招 标 文 件

（服务类）

采购项目名称：智慧锦江网络安全治理体系服务采购项目

采购项目编号：**N5101042023000209**

成都市锦江区人民政府办公室

四川公众项目咨询管理有限公司共同编制

2023年**11**月**17**日

第一章 投标邀请

四川公众项目咨询管理有限公司（以下简称“代理机构”）受成都市锦江区人民政府办公室委托，拟对智慧锦江网络安全治理体系服务采购项目进行国内公开招标，兹邀请符合本次招标要求的供应商参加投标。

一、采购项目编号：**N5101042023000209**

二、采购项目名称：智慧锦江网络安全治理体系服务采购项目

三、招标项目简介

智慧锦江网络安全治理体系服务采购。

四、供应商参加本次政府采购活动应具备的条件

（一）满足《中华人民共和国政府采购法》第二十二条规定；

（二）落实政府采购政策需满足的资格要求：

执行政府采购促进中小企业发展的相关政策：

本项目所有采购包不专门面向中小企业。

注：监狱企业和残疾人福利性单位视同小微企业，符合中小企业划分标准的个体工商户视同中小企业。

（三）本项目的特定资格要求：

采购包1：

无

五、电子化采购相关事项

本项目实行电子化采购，使用的电子化交易系统为：四川省政府采购一体化平台的项目电子化交易系统（以下简称“项目电子化交易系统”），登录方式及地址：通过四川政府采购网（www.ccgp-sichuan.gov.cn）首页供应商用户登录四川省政府采购一体化平台（以下简称“采购一体化平台”），进入项目电子化交易系统。供应商应当按照以下要求，参与本次电子化采购活动。

（一）供应商应当自行在四川政府采购网-办事指南查看相应的系统操作指南，并严格按照操作指南要求进行系统操作。在登录、使用采购一体化平台前，应当按照要求完成供应商注册和信息完善，加入采购一体化平台供应商库。

(二)供应商应当使用纳入全国公共资源交易平台（四川省）数字证书互认范围的数字证书及签章（以下简称“互认的证书及签章”）进行系统操作。供应商使用互认的证书及签章登录采购一体化平台进行的一切操作和资料传递，以及加盖电子签章确认采购过程中制作、交换的电子数据，均属于供应商真实意思表示，由供应商对其系统操作行为和电子签章确认的事项承担法律责任。

已办理互认的证书及签章的供应商，校验互认的证书及签章有效性后，即可按照系统操作要求进行身份信息绑定、权限设置和系统操作；未办理互认的证书及签章的供应商，按要求办理互认的证书及签章并校验有效性后，按照系统操作要求进行身份信息绑定、权限设置和系统操作。互认的证书及签章的办理与校验，可查看四川政府采购网-办事指南。

供应商应当加强互认的证书及签章日常校验和妥善保管，确保在参加采购活动期间互认的证书及签章能够正常使用；供应商应当严格互认的证书及签章的内部授权管理，防止非授权操作。

（三）供应商应当自行准备电子化采购所需的计算机终端、软硬件及网络环境，承担因准备不足产生的不利后果。

（四）采购一体化平台技术支持：

在线客服：通过四川政府采购网-在线客服进行咨询

400服务电话：4001600900

CA及签章服务：通过四川政府采购网-办事指南进行查询

六、招标文件获取时间、方式及地址

（一）招标文件获取时间：详见采购公告或邀请书

（二）在招标文件获取开始时间前，采购人或代理机构将本项目招标文件上传至项目电子化交易系统，免费向供应商提供。供应商通过项目电子化交易系统获取招标文件。成功获取招标文件的，供应商将收到已获取招标文件的回执函。未成功获取招标文件的供应商，不得参与本次采购活动，不得对招标文件提起质疑。

成功获取招标文件后，采购人或代理机构进行澄清或者修改的，澄清或者修改的内容可能影响投标文件编制的，采购人或代理机构将通过项目电子化交易系统发布澄清或者修改后的招标文件，供应商应当重新获取招标文件。供应商未重新获取招标文件或者未按照澄清或者修改后的招标文件编制投标文件进行投标的，自行承担不利后果。

注：获取的招标文件主体格式包括pdf、word两种格式版本，其中以pdf格式为准。

七、投标文件提交截止时间及开标时间、地点、方式

（一）投标文件提交截止时间及开标时间：详见采购公告或邀请书

（二）投标文件提交方式、地点：供应商应当在投标文件提交截止时间前，通过项目电子化交易系统提交投标文件。成功提交的，供应商将收到已提交投标文件的回执函。

（三）本项目采取网上开标，即采购人或代理机构通过项目电子化交易系统“开标/开启大厅”组织在线开标。

八、本投标邀请在四川政府采购网以公告形式发布

九、供应商信用融资

根据《四川省财政厅关于推进四川省政府采购供应商信用融资工作的通知》（川财采〔2018〕123号）文件，为助力解决政府采购成交供应商资金不足、融资难、融资贵的困难，促进供应商依法诚信参加政府采购活动，有融资需求的供应商可登录四川政府采购网—金融服务平台，选择符合自身情况的“政采贷”银行及其产品，凭项目成交结果、成交通知书等信息在线向银行提出贷款意向申请、查看贷款审批情况等。

十、联系方式

采购人： 成都市锦江区人民政府办公室

地址： 成都市锦江区南三环二段1号

邮编： 610000

联系人： 赵老师

联系电话： 028-86623931

代理机构：四川公众项目咨询管理有限公司

地址： 四川省成都市市辖区中国（四川）自由贸易试验区成都高新区府城大道西段399号6号楼9楼

邮编： 610000

联系人： 杨先生

联系电话： 17628091244

第二章 投标人须知

2.1投标人须知前附表

序号	应知事项	说明和要求
1	采购预算（实质性要求）	本项目各包采购预算金额如下： 采购包1：3,962,200.00元 投标人的采购包投标报价高于采购包采购预算的，其投标文件将按无效处理。
2	最高限价（实质性要求）	详见第三章。 投标人的采购包投标报价高于最高限价的，其投标文件将按无效处理。
3	评标方法	采购包1：综合评分法 （详见第五章）
4	是否接受联合体	采购包1：不接受
5	落实节能、环保、无线局域网	1.根据《财政部发展改革委生态环境部市场监管总局关于调整优化节能产品、环境标志产品政府采购执行机制的通知》（财库〔2019〕9号）相关要求，政府采购节能产品、环境标志产品实施品目清单管理。财政部、发展改革委、生态环境部等部门确定实施政府优先采购和强制采购的产品类别，以品目清单的形式发布并适时调整。 2.本项目采购 无 产品属于节能产品政府采购品目清单中应强制采购的产品范围，供应商应当提供国家确定的认证机构出具的、处于有效期之内的节能产品认证证书，否则作无效投标处理。 3.本项目采购 无 产品属于节能产品政府采购品目清单中应优先采购的产品范围，本项目采购 无 产品属于环境标志产品政府采购品目清单中应优先采购的产品范围，评审得分/响应报价相同的，按供应商提供的优先采购产品认证证书数量由多到少顺序排列。 4.响应产品属于中国政府采购网公布的《无线局域网认证产品政府采购清单》且在有效期内的，按《财政部国家发展改革委信息产业部关于印发无线局域网产品政府采购实施意见的通知》（财库〔2005〕366号）要求优先采购。
6	小微企业（监狱企业、残疾人福利性单位视同小微企业）价格扣除（仅非预留份额采购项目或预留份额采购项目中的非预留部分采购包适用）	关于本项目采购包中执行小微企业（监狱企业、残疾人福利性单位视同小微企业）价格扣除情况、具体扣除比例和规则详见第五章。

