设重难点识别分析、网络安全重难点应对方案、数据安全重难点应对方案、平台部署与业务兼容重难点应对方案、项目实施及运维保障重难点应对方案。

（四）投标人应制定总体架构设计方案，确保最终服务方案和满足采购方的各项安全需求，内容需包括总体运营架构、总体系统架构、业务平台关系、数据采集传输、安全服务体系等内容。

（五）投标人应充分理解城市网络安全运营中心的架构，包括平台定位、平台架构设计、平台功能设计、应急响应中心、基础配套设施等内容。

（六）投标人应根据采购需求，制定合理的安全服务方案，包括应急演练服务方案、网络安全意识培训服务方案、IT资产梳理服务方案、安全配置核查服务方案、互联网暴露面梳理服务方案、漏洞管理服务方案、渗透测试服务方案、数据安全风险评估服务方案、安全策略梳理服务方案、蜜罐诱捕服务方案、安全巡检服务方案等内容。

（七）投标人应制定项目服务质量保障方案，包括项目人员保障措施、系统及安全设备保障措施、服务质量保障措施、项目风险管理及保密措施、网络安全应急响应预案等内容。

（八）投标人应制定售后服务方案，包括售后服务人员安排、售后服务响应时间和解决故障时间、售后服务承诺、售后保障措施等内容。

（九）投标人应制定注意项目保密，制定保密保障措施方案，包括保密管理、保密措施、保密制度等内容。

（十）投标人应提供城市网络安全运营中心标准规范编制服务，制定城市网络安全运营中心内部规范性文件，包括《呼和浩特市城市网络安全运营中心安全服务标准体系总纲》、《应急演练服务规范》、《网络安全意识培训服务规范》、《IT资产梳理服务规范》、《安全配置核查服务规范》、《互联网暴露面梳理服务规范》、《漏洞管理服务规范》、《渗透测试服务规范》、《数据安全风险评估服务规范》、《安全策略梳理服务规范》、《蜜罐诱捕服务规范》、《安全巡检服务规范》、《城市网络安全运营中心安全服务质量考核评价标准》、《城市网络安全运营中心7×24小时现场值守管理规范》、《城市网络安全运营中心岗位设置与人员管理规范》、《城市网络安全运营中心

		安全事件上报与协同联动规范》、《城市网络安全运营中心安全工具与数据保密管理规范》、《安全服务交付成果与文档归档管理规范》。 （十一）投标人应提供专业的服务团队，项目负责人具有信息系统项目管理师证书，团队其他人员（项目负责人除外）具备计算机、电子工程、通信工程方面的中级及以上职称或系统集成项目管理工程师、信息系统项目管理师、网络工程师证书。在项目实施过程中变更服务团队投标人应提前告知采购人，且具备切实可行的工作衔接方案、确保项目实施不受影响。 （十二）标“★”为核心重要参数，不允许负偏离，标“▲”为一般重要参数，投标人在投标文件中需提供证明材料以证明实质性满足。 **三、其它要求** （一）过渡保障服务要求 在下一期安全运营服务稳定运行之前投标人需提供过渡保障服务，保障政务云网数端等整体安全服务正常运行，合同到期后提供的服务，参照原合同计。 （二）保密要求 1.工作人员不得将掌握的客户设备信息未经客户许可泄露给其他人知道。 2.工作人员任何时候不得私自打开机房内客户设备。 3.工作人员任何时候不得私自拷贝、更改、删除客户服务器数据。 4.非工作需要，驻场运维人员不得掌握非工作范围内设备的口令。 5.办公电脑中若有敏感信息，人员离开时必须锁定屏幕或者关闭主机，主机必须设置强口令。 6.工作人员需签订服务保密协议。 7.工作人员需遵守国家有关的政策、法律、法规和制度。 8.工作人员需要按照工作规范进行工作，凡接收到的重大服务请求，需要经用户同意才做处理。 9.工作人员不得向外泄漏任何业务和相关数据。 10.工作人员不得向外泄漏任何保密的资料。 （三）合规性要求 投标人提供的所有产品、服务，须遵循国家、行业通用标准和规范。在服务期内，如果国家、行业通用标准和规范出现调整（变更、废止、新增）的，投标人所提供的服务须符合调整后的标准，所需费用由投标人承担。在项目的实施、运维和验收过程中，严格执行国家、行业以及采购人的管理制度和标准规范。投标人提供的服务需要符合安全行业各类法律、法规、标准及其他要求，并且按照有关规定和各级监管部门的要求进行动态整改。 （四）通用要求 1.本招标内容与技术要求作为投标人提出技术建议书和报价的依据，采购人拥有本招标内容与技术要求的最终解释权。 2.投标人必须根据本项目的各功能要求，提供科学、合理、先进、可行、适合采购人实际情况的服务。 3.投标人负责本次采购服务的部署、实施、调试并提供相关服务。 4.当用户单位需要增加服务资源时，投标人须按采购人要求及时提供相应服务。 5.服务费按照采购人考核标准，以实际使用的服务为基础，综合考虑服务质量绩效

评价情况进行结算，计算方式为：服务费用×绩效评价系数。（绩效评价系数按当前结算期计），在年度结算中，年服务费不超过投标人年度中标金额，超出部分不额外计费。

（五）兼容与可扩展性要求

根据本次购买服务的特点，投标人提供的软硬件产品及服务须具有兼容性和可扩展性。如果投标产品在软硬件产品及服务出现兼容性问题，投标人必须在采购人规定的期限内予以免费解决。

（六）知识产权

1.针对投标人提供的产品、服务，投标人保证采购人享有合法的使用权，如有法律纠纷由投标人负责。

2.针对投标人提供的产品、服务，投标人保证采购人在使用过程中不受到第三方关于侵犯专利权等知识产权的指控。任何第三方如果提出指控，投标人须与第三方交涉并承担可能发生的一切法律责任和费用。

四、服务内容要求

（一）网络安全运营服务

1、安全运营管理系统服务（城市网络安全运营中心-运营端）

(1)本项服务需配套专业的安全运营管理系统以及硬件服务器资源，服务器资源不少于3节点，单节点配置不低于24核CPU、256G内存、2块960G SSD硬盘、12块4T SATA硬盘、≧4千兆电口、≧2万兆光口。

(2)▲资产梳理：支持用设备资产关系图、域名资产关系图、IP信息关系图、服务信息关系图、外网暴露信息关系图、软件信息关系图、域名解析信息关系图、访问信息关系图、人员信息关系图来可视化呈现设备资产与其他资产以及资产属性详情之间的联系。

(3)资产配置：支持对资产标签的枚举值自定义配置，支持标签色卡自定义配置。支持将从影子资产、幽灵资产、僵尸资产转变过来的待审核资产进行统一管理。

(4)资产梳理：当资产的数据源是原始告警日志/系统漏洞/web漏洞/系统弱口令/检查项时，点击资产的出现次数，支持跳转查看资产关联的告警/系统漏洞/web漏洞/系统弱口令/检查项信息

(5)工单管理：支持根据不同用户创建工单任务，单个用户创建任务数无限制。任务内容包括：用户名称、任务名称、执行周期、任务周期、任务最近执行时间、任务下次执行时间、创建人、最近修改人、任务最近更新时间、启停状态、流程选择、工单创建人、工单责任人以及引用的流程中动态表单的参数和流程中剧本子流程节点的资产扫描/资产采集任务的参数等内容

(6)资产工单：支持管理可被所有资产和资产属性详情引用的通用属性字段。支持新增、编辑、删除、查看和检索通用属性，支持查看通用属性当前被哪个资产或资产属性详情所引用。

(7)▲资产发现：支持管理资产的影子资产、幽灵资产、僵尸资产、待审核资产基本信息，包括有：资产名（英文）、中文别名、唯一标识、默认排序，支持修改默认排序。

(8)资产信息：支持编辑属性的属性名（英文）、中文别名、输入框类型、是否支持编辑、是否必填、是否隐藏别名、正则校验、提示内容、默认值、是否支持列表展示、

		是否默认列表展示、是否可排序、是否支持搜索。 (9)资产信息：支持管理资产的忽略资产基本信息，包括有：资产名（英文）、中文别名、唯一标识、默认排序，支持修改默认排序。 (10)告警原始数据展示：支持以原始数据发生时间轴形式展示原始数据列表；支持查看原始数据全字段详情；支持原始数据创建快捷搜索与快捷复制；支持表单格式&json格式切换；支持批量对告警生成事件，生成的事件支持自动调用事件知识库进行引用填充。 (11)▲报告管理：支持一键自动化生成不同格式的安全事件报告，支持引用事件报告word类文档模版，根据模板配置的变量信息自动填充事件相关字段，支持在生成事件报告后修改报告内容。 (12)智能分诊：支持根据不同用户创建规则，单个用户/单位对象创建规则数无限制。支持配置规则响应打上的黑、白、红、蓝名单，降噪、精准标签；支持配置规则名称、描述、置信度、日志类型等信息的配置，置信度能够用于判断规则的打标优先级。支持对规则进行筛选条件配置，条件支持AND/OR/NOT等逻辑运算、多层级嵌套。支持在筛选条件中引用对象资源与过滤器。 (13)关联分析：支持对接入的各种日志类型数据进行关联分析，包括：各类告警日志，告警。日志类型及数据采集模块实时同步。 (14)事件管理：支持查看事件知识名称、处置建议、危害描述、研判依据等信息 (15)情报运营：支持管理事件知识库内容，可新增、编辑与删除知识内容，也支持批量导入导出知识内容。 (16)情报运营：支持管理ATT&CK知识库内容，全量导入ATT&CK知识内容，覆盖历史数据。 (17)情报运营：支持手动创建正式情报运营数据进行管理，也可管理从可疑情报转入过来的正式情报运营数据，在可疑情报的内容基础上补充了处置情况和情报来源的信息 (18)情报运营：支持新增、编辑、删除、检索、导入、导出情报运营数据，支持将情报运营上架到安全情报库进行使用，支持配置更新提醒时间，定时更新情报运营数据，支持在情报运营数据上留言备注 (19)脆弱性工单：支持管理所有通过工单流转引用关联剧本创建并执行的脆弱性扫描任务，支持查看任务详情，包括有：执行ID、用户名称、单位名称、任务类型、设备类型、设备名称、任务名称、扫描目标、节点标识、关联信息、下发状态、下发时间、操作人 (20)脆弱性识别：支持管理的任务类型：远程安全评估系统的系统漏扫、口令猜测任务；系统漏扫、web应用漏扫、口令猜测任务 (21)脆弱性分析：能够根据脆弱性反向查询资产，识别脆弱性关联的资产信息，支持根据不同用户和不同单位管理系统漏洞，单个对象创建漏洞数无限制，支持关联设备、域名、系统资产。 (22)工单管理：支持查看威胁对象的处置记录，展示该威胁对象发起处置工单后生成的任务信息，包括任务ID、处置指令、联动设备、关联信息、下发状态等 (23)工单管理：支持对威胁情报发起威胁情报处置工单，对威胁对象进行联动处置

，同一条威胁情报支持发起处置工单不超过3条

(24)联动组件：联动设备能力调用：支持下一代防火墙、服务器安全管理系统、终端安全管理系统等设备联动处置能力调用；支持漏洞扫描系统漏扫能力、web应用漏扫能力、口令猜测能力调用；支持资产探查系统资产扫描能力调用；支持服务器安全管理系统资产采集能力调用；

(25)剧本管理：剧本查看与检索：支持根据剧本分类查看业务引用剧本和自动化剧本信息，支持查看剧本详情包括剧本ID、剧本名称、剧本状态、用户名称、数据包、剧本支持的处置对象集合、剧本描述、剧本搭建的流程信息及剧本流程各节点的处置信息及节点输出参数；支持查看剧本版本更新记录，包括版本号、更新时间和版本快照；支持通过剧本名称、剧本类型、剧本状态、用户名称、更新人、更新时间等字段进行剧本检索；支持通过用户卡片筛选剧本；支持查看业务引用剧本引用次数和引用明细，包括引用剧本的工单标题、工单创建人、工单状态等；支持剧本调用脚本节点；