7	充分、公平竞争保障措施（实质性要求）	核心产品允许有多个，不同供应商提供了任意一个相同品牌的核心产品，即视为提供相同品牌的供应商。 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采取随机抽取方式确定一个投标人获得中标人推荐资格，其他同品牌投标人不作为中标候选人。 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随机抽取方式确定一个参加评标的投标人，其他投标无效。 核心产品清单详见第三章。 在符合性审查环节提供核心产品品牌不足3个的，视为有效投标人不足3家。
8	不正当竞争预防措施（实质性要求）	在评标过程中，评标委员会认为投标人投标报价明显低于其他通过符合性审查投标人的投标报价，有可能影响产品质量或者不能诚信履约的，评标委员会应当要求其在合理的时间内通过项目电子化交易系统进行书面说明，必要时提交相关证明材料。投标人提交的书面说明，应当加盖投标人公章，在评标委员会要求的时间内通过项目电子化交易系统进行提交，否则视为不能证明其投标报价合理性。投标人不能证明其投标报价合理性的，评标委员会应当将其投标文件作为无效投标处理。
9	投标保证金	本项目不收取投标保证金。
10	履约保证金（实质性要求）	采购包1：不收取
11	投标有效期（实质性要求）	提交投标文件的截止之日起不少于90天。
12	招标代理服务费（实质性要求）	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：代理服务费按照成本加合理利润原则收取，代理服务费以总中标金额为计算基数，采用差额累进法计算收取，中标金额100万（含）以内的部分*1.5%计算，中标金额100万以上的部分*0.8%；按上述方式计算后合计收取。
13	采购结果公告	采购结果将在四川政府采购网予以公告。
14	中标通知书	采购结果公告后，采购人或代理机构通过项目电子化交易系统向中标供应商发出中标通知书；中标供应商通过项目电子化交易系统获取中标通知书。
15	政府采购合同公告、备案	政府采购合同签订之日起2个工作日内，采购人将政府采购合同在四川政府采购网予以公告；政府采购合同签订之日起7个工作日内，采购人将政府采购合同报本级财政部门备案。
16	进口产品	不允许
17	是否组织潜在投标人现场考察	采购包1：组织现场踏勘：否

18	特殊情况	出现下列情形之一的，采购人或者代理机构应当中止电子化采购活动，并保留相关证明材料备查： （一）交易系统发生故障（包括感染病毒、应用或数据库出错）而无法正常使用的； （二）因组织场所停电、断网等原因，导致采购活动无法继续通过交易系统实施的； （三）其他无法保证电子化交易的公平、公正和安全的情况。 出现上述的情形，不影响采购公平、公正的，采购人或者代理机构可以待上述情形消除后继续组织采购活动；影响或者可能影响采购公平、公正的，采购人或者代理机构应当依法废标。
19	报价/分值精确度	所有数据项默认最多可输入/展示至小数点后2位，超出小数点位的数值采用四舍五入的方式进行精确。

2.2总则

2.2.1适用范围

一、本招标文件仅适用于本次公开招标采购项目。

二、本招标文件的最终解释权由成都市锦江区人民政府办公室和四川公众项目咨询管理有限公司享有。对招标文件中供应商参加本次政府采购活动应当具备的条件，招标项目技术、服务、商务及其他要求，评标细则及标准由成都市锦江区人民政府办公室负责解释。除上述招标文件内容，其他内容由四川公众项目咨询管理有限公司负责解释。

2.2.2有关定义

一、“采购人”是指依法进行政府采购的各级国家机关、事业单位、团体组织。本次招标的采购人是成都市锦江区人民政府办公室。

二、“投标人”是指按照采购公告规定获取了招标文件，拟参加投标和向采购人提供货物及相应服务的法人、其他组织或者自然人。

三、“代理机构”是指政府采购集中采购机构和从事政府采购代理业务的社会中介机构。本项目的代理机构是四川公众项目咨询管理有限公司。

四、“网上开标”是指代理机构通过项目电子化交易系统在线完成签到、开标、唱标和记录等活动，供应商通过项目电子化交易系统在线完成投标文件解密、参与开标活动。

五、“电子评标”是指通过项目电子化交易系统在线完成评标委员会组建，开展资格和符合性审查、比较与评价、出具评标报告、推荐中标候选供应商等活动。

2.3招标文件

2.3.1招标文件的构成

一、招标文件是投标人准备投标文件和参加投标的依据，同时也是资格审查、评标的重要依据。招标文件用以阐明招标项目所需的资质、技术、服务及报价等要求、招标投标程序、有关规定和注意事项以及合同主要条款等。本招标文件包括以下内容：

（一）投标邀请；

（二）投标人须知；

（三）招标项目技术、服务、商务及其他要求；

（四）资格审查；

（五）评标办法；

（六）投标文件格式；

（七）拟签订采购合同文本。

二、投标人应认真阅读和充分理解招标文件中所有的事项、格式条款和规范要求。投标人没有对招标文件全面作出实质性

响应所产生的风险由投标人承担。

2.3.2招标文件的澄清和修改

一、在投标文件提交截止时间前，采购人或者代理机构可以对已发出的招标文件进行必要的澄清或者修改。

二、澄清或者修改的内容为招标文件的组成部分，采购人或者代理机构将在四川政府采购网发布更正公告，投标人应及时关注本项目更正公告信息，按更正后公告要求进行响应。更正内容可能影响投标文件编制的，采购人或者代理机构将通过项目电子化交易系统发布更正后的招标文件，投标人应依据更正后的招标文件编制投标文件。若投标人未按前述要求进行投标响应的，自行承担不利后果。

2.4投标文件

2.4.1投标文件的语言

一、投标人提交的投标文件以及投标人与采购人或代理机构就有关投标的所有来往书面文件均须使用中文。投标文件中如附有外文资料，主要部分要对应翻译成中文并附在相关外文资料后面。未翻译的外文资料，评标委员会将其视为无效材料。

二、翻译的中文资料与外文资料如果出现差异和矛盾时，以中文为准。涉嫌提供虚假材料的按照相关法律法规处理。

三、如因未翻译而造成对投标人的不利后果，由投标人承担。

2.4.2计量单位（实质性要求）

除招标文件中另有规定外，本项目均采用国家法定的计量单位。

2.4.3投标货币（实质性要求）

本次项目均以人民币报价。

2.4.4知识产权（实质性要求）

一、投标人应保证在本项目中使用的任何技术、产品和服务（包括部分使用），不会产生因第三方提出侵犯其专利权、商标权或其它知识产权而引起的法律和经济纠纷，如因专利权、商标权或其它知识产权而引起法律和经济纠纷，由投标人承担所有相关责任。采购人享有本项目实施过程中产生的知识成果及知识产权。

二、投标人将在采购项目实施过程中采用自有或者第三方知识成果的，使用该知识成果后，投标人需提供开发接口和开发手册等技术资料，并承诺提供无限期支持，采购人享有使用权（含采购人委托第三方在该项目后续开发的使用权）。

三、如采用投标人所不拥有的知识产权，则在投标报价中必须包括合法使用该知识产权的相关费用。

2.4.5投标文件的组成

投标人应当按照招标文件的要求编制投标文件。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。

投标文件具体内容详见第六章。

2.4.6投标文件格式

一、投标人应按照招标文件第六章中提供的“投标文件格式”填写相关内容。

二、对于没有格式要求的投标文件由投标人自行编写。

2.4.7投标报价（实质性要求）

一、投标人的报价是投标人响应招标项目要求的全部工作内容的价格体现，包括投标人完成本项目所需的一切费用。

二、投标人每种货物及服务内容只允许有一个报价，并且在合同履行过程中是固定不变的，任何有选择或可调整的报价将不予接受，并按无效投标处理。

三、投标文件报价出现前后不一致的，按照招标文件第五章评标办法规定予以修正，修正后的报价经投标人通过项目电子化交易系统进行确认，并加盖投标人（法定名称）电子印章，投标人未在规定时间内确认的，其投标无效。

2.4.8投标有效期（实质性要求）

投标有效期详见第二章“投标人须知前附表”，投标文件未明确投标有效期或者投标有效期小于“投标人须知前附表”中投标有效期要求的，其投标文件按无效处理。

2.4.9投标文件的制作、签章和加密（实质性要求）

一、投标文件应当根据招标文件进行编制，投标人应通过四川政府采购网-办事指南下载投标（响应）客户端，使用客户端编制投标文件。

二、投标人应按照客户端操作要求，对应招标文件的每项实质性要求，逐一如实响应；未如实响应或者响应内容不符合招标文件对应项的要求的，其投标文件作无效处理。

三、投标人完成投标文件编制后，应按照招标文件第一章明确的签章要求，使用互认的证书及签章对投标文件进行电子签章和加密。

四、招标文件澄清或者修改的内容可能影响投标文件编制的，代理机构将重新发布澄清或者修改后的招标文件，投标人应重新获取澄清或者修改后的招标文件，按照澄清或者修改后的招标文件进行投标文件编制、签章和加密。