(26)▲脚本管理：支持Python脚本的创建、编辑、发布及执行下发能力，支持告警、威胁情报、事件工单等业务数据及手动输入作为动态参数注入，实现脚本与业务上下文的灵活绑定；。

(27)脚本管理：具备脚本版本管理与变更留痕能力，支持版本差异对比及引用方同步更新；提供脚本模板管理能力，支持通用逻辑沉淀与快速实例化生成；构建脚本执行异常处理与补偿机制，支持失败任务的自动识别、重试与重发，保障任务执行的稳定性与闭环管理；通过沙箱环境隔离、访问控制策略及执行节点分配管理，实现脚本执行过程的安全管理与资源调度优化。

(28)安全重保管理：支持创建并管理重保项目，最大支持1w个项目同时运行，每个项目独立运行，数据与权限按不同项目域隔离。支持对基于编号、名称、人员、用户、等级、状态等信息检索项目。

(29)重保配置：支持对重保项目人员、项目责任人、项目服务用户、项目权限、项目通知、项目名称、项目等级、开始时间、持续时长、项目状态等信息进行统一管理和维护。

(30)重保分诊：支持区分日常与重保告警，告警独立分流至指定重保项目域中；

(31)归属管理：支持控制对系统内所支持的不同数据源进行分流的开启与关闭

(32)▲用户管理：支持创建用户，创建时包含单位名称、单位简称、所属行业、行政区域、用户类型、经纬度、联系人、联系电话、详细地址、单位星级、备注信息等内容。

(33)单位管理：支持通过excel批量导入单位

(34)单位管理：支持对用户对象的信息的查看与检索，支持查看单位名称、所属行业、行政区域、服务平台账号数等信息。

(35)单位管理：支持对单个单位或多个单位进行用户授权，授权后将变为用户，不再单位列表展示

(36)单位管理：支持通过组织数查看单位被用户对象纳管情况

(37)门户管理：支持查看portal账号，支持以组织树形式查看与检索portal账号，支持查看组织节点、账号、姓名、手机号码、账号角色、启用状态等信息

(38)门户管理：支持创建portal账号，portal账号用户登录安全运营管理平台服务门户平台，创建内容包括用户姓名、所属组织节点、手机号、邮箱、备注、账号、角色

、密码二次确认等。

(39)门户管理：支持对账号开启与停用，支持删除账号，支持编辑账号相关内容

2、安全运营服务系统服务（城市网络安全运营中心-用户端）

(1)本项服务需配套专业的安全运营服务系统以及硬件服务器资源，服务器资源不少于2节点，其中一节点配置不低于10核CPU、32G内存、2块500G SSD硬盘、2块4T SATA硬盘、≧4千兆电口、≧2万兆光口。另一节点配置不低于24核CPU、64G内存、2块500G SSD硬盘、4块4T SATA硬盘、≧4千兆电口、≧2万兆光口。

(2)事项协同：支持查看与账号运营主体相关的工单数据统计，其中包括统计整体处置闭环率，平均处置时长，待处置，处置中，已处置的分类占比与数量

(3)资产安全运营：支持查看与账号运营主体相关的资产数据统计，包括纳管的下级单位数量，网站数量，应用系统数量，所有IP数量

(4)资产安全运营：支持检索影子资产；支持检索僵尸资产；支持检索幽灵资产；当资产的数据源是系统漏洞/web漏洞/系统弱口令/检查项时，点击资产的出现次数，支持跳转查看资产关联的系统漏洞/web漏洞/系统弱口令/检查项信息

(5)工单管理：支持快捷查询与该账号运营主体相关最近的待处置工单事项，工单事项支持快速跳转

(6)▲工单管理：支持查看由告警处置工单、事件处置工单、重保告警处置工单、重保事件处置工单等响应工单和自动化剧本执行生成的全量任务信息，支持查看任务详情包括任务执行ID、用户名称、设备类型、设备名称、处置指令、节点标识、下发状态、关联信息、生效时间、下发时间、任务处置记录等。

(7)工单管理：支持查看与该账号主体相关的各类工单事项数据，包括但不限于平台支持事件工单、联动处置工单，资产扫描/采集工单、发现资产审核工单、变更资产审核工单、脆弱性扫描工单、系统漏洞处置工单、web漏洞处置工单、系统弱口令处置工单、检查项处置工单等多个种类工单事项；

(8)工单管理：支持对工单进行条件检索，包括工单名称、工单类型、优先级、下发时间、工单状态、节点处理截止时间等条件对事项工单进行检索

(9)预警通报：支持展示至少最新4条预警通报，支持快捷入口查看所有预警通报；支持展示至少最新5条接收到的通知公告，查看的内容为标题、信息来源、附件、发布时间、发布状态。

(10)▲域名资产管理：支持检索、查看域名资产；支持查看域名资产的资产属性详情以及关系资产内容，包括域名解析、系统、人员、访问信息。支持查看每个域名资产与其他关系资产数据之间的资产关系图。

(11)事件管理：事件查看与检索：支持查看与该账号主体相关的事件数据；支持对事件条件检索，包括但是不限于事件名称、事件类型、威胁程度、事件状态等条件；支持自定义配置联动事件列表展示字段；支持查看事件详细信息，包括事件基础信息、影响范围、举证信息、事件线索库、事件流转动态等内容；

(12)漏洞管理：支持根据漏洞处置状态分类管理安全运营服务平台侧发现的用户所有系统漏洞；支持根据漏洞处置状态分类管理安全运营服务平台侧发现的用户管辖单位所有系统漏洞；支持查看、检索系统漏洞；支持查看漏洞关联的处置工单；支持查看漏洞关联的资产信息（设备、系统、域名）。

(13)安全重保管理：支持管理和查看重保项目名称、编号、状态、等级、时间周期

		、概述、服务人员信息、工单处置情况信息以及项目攻击类型top10统计、被攻击资产top10统计等内容 (14)安全重保管理：支持管理和查看用户在重保项目中重点被保护的系统资产信息情况 (15)安全重保管理：支持管理和查看重保关联事项列表，其中按状态划分，状态为待处置、已处置、处置中三种状态，支持查看的事项列表信息有事项名称、事项类型、责任单位、用户名称、紧急程度、危害程度、下发时间、响应时长、整改次数等内容 (16)安全重保管理：支持对重保事项进行流程化处置，其中支持上下级单位的事项下发与确认，事件处置、审核意见、事项退回、事项复测等操作，支持跟踪事项全流程节点动态 (17)报告同步：支持对附件报告进行word 方式在线预览 (18)▲安全重保工单：支持查看由重保告警处置工单、重保事件/工单处置工单等响应工单和自动化剧本执行生成的全量任务信息，支持查看任务详情包括任务执行ID、用户名称、设备类型、设备名称、处置指令、节点标识、下发状态、关联信息、生效时间、下发时间、任务处置记录等。 (19)安全重保管理：支持查看与该账号主体相关的重保事件数据 (20)安全事件管理：支持对事件条件检索，包括但不限于事件名称、事件类型、威胁程度、事件状态等条件 (21)安全事件管理：支持查看事件详细信息，包括事件基础信息、影响范围、举证信息、事件线索库、事件流转动态等内容 (22)单位信息配置：支持自动同步真实单位数据，包括单位名称、单位区域、单位经纬度、单位行业、单位地址、联系人、管辖关系，联系电话，便于使用 (23)联动组件：支持自定义配置联动事件列表展示字段 (24)联动组件：支持查看联动组件基础信息和联动信息/资产采集信息/资产扫描信息，包括组件类型、组件名称、用户名称、组件厂商、组件版本、组件序列号、组件来源、组件用途、最大处理量、管理IP、端口、连接方式、用户名、密码等信息 (25)联动组件：支持通过组件类型、组件名称、组件版本、组件序列号、组件来源、组件用途、最近交互时间、创建人、创建时间进行联动组件信息检索 (26)联动组件：支持自定义配置联动组件信息列表展示字段 (27)通知公告：支持展示最新全部接收到的通知公告，查看的内容为标题、信息来源、附件、发布时间、发布状态 (28)通知公告：支持创建通知公告，并发送至指定下级单位 3、安全运营数据可视化服务（城市网络安全运营中心-可视化） (1)依托呼和浩特市智慧城市指挥中心当前指挥大厅环境，提供城市网络安全运营成果可视化服务，展示呼和浩特城市网络安全运营成果，包括呼和浩特城市地图打点、运营中心资产纳管情况、整体安全态势、可疑事件监测、风险类型分布、漏洞预警通报、行业/单位风险概况、安全运营能力、安全事件处置情况、事件实时处置情况、安全运营流程、专项工作开展、安全运营人员、安全值守情况等内容。 (2)▲可视化大屏管理：提供创建大屏组件合方案，支持将预置的主视觉组件，视图组件，条件组件进行自由组合与调整位置。支持配置大屏组合方案名称、预览图、解说脚本。组合方案支持16：9，21：9，32：9三种屏幕尺寸，可根据实际使用场景定义

三种比例。支持对大屏进行发布状态的变更。支持大屏列表排序调整。支持在编辑时重新对各组件属性进行二次调整。

(3)主视觉管理：预置主视觉组件，包括地图视角、攻击者视角、资产视角、运营视角组件。支持对组件名称、描述、预览图、进行自定义配置。支持对组件进行动态、静态数据切换,数据刷新频率配置， 脱敏配置,输入事件参数配置。支持对组件进行数据类型配置，包括但不限于各组件定义好的数据范围。

(4)视图组件管理：预置视图组件，包括安全事件、威胁告警、脆弱性、资产、威胁情报、工单、联动处置等运营场景下各类组件 20 余种。

(5)条件组件管理：预置时间条件组件，时间条件支持48小时，7天，30天，90天四种范围选择。支持对组件名称、描述、预览图、进行自定义配置。支持对组件进行动态、静态数据切换,数据刷新频率配置， 脱敏配置,输入事件参数配置。支持对组件进行数据类型配置，包括但不限于各组件定义好的数据范围。

(6)脱敏规则管理：支持创建编辑脱敏规则，预置保留前n后m，前n至m，关键词前后遮盖，全脱敏5种脱敏算法。支持脱敏规则对各组件进行引用，引用后，组件数据将根据配置的规则进行脱敏。支持脱敏规则配置后测试效果，效果可随时展示。

(7)运营单位数据管理：支持新增、删除、编辑单位数据，属性包括单位名称、单位区域、单位经纬度、单位行业、单位地址、联系人、管辖关系，联系电话，可被大屏组件静态数据调用。

(8)自动同步单位数据：支持自动同步真实单位数据，包括单位名称、单位区域、单位经纬度、单位行业、单位地址、联系人、管辖关系，联系电话，便于使用。

(9)数据权限：支持查看与账号相关主体的下级管辖单位（非用户）以及本主体的数据范围，支持在组件中进行可看范围“仅看自己”“包含自己与下级”“仅看下级”三种配置，其余数据无法查看。

4、政务云安全数据采集服务

(1)本项服务需配套3台专业的网络安全采集探针，2U标准上架设备，≥10GB实时流量处理性能，≥2个千兆电口，≥4个万兆光口，≥2个40GE光口，≥8TB SATA硬盘，冗余电源。

(2)双协议栈检测：支持IPv4和IPv6网络环境下的部署，接口支持IPv4、IPv6配置，支持对IPv4路由监控和对IPv6路由监控，可同时对IPv4和IPv6网络流量分析检测；

(3)流量过滤：支持通过ip、ip段、端口、协议、VLAN等进行流量过滤，过滤条件支持and、or、not等逻辑运算创建的BPF过滤语法过滤数据；

(4)网络协议识别：支持包括tcp、udp、icmp、http、dns、dhcp、smtp、pop3、imap、webmail、sctp、smb、sip、ftp、snmp、telnet、nfs、ssl、ssh、ldap、radius、kerberos、netbios、ntp、vnc、ipv6、gtp、mqtt在内的至少28种常见网络协议识别并还原网络流量；

(5)数据库协议识别：支持包括db2、oracle、mysql、mssql-db、sybase、tidb、kingbase、人大金仓、达梦、优炫数据库等数据库协议识别、流量还原；

(6)WEB攻击检测：支持常见攻击行为检测，支持HTTP双向流量动态检测，检出类型包括：SQL注入，命令执行，代码执行，跨站脚本攻击，权限绕过，暴力破解，扫描工具，数据库攻击，敏感信息泄露，挖矿检测，蠕虫传播，目录遍历，文件包含等至少

13种Web攻击检测，检测规则数量不低于11000条；

(7)网络攻击检测：支持网络攻击检测，检出类型包括：各种协议的帐号暴力破解，Mysql UDF提权攻击、Microsoft Windows NetLogon权限提升漏洞攻击，向日葵、TeamViewer，psexec远程执行、smbexec在目标上远程执行命令，DCSync_DCShadow疑似攻击、域用户口令爆破行为、域内密码喷洒攻击，njRat后门程序变种通信行为、Cobaltstrike HTTPS beacon通信等，检测规则不低于7200条；。

(8)▲AI检测能力：支持灵活开启机器学习模型，增强检测精度；支持包括：ICMP隧道检测、DNSTunnel检测、HTTP隧道检测、CS流量检测、MSF检测、挖矿流量检测、代理流量检测、暗网流量检测、弱口令检测、SSH爆破登录成功检测、加密webshell检测(http/s)在内的至少11种机器学习检测模型，提高威胁行为检出率；。

(9)自定义漏洞规则：支持自定义漏洞规则；支持根据攻击载荷自定义漏洞检测规则，可自定义检测规则的四元组、以及检测规则的协议类型，包括：TCP/UDP/HTTP协议；HTTP协议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）、匹配载荷内容，TCP/UDP协议可自定义上下行payload，并且单条规则可指定多个检查项，同时可定义漏洞威胁级别、威胁分类、攻击结果、CVE编号、CNNVD编号、漏洞描述、漏洞危害、解决方案；

(10)内置威胁情报：系统本地集成威胁情报数据，威胁情报总量不低于800万+，系统统计、展示威胁情报检测命中数；

(11)加密流量攻击检测：支持隐秘信道检测；检测类型包括：ICMP、DNS协议等隐蔽隧道攻击检测，恶意软件加密通信的检测，加密web应用的流量检测，非法应用加密通信的检测，SSL加密协议相关的漏洞与攻击的检测，加密通道攻击行为检测，支持JA3指纹检测；

(12)暴力猜解检测：支持包括rdp/ftp/telnet/smtp/redis/rlogin/ssh/mysql/mssql/imap/POP3等在内的至少11种网络协议的账号暴力猜解检测；支持撞库、登录页面爆破行为检测；支持手动配置暴力猜解告警阈值，减少业务行为误报；

5、政务外网安全数据采集服务-市本级

(1)本项服务需配套2台专业的网络安全采集探针，2U标准上架设备，≥10GB实时流量处理性能，≥2个千兆电口，≥4个万兆光口，≥2个40GE光口，≥8TB SATA硬盘，冗余电源。

(2)双协议栈检测：支持IPv4和IPv6网络环境下的部署，接口支持IPv4、IPv6配置，支持对IPv4路由监控和对IPv6路由监控，可同时对IPv4和IPv6网络流量分析检测；

(3)流量过滤：支持通过ip、ip段、端口、协议、VLAN等进行流量过滤，过滤条件支持and、or、not等逻辑运算创建的BPF过滤语法过滤数据；

(4)网络协议识别：支持包括tcp、udp、icmp、http、dns、dhcp、smtp、pop3、imap、webmail、sctp、smb、sip、ftp、snmp、telnet、nfs、ssl、ssh、ldap、radius、kerberos、netbios、ntp、vnc、ipv6、gtp、mqtt在内的至少28种常见网络协议识别并还原网络流量；

(5)数据库协议识别：支持包括db2、oracle、mysql、mssql-db、sybase、tidb、kingbase、人大金仓、达梦、优炫数据库等数据库协议识别、流量还原；

(6)WEB攻击检测：支持常见攻击行为检测，支持HTTP双向流量动态检测，检出类型包括：SQL注入，命令执行，代码执行，跨站脚本攻击，权限绕过，暴力破解，扫描工具，数据库攻击，敏感信息泄露，挖矿检测，蠕虫传播，目录遍历，文件包含等至少13种Web攻击检测，检测规则数量不低于11000条；。

(7)网络攻击检测：支持网络攻击检测，检出类型包括：各种协议的帐号暴力破解，Mysql UDF提权攻击、Microsoft Windows NetLogon权限提升漏洞攻击，向日葵、TeamViewer，psexec远程执行、smbexec在目标上远程执行命令，DCSync_DCShadow疑似攻击、域用户口令爆破行为、域内密码喷洒攻击，njRat后门程序变种通信行为、Cobaltstrike HTTPS beacon通信等，检测规则不低于7200条；

(8)AI检测能力：支持灵活开启机器学习模型，增强检测精度；支持包括：ICMP隧道检测、DNSTunnel检测、HTTP隧道检测、CS流量检测、MSF检测、挖矿流量检测、代理流量检测、暗网流量检测、弱口令检测、SSH爆破登录成功检测、加密webshell检测(http/s)在内的至少11种机器学习检测模型，提高威胁行为检出率；

(9)▲自定义漏洞规则：支持自定义漏洞规则；支持根据攻击载荷自定义漏洞检测规则，可自定义检测规则的四元组、以及检测规则的协议类型，包括：TCP/UDP/HTTP协议；HTTP协议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）、匹配载荷内容，TCP/UDP协议可自定义上下行payload，并且单条规则可指定多个检查项，同时可定义漏洞威胁级别、威胁分类、攻击结果、CVE编号、CNNVD编号、漏洞描述、漏洞危害、解决方案；。

(10)内置威胁情报：系统本地集成威胁情报数据，威胁情报总量不低于800万+，系统统计、展示威胁情报检测命中数；

(11)加密流量攻击检测：支持隐秘信道检测；检测类型包括：ICMP、DNS协议等隐蔽隧道攻击检测，恶意软件加密通信的检测，加密web应用的流量检测，非法应用加密通信的检测，SSL加密协议相关的漏洞与攻击的检测，加密通道攻击行为检测，支持JA3指纹检测；

(12)暴力猜解检测：支持包括rdp/ftp/telnet/smtp/redis/rlogin/ssh/mysql/mssql/imap/POP3等在内的至少11种网络协议的账号暴力猜解检测；支持撞库、登录页面爆破行为检测；支持手动配置暴力猜解告警阈值，减少业务行为误报；

6、政务外网安全数据采集服务-旗县区

(1)本项服务需配套9台专业的网络安全采集探针，≥3GB实时流量处理性能，≥32GB内存；≥4TB SATA盘；≥6个千兆电口，≥2个万兆光口。

(2)双协议栈检测：支持IPv4和IPv6网络环境下的部署，接口支持IPv4、IPv6配置，支持对IPv4路由监控和对IPv6路由监控，可同时对IPv4和IPv6网络流量分析检测；

(3)流量过滤：支持通过ip、ip段、端口、协议、VLAN等进行流量过滤，过滤条件支持and、or、not等逻辑运算创建的BPF过滤语法过滤数据；

(4)▲网络协议识别：支持包括tcp、udp、icmp、http、dns、dhcp、smtp、pop3、imap、webmail、sctp、smb、sip、ftp、snmp、telnet、nfs、ssl、ssh、ldap、radius、kerberos、netbios、ntp、vnc、ipv6、gtp、mqtt在内的至少28种常见网络协议识别并还原网络流量；。

		(5)数据库协议识别：支持包括db2、oracle、mysql、mssql-db、sybase、tidb、kingbase、人大金仓、达梦、优炫数据库等数据库协议识别、流量还原；。 (6)WEB攻击检测：支持常见攻击行为检测，支持HTTP双向流量动态检测，检出类型包括：SQL注入，命令执行，代码执行，跨站脚本攻击，权限绕过，暴力破解，扫描工具，数据库攻击，敏感信息泄露，挖矿检测，蠕虫传播，目录遍历，文件包含等至少13种Web攻击检测，检测规则数量不低于11000条； (7)网络攻击检测：支持网络攻击检测，检出类型包括：各种协议的帐号暴力破解，Mysql UDF提权攻击、Microsoft Windows NetLogon权限提升漏洞攻击，向日葵、TeamViewer，psexec远程执行、smbexec在目标上远程执行命令，DCSync_DCShadow疑似攻击、域用户口令爆破行为、域内密码喷洒攻击，njRat后门程序变种通信行为、Cobaltstrike HTTPS beacon通信等，检测规则不低于7200条； (8)AI检测能力：支持灵活开启机器学习模型，增强检测精度；支持包括：ICMP隧道检测、DNSTunnel检测、HTTP隧道检测、CS流量检测、MSF检测、挖矿流量检测、代理流量检测、暗网流量检测、弱口令检测、SSH爆破登录成功检测、加密webshell检测(http/s)在内的至少11种机器学习检测模型，提高威胁行为检出率； (9)自定义漏洞规则：支持自定义漏洞规则；支持根据攻击载荷自定义漏洞检测规则，可自定义检测规则的四元组、以及检测规则的协议类型，包括：TCP/UDP/HTTP协议；HTTP协议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）、匹配载荷内容，TCP/UDP协议可自定义上下行payload，并且单条规则可指定多个检查项，同时可定义漏洞威胁级别、威胁分类、攻击结果、CVE编号、CNNVD编号、漏洞描述、漏洞危害、解决方案； (10)内置威胁情报：系统本地集成威胁情报数据，威胁情报总量不低于800万+，系统统计、展示威胁情报检测命中数； (11)加密流量攻击检测：支持隐秘信道检测；检测类型包括：ICMP、DNS协议等隐蔽隧道攻击检测，恶意软件加密通信的检测，加密web应用的流量检测，非法应用加密通信的检测，SSL加密协议相关的漏洞与攻击的检测，加密通道攻击行为检测，支持JA3指纹检测； (12)暴力猜解检测：支持包括rdp/ftp/telnet/smtp/redis/rlogin/ssh/mysql/mssql/imap/POP3等在内的至少11种网络协议的账号暴力猜解检测；支持撞库、登录页面爆破行为检测；支持手动配置暴力猜解告警阈值，减少业务行为误报； 7、自治区电子政务外网安全监测平台对接服务 (1)本项服务需配套政务外网安全监测对接平台1套。配套服务器资源不少于1节点，单节点配置不低于24核CPU、256G内存、2块960G SSD硬盘、12块4T SATA硬盘、≧4千兆电口、≧2万兆光口。 (2)日志采集：支持对网络设备、安全设备、主机系统的日志、网络流量等多种数据源的采集；支持对日志采集器进行采集配置并下发；提供Syslog、SNMP Trap、文本格式日志、数据库、WMI、Netflow、HTTP、Script等采集方式；并支持数据源信息导入、导出、数据源迁移操作； (3)日志范化：预置支持≥700种设备进行日志解析，支持统计展示已接入设备总数

、日志源的总数及其中在线和离线数量；支持实时展示平台整体及各安全设备的日志采集EPS、处理EPS指标变化趋势；支持监控和展示各设备全流程数据处理结果统计（即日志接入、解析、存储、外发、产生告警、事件各环节数据统计）。

(4)日志字段富华：支持通过界面配置字段映射方法，实现字段富化，包括但不限于字段值映射、XML提取、时间格式转换、脚本等方式。

(5)日志类型管理：支持新增日志类型功能，可在线新增字段信息，支持数据存储类型的配置，包括：ES、Kingbase、mysql，支持存储基础信息的配置：包括数据库名、存储时间、分区方式等基础属性信息，从而达到分类存储日志的目的。