2.4.10投标文件的提交

一、（实质性要求）投标人应当在投标文件提交截止时间前，通过项目电子化交易系统完成投标文件提交。

二、在投标文件提交截止时间后，采购人或者代理机构不再接受投标人提交投标文件。投标人应充分考虑影响投标文件提交的各种因素，确保在投标文件提交截止时间前完成提交。

2.4.11投标文件的补充、修改、撤回（实质性要求）

投标文件提交截止时间前，投标人可以补充、修改或者撤回已成功提交的投标文件；对投标文件进行补充、修改的，应当先行撤回已提交的投标文件，补充、修改后重新提交。

供应商投标文件撤回后，视为未提交过投标文件。

2.5开标、资格审查、评标和中标

2.5.1开标及开标程序

一、本项目为网上开标项目。网上开标的开始时间为投标文件提交截止时间。成功提交或成功提交和解密电子投标文件的投标人不足3家的，不予开标，采购人或代理机构将作废标处理。

二、开标准备工作

投标文件开启时间前，供应商登录项目电子化交易系统-“开标/开启大厅”，等待代理机构开标。

投标文件提交截止时间前30分钟，投标人登录项目电子化交易系统-“开标/开启大厅”参与开标。

三、解密投标文件（实质性要求）

投标文件提交截止时间后，成功提交投标文件的投标人符合招标文件规定数量的，代理机构将启动投标文件解密程序，解密时间为30分钟；投标人应在规定的解密时间内，使用互认的证书及签章通过项目电子化交易系统进行投标文件解密。投标人未在规定的解密时间内完成解密的，按无效投标处理。

四、开标

解密时间截止或者所有投标人投标文件均完成解密后（以发生在先的时间为准），由代理机构通过项目电子化交易系统对投标人名称、投标文件解密情况、投标报价进行展示。

开标过程中，各方主体均应遵守互联网有关规定，不得发表与采购活动无关的言论。投标人对开标过程和开标记录有疑义，以及认为采购人或代理机构相关工作人员有需要回避的情形的，及时向工作人员提出询问或者回避申请。采购人或代理机构对投标人提出的询问或者回避申请应当及时处理。

投标人完成投标文件解密后，自主决定是否参加网上在线开标，未参加的，视同认可开标结果。

2.5.2查询及使用信用记录

开标结束后，采购人或代理机构根据《关于在政府采购活动中查询及使用信用记录有关问题的通知》（财库〔2016〕125号）的要求，通过“信用中国”网站（www.creditchina.gov.cn）、“中国政府采购网”网站（www.ccgp.gov.cn）等渠道，查询投标人在投标文件提交截止时间前的信用记录并保存信用记录结果网页截图，拒绝列入失信被执行人名单、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单中的供应商参加本项目的采购活动。

两个以上的自然人、法人或者其他组织组成一个联合体，以一个投标人的身份共同参加政府采购活动的，将对所有联合体

成员进行信用记录查询，联合体成员存在不良信用记录的，视同联合体存在不良信用记录。

2.5.3资格审查

详见招标文件第四章。

2.5.4评标

详见招标文件第五章。

2.5.5中标通知书

一、采购人或者评标委员会确认中标供应商后，代理机构在四川政府采购网发布中标结果公告、通过项目电子化交易系统发出中标通知书，中标供应商通过项目电子化交易系统获取中标通知书。

二、中标通知书是采购人和中标供应商签订政府采购合同的依据，是合同的有效组成部分。如果出现政府采购法律法规、规章制度规定的中标无效情形的，将以公告形式宣布发出的中标通知书无效，中标通知书将自动失效，并依法重新确定中标供应商或者重新开展采购活动。

三、中标通知书对采购人和中标供应商均具有法律效力。

2.6签订及履行合同和验收

2.6.1签订合同

一、采购人应在中标通知书发出之日起三十日内与中标人签订采购合同。

二、采购人和中标人签订的采购合同不得对招标文件确定的事项以及中标人的投标文件作实质性修改。

2.6.2合同分包和转包（实质性要求）

2.6.2.1合同分包

一、投标人根据招标文件的规定和采购项目的实际情况，拟在中标后将中标项目的非主体、非关键性工作分包的，应当在投标文件中载明分包承担主体，分包承担主体应当具备相应资质条件且不得再次分包。

二、分包履行合同的部分应当为采购项目的非主体、非关键性工作，不属于中标人的主要合同义务。

三、采购合同实行分包履行的，中标人就采购项目和分包项目向采购人负责，分包供应商就分包项目承担责任。

四、中小企业依据《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）规定的政策获取政府采购合同后，小型、微型企业不得将合同分包或转包给大型、中型企业，中型企业不得将合同分包或转包给大型企业。

采购包1：不允许合同分包；

2.6.2.2合同转包

一、严禁中标供应商将本项目转包。本项目所称转包，是指将本项目转给他人或者将本项目全部肢解以后以分包的名义分别转给他人的行为。

二、中标供应商转包的，视同拒绝履行政府采购合同，将依法追究法律责任。

2.6.3采购人增加合同标的的权利

采购合同履行过程中，采购人需要追加与合同标的相同的货物或者服务的，在不改变合同其他条款的前提下，可以与中标人协商签订补充合同，但所有补充合同的采购金额不得超过原合同采购金额的百分之十。

2.6.4履行合同

一、合同一经签订，双方应严格履行合同规定的义务。

二、在合同履行过程中，如发生合同纠纷，合同双方应按照《中华人民共和国民法典》规定及合同条款约定进行处理。

2.6.5履约验收方案

采购包1：

1）验收组织方式：自行验收

2）是否邀请本项目的其他供应商：否

3）是否邀请专家：否

4）是否邀请服务对象：否

5）是否邀请第三方检测机构：否

6）履约验收程序：一次性验收

7）履约验收时间：

供应商提出验收申请之日起30日内组织验收

8）验收组织的其他事项：履约验收各条款间有不一致时，按较高标准进行。

9）技术履约验收内容：按招标文件要求及中标人应答服务内容验收。

10）商务履约验收内容：按招标文件要求及中标人应答服务内容验收。

11）履约验收标准：

采购人将按照本项目采购文件、中标人投标文件、合同约定的考核内容与《财政部关于进一步加强政府采购需求和履约验收管理的指导意见》(财库〔2016〕205号)等有关法律法规的规定进行考核验收。

12）履约验收其他事项：以合同签订时约定为准。

2.6.6资金支付

采购人按财政部门的相关规定及采购合同的约定进行支付。

2.7纪律要求

2.7.1评标活动纪律要求

采购人、代理机构应保证评标活动在严格保密的情况下进行，采购人、代理机构、投标人和评标委员会成员应当严格遵守政府采购法律法规规章制度和本项目招标文件以及代理机构现场管理规定，接受采购人委派的监督人员的监督，任何单位和个人不得非法干预和影响评标过程和结果。

对各投标人的商业秘密，评标委员会成员应予以保密，不得泄露给其他投标人。

2.7.2投标人不得具有的情形（实质性要求）

投标人参加投标不得有下列情形：

一、有下列情形之一的，视为投标人串通投标：

（一）不同投标人的投标文件由同一单位或者个人编制；

（二）不同投标人委托同一单位或者个人办理投标事宜；

（三）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；

（四）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；

（五）不同投标人的投标文件相互混装；

二、提供虚假材料谋取中标；

三、采取不正当手段诋毁、排挤其他投标人；

四、与采购人或代理机构、其他投标人恶意串通；

五、向采购人或代理机构、评标委员会成员行贿或者提供其他不正当利益；

六、在招标过程中与采购人或代理机构进行协商谈判；

七、中标后无正当理由拒不与采购人签订政府采购合同；

八、未按照招标文件确定的事项签订政府采购合同；

九、将政府采购合同转包或者违规分包；

十、提供假冒伪劣产品；

十一、擅自变更、中止或者终止政府采购合同；

十二、拒绝有关部门的监督检查或者向监督检查部门提供虚假情况；

十三、法律法规规定的其他禁止情形。

投标人有上述情形的，按照规定追究法律责任，具有前述一至十三条情形之一的，其投标文件无效，或取消被确认为中标供应商的资格或认定中标无效。

2.7.3采购人员及相关人员回避要求

政府采购活动中，采购人员及相关人员与投标人有下列利害关系之一的，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；

（2）参加采购活动前3年内担任投标人的董事、监事；

（3）参加采购活动前3年内是投标人的控股股东或者实际控制人；

（4）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；

（5）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。

投标人认为采购人员及相关人员与其他投标人有利害关系的，可以向代理机构书面提出回避申请，并说明理由。代理机构将及时询问被申请回避人员，有利害关系的被申请回避人员应当回避。

2.8询问、质疑和投诉

一、询问、质疑、投诉的接收和处理严格按照《中华人民共和国政府采购法》《中华人民共和国政府采购法实施条例》《政府采购质疑和投诉办法》等规定办理。

二、供应商询问、质疑的答复主体：

根据委托代理协议约定，供应商对招标文件中采购需求的询问、质疑由 成都市锦江区人民政府办公室 负责答复；供应商对除采购需求外的采购文件的询问、质疑由四川公众项目咨询管理有限公司 负责答复；供应商对采购过程、采购结果的询问、质疑由 四川公众项目咨询管理有限公司 负责答复。

三、供应商提出的询问，应当明确询问事项，如以书面形式提出的，应由供应商签字并加盖公章。

为提高采购效率，降低社会成本，鼓励询问主体对于不损害国家及社会利益或自身合法权益的问题或情形采用询问方式处理解决（包含但不限于文字错误、标点符号、不影响投标文件的编制的情形）。

四、供应商认为采购文件、采购过程、中标或者成交结果使自己的权益受到损害的，可以在知道或者应知其权益受到损害之日起7个工作日内，以书面形式向采购人、代理机构提出质疑。供应商应在法定质疑期内一次性提出针对同一采购程序环节的质疑。供应商应知其权益受到损害之日，是指：

（一）对可以质疑的采购文件提出质疑的，为收到采购文件之日或者采购文件公告期限届满之日；

（二）对采购过程提出质疑的，为各采购程序环节结束之日；

（三）对中标或者成交结果提出质疑的，为中标或者成交结果公告期限届满之日。

五、本项目不接受在线提交质疑，供应商通过书面形式线下向采购人或代理机构提交质疑资料。

六、供应商提出质疑时应当准备的资料

（一）质疑函正本1份；（政府采购供应商质疑函范本详见附件一）

（二）法定代表人或主要负责人授权委托书1份（委托代理人办理质疑事宜的需提供）；

（三）法定代表人或主要负责人身份证复印件1份；

（四）委托代理人身份证复印件1份（委托代理人办理质疑事宜的需提供）；

（五）针对质疑事项必要的证明材料（针对招标文件提出的质疑，需提交从项目电子化交易系统获取的招标文件回执单）。

答复主体：代理机构

联系人：杨先生

联系电话：17628091244

地址：四川省成都市市辖区中国（四川）自由贸易试验区成都高新区府城大道西段399号6号楼9楼

邮编：610000

注：根据《中华人民共和国政府采购法》的规定，供应商质疑不得超出招标文件、采购过程、采购结果的范围。

七、供应商对采购人或代理机构的质疑答复不满意，或者采购人或代理机构未在规定期限内作出答复的，供应商可以在答复期满后15个工作日内向同级财政部门提起投诉。

投诉受理单位：本采购项目同级财政部门。（政府采购供应商投诉书范本详见附件二）

第三章 招标项目技术、服务、商务及其他要求

（注：当采购包的评标方法为综合评分法时带“★”的参数需求为实质性要求，供应商必须响应并满足的参数需求，采购人、采购代理机构应当根据项目实际需求合理设定，并明确具体要求。带“▲”号条款为允许负偏离的参数需求，若未响应或者不满足，将在综合评审中予以扣分处理。）

（注：当采购包的评标方法为最低评标价法时带“★”的参数需求为实质性要求，供应商必须响应并满足的参数需求，采购人、采购代理机构应当根据项目实际需求合理设定，并明确具体要求。）

3.1采购项目概况

为贯彻落实“一流城市要有一流治理，要注重在科学化、精细化、智能化上下功夫”的重要论述精神和网络强国、数字中国、智慧社会等系列决策部署，根据市委、市政府有关“智慧蓉城”建设的工作部署，加快推进城市运行“一网统管”建设，进一步推动超大型城市安全运行、服务完善、科学治理。 成都市第十四次代表大会提出，“今后五年，成都将积极探索超大城市现代化治理新路径，提升城市智慧治理水平”，成都市政务服务管理和网络理政办公室同时也正式印发《成都市“十四五”新型智慧城市建设规划》（以下简称《规划》），系统谋划了未来五年，成都建设智慧城市的发展路径。《规划》中明确要求，建设全域安全支撑体系和协同保障支撑体系，具体包括围绕安全保障机制、网络安全保障、数据安全防护和安全技术创新，构建全域网络和数据安全支撑体系；建立完善的运营运维保障支撑体系，建立健全安全保障机制，增强网络安全保障能力，提高数据安全防护水平，加强网络安全技术创新，全面支撑智慧蓉城建设高效运行。 当前，锦江区正持续推动数字赋能智慧锦江建设，全面推动城市经济、生活、治理数字化转型，让城市运转更聪明、更智慧。本次安全治理体系服务采购正是立足实际需求，构建起与“智慧锦江”运行中心配套的网络安全治理体系服务，提升系统安全防范能力，为安全运行保驾护航。 本次“智慧锦江”网络安全治理体系服务采购，主要的建设目标如下： 1、满足安全合规性要求。依据网络安全等级保护2.0 三级标准，按照“统一规划、重点明确、合理建设”的基本原则，在安全物理环境、安全通信网络、安全区域边界、安全计算环境和安全管理中心等方面进行安全规划与建设，确保“网络建设合规、系统安全防护到位”。 2、提高数据安全保障能力。通过专业的数据安全治理服务，针对“智慧锦江”相关业务系统进行专项治理，围绕数据分类分级与风险合规服务为核心，为锦江区智慧城市提供数据安全治理服务各项能力。 3、为智慧锦江项目提供全面的网络安全服务，确保信息系统和数据的安全性、完整性和可用性，并帮助客户应对潜在的安全风险，同时提供全天候威胁实时监测处置服务，在发生安全事件或紧急情况时，提供快速响应和支持，帮助客户完成应急响应、溯源分析、处置加固等工作，以最小化安全事件带来的损失。

3.2服务内容及服务要求

3.2.1服务内容

采购包1：

采购包预算金额（元）: 3,962,200.00

采购包最高限价（元）: 3,962,200.00

序号	标的名称	数量	标的金额 （元）	计量单位	所属行业	是否涉及核心产品	是否涉及采购进口产品	是否涉及采购节能产品	是否涉及采购环境标志产品
1	智慧锦江网络安全治理体系服务	1.00	3,962,200.00	项	软件和信息技术服务业	否	否	否	否