(6)告警加白：支持加白分诊规则，以避免产生误报。支持对源IP、目的IP、数据源IP、攻击者（IP类型）、受害者（IP类型）、域名、文件哈希、URI资源的类型直接进行全局加白；支持根据单个、多个或者全部检测规则进行加白，如果选择了特定的关联规则，则加白只针对选中规则范围内产生的告警生效，并且支持配置生效时间。

(7)▲日志统计：支持分析不同厂商、不同种类安全设备上报的告警日志，对其进行威胁分类、危害定级、有效性筛选以及重复告警归并；支持按照归并条件针对重复告警进行归并，归并条件包括不限于：检测规则ID、数据源IP、攻击链阶段、ATT&CK技术项、失陷状态、攻击结果、攻击者、受害者、CVE编号、协议、漏洞名称、漏洞描述、漏洞危害、CNNVD等条件；。

(8)日志报表：自定义报表模板：支持自定义模板可加入多种统计分析视图（含自定义）和智能备注信息（可根据数据不同展示不同的备注说明）；支持灵活编辑和布局调整以形成整体报表；可添加不限于告警统计、工单统计、异常行为统计、弱口令统计、攻击者统计、日志统计、系统维护、脆弱性统计、调查统计、资产统计、风险统计等；报表模板可被快速报表和周期报表任务引用。

(9)日志转发：支持告警日志采集、日志范化、日志外发以及政务外网安全监测平台对接等功能。收集市本级电子政务外网安全监测探针的告警数据，并按照电子政务外网安全监测平台要求的数据格式将范式化后的数据推送到自治区电子政务外网安全监测平台。

8、政务外网安全防护服务

(1)本项服务需配套吞吐不低于40Gbps的下一代防火墙4台，吞吐不低于4Gbps的下一代防火墙9台，流量处理性能不低于6Gbps的网络准入设备1台（配置2000点准入授权），配套不少于100日志源授权的日志审计1台，不少于100运维授权的堡垒机1台。

(2)40G防火墙性能要求：网络层吞吐量≥40G，并发连接≥1000万，每秒新建连接数≥30万；2U机箱，冗余电源；≥8个千兆电口，≥4个千兆光口，≥4万兆光口，≥1 TB SSD固态硬盘。

(10)40G防火墙功能要求：开启应用识别库、URL分类特征库、病毒防护特征库、入侵防御特征库、威胁情报监测授权等全功能授权。支持对HTTP/FTP/POP3/SMTP/IMAP/SMB/IPTUX七种协议进行病毒查杀；本地病毒库规模大于3000万，支持样本留存。

(3)4G防火墙性能要求：网络层吞吐量≥4G，并发连接≥300万，每秒新建连接数≥6万；双电源；千兆电口≥4个，千兆光口≥4个，≥1T SSD固态硬盘。

1		(4)4G防火墙功能要求：开启应用识别库、URL分类特征库、病毒防护特征库、入侵防御特征库、威胁情报监测授权等全功能授权。支持策略命中时间分析和安全策略推荐。命中时间分析展示被命中的安全策略的名称、状态、命中数、策略创建时间、首次命中时间和最近命中时间；安全策略推荐定可以指定策略流量，分析后自动生成源地址精度更高的安全策略。能够基于源地址精确合并和源地址子网合并，并自动生成策略名称、源对象、目的对象和服务对象。支持对HTTP/FTP/POP3/SMTP/IMAP/SMB/IPTUX七种协议进行病毒查杀；本地病毒库规模大于3000万，支持样本留存。 (5)准入设备性能要求：≥5G网络流量处理能力；≥6个千兆电口，≥2个万兆光口，≥4TB 硬盘，冗余电源，2U设备。配置≥2000点准入授权 (6)▲准入设备功能要求：具备策略路由、端口镜像、透明网桥、802.1X、Portal、DHCP准入、MAB、VLAN隔离等多种准入控制方式。支持准入技术自由组合使用，满足各种复杂网络环境。支持入网设备的审批机制，强制接入设备必须在已审批资产清单中方可入网。支持管理员修改资产清单中设备登记的资产信息字段。 (7)日志审计性能要求：机箱高度≥2U，综合日志处理性能≥3000条/秒(EPS)，日志采集处理均值≥6000EPS，千兆电口≥6个，千兆光口≥4个，冗余电源，系统盘≥256GB mSATA卡，数据盘≥4TB SATA硬盘，提供≥100个日志源接入授权。 (8)日志审计功能要求：支持通过Syslog/Syslog-ng、SNMP Trap、Net flow、JDBC、Agent日志代理(Windows/Linux)、WMI、远程FTP、远程SFTP、文件共享(SMB、NetBIOS)、文件/目录读取、Kafka、WebService等多种方式完成各种日志的收集功能，支持页面文件导入，支持多行日志采集合并为一行。日志解析字段内置150个字段，属性字段可扩展，用户可根据审计需要自行创建字段，属性类型包括IP、字符串、整型、IP、布尔、布尔等15种，可选择映射函数8种可选项等。内置及新增的所有字段均可参与事件查询、关联分析和报表数据源统计。 (9)堡垒机性能要求：机箱高度≥2U，千兆电口≥6个，千兆光口≥4个,硬盘≥4TB，冗余电源。支持≥1000个字符会话或≥300个图形会话。配置≥100点运维授权。 (10)堡垒机功能要求：产品支持的运维协议包含SSH、RDP、Telnet、VNC、FTP、SFTP、SCP、DB2、MySQL、SQL Server、Oracle、Rlogin、DM、Redis、PostgreSQL等；产品支持通过windows应用发布的方式实现对MySQL、IE、Firefox、Oracle、Chrome、VNC Client、SQL Server、SecBrowser、VSphere Client、Radmin、dbisql、Navicat for MySQL、Toad for DB2、Navicat for PgSQL、MongoDB、Dbeaver for Clickhouse、Dbeaver for Hive、AquaDataStudio for KT等应用程序/协议的扩展支持；产品支持管理员设置全局标签和运维人员自定义标签，全局标签全员可见、可筛选，运维人员自定义标签本人可见、可筛选，方便设备管理与查找。 9、零信任服务 (1)本项服务需配套零信任综合网关1台，2U机箱，冗余电源，≥6千兆电口，≥4个千兆SFP，国产CPU；≥32G内存；≥256G SSD，4T HDD硬盘，最大理论加密加密吞吐≥300Mbps；最大并发用户数≥50； (2)支持UDP+TCP单包授权机制，UDP+TCP方式默认不开放端口，可避免业务应用的端口被扫描，进而避免利用端口对业务应用发起攻击的风险； (3)提供用户组管理，支持动态用户组，可按照规则进组，使得满足规则的用户自动

		能够进入组，并继承组所拥有的权限、访问策略等，而不需要依次手工添加，减轻了管理的负担。 (4)支持用户身份打标签，以实现对不同的用户打不同标签，并可以基于标签进行细粒度访问控制。 (5)支持建立用户与设备绑定/解绑维护和管理，支持设置设备绑定策略，包括单个用户可绑定的PC设备数、可绑定的移动设备数，支持按照用户组分别设置可绑定的PC设备数、可绑定的移动设备数等，从而加强设备的管控。 (6)支持设备归属的设置规则，系统可自动为设备标记为COPE（企业签发设备）、BYOD(自带设备），并可根据设备归属用于相应访问控制策略，从而实现针对企业的、个人自带的设备实施不同程度的管控。 (7)支持从用户属性、环境属性、行为属性、终端属性维度设置准入策略，便于对用户准入进行控制。 (8)支持用户两次登录设备发生变化、异常旅行速度设置行为属性，以实现从用户行为维度进行准入控制，缓解因用户账号被盗用、身份被仿冒的用户进入系统的安全风险。 (9)▲支持用户身份属性的自定义扩展，以便管理员可以根据自身需要对用户属性扩展，而不需要重新部署或升级系统程序；。 10、终端安全运营系统服务 (1)本项服务需配套终端安全运营系统1套，配置不少于200点授权。 (2)资产信息统计：支持根据分组、计算机名称、IP地址、MAC地址、通信IP地址、接入点、用户端类型、操作系统类型、操作系统版本等条件的组合筛选出符合条件的终端进行管理，自由对终端进行转移分组、删除终端、重启系统和终端跃迁。 (3)硬件信息展示：支持单个页面展示在线终端数量、风险终端数量及占比、今日风险告警数、控制中心当前CPU、内存、硬盘使用百分比、终端在线率、终端正常率、终端平台统计、基线核查统计、病毒查杀趋势、感染病毒终端、漏洞补丁统计等信息，均可通过图形化展示。 (4)资产分组管理：支持自动自定义分组，按IPv4地址、IPv6地址、MAC地址、NAT.IPv4地址、NAT.IPv6地址、用户端类型、接入点、一体化安装包、操作系统版本、操作系统内部版本号、操作系统域、CPU数量、CPU架构、内存容量、终端名、终端硬件标识、计算机工作组、主板序列号、终端型号、终端、终端分组等参数进行自动动态调整自定义分组。 (5)支持对压缩包内的病毒扫描，支持多层压缩包的扫描，可自定义配置压缩包的扫描层数，至少大于20层模式下的扫描。 (6)防病毒引擎：支持不少于三个杀毒引擎混合使用，提高病毒检出率。 (7)▲补丁管理：支持管理中心自动获取最新版本补丁库。支持获取的最新版本补丁库在正式更新到全网终端前，自动做灰度测试发布：支持在管理中心设置好灰度测试发布的终端；支持终端分批次发布；支持设置灰度测试发布持续时间；支持补丁库版本灰度测试发布后自动转为全网可更新版本。支持用户端可自动更新全网可更新版本。支持以上配置后，管理中心从获取最新版本补丁库、灰度测试、全网发布的自动化编排。 (8)▲终端管控：支持对终端各种外设（USB存储、硬盘、存储卡、光驱、打印机、

扫描仪、摄像头、手机、平板等）、接口（USB口、串口、并口、1394、PCMIA）设置使用权限，并支持生效时间设置；支持外设库管理，可统计终端外接的各种设备，包括厂商和设备类型、产品、数量、PID、VID和设备来源。

(9)终端管控：支持对终端节能管理，支持对长时间运行、定时关机、空闲节能、工作时间外开机等节能类型设定策略，支持仅提示、关机、注销、锁定、关闭显示器、锁定+关闭显示器、休眠和睡眠处理。并支持提示倒计时弹窗，可设置在终端取消后下一次提醒时间。

11、服务器安全运营系统服务

(1)本项服务需配套服务器安全运营系统1套，配置不少于150点授权。

(2)服务器资产梳理：提供服务器资产的自定义采集能力，支持自动采集和任务采集两种资产收集方式，自动采集支持设置不同类型资产以小时/天/周/月的不同频率采集，任务采集支持选择不同类型资产、收集频率、服务器范围和超时时间；

(3)服务器变更监控：提供账号、端口、计划任务的新增、修改、删除等变更行为的监控能力；支持展示上述资产变更的变更类型、变更内容、变更详情，支持设置资产变更监控频率；

(4)服务攻击监控：支持以图形化的形式统计展示服务器受到的告警信息/可疑威胁、拦截事件，包括：可疑威胁事件统计、可疑威胁分布、可疑威胁趋势以及具体的威胁事件列表；

(5)访问异常监控：支持对攻击者发起的恶意扫描行为进行识别，可防护端口扫描和扫描器扫描行为，以攻击和受害两种视角展示扫描信息包括：发生时间、受害IP、攻击IP、攻击类型、扫描端口、扫描次数、在威胁情报中是否为黑IP等信息；

(6)暴力破解监控：支持检测包括不限于SSH、RDP、GoldenDB、MySql、Oracle、SQLServer、VsFtpd、PostgreSQL、SMB、Tomcat等服务的暴力破解检测及防护；