3.2.2服务要求

采购包1：

标的名称：智慧锦江网络安全治理体系服务

参数性质	序号	技术参数与性能指标
		一、服务要求 （一）本项目主要是服务锦江区智慧蓉城运行管理平台以及配套基础设施，保障其网络安全、数据安全，促进数据安全流转。从而间接实现采购人的政务目标，主要包括： 1、提高锦江区城市精细化管理服务水平 聚焦群众需求和城市治理的突出问题，围绕“高效处置一件事”，重点从城市规划、城市建设、城市管理、公共卫生、应急管理、公共安全、生态环境、交通管理、公园城市、水务管理、市场监管等领域着手，充分利用现有信息系统和数据资源，打造“一件事”高效处置应用场景，实现城市运行管理服务快速反应、信息交互、联勤联动。促进城市管理工作中实现从任务导向向需求导向的转变，从局部治理向体系化治理的转变，从二维空间向立体空间的转变，从硬件为主向软硬件结合为主的转变，全面提高资源整合效率、信息流转效率、综合统筹效率、精细管理效率以及预警、发现和处置效率。 2、深化锦江区城市综合管理上下联动多方协同 城市管理涉及面广、领域宽泛、具有综合性、开放性、动态性三大特点，城市管理主体需由单一向多元转变提升，城市管理理念由粗放型向精细化转变提升，涉及市政配套、林园管护、市场规范、交通畅通等方方面面，单兵作战，力量有限。依托锦江区城市运行管理服务平台，将市容市貌、园林绿化、市政基础设施运行、在建工程项目管理、房屋安全、小区管理、公共空间秩序、突发事件处置等城市治理事项统一纳入平台管理，推动跨部门、跨区域、跨层级应用，强化综合治理、统筹协调、指挥监督和综合评价。通过整合各方资源，建立部门之间信息互通、资源共享、协调联动的工作机制，形成管理合力，推送城市管理手段由传统向现代转变提升，城市环境由无序向有序转变提升，城市品位由低端小气向高端大气转变提升，逐步实现真正意义上的城市综合管理。 3、提升锦江区城市运行风险感知防控能力 积极适应锦江区城市运行安全管理需要，利用物联网、数字孪生、虚拟仿真等技术，依托锦江区城市运行管理服务平台建设，汇聚应急、住建、城管、交通运输、旅游等数据资源，面向城市安全高风险区域，在重点行业领域，持续拓展全域安全感知网络，实时监测城市建设运营重大项目、重点工程、重要部位安全运行状况，洞察城市运行安全全局，提升城市安全风险感知灵敏度、风险研判准确度和应急反应及时度。用信息化手段助推成都市城市安全发展，让感知神经遍布城市肌理，不断夯实锦江区城市安全发展本底，提升锦江区城市安全智慧治理能力，不断增强群众的安全感、获得感、幸福感。 4、推动锦江区城市运行管理服务数据资源整合汇聚 打通区规划和自然资源局、区住建局、区城管委、区卫健委、区应急局、区公安局、区生态环境局、区交通运输局、区公园城市局、区水务局、区市场监管局等多个横向部门，国家、省级、区（县）多个纵向平台的网络和系统，推动整合人口、交通、能源、建设等公共设施信息和公共基础服务，形成综合性城市管理数据库，汇聚多种类型的锦江区城市运行综合管理政务数据，为统筹全区城市运行综合管理数据资源奠定基础。基于“运行中心”和数据资源共享交换体系，依托区级CIM基础平台，汇聚锦江区城市运行管理服务基础数据、锦江区城市管理部件事件数据、行业应用场景数据、公众诉求数据、监测数据等，加强数据治理，构建锦江区城市运行管理服务数据资源池，支撑各类“一件事”高效处置应用场景。进一步融合数据、技术及业务三大智慧应用基本要素，建设信息能力、技术能力、

业务能力，实现锦江区城市运行综合管理数据资源的有效分类、技术资源充分共享、业务服务高度协同，快速响应各类智慧应用建设需求，解决要素流通过程中存在的安全问题、协同问题等。

5、符合相关法律法规及上级单位的安全保障要求

使锦江区城运平台的安全体系的设计可以符合市智慧蓉城建设中安全运行能力构建的指导意见，同时提前规避在推进智慧蓉城建设中的各个方面的可能遭遇的网络安全风险，建设符合锦江区信息化实际情况的网络安全保障体系。并且，梳理锦江区城运平台进行整体安全防护在等级保护的基础之上进行整改工作，促进安全体系的建设成果通过国家权威测评机构测评，最终满足智慧蓉城建设的安全防护要求。

（二）具体服务要求：

说明：投标人必须真实响应以下服务要求的满足情况，标“★”项需提供承诺函承诺并加盖投标人公章。在中标后，采购人可要求投标人在一定时间内进行实网测试。

序号	服务工具名称	服务工具要求

		1	网络安全态势感知服务	1、★配置流量处理能力≥4G； 2、支持流量探针统一升级管理，并监控流量探针与安全组件的运行状态，包含日志传输模式、日志传输量、最近同步信息； 3、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（上传下载）阶段的异常，对挖矿早期的准备动作即告警； 4、支持不少于16个大屏的展示界面，包括全网安全态势感知大屏、分支安全态势、安全事件态势、通报预警态势、资产态势大屏，同时能满足多种场景的监控，比如日常运维、护网场景； 5、支持自定义资产管理，新增安全业务域，自定义安全域名称、属性、责任人、邮箱、IP，并将配置文件通过CSV形式导入导出； 6、支持利用EBA技术进行资产的行为分析，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。并支持用户对EBA基线进行自定义调整，优化模型； 7、支持一建检测评估配置的状态和探针配置的状态，已告警的方式提醒和处置建议提醒用户解决和闭环，包括基础配置、平台运行状况、接入设备状况、流量检测情、代理识别、探针加固检测、平台加固检测； 8、▲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；（提供服务工具功能截图并加盖投标人公章） 9、弱密码检测规则支持高度自定义，包括规则名称、生效域名、长度规则、字符规则、字典序、web空密码、账号白名单、密码白名单、txt文件格式导入； 10、支持WEB应用防护识别库、IPS漏洞利用检测识别库、实时漏洞分析识别库、黑客工具检测识别库，且具备自定义的web防护识别库、漏洞利用检测检测引擎； 11、▲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（上传下载）阶段的异常，对挖矿早期的准备动作即告警；（提供服务工具功能截图并加盖投标人公章） 12、服务工具支持资产身份认证功能，并与流量探针做资产用户名对接，实现精准识别终端资产责任人；

		2	日志审计服务	1、★配置资产授权数量≥300个； 2、服务工具内置日志处理模型，自动解析主流网络设备、安全设备和中间件的日志数据，标准化自动识别系统类型至少达到200种； 3、▲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，并对对解析结果字段进行新增、合并、映射；（提供服务工具功能截图并加盖投标人公章） 4、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； 5、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、指定语段进行语法搜索；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（可具体到外网、内网资产）、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； 6、支持单条事件进行展开，显示事件详细信息和事件原始信息，支持事件详情中任意字段作为查询条件无限制进行二次检索分析； 7、▲为了实现对不同编码格式的解析，服务工具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；（提供服务工具功能截图并加盖投标人公章） 8、支持可视化展示，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，可提供设备专项分析场景。如防火墙外部攻击场景分析、VPN账号异常场景分析、Windows服务器主机异常场景分析，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； 9、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，指定IP免认证直接进入平台； 10、▲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。（提供服务工具功能截图并加盖投标人公章）

3	主机入侵检测服务	1、★客户端授权大于等于200个； 2、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； 3、支持首页展示全网风险、安全事件，包括但不限于安全事件统计、弱密码检测Top5、漏洞影响面Top5、未处理的安全事件、实时风险监控、资产概览等模块； 4、支持依据指纹信息统计并显示关联的主机数量及详细信息，可从监听端口、运行进程、系统账号、数据库、软件资产、web资产的角度统计并显示相关信息； 5、支持基于语法分析、AI检测等技术从脚本文件静态分析的角度来对webshell后门文件实时检测，并提供文件md5值、下载路径，影响域名等信息，管理员可对其做批量处理； 6、▲支持windows服务器RDP远程登录保护，可开启RDP远程登录二次认证，以防止黑客对服务器的入侵；（提供服务工具功能截图并加盖投标人公章） 7、▲支持Linux服务器SSH远程登录保护，可开启SSH远程登录二次认证，以防止黑客利用弱密码脆弱性对服务器的入侵；（提供服务工具功能截图并加盖投标人公章） 8、支持对黑客常用的恶意命令，异常编码绕过命令进行检测，对于符合特征的行为进行实时告警，并提供进程执行的详细进程树信息； 9、支持ssh端口转发检测，对符合端口转发特征的行为实时告警，并提供进程执行的详细进程树信息； 10、▲支持跳转链接至云端威胁情报中心，针对已发生的威胁提供详细的分析结果，包含威胁分析、网络行为、静态分析、分析环境和影响分析。（提供服务工具功能截图并加盖投标人公章） 11、支持对入侵检测事件通过隔离主机操作进行响应,阻断主机网络访问行为；支持对全部主机，全部漏洞进行全局检测，并可自定义漏洞扫描策略，进行漏洞作业的新建、编辑、删除和执行；支持与网络安全态势感知服务联动，主机入侵检测服务采集主机侧流量、行为分析上报给网络安全态势感知服务，帮助网络安全态势感知服务定位和分析问题。

		4	终端威胁检测与响应服务	1、★配置PC版授权≥300套； 2、具备高兼容性，在识别到终端存在非适配的第三方软件时可使用兼容模式进行安装，灵活调整agent策略，提供流畅的终端体验； 3、采用B/S架构的管理控制中心，对终端进行安全可视化、终端统一管理、统一威胁处置、统一漏洞修复、威胁响应处置、日志记录与查询； 4、▲为避免终端因威胁导致终端无法正常开展业务，服务工具需支持跳转链接至云端安全威胁响应系统，针对已发生的威胁提供详细的威胁分析、网络行为、静态分析、分析环境和影响分析；（提供第三方检测机构出具的相关证明材料并加盖投标人公章） 5、支持终端全网风险展示，包括但不限于未处理的勒索病毒数量、高级威胁、暴力破解、僵尸网络、WebShell后门、高危漏洞及其各自影响的终端数量； 6、支持安全策略一体化配置，通过单一策略即可实现不同安全功能的配置，包括：终端病毒查杀的文件扫描配置、文件实时监控的参数配置、WebShell检测和威胁处置方式、暴力破解的威胁处置方式和Windows白名单信任目录； 7、▲支持全网风险状况展示，如未处理的（勒索）病毒数量、暴力破解数量、WebShell后门数量、高危漏洞及其各自影响的终端数量；（提供第三方检测机构出具的检测报告并加盖投标人公章） 8、支持终端自动分组管理，新接入的终端可以根据网段自动分配到对应的分组； 9、支持导出针对全网终端的终端风险报告，从整体分析全网安全状况，快速了解业务和网络的安全风险，提供安全规划建设建议； 10、支持收集并展示单个终端的基本信息，包括：主机名、在线/离线状态、IPv4地址、MAC地址、操作系统、终端agent版本、病毒库版本、最近登录时间、最近登录的用户名；终端信息变更能自动更新； 11、▲具备终端侧系统层、应用层行为数据采集能力，数据采集面覆盖ATT&CK技术面不少于163项；（数据覆盖面需提供第三方机构出具的证明材料并加盖投标人公章） 12、为了防止挖矿攻击对业务的影响，本次方案需提供挖矿病毒巡检工具，通过内存、进程和启动项来检索病毒相关信息；

5	终端安全认证服务	★1、配置接入终端授权许可≥1000个终端设备； ▲2、提供多因素认证方式，包括动态口令、指纹、人脸、扫码认证方式集成，支持多种认证方式支持组合使用；（提供服务工具功能截图并加盖投标人公章） 3、提供终端人员安全防护能力，支持离席锁屏、围观锁屏、外设脱机锁屏、异地脱机登录等能力； 4、终端设备安全绑定功能，能够与用户绑定、解绑能力； 5、系统具备应急逃生能力，保留原有操作系统的认证方式（多认证方式共存），可在任何紧急情况可选择原有操作系统的认证方式登入系统，也可在网络中断后离线完成终端桌面登录； 6、认证页面支持进行自定义管理，对于登录界面的背景图、登录界面的Logo均可进行自定义切换； 7、终端用户能够智能安全无感接入网络，实现真正的无感登录SSO体验。仅执行一次认证，所有C/S应用、Web应用可以使用认证票据，自动完成应用的单点登录、全网漫游从而提升终端用户体验

		6	脆弱性检测服务	1、★配置系统漏扫授权IP数≥1000，WEB漏扫授权URL数≥200； 2、支持全局风险统计时段自定义，展示近3个月、6个月、1年或自定义统计区间的风险分布和详情，时间跨度不限制； 3、▲支持全局风险统计功能，通过扇形图、条状图、标签、表格形式直观展示资产风险分布、漏洞风险等级分布、紧急漏洞、风险资产清单信息，并可查看详情；（提供服务工具功能截图并加盖投标人公章） 4、支持从“高危”、“中危”、“低危”、“信息”四个安全级别展示漏洞风险等级的分布情况； 5、支持从漏洞视角分类型呈现风险概览和详情信息，支持在线查看展示“系统漏洞”、“WEB漏洞”、“弱口令”和“基线风险”的名称、风险等级、影响资产数、漏洞数、最近发现时间，并可关联漏洞详情。漏洞详情可支持展示漏洞名称、漏洞类型、发现时间、影响资产、漏洞描述、漏洞影响、修复建议、CVE编号和举证信息； 6、支持全面扫描、资产发现、系统漏洞扫描、弱口令扫描、WEB漏洞扫描、基线配置核查六种任务类型，其中全面扫描支持系统漏洞扫描、WEB漏洞扫描、弱口令扫描同时执行； 7、资产发现支持并发扫描数量自定义，最大并发扫描IP数为1024； 8、▲提供检测结果综述分析，按照等保2.0的检测项要求，统计客户业务系统存在的不符合、部分符合、符合、待确认、不适用检测项，直观了解自身业务系统合规情况；（提供服务工具功能截图并加盖投标人公章） 9、资产发现支持任务立即执行、指定时间执行和周期执行三种执行方式，且指定时间可以精确到分钟，周期执行可精确到每日、每周、每月和自定义周期等； 10、支持检测的漏洞数大于等于230000条，兼容CVE、CNNVD、CNVD、Bugtraq等主流标准； 11、▲支持域管理功能，系统默认内置数据域、终端接入域、运维管理域、其他业务域、核心业务域、核心交换域、对外服务域、外联域、互联网出口域等，可根据客户实际情况进行自定义管理；（提供服务工具功能截图并加盖投标人公章） 12、支持报表过滤功能，支持从任务类型、任务/资产、风险等级、漏洞/基线类型等角度筛选和过滤报表生成条件；系统漏洞扫描支持任务立即执行、指定时间执行和周期执行三种执行方式，且指定时间可以精确到分钟，周期执行可精确到每日、每周、每月和自定义周期。

		7	WEB应用防护服务	1、★配置带宽性能≥800Mbps，七层新建会话数≥8万/秒，七层并发会话数≥400万；本服务要求提供≥6套服务工具，本服务接入服务总访问带宽流量大于等于4G。 2、▲服务工具内置不低于10000种漏洞规则，同时支持在控制台界面通过漏洞ID、漏洞名称、危险等级、漏洞CVE标识、漏洞描述条件查询漏洞特征信息，支持用户自定义IPS规则；（提供服务工具功能截图并加盖投标人公章） 3、服务工具通过协议对链路连通性进行探测，探测协议至少包括DNS解析、ARP探测、PING和BFD等方式； 4、为保证链路带宽和链路可靠性，服务工具支持链路聚合功能，将多个物理链路组合成一个性能更高的逻辑链路接口； 5、支持NAT穿透技术ALG，支持FTP、TFTP、SQLNET、PPTP、RTSP、SIP、H.323等协议； 6、服务工具支持基于应用、服务、时间、域名、IPv6对象等维度的访问控制； 7、▲服务工具支持对不少于9000种应用的识别和控制，应用类型包括游戏、购物、图书百科、工作招聘、P2P下载、聊天工具、旅游出行、股票软件等类型应用进行检测与控制；（提供服务工具功能截图并加盖投标人公章） 8、服务工具支持异常数据包攻击防御，防护类型包括IP数据块分片传输防护、Teardrop攻击防护、Smurf攻击防护、Land攻击防护、WinNuke攻击防护等攻击类型； 9、服务工具支持对压缩病毒文件进行检测和拦截，压缩层数支持15层及以上。 10、服务工具支持杀毒白名单设置，可以例外排除特定MD5和URL的病毒文件，针对特定文件不进行查杀； 11、服务工具支持僵尸主机检测功能，内置僵尸网络特征库超过128万种，可识别主机的异常外联行为； 12、▲为降低采购人内网遭受勒索病毒攻击的概率，服务工具需支持勒索病毒检测与防御功能；（并服务工具功能截图证明以及第三方法检测机构出具关于“勒索病毒”的证书或检测报告证明功能有效性） 13、服务工具内置超过4500种WEB应用攻击特征，支持对跨站脚本（XSS）攻击、SQL注入、文件包含攻击、信息泄露攻击、WEBSHELL、网站扫描、网页木马等攻击类型进行防护； 14、支持安全策略有效性分析功能，分析内容至少包括策略冗余分析、策略匹配分析、风险端口风险等内容，提供安全策略优化建议； 15、▲支持与网络安全态势感知服务联动，将安全日志等数据上报至网络安全态势感知服务，并在网络安全态势感知服务进行威胁展示。（提供服务工具功能截图并加盖投标人公章）