(7)登陆异常监控：能通过检测非常用时间登录、非常用IP登录、非常用账号登录等异常模式，一旦识别到任何潜在的安全风险，系统将立即触发警报。用户可随时查看异常登录事件的详细信息，包括登录时间、地点、IP地址、账号等关键信息；

(8)文件异常监控：支持在控制台展示每台服务器本地隔离区的病毒文件信息，支持展示隔离病毒文件的隔离时间、隔离人、隔离方式、文件路径、HASH等信息；

(9)服务器漏洞管理：支持增强漏洞扫描、标准漏洞扫描两种模式，增强漏洞扫描支持检测的漏洞数量应不低于4000个；厂商应提供推荐扫描的漏洞项，形成模板供用户快速选择；同时支持按照漏洞名称、漏洞编号、漏洞等级、漏洞类型、系统类型、应用名称、检测原理、披露时间、存在EXP、本地提权、内核风险、修复影响、是否可防护等信息搜索或筛选特定漏洞进行扫描。

（二）数据安全运营服务

1、数据流转监测系统服务

(1)本项服务需配套数据流转监测系统1套。配套服务器资源不少于2节点，单节点配置不低于24核CPU、256G内存、2块960G SSD硬盘、12块4T SATA硬盘、≧4千兆电口、≧2万兆光口。

(2)数据发现：支持对数据库/实例进行自动扫描与解析，自动发现并提取数据库/实例信息、表信息、字段信息、表记录总条数等元数据信息，并识别其中的数据资产；

(3)数据标签管理：支持从数据标签维度查看敏感数据资产，可查看每种数据标签的敏感数据量、应用数、API数、数据库数、告警数、风险数、事件数，并支持下钻查看；

(4)数据动态识别：对接入日志进行分析处理，发现流动中的敏感数据，并发现相关联的数据库、应用、API、账号信息。

(5)应用资产管理：支持查看应用资产列表，并可查看每条应用资产的业务应用、Host、API数、账号数、应用标签、发现时间、数据标签、敏感数据访问量、去重访问量、告警数、风险数;

(6)账号数据风险监测：支持查看账号资产列表，并可查看每条账号资产的账号名称、类型（应用或数据库）、业务应用/数据库资产名称、应用Host/数据库地址、发现时间、数据标签、敏感数据访问量、去重访问量、告警数;

(7)数据分类分级模板：系统内置数据分类分级模板，模板可按照场景需求进行自定义修改，分类分级模版支持多级设置，至少内置个人敏感信息、金融、政务大数据模版。

(8)数据分类分级信息展示：支持基于数据资产识别结果，支持分类分级资产总量、数据级别分布、数据资产数据源分布、数据源类型所含数据量统计、分类分级时间线、分类数据量排行、数据标签数据量排行、数据源数据量Top10、部门数据资产信息、敏感表数据量Top10等信息

(9)数据流转风险监测：支持以链路的形式展示一段时间内的源IP通过应用访问数据库或者直接访问到数据库的行为，可以查看数据流转的节点、数据泄露的路径、访问者的源IP、访问时间和访问的数据内容等信息。

(10)数据跨境风险监测：支持在流动图谱中针对境外IP访问、外网访问的路径等进行高亮展示，帮助用户发现可能存在的异常访问。

(10)数据风险告警降噪：支持告警降噪，支持根据告警的类型、等级等配置告警归并规则，支持基于告警信息配置后置过滤规则，增强告警信息的可读性，避免告警数据过多，运营人员精力过渡分散。

(11)数据资源管理：支持资源管理和过滤器配置，通过引用过滤器和提前配置好的资源快速生成策略，以便提高策略配置效率。

(12)数据流转风险规则自定义：支持通过自学习和用户自定义规则/场景，对流量、日志进行实时统计和分析。内置规则包括：数据共享外发场景、接口流动安全、数据运维场景、跨境传输场景、数据异常访问场景、开发测试环境数据泄露、账号访问安全场景、数据接口风险、账号安全场景等九大类。内置规则支持通过库升级方法进行能力迭代升级优化。

(13)数据安全风险报告：系统提供数据安全评估报告模板管理功能，预置至少5种不同内容框架如组织架构、制度保障、数据风险、权限管理、安全审计等的报告模板，支持自定义数据安全评估报告的内容框架、样式格式，并建立评估报告的分类体系;

(14)数据安全事件管理：支持数据安全事件查询与展示，展示内容包括事件名称、事件等级、事件描述和事件危害等。

(15)敏感数据传输检测：通过图形化的方式展示企业内敏感数据的流动情况，包括敏感数据的来源、去向、趋势等；可直观展示敏感数据流出趋势、敏感数据流出TOP5、敏感数据访问量TOP5、涉敏资产统计及敏感数据流动实时监测；帮助用户更好地了

解敏感数据的流动趋势和热点情况。

(16)敏感数据分布：通过图形化的方式展示企业内的数据分布情况，包含敏感数据的数据源和敏感数据的维度展示数据源的分布情况、敏感数据的类型、级别、新发现的包含敏感数据的库表等。

2、API风险监测系统服务

(1)本项服务需配套API风险监测系统1套。配套服务器资源不少于1节点，单节点配置不低于24核CPU、256G内存、2块960G SSD硬盘、12块4T SATA硬盘、≧4千兆电口、≧2万兆光口。

(2)API资产管理：支持对流量采集Agent的统一管理，采集Agent部署终端IP地址、CPU利用率、内存利用率、发送/接收流量信息以及设备状态、版本信息、注册时间等。

(3)API服务启停：支持手动一键开启、关闭API安全服务。

(4)API基线建立：支持自定义API日志中请求头、请求体、响应头、响应体长度，最大8KB，满足用户不同场景的Payload信息长度配置。

(5)API安全基线：支持基于统计模型自动生成API聚合规则，支持API归并阈值配置。

(6)API安全基线：支持API访问基线配置，学习模式支持固定时长、固定时段。基线指标包括：请求大小、响应大小、响应时延、请求速率、出错速率、吞吐量、请求流量、请求次数。

(7)API分类模板：支持内置敏感数据检测模板，包括：通用模板、政务模板、金融模板、能源模板、医疗模板、工业模板、计算机行业模板、个人信息模板、文件模板、其它、全集模板，支持根据业务场景自主切换敏感数据检测模板。

(8)API数据采集：支持启停控制敏感文件留存，存储文件不低于1W个。

3、数据安全采集服务

(1)本项服务需配套数据安全采集探针3套。CPU≥32核，内存≥128G，硬盘≥4T，2U机箱，冗余电源，≥2个千兆电口，≥2个万兆光口，≥3个扩展槽。

(2)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；

(3)采集过滤条件支持但不限于源地址、目的地址、时间、例外应用等；

(4)支持Oracle、MySQL、MSSQL、PostgreSQL、MongoDB、DB2、人大金仓、瀚高、南大通用、优炫等数据库行为的解析。

(5)支持如ftp、smb、oracle、mysql、mssql、postgresql、ssh、pop3、smtp的登录动作解析。

(6)▲通过内容深度分析技术可实现针对结构化数据/非结构化数据/半结构化数据的检测分析，如文件类型检测、文件内容提取及分析、压缩文件内容提取及分析、图片文件内容提取及分析、JSON/XML内容提取及分析等，可结合用户业务数据特点进行深度内容分析，判断当前文件内容是否包含敏感信息（法律法规政策规定和或者您自定义配置的相关敏感数据），并产生敏感信息文件告警，为数据安全的进一步处理提供依据。

(7)支持非结构化数据检测分析，包含doc、docx、xls、xlsx、ppt、pptx、pdf、rtf、cebx、ceb、odt、ofd、odp、wps、et、dps、zip、gz、tar、rar、7z、bz2、xz等

(8)支持自定义敏感数据检测规则，定义规则内容包括但不限于类型、子类型、敏感

		程度、匹配条件等字段，规则类型需支持正则和关键字两种方式； (9)支持以流转途径维度查看数据流转情况，展现内容包括应用名称、访问用户数、行业类型、数据标签、访问总条数、去重后条数、访问数据量、首次访问时间、最新访问时间等。 (10)支持以受害者维度展现数据窃取风险，展现内容包括受害者、风险名称、风险等级，首次发现时间，最新发现时间等。 (11)支持以访问者维度展现可疑访问风险，展现内容包括访问者、风险名称、风险等级、流量上行字节数、流量下行字节数等。 (12)通信模式支持但不限于KAFKA、SYSLOG等协议。 4、数据库安全监测服务 (1)本项服务需配套数据库安全监测系统1套。标准2U机箱，采用国产化CPU，集成国产化操作系统， ≥ 32G内存，≥4T硬盘，≥6个千兆电口，≥4个千兆光口，2个USB，≥2个扩展槽位，冗余电源。 (2)支持监测的数据库：Oracle、SQL-Server、DB2、Informix、Sybase、MySQL、PostgreSQL、达梦、人大金仓、南大通用Gbase、神舟通用、Caché、IRIS、HBase、Hive、MongoDB等。 (3)支持B/S架构Http应用三层审计，可提取包括应用系统的人员工号（账号）的身份信息，精确定位到人，支持框架：Tomcat、Apache、WebLogic、JBoss。 (4)支持Agent模式监测，Agent属轻量级，运行时占用资源少，不影响业务正常运行，并且还可以设置占用资源上限。 (5)支持通过手动添加或主动发现数据库中的存储过程、触发器，并对其具体操作进行行为审计，存储过程审计可审计到调用行为及具体操作风险；触发器审计可审计到触发行为及其具体操作风险。 (6)审计规则支持多个分项响应条件；支持规则类型、风险级别、操作类型、关键字、语句长度、语句执行回应、语句执行时间、返回内容、影响行数、数据库名、应用账户、用户端操作系统主机名、用户端操作系统用户名、用户端MAC、用户端IP、访问工具、规则生效时间、数据库表、字段等条件。 5、数据库防火墙服务 (1)本项服务需配套数据库防火墙1套。标准2U机箱，采用国产化CPU，集成国产化操作系统， ≥32G内存，≥4T硬盘，≥6个千兆电口，≥4个千兆光口，2个USB，≥2个扩展槽位，冗余电源。 (2)支持传统关系型数据库，如：SQL Server、MySQL、Oracle、Sybase、DB2、Informix、PostgreSQL、MariaDB等数据库的安全防护。 (3)支持后关系型数据库，如Caché、IRIS的安全审计或防护。 (4)会话阻断：对需要阻断的访问，中断数据库连接；操作阻断：当前语句被拦截后，该会话不中断。 (5)支持通过代理模式实现java web环境100%准确关联，支持框架：tomcat、weblogic、jboss；支持B/S业务系统三层关联阻断；支持B/S三层架构下的真实用户名关联配置。 (6)▲支持对阻断行为支持审批放行，支持操作类型、关键字、访问工具、用户端IP

、正则表达式、返回行数阈值等条件设置放行规则，实现灵活管控数据库操作行为，满足特殊运维场景的需要。

(7)内置安全特征库和审计规则库不少于1000条，无需单独配置，直接调用。如SQL注入攻击、跨站脚本攻击、权限管理、数据篡改等。

(8)系统内置敏感数据类型，并支持自定义添加，自动发现数据库对象中包含的敏感数据；支持根据发现结果，自定义敏感规则，包括操作类型、风险级别、处理动作、敏感级别等进行敏感数据的操作行为监控、阻断防护。

(9)支持基于时间、风险级别、保护对象、操作类型、用户端IP、访问工具、数据库账户、应用账户、规则类型、规则名、规则组名、操作系统主机名、操作系统用户名、用户端MAC地址、用户端端口、服务端IP、服务端口、数据库名、语句长度、语句执行回应、语句执行时间、返回行数、返回结果、审阅状态、会话ID、记录编号、关键字等25种以上条件的检索查询；查询条件易于使用，支持等于或不等于、大于等于或小于等逻辑关系。

6、数据安全防护服务

(1)本项服务需配套数据安全网关1套。代理带宽≥1G，代理并发连接数≥60万，代理新建连接数≥3.5万，2U硬件，≥1T硬盘，交流冗余电源，≥2千兆电口，≥2万兆光口。