8	高级威胁分析服务	1、★配置网络层吞吐量≥2Gbp，本服务接入服务总访问带宽流量大于等于4G； 2、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； 3、支持Application漏洞攻击、File漏洞攻击、Scan漏洞攻击、Shellcode漏洞攻击、System漏洞利用攻击、Web Activex等客户端漏洞攻击检测； 4、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； 5、▲支持不少于5种类型日志传输模式，包含标准模式、精简模式、高级模式、局域网模式、自定义模式，适应不同应用场景需求；（提供服务工具功能截图并加盖投标人公章） 6、支持传输访问检测日志，包括正常访问、风险访问、违规访问； 7、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； 8、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、自定义WAF规则、WAF云防护； 9、支持设备内置简单命令行管理窗口，便于基础运维调试； 10、▲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，端口类型至少包括3389、53、80/8080、21、69、443、25、110、143、22；（提供服务工具功能截图并加盖投标人公章） 11、支持FTP、IMAP、MS Sql、Mysql、Oracle、POP3、RDP、SMTP、SSH、Telnet、VNC等协议暴力破解检测。

9	零信任安全访问服务	1、★配置接入授权许可≥300套； 2、为充分利用设备的网络性能，控制中心部署时支持配置聚合网口，并支持将聚合网口作为控制中心的网络部署IP； 3、为了使系统资源利用最大化，本地集群与分布式集群下各节点的零信任授权数均可共享使用，集群的总接入授权数是各节点授权数的总和； 4、▲支持终端环境诊断排查，提供终端诊断工具，支持对当前终端的基本环境进行扫描和一键修复，便于员工自行排查修复终端问题，减少IT运维人员工作；（提供服务工具功能截图并加盖投标人公章） 5、通过WEB模式，可以支持基于http或https协议代理访问业务资源，支持发布IP或域名形式的后端服务器地址，可配置业务应用的具体访问URL路径； 6、▲为提升业务应用的安全性，零信任系统应支持业务隐身，最大程度缩小网络、业务暴露面，提供单包授权能力，支持UDP+TCP组合的单包授权技术，未授权用户无法连接零信任设备，无法扫描到服务端口，不会出现敲门放大漏洞；授权方式通过安全码激活客户端，从而可进行敲门和连接，安全码支持共享码和一人一码两种模式，支持短信分发安全码，保障业务的安全性；（提供服务工具功能截图并加盖投标人公章） 7、支持以私有DNS发布企业资源，无需额外购买DNS服务即可使用域名访问内网资源，支持管理员自主配置是否允许从具体网络区域（局域网/互联网）接入时使用此私有DNS解析地址； 8、为符合单位合规性要求，管理员可自主编辑用户访问未授权应用时的告警内容； 9、▲为节省资源，可灵活启用工作空间，允许用户在满足特定条件的情况下才启用沙箱策略，如资产的终端在内网使用时无需启用沙箱办公、员工个人终端在互联网接入时才需要启用沙箱办公，应支持对指定工作空间或全部工作空间配置沙箱准入策略；（提供服务工具功能截图并加盖投标人公章） 10、支持终端设备的可视管理，如查看同账号登录过的终端信息，包括但不限于设备名称、设备系统类型、接入地址、最后登录时间等； 11、▲支持将用户访问零信任系统的认证及策略类请求加密流量解密后镜像给外部系统，如虚拟化安全感知管理平台，以完善系统的用户行为审计溯源能力；（提供服务工具功能截图并加盖投标人公章） 12、为了进一步保障用户身份安全，需支持多因素认证，支持管理员结合已对接的主认证和辅认证类型进行设置，可自由选择采用首次认证+二次认证+终端认证+增强认证等方式；	

0	数据安全管理体系建设服务	**★1、服务范围：** 成都市锦江区，采购人指定范围。 **★2、服务频率：** 1年，每年1次。 **3、服务内容要求：** 基于数据安全法、等级保护管理要求、DSMM数据安全能力成熟度模型等相关法律法规、标准规范要求，结合实际情况，通过提供咨询完善数据安全管理组织，协助完善制定数据安全策略、制度和流程等管理体系。具体服务内容包括： **（1）数据安全组织规划** 按照决策层、管理层、执行层、供应商/服务商、监督层的组织架构，提供设计锦江区数据安全组织规划设计服务，明确已有安全团队与其它相关部门数据安全的工作职能。 **（2）数据安全制度体系建设** 参考政务数据安全保障的地方性法规、顶层设计以及标准规范等，建立锦江区内部制度规范去约束和规范相关人员开展锦江区智慧蓉城数据安全保障工作，并赋予管理人员监督管理职责。 **4、服务方式：** 数据安全管理体系建设服务采用现场人工服务的方式开展，由中标人指派数据安全专家现场开展。 **★5.服务交付物：** 协助编制和优化一级方针总纲、二级数据安全管理制度，指导编制三、四级文档。

11	数据安全资产梳理服务	**★1、服务范围：** 为锦江区城市运行管理大屏、城市运行管理中屏、城市运行管理小屏、事件枢纽系统、数据资源平台、报表通、数据资源调度平台、居民端八个核心业务系统提供数据安全资产梳理服务。 **★2、服务频率：** 1年，每年1次统一梳理，并根据业务资产变化进行持续更新。 **3、服务内容要求：** 通过发现网络环境内各类数据资产，并对数据资产主机、数据资产的内部结构信息进行梳理，如数据库的表、字段；大数据内部的表、列族、XML、属性等。并根据发现和梳理的数据资产形成数据资产视图。具体服务内容包括： **（1）数据的存储与分布梳理** 提供数据存储与分布梳理服务，全面掌握数据分布情况，为数据安全各类管控措施提供依据。 **（2）数据的使用状况梳理** 在明确数据的存储分布的基础上，梳理数据使用状况，为细化业务系统工作人员对敏感数据访问的权限策略和管控措施进一步提供依据。 **4、服务方式：** 通过专业数据安全驻场服务人员，对数据安全资产梳理服务借助人工方式开展相关服务。 **★5、服务交付物：** 《数据资产清单》、《数据资产梳理报告》。
12	数据安全分类分级咨询服务	**★1、服务范围：** 为锦江区城市运行管理大屏、城市运行管理中屏、城市运行管理小屏、事件枢纽系统、数据资源平台、报表通、数据资源调度平台、居民端八个核心业务系统提供数据安全分类分级咨询服务。 **★2、服务频率：** 1年，每年1次。 **3、服务内容要求：** 根据国家、地方、行业的数据分类分级相关政策、规范和标准要求，结合业务系统自身情况和需求，通过专业数据安全服务团队提供数据分类分级工作的组织架构建议、建立数据分类分级策略、数据分类分级框架、重要数据识别方法等，协助完善建立数据分类分级标准。 **4、服务方式：** 数据安全分类分级咨询服务采用现场人工服务的方式开展，由数据安全专家现场开展。 **★5、服务交付物：** 《数据分类分级指南》。

13	数据安全分类分级执行服务	**★1、服务范围：** 为锦江区城市运行管理大屏、城市运行管理中屏、城市运行管理小屏、事件枢纽系统、数据资源平台、报表通、数据资源调度平台、居民端八个核心业务系统提供数据安全分类分级执行服务。 **★2、服务频率：** 1年，每年1次。 **3、服务内容要求：** 结合数据分类分级指南，明确数据分类分级的基本原则、基本方法、策略等，根据已制定的数据分类原则，定义包含多个层级的数据类别清单，对数据资源清单中的数据逐个进行分类，同时从数据安全保护的角度，考虑影响对象、影响程度两个要素对数据所在的安全级别进行判定，按照数据安全分类分级指南以及单位的数据安全规范，将敏感数据分为低敏感、较敏感、敏感、极度敏感等级别，并协助在数据安全治理平台服务的服务工具上建立和配置数据安全分类分级相关策略规则。 **4、服务方式：** 数据安全分类分级执行服务借助人工方式开展相关服务，由数据安全专家现场开展。 **★5、服务交付物：** 《数据分类分级清单》。