(2)支持反向代理发布web业务，实现web应用的暴露面收缩和隐藏；在不改造现有web应用的情况下完成上线，通过代理能力提供对web应用的隔离保护、协议的转换等功能；支持SSL卸载，将HTTPS业务发布为HTTP，减轻服务器加解密压力；支持SSL加载，可以将HTTP业务发布为HTTPS，满足安全性要求。支持阻塞提醒页面自定义配置；

(3)支持反向代理逃生和DNAT逃生两级逃生方式。可通过策略配置逃生条件，对指定源IP到目的IP或域名端口配置逃生策略。反向代理逃生即放通代理转发直通，不进行任何数据包的处理和管控；DNAT逃生即放通NAT转发，不进行代理及任何数据包的处理和管控。适用于排障及紧急加白场景。

(4)支持镜像旁路部署；可在无任何侵入性下采集流量数据包分析，发现敏感数据访问与流转；

(5)支持显式代理模式，且支持针对指定IP范围代理或IP例外不代理；支持透明代理模式，且可设定特定代理的IP范围或例外IP，满足不同终端的业务访问需求。支持代理服务器端口自定义（80端口可用作代理），代理端口可以配置多个。

(6)系统内置敏感信息规则库，包含手机号、身份证号、护照号、地址、邮箱、银行卡号、统一社会信用代码、营业执照编号、组织机构代码、车牌号、车架号等常见的数十种敏感信息。

(7)系统内置文件类型识别库，可基于特征识别office系列、工程制造、压缩文件、加密文件、脚本文件、源码文件等类型。系统支持对压缩文件进行真实类型检测。

(8)系统支持针对业务系统的访问控制管理，支持基于用户身份和角色、位置和工具、时间条件等多维度条件，属于/不属于，包含/不包含，满足/不满足的细粒度的访问控制策略。

(9)系统支持对业务系统上传和下载文件，以及上传下载文件类型分别进行管理，以黑白名单的方式灵活保护系统文件的安全可见范围。可以通过用户和时间等条件，属于

/不属于，包含/不包含，满足/不满足配置细粒度的访问控制策略。系统支持对压缩文件层级管理，支持选择超过系统解压层数阻断还是放行。

(10)支持对业务系统网页接口和API接口传输的敏感信息进行动态脱敏；识别并脱敏用户输入/输出中的个人隐私信息：包含手机号、身份证号、护照号、地址、邮箱、银行卡号、IP、MAC等进行遮蔽、可逆、仿真脱敏，支持脱敏规则遮蔽位置、替换字符等细节配置；

(11)支持对业务系统返回的网页和文件、图片动态添加水印；支持网页明水印、文档暗水印、文档明水印、图片水印。支持自定义水印内容，支持配置水印字体大小、水印不透明度、水印密度等；支持水印溯源。

（三）安全运营专业技术服务

1、应急演练服务

（1）服务范围：市大数据管理局职责范围内

（2）服务内容：紧密配合用户参与应急预案制定与应急演练全流程工作。在预案制定阶段，结合数据安全管理实际需求，协助梳理数据泄露、系统故障、网络攻击等典型安全风险场景，明确各部门职责分工、响应时限及处置步骤，确保预案内容贴合实战需求。在应急演练环节，协助设计模拟真实安全事件的演练脚本，组织技术人员、管理人员等多角色参与，通过实战化操作检验预案中风险识别、应急启动、协同处置、事后复盘等全流程的合理性与可操作性。通过系列工作，及时发现并优化处置流程中的薄弱环节，进一步规范应急操作标准，有效提升安全事件发生后的快速响应与高效处置能力，为保障呼和浩特市数据安全与政务信息化稳定运行筑牢防线。

（3）服务频率：2次/年

2、网络安全意识培训服务

（1）服务范围：市大数据管理局职责范围内

（2）服务内容：开展网络安全培训服务，构建“全员普及+专业深耕”的培训体系。面向全体人员，聚焦网络安全和数据安全意识提升与基础防护技能强化，内容涵盖钓鱼邮件识别、弱口令设置、办公设备安全使用、数据保密规范等实用知识。针对网络安全工作人员，重点覆盖应急处置、安全设备运维、新技术防护策略等核心能力。培训过程中，系统宣讲《中华人民共和国网络安全法》《中华人民共和国数据安全法》等相关法律法规，明确各岗位安全责任清单及违规操作惩戒措施，强化“谁主管、谁负责”的安全意识。培训按每年一次常态化开展，确保培训覆盖全面、落地有效，助力构建全员参与的网络安全防护格局。

（3）服务频率：1次/年

（4）服务工具：提供网络安全社会工程学防范场景演示工具，包括但不限于钓鱼邮件伪装攻击演示工具、手机二维码钓鱼演示工具、WiFi欺骗与账号窃密演示工具、弱口令破解与暴力攻击演示工具、特制U盘恶意程序传播演示工具、ID卡读取与门禁仿冒演示工具、针孔摄像头隐蔽窃密演示工具、AI换脸社会工程学诈骗演示工具、手机木马植入与全量信息窃取演示工具。培训场景可根据培训要求进行定制开发，培训前需提前部署到培训场地。

3、IT资产梳理服务

（1）服务范围：市本级政务云（三个云基地）和市本级政务网的IT资产（不包括政务网内的政务终端）

（2）服务内容：为保障呼和浩特市本级政务系统安全稳定运行、夯实数字化政务服务基础，开展全面的IT资产发现与识别工作。依托自动化扫描工具、资产指纹识别等专业技术手段，结合人工实地核查、跨部门台账核对的双重校验模式，对政务外网内分散的硬件设备、软件授权、网络信息进行全维度梳理。最终建立标准化、可追溯的统一电子台账，实现资产信息动态更新与精准管控，为后续安全防护、风险评估及合规管理提供坚实数据支撑。为保障IT资产信息的准确性，至少每季度开展1次梳理与资产信息更新工作。

（3）服务频率：4次全量梳理，全年动态跟进

（4）服务工具：服务期内提供资产梳理工具进行本地化部署，防止敏感数据泄露。并具备以下功能：

1）设备类别分析：支持识别“打印机、网络摄像头、安全设备、投影仪、安全设备、路由器”等设备类型，具备大于40000条指纹特征库，

2）多网卡探测：通过对历史资产探测任务进行二次扫描探测，发现探测网络上的主机是否存在多网卡，结果信息需包括主机网卡IP及多网卡IP，

3）资产台账：支持自动识别网站资产信息，包括：“中间件信息、web框架信息、CMS&OA、程序语言”等指纹信息，支持爬取网站后台、ICP备案编号、网站标题、网站返回码等属性，形成网站资产台账。支持通过导入现有资产信息，或在线编辑方式，录入网站资产的管理信息，比如网站所属部门、负责人、联系方式、资产价值、物理位置等。支持对状态码、IP、资产组、部门、责任人、URL、子域名、易危组件、中间件、ICP备案号、公安备案号、归属地等进行精准搜索或模糊搜索。支持对已知url资产进行深度扫描，进一步发现登录后台和API接口，并识别是否暴露外网。agent模式下，可识别精细化识别主机的硬件信息（包括cpu、线程、内存、磁盘等使用率信息），网卡信息，运行进程、自启动服务、安装软件等。可自定义展示列，可排序、选择是否显示。

4）▲mac地址自动识别：不需要联动第三方设备、不需要在主机中安装任何代理、无需主机开放任意端口，就可支持对跨网段的IP或多个网段对进行MAC地址探测识别，支持识别MAC地址的设备类型包含:“Windos、Linux、国产操作系统、交换机\路由器、安全设备、打印机等”，

5）可管理主机资产授权数：无限制；

4、安全配置核查服务

（1）服务范围：市大数据管理局负责管理的14个业务系统

（2）服务内容：为强化系统安全防护基础、规避配置不当引发的安全漏洞与数据泄露风险，开展全方位安全策略梳理服务工作。核查范围覆盖系统核心组件，包括网络设备的访问控制策略与端口配置、操作系统的账户权限与安全策略、数据库的账户管理与审计配置、应用服务器的部署参数与权限管控。通过对照行业安全标准与最佳实践，全面排查配置缺陷，最终输出包含问题清单、风险等级划分的安全配置评估报告，并同步提供可落地的配置优化方案与整改步骤，助力快速补齐配置安全短板。

（3）服务频率：2次全量核查，全年动态跟进

（4）服务工具：服务期内提供配置核查工具进行本地化部署，防止敏感数据泄露。并具备以下功能：

1）操作系统，支持Windows 2003/2008/2012/2016/2019/7/8/10/11；支持li

		nux（Centos、Redhat、suse等）； 2）国产操作系统：支持银河麒麟、统信、欧拉、龙蜥、大云天元等国产操作系统； 3）应用服务：支持Linux、Windows下的Apache、Weblogic、TOMCAT、Nginx、东方通、宝蓝德、中创中间件等，以及windows 2003/2008/2012/下IIS 6/7/8； 4）数据库：支持Linux、Windows下Oracle8i/9i/10/11g、Mysql、达梦、人大金仓、神舟通用、优炫数据库等。 5）大数据应用：如Flume、HBase、Hadoop、Spark、Storm、Hadoop、ZooKeeper。 5、互联网暴露面梳理服务 （1）服务范围：市本级政务云上约170个存在互联网暴露面的信息系统 （2）服务内容：本服务采用自动化安全工具与专业人工研判相结合的模式，针对市本级政务云上约 1 7 0 个存在互联网暴露面的政务信息系统开展全面的互联网暴露面梳理工作。一方面全域摸排全量公网 IP、云服务资产及未登记在册的影子资产，厘清资产归属与网络边界，形成完整清晰、规范可查的互联网暴露面资产台账，彻底摸清外部攻击底数；另一方面深度识别各资产的开放端口、服务组件及版本信息，同步开展通用系统漏洞、W e b 应用安全风险、配置安全缺陷及公开渠道敏感信息泄露专项检测，对排查发现的高危风险逐项进行人工核验确认，并全程跟进整改闭环处置进展，最终推动市本级政务信息系统互联网高危风险清零，切实收敛外部攻击面，夯实政务网络安全防护根基。 （3）服务频率：2次全量梳理，全年动态跟进 （4）服务工具：服务期内提供暴露面梳理工具进行本地化部署，防止敏感数据泄露。并具备以下功能： 1）暴露面监测：通过单位全称、关键字、出口IP等信息，收集单位/企业信息、邮箱信息、敏感代码、敏感文档、app程序、微信小程序、微信公众号等外部/互联网攻击面信息。 2）二级域名扫描：支持二级域名扫描功能，输入一级域名进行一键扫描，通过搜索互联网数据，自动获取到该域名的二级域名、网站标题、解析IP地址； 3）IP反查域名监测：输入IP或者网段，通过搜索互联网数据，自动获取到IP对应的域名、url链接、网站标题、返回状态码； 4）网站资产相关度分析：通过爬取企业单位已知的网站页面，分析网页中是否包含企业单位相关的网站链接，从而发现未知网站；可配置“网段、域名”等命中规则，自动判断是否属于企业单位的网址； 5）可管理主机资产授权数：无限制；提供可管理网站资产授权数：无限制。 6、漏洞管理服务 （1）服务范围：市大数据管理局负责管理的14个业务系统 （2）服务内容：提供全周期漏洞管理服务，聚焦市大数据管理局负责管理的14个业务系统，构建漏洞闭环管理体系。采用自动化扫描工具与人工深度验证相结合的方式，开展全量漏洞探测，同步监测高危漏洞实时预警，确保漏洞无遗漏。对发现的漏洞第

一时间同步相关运维人员，提供针对性修复指南与技术支持，跟踪整改进度并督促限期完成。修复后开展专项复测，验证漏洞闭环效果，全程留存扫描报告、修复记录等资料，满足合规与安全审计要求，从源头降低漏洞被利用风险，保障业务系统安全稳定运行，需配合用户跟进业务系统漏洞修复情况。

（3）服务频率：2次全量扫描，全年动态跟进

（4）服务工具：服务期内提供漏洞扫描与漏洞管理工具进行本地化部署，防止敏感数据泄露。并具备以下功能：

1）完善的漏洞库：漏洞库漏洞信息大于360000条，集成大于5000条漏洞验证POC对内网资产进行自动漏洞验证与渗透，提供详细的漏洞描述和对应的解决方案描述。扫描结果需包含漏洞利用证明，包括但不限于攻击Payload、目标响应结果、漏洞利用点、关键参数等内容。

2）漏洞生命周期管理：支持漏洞跟踪管理，能够自动对漏洞状态进行处置，自动识别“新增、已修复、未修复”的漏洞，同时支持人工方式进行漏洞状态处置，以及编写漏洞备注，

3）弱口令扫描研判工具：支持用户针对指定的目标IP与应用，通过在web界面上手工输入“用户名、密码”，系统将返回口令登录后的校验结果，确认弱口令是否真实存在。

4）扫描次数授权：无限制；扫描IP/域名范围授权：无限制。

7、渗透测试服务

（1）服务范围：市大数据管理局负责管理的14个业务系统

（2）服务内容：为提前排查业务系统潜在安全风险，构建主动防护屏障，开展常态化渗透测试服务。测试过程严格模拟恶意黑客常用的攻击工具、技术手段与分析逻辑，从外部攻击视角深入探测系统架构、应用程序、数据传输、权限管理等关键环节，精准挖掘隐藏的高危漏洞与安全薄弱点。测试以半年为周期定期开展，每个业务系统每半年完成1次全面渗透测试，确保风险监测无间断。测试结束后，将输出包含漏洞等级划分、成因分析、攻击路径还原、风险影响评估及针对性整改方案的专业渗透测试报告，为系统安全加固提供明确依据，从源头防范网络攻击事件发生。

（3）服务频率：2次/年

（4）服务工具：服务期内提供AI渗透测试工具进行本地化部署，防止敏感数据泄露。并具备以下功能：

1）多智能体并行web渗透测试：提供不少于6种智能体Agent进行自动化渗透测试，包括但不限于injection-agent、auth-agent、file-agent、api-agent、business-agent、misc-agent，要求每个智能体能独立输出以下内容，包含但不限于测试接口、漏洞列表、类型/严重程度、是否需要登录、完整HTTP请求/响应证据，

2）渗透测试台账：支持以excel报表格式导入渗透测试报告，形成渗透测试台账。可在系统查看渗透测试结果，以图表形式可视化展现漏洞风险级别比例、风险应用比例，可对渗透报告中的漏洞进行跟踪确认，处置漏洞状态：未整改、已整改、忽略、未整改。

8、数据安全风险评估服务

（1）服务范围：市大数据管理局公共数据一体化平台相关政务业务系统（不低于3个独立业务系统）

（2）服务内容：数据安全风险评估服务聚焦数据安全防护与合规建设需求，围绕数据采集、传输、存储、使用、共享、销毁全生命周期流转场景，结合数据分级分类成果，从管理体系、技术防护、运营流程、人员能力等多个维度，通过资产梳理、漏洞检测、威胁研判、合规对标等专业手段，系统排查数据安全脆弱点与潜在风险，量化风险等级与影响程度，并输出完整的评估报告与可落地的整改加固建议，帮助组织补齐数据安全防护短板、满足法律法规合规要求，切实降低数据泄露、非法篡改、违规滥用等安全风险。

（3）服务频率：1次/年

（4）服务工具：服务期内提供数据安全风险评估工具进行本地化部署，防止敏感数据泄露。并具备以下功能：

1）服务期内提供数据安全风险评估工具进行本地化部署，防止敏感数据泄露。支持评估项目管理与评估范围设定，可对待评估的数据库、操作系统、应用服务、大数据平台等评估对象进行建档管理，支持评估任务创建、分派与进度跟踪。

2）支持数据安全基线核查功能。操作系统支持Windows 2003/2008/2012/2016/2019/7/8/10/11，支持Linux（CentOS、Redhat、SUSE等），支持银河麒麟、统信、欧拉、龙蜥等国产操作系统；大数据应用支持Flume、HBase、Hadoop、Spark、Storm、ZooKeeper。

3）支持脆弱性识别功能，包括安全配置核查、弱口令检测、敏感数据明文存储检测、漏洞扫描，可对识别结果进行脆弱性赋值，并分析现有安全措施的有效性。

4）支持威胁识别与综合风险分析功能。威胁识别覆盖数据泄露、数据篡改、数据滥用、数据勒索等威胁场景，支持从内部人员、外部攻击、第三方合作等维度开展威胁分析与威胁赋值；综合风险分析采用定性与定量相结合的方法，自动完成风险值计算与风险等级判定。

9、安全策略梳理服务

（1）服务范围：市本级政务云（三个云基地）和市本级政务网

（2）服务内容：针对政务云安全设备开展系统化配置核查工作，核查对象涵盖边界防火墙、Web 应用防火墙（WAF）、入侵防御系统、VPN 网关、负载均衡等设备的安全策略。重点开展两方面工作：一是访问控制策略合理性核查，全面梳理南北向（互联网至政务云）、东西向（云内租户间、业务系统间）全量访问规则，排查过度通配、权限过宽、冗余过期的无效策略，整治“全端口放通”“全 IP 放行”等极不合理配置，从源头收窄内网暴露面，防范跨租户、跨业务的横向渗透风险；二是高危端口暴露专项核查，全量摸排对外开放端口，识别 SSH、RDP、数据库服务等高危端口无防护直接暴露的风险，校验端口映射、地址转换规则的必要性与合规性，推动关停非必要暴露端口。

（3）服务频率：2次全量梳理，全年动态跟进

10、蜜罐诱捕服务

（1）服务范围：市本级政务网

（2）服务内容：在市本级政务网络体系内部署蜜罐，构建“主动发现、精准诱捕、全程溯源、联动防御”的实战化主动安全防护体系，弥补传统边界防护被动响应的短板，主动识别并捕获针对政务网络的各类潜在攻击行为。依托高仿真服务伪装、全攻击链行为记录、智能威胁研判能力，系统可完整捕获攻击者的端口扫描、漏洞探测、权限突

		破、横向移动、数据窃取等全流程攻击行为，留存完整的攻击操作日志与流量证据；一旦蜜罐节点被探测、访问或突破，将立即触发高优先级安全告警，辅助安全运营人员快速发现自动化批量扫描、定向渗透攻击、内网潜伏威胁及未知漏洞攻击等传统安全设备难以有效识别的风险。 （3）服务频率：全年 （4）服务工具：服务期内提供威胁诱捕工具进行本地化部署，防止敏感数据泄露。并具备以下功能： 1）病毒诱饵类型：支持高交互病毒监测诱饵，并可同时启用：“samba、ftp、ssh、rdp、telnet、mssql、mysql、mongoDB、postgresql、tomcat、weblogic、jenkins、redis、hadoop、memcache、solr、activeMQ、struts2、wordpress、nginx、jboss、joomla、smtp”等，以上服务须为真实应用服务，能够正常交互，欺骗攻击者， 2）失陷主机微隔离：不需要联动第三方设备、不需要在主机上安装agent脚本，就能对失陷主机进行网络隔离，隔离后失陷主机无法访问同网段以及其它网段IP， 3）默认仿真蜜罐：支持至少10种可自定义logo和公司名称的仿真蜜罐，仿真蜜罐类型包括但不限于：“齐治堡垒机、启明堡垒机、深信服VPN、泛微OA、通达OA、u8 crm、wiki、mailcow、bbs论坛、订单管理系统”。 4）完全仿真蜜罐：支持通过反向代理的方式，接入用户自身搭建的应用系统，从而实现完全仿真真实业务系统，生成完全仿真蜜罐， 5）钓鱼邮件演练：可在平台中统计打开钓鱼邮件的账号、点击连接的账号、提交敏感数据的账号等数据，统计维度包括账号名称、访问ip、提交敏感数据内容、访问时间等。 6）引流防御：可将访问真实业务系统的流量引流到仿真蜜罐，使攻击无法命中真实业务系统。 7）入侵攻击链检测：参考MITRE ATT&CK，形成黑客攻击链，攻击链检测包含：“针对蜜罐的探测扫描、渗透攻击、攻陷蜜罐、在蜜罐上安装后门远控程序、利用蜜罐进行跳板攻击”等入侵过程。 8）时间轴告警：支持时间轴告警分析：可根据基于告警时间/攻击类型/地理位置等对攻击行为进行筛查，其中攻击类型可分类为：“可疑访问、尝试登陆、端口扫描、攻击尝试、强力攻击、异常进程、暴力破解、登陆成功、命令执行、可疑文件、恶意文件、跳板攻击”等类型，对于攻击事件分析起关键作用。 9）攻击者社交信息溯源：支持记录攻击者的“黑客社交画像”信息，包括社交账号、昵称、头像等信息，比如溯源百度等不同类型的社交账号。 10）攻击者指纹溯源：设备指纹溯源至少包括：操作系统信息、浏览器指纹、浏览器类型、mac地址、设备厂商、屏幕分辨率，浏览器历史记录、计算机名、显卡成像参数、CPU等硬件信息。 11）位置信息溯源至少包括：真实攻击IP（攻击者拨VPN也可获得真实攻击IP）、代理转发前的IP地址、IP地理位置、经纬度。 12）威慑反制：可灵活指定对某个攻击源IP地址发起威慑反制，比如灌输国家网络安全法、告知已获得相关溯源信息。 13）拒绝服务反制：可使攻击者浏览器拒绝服务，可灵活指定对某个攻击源IP地址

		发起拒绝服务反制。 14）木马诱骗反制：可使攻击者下载某个文件时，替换成木马文件，诱骗攻击者下载安装。 15）提供仿真业务陷阱授权数：无限制。 11、安全巡检服务 （1）服务范围：市本级政务云（三个云基地）和市本级政务网 （2）服务内容：面向市本级政务云（下辖三个云基地）及政务网全量安全设备开展专业化安全巡检，全面排查设备不合理配置、配置缺失等风险隐患并出具分级整改建议，整改完成后组织“回头看”复核验证确保问题闭环落地，最终输出完整规范的安全巡检报告。 （3）服务频率：4次/年 12、7*24小时安全监测服务 （1）服务范围：城市网络安全运营中心 （2）服务内容：提供 7×2 4 小时不间断网络安全监测服务，全天候对呼和浩特城市网络安全运营中心收集的网络安全告警开展实时深度分析与风险研判。实时识别外部入侵攻击、恶意渗透、勒索病毒、高危漏洞隐患、内部违规访问等各类安全事件，对产生的告警信息进行人工甄别降噪，第一时间推送风险预警并提供应急处置建议，全程跟踪安全事件处理结果，定期输出安全监测分析报告，全方位保障客户信息系统与核心业务持续稳定、安全可靠运行。监测服务的值守排班需符合《中华人民共和国劳动法》的相关要求，每人周工作时间不得超过40小时。 （3）服务频率：7*24小时不间断 （四）机柜租用服务 （1）标准IT机柜服务，机柜高度42U，单机柜功率≥5KW，符合国家 A 级电子信息系统机房建设标准，具备双路冗余供电、U P S 不间断电源后备保障、精密空调恒温恒湿管控、全维度物理安防与环境实时监控能力，配套提供高可靠冗余网络接入链路及7×24 小时现场运维技术支撑。
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5人组成， 其中由评审专家库产生的评审专家4人， 由采购人派出的采购人代表1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。	投标人基本情况表 技术偏离表 投标人（供应商）应提交的相关证明 法定代表人授权委托书 项目组成人员一览表 中小企业声明函 监狱企业证明文件 目录 封面 具有独立承担民事责任的能力证明文件 主要商务要求承诺书 投标人承诺函 具有良好的商业信誉和健全的财务会计制度的相关材料 缴纳投标保证金证明材料 其他材料 项目实施方案、质量保证及售后服务承诺 残疾人福利性单位声明函 联合体协议 依法缴纳税收和社会保障资金的良好记录的相关材料 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 投标人业绩情况表 具备履行合同所必需设备和专业技术能力的声明函

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。

3.对本国产品的支持政策的相关要求

3.1按照《国务院办公厅关于在政府采购中实施本国产品标准及相关政策的通知》（国办发〔2025〕34号）、《关于贯彻落实《国务院办公厅关于在政府采购中实施本国产品标准及相关政策的通知》的意见》（财库〔2025〕30号）相关要求，本国产品标准适用于货物，包括政府采购货物项目和服务项目中涉及的货物。适用本国产品标准的货物具体是指《政府采购品目分类目录》中的货物类产品，但不包括其中的房屋和构筑物，文物和陈列品，图书和档案，特种动植物，农林牧渔业产品，矿与矿物，电力、城市燃气、蒸汽和热水、水，食品、饮料和烟草原料，无形资产。

本国产品应当在中国境内生产，即在中华人民共和国关境内实现从原材料、组件到产品的属性改变。从具体情形看，在国内保税区、综合保税区等海关特殊监管区域生产的产品，属于在中国境内生产的产品；对医疗器械产品，取得药品监督管理部门授予的准字号医疗器械注册证的，属于在中国境内生产的产品；对其他产品，根据实际情况判断是否在中国境内生产。

3.2政府采购活动中既有本国产品又有非本国产品参与竞争的，依法对本国产品给予价格评审优惠，对本国产品的报价给予20%的价格扣除，用扣除后的价格参与评审。

当采购项目或者采购包中含有多种产品，供应商为该采购项目或者采购包提供的符合本国产品标准的产品成本之和占该供应商提供的全部产品成本之和的比例达到80%以上时，依法对该供应商提供的全部产品给予价格评审优惠，即对该供应商提供的全部产品的总报价给予20%的价格扣除，使用扣除后的价格参与评审。

3.3供应商出具符合要求的《关于符合本国产品标准的声明函》、《本国产品成本比例声明表》（格式附后，不可修改）或有关证明文件的，该产品视为本国产品，采购人、采购代理机构不得再要求供应商提供其他证明材料。供应商提供虚假《关于符合本国产品标准的声明函》、《本国产品成本比例声明表》、虚假证明文件谋取中标、成交的，依照《中华人民共和国政府采购法》等法律法规规定追究相应责任。

符合本国产品的支持政策的相关要求的，按照以下比例进行扣除：

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
无					

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：安全运营服务

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.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**

	投标技术参数与招标文件的满足程度	标记“▲”（20个）号条款为一般重要参数，根据具体技术或参数要求提供相关佐证材料，“▲”项参数每有一条不满足扣1分，扣完为止，本项满分得20分。（注：以上具体技术或参数要求相关佐证材料均需加盖投标人公章，否则视为无效，不能提供或所提供的材料不足以佐证参数要求的不得分）	20.0000	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

总体架构设计方案	投标人须针对本项目采购需求，提供全面、科学的总体架构设计方案。具体包括但不限于以下内容：（1）总体运营架构；（2）总体系统架构；（3）业务平台关系；（4）数据采集传输；（5）安全服务体系。针对以上5项内容进行评审，每项2分。每缺少一项内容扣2分；每项中每存在一处缺陷或不足扣0.5分，最多扣2分。（注：“缺陷”或“不足”是指不切合行业实际、不符合国家法规政策，或仅有框架或标题、内容过于简略或方案内容生搬硬造，与实际情况不符，存在偏差或存在与项目无关的文字内容，或内容逻辑漏洞或原理错误，或前后内容互相矛盾。）	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

	城市网络安全运营中心设计方案	针对本项目的采购需求，投标人提供城市网络安全运营中心设计方案。城市网络安全运营中心设计方案具体包括但不限于以下内容：（1）平台定位；（2）平台架构设计；（3）平台功能设计；（4）应急响应中心；（5）基础配套设施方案。针对以上5项内容进行评审，每项2分。每缺少一项内容扣2分；每项中每存在一处缺陷或不足扣0.5分，最多扣2分。（注：“缺陷”或“不足”是指不切合行业实际、不符合国家法规政策，或仅有框架或标题、内容过于简略或方案内容生搬硬造，与实际情况不符，存在偏差或存在与项目无关的文字内容，或内容逻辑漏洞或原理错误，或前后内容互相矛盾。）	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

	安全服务方案	针对本项目的采购需求，投标人提供安全服务方案，安全服务方案具体包括但不限于以下内容：（1）应急演练服务方案；（2）网络安全意识培训服务方案；（3）IT资产梳理服务方案；（4）安全配置核查服务方案；（5）互联网暴露面梳理服务方案；（6）漏洞管理服务方案；（7）渗透测试服务方案；（8）数据安全风险评估服务方案；（9）安全策略梳理服务方案；（10）蜜罐诱捕服务方案；（11）安全巡检服务方案；针对以上11项内容进行评审，每项1分。每缺少一项内容扣1分；每项中每存在一处缺陷或不足扣0.5分，最多扣1分。（注：“缺陷”或“不足”是指不切合行业实际、不符合国家法规政策，或仅有框架或标题、内容过于简略或方案内容生搬硬造，与实际情况不符，存在偏差或存在与项目无关的文字内容，或内容逻辑漏洞或原理错误，或前后内容互相矛盾。）	11.0000	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
技术评审					

技术评审	项目重难点分析及应对方案	投标人结合本项目网络安全运营、平台建设、安全服务落地、数据安全防护等实际建设内容，提供完整、贴合本项目的重难点分析及专项应对解决方案。方案具体包括但不限于以下内容：（1）项目建设重难点识别分析；（2）网络安全重难点应对方案；（3）数据安全重难点应对方案；（4）平台部署与业务兼容重难点应对方案；（5）项目实施及运维保障重难点应对方案。针对以上5项内容进行评审，每项1分。每缺少一项内容扣1分；每项中每存在一处缺陷或不足扣0.5分，最多扣1分。（注：“缺陷”或“不足”是指不切合行业实际、不符合国家法规政策，或仅有框架或标题、内容过于简略或方案内容生搬硬造，与实际情况不符，存在偏差或存在与项目无关的文字内容，或内容逻辑漏洞或原理错误，或前后内容互相矛盾。）	5.0000	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

售后服务方案	投标人根据对本项目的理解程度提供售后服务方案，具体包括但不限于以下内容：（1）售后服务人员安排；（2）售后服务响应时间和解决故障时间；（3）售后服务承诺；（4）售后保障措施；针对以上4项内容进行评审，每项2分。每缺少一项内容扣2分；每项中每存在一处缺陷或不足扣0.5分，最多扣2分。（注：“缺陷”或“不足”是指不切合行业实际、不符合国家法规政策，或仅有框架或标题、内容过于简略或方案内容生搬硬造，与实际情况不符，存在偏差或存在与项目无关的文字内容，或内容逻辑漏洞或原理错误，或前后内容互相矛盾。）	8.0000	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

项目服务质量保障方案	投标人根据对本项目的理解程度提供项目服务质量保障方案，具体包括但不限于以下内容：（1）项目人员保障措施；（2）系统及安全设备保障措施；（3）服务质量保障措施；（4）项目风险管理及保密措施；（5）网络安全应急响应预案。针对以上5项内容进行评审，每项2分。每缺少一项内容扣2分；每项中每存在一处缺陷或不足扣0.5分，最多扣2分。（注：“缺陷”或“不足”是指不切合行业实际、不符合国家法规政策，或仅有框架或标题、内容过于简略或方案内容生搬硬造，与实际情况不符，存在偏差或存在与项目无关的文字内容，或内容逻辑漏洞或原理错误，或前后内容互相矛盾。）	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

	保密保障措施方案	投标人根据对本项目的理解程度提供保密保障措施方案，具体包括但不限于以下内容：（1）保密管理；（2）保密措施；（3）保密制度；针对以上3项内容进行评审，每项2分。每缺少一项内容扣2分；每项中每存在一处缺陷或不足扣0.5分，最多扣2分。（注：“缺陷”或“不足”是指不切合行业实际、不符合国家法规政策，或仅有框架或标题、内容过于简略或方案内容生搬硬造，与实际情况不符，存在偏差或存在与项目无关的文字内容，或内容逻辑漏洞或原理错误，或前后内容互相矛盾。）	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

商务评审	服务团队能力	根据投标人提供的服务团队能力进行评审：1.项目负责人具有信息系统项目管理师证书，满足得4分，不满足或未提供不得分。2.团队其他成员：投入本项目的实施团队人员（项目负责人除外）具备计算机、电子工程、通信工程方面的中级及以上职称或系统集成项目管理工程师、信息系统项目管理师、网络工程师证书的，每提供1个得1分，满分2分，重复提供或一人多证不得分。3.投标人明确承诺项目实施过程中变更服务团队会提前告知采购人，且具备切实可行的工作衔接方案、确保项目实施不受影响的，得2分；未提供承诺或承诺不符合要求的，不得分。（注：以上人员须提供相关证书原件扫描件，证书扫描件应当清晰可见，未提供不得分，同一人不重复得分）	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

商务评审	项目业绩	投标人近三年（2023年9月1日至今）承担过类似业绩，每提供一份业绩得2分,最高得2分。（需提供合同扫描件,以合同签订日期为准。）	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

价格评审	价格评审	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。	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

异常低价审查:

采购包1:

序号	评审点要求概况	异常低价的情形

1	异常低价审查	根据《关于推动解决政府采购异常低价问题的通知》（财库〔2026〕2号）等相关规定，政府采购评审中出现下列情形之一的，评审委员会应当启动异常低价投标（响应）审查程序： （1）投标（响应）报价低于全部通过符合性审查供应商投标（响应）报价平均值50%的，即投标（响应）报价<全部通过符合性审查供应商投标（响应）报价平均值×50%。 （2）投标（响应）报价低于通过符合性审查且报价次低供应商投标（响应）报价50%的，即投标（响应）报价<通过符合性审查且报价次低供应商投标（响应）报价×50%。 （3）投标（响应）报价低于最高限价45%的，即投标（响应）报价<最高限价×45%。 （4）评审委员会基于专业判断，认为供应商报价过低，有可能影响产品质量或者不能诚信履约的其他情形。 评审委员会启动异常低价投标（响应）审查后，应当要求相关供应商在评审现场合理的时间内对投标（响应）价格作出解释，提供项目具体成本测算等与报价合理性相关的书面说明及必要的证明材料，包括但不限于原材料成本、人工成本、制造费用等，给予相关供应商的合理时间一般不少于30分钟。其中，属于第3项情形，供应商已随投标（响应）文件一并提交相关书面说明及必要的证明材料的，在评审现场可不再重复提交。评审委员会依据专业经验，参考同类项目中标（成交）价格、类似产品市场价格水平、行业人工费用标准、国家有关部门指导行业协会发布的行业平均成本等情况，对报价合理性进行判断。投标（响应）供应商不能提供书面说明、证明材料，或者提供的书面说明、证明材料不能证明其报价合理性的，评审委员会应当将其作为无效投标（响应）处理。

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。

8.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。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和有关部门备案。

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进行整改，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—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进行整改，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.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	1.政府采购合同（合同名称及编号） 2.中标（成交）公告或中标（成交）通知书 3.招标（磋商、谈判）文件或询价通知书 4.投标（响应）文件 5.供应商的承诺、声明或保证（如有） 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。
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：□通过 □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）	□同意验收结论。 □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

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	1.政府采购合同（合同名称及编号） 2.中标（成交）公告或中标（成交）通知书 3.招标（磋商、谈判）文件或询价通知书 4.投标（响应）文件 5.供应商的承诺、声明或保证（如有） 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。
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：□通过 □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）	□同意验收结论。 □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

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：□通过 □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）	□同意验收结论。 □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：安全运营服务

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