14	数据安全风险评估服务	**★1、服务范围：** 为锦江区城市运行管理大屏、城市运行管理中屏、城市运行管理小屏、事件枢纽系统、数据资源平台、报表通、数据资源调度平台、居民端八个核心业务系统提供数据安全风险评估服务。 **★2、服务频率：** 1年，每年1次。 **3、服务内容要求：** 根据《GB/T37988-2019信息安全技术　数据安全能力成熟度模型》中的安全要求，针对锦江区数据资源体系及人口库的数据安全能力进行评估。从组织建设、制度流程、技术保障以及人员能力等方面开展风险评估，并输出差距分析报告，识别与目标等级的差距，协助用户认知自身数据安全能力水平。具体服务内容如下： **1）标准文件收集** 标准文件收集，既对《网络安全法》、《个人信息保护法》、《数据安全法》、GB/T37988-2019信息安全技术 数据安全能力成熟度模型》和政务行业数据安全管理相关标准进行收集和整理，对文件中关于数据安全相关的要求内容进行梳理。 **2）数据安全合规检查标准制定** 依据数据安全法律法规及标准文件解读，制定数据安全合规检查标准，对要求的实现方式及检查点进行描述，以便于数据安全风险评估的准确性和高效性。 **3）人工审计** 参照数据安全合规检查标准，对现有环境进行人工访谈和人工检查，并整理不满足项目，编写人工审计报告。 **4、服务方式：** 数据安全风险评估服务采用工具+现场人工服务的方式开展，由数据安全专家现场开展。 **★5、服务交付物：** 《数据安全风险评估报告》、《数据安全风险全景图表单》。

15	数据安全权限稽查服务	**★1、服务范围：** 为锦江区城市运行管理大屏、城市运行管理中屏、城市运行管理小屏、事件枢纽系统、数据资源平台、报表通、数据资源调度平台、居民端八个核心业务系统提供数据安全权限稽查服务。 **★2、服务频率：** 1年，每年1次。 **3、服务内容要求：** 通过人工现场服务使用人工检测的方式，基于业务运维场景、数据使用场景、数据导出场景、终端业务等多类场景进行业务账号权限的梳理，发现预设流程范围内权限与模拟异常业务操作等核查账号权限。协助用户梳理现有业务中，所有角色账号的数据权限配置情况，如数据提供方、数据使用方、数据监管方、数据管理方、数据运营方和平台开发方等六类角色。为管理角色账号权限管理提供依据。 **4、服务方式：** 数据安全权限稽查服务采用现场人工服务的方式开展，由数据安全专家现场开展。 **★5、服务交付物：** 《数据安全访问权限稽查报告》、《数据安全访问权限稽查清单》。
16	数据安全应急演练服务	**★1、服务范围：** 成都市锦江区，采购人指定范围。 **★2、服务频率：** 1年，每年1次。 **3、服务内容要求：** 编制应急演练方案，并加强与其它服务支持单位的协调，组织和指导开展数据安全应急演练工作，提供数据安全应急演练所需的相关材料，制定数据安全应急演练工作流程，开展数据安全应急演练，并在演练结束后输出数据安全应急演练报告。 **4、服务方式：** 数据安全应急演练服务采用现场人工服务的方式开展，采用沙盘或桌面推演，由数据安全专家现场开展。 **★5、服务交付物：** 《数据安全应急演练方案》、《数据安全应急演练总结报告》。

	1	17	数据安全应急响应处置服务	**★1、服务范围：** 为锦江区城市运行管理大屏、城市运行管理中屏、城市运行管理小屏、事件枢纽系统、数据资源平台、报表通、数据资源调度平台、居民端八个核心业务系统在发生黑客入侵攻击、敏感数据资产泄露等安全事件时，提供数据安全专家开展应急响应支撑服务。 **★2、服务频率：** 1年，按需提供。 **3、服务内容要求：** 在核心业务系统遭受黑客入侵攻击窃取敏感数据资产时，协调数据安全专家根据数据安全重大事件的动态数据，对数据安全重大事件进行紧急处置。应急处置完成后，在业务侧组织复盘分析，明确数据安全事件发生的根本原因，做好应急总结，并提供相关防护手段、防护策略和应急预案的优化建议。 **4、服务方式：** 数据安全应急响应处置服务采用现场人工服务的方式开展，由数据安全专家现场开展。 **★5、服务交付物：** 《数据安全应急响应处置报告》。
		18	数据安全监测及告警服务	**★1、服务范围：** 为锦江区城市运行管理大屏、城市运行管理中屏、城市运行管理小屏、事件枢纽系统、数据资源平台、报表通、数据资源调度平台、居民端八个核心业务系统提供数据安全监测及告警服务。 **★2、服务频率：** 1年，由现场驻场人员提供给该服务。 **3、服务内容要求：** 针对核心业务数据流转过程，利用数据安全工具对数据相关事件内容进行集中分析，包含：日志采集、日志范式化、人物行为画像分析、数据流转地图、数据泄露行为分析建模、数据异常行为告警、数据风险展示、数据日志展示、数据多维度查询等多个角度，监测发现业务数据流转过程中存在的异常行为、安全告警，并提供预警通告，定期输出数据安全风险监测服务报告，同时根据业务实际现状需求，持续对部署的数据安全设备服务工具的安全策略配置进行优化，提供后续增加优化改进建议。 **4、服务方式：** 通过专业数据安全驻场服务人员，对数据安全监测及告警服务采用现场人工服务的方式开展。 **★5、服务交付物：** 《数据安全风险监测运营月报》、《数据安全风险监测运营年报》。

		19	数据安全培训服务	**★1、服务范围：** 锦江区智慧蓉城全员或用户指定。 **★2、服务频率：** 1年，每年2次。 **3、服务内容要求：** 针对锦江区智慧蓉城组织内人员开展数据安全意识宣导和培训，逐步提升数据安全工作人员的能力水平和安全意识。培训采用现场培训和远程培训的方式，覆盖项目负责领导和相关负责人、运维单位负责人、建设单位人员等（具体用户指定）。培训包括：培训材料筹备、培训专家聘请、培训实施、培训总结评估。 **4、服务方式：** 采用现场人工服务的方式线上或线下方式开展，由数据安全专家现场开展。 **★5、服务交付物：** 《数据安全培训记录》、《数据安全培训课件》。
		20	数据安全治理平台服务	1、★服务要求配置≥100个资源授权； 2、服务工具要求支持资产管理功能，支持接入资产数量、资产存储数、资产执行敏感发现情况、资产敏感数据占比四个维度呈现资产概览；其中接入资产数量呈现接入平台的数据库、服务器、大数据组件、终端等不同类型资产数量；资产存储数呈现接入平台的资产的存储量，展示存储量最大的TOP10资产；资产执行敏感发现情况呈现接入平台的资产的扫描情况，展示已完成敏感数据扫描和未进行敏感数据扫描的资产数量；资产敏感数据占比从资产维度呈现不同资产敏感数据数量、非敏感数据数量及占比情况，展示TOP10资产。 3、服务工具要求支持敏感数据管理功能，支持对多种类型的资产自动识别敏感数据，支持类型包括但不限于：数据库：Oracle、DB2、SQL Server、MySQL、PostgreSQL、Sybase、Informix、MariaDB、RDS、MongoDB、达梦、Gbase、TeleDB、MaxCompute、ADS；大数据组件：HIVE、HBASE、HDFS、ElasticSearch、ODPS；主机类型：Windows、Linux。 4、▲服务工具要求支持数据分类分级管理功能，支持以资产组、数据分类、数据分级三种维度展示数据分类分级结果，其中数据分类分级策略支持多套分类分级规范启用，支持拖拽切换规范顺序，并且生成不同规范的分类分级结果报告，并支持手动修改敏感数据的分类分级，支持数据分类、数据分级维度对敏感数据进行批量标注，通过标注把数据资产筛选为重要数据，支持文件分类分级。（提供服务工具功能截图证明，并加盖投标人公章） 5、服务工具要求支持系统支持DSMM（三级）等的数据安全合规检查，并支持对合规检查结果生成数据安全合规检查报告。 6、▲服务工具要求支持数据风险可视化，提供风险中心监测视图，主要包含风险等级、风险事件总量、已处理事件数、未处理事件数、事件详情展示。（提供服务工具功能截图证明，并加盖投标人公章） 7、服务工具要求支持审计报表管理功能，提供报表文件、报表任务、报表模板三部分，并支持自定义报表，下载格式支持word、excel、pdf等格式。 8、▲服务工具要求支持不同视角展示数据流转情况，至少包含数据视角和用户视角，其中数据视角支持运维、业务、共享三种场景的展示，呈现不同类型的数据在哪

				些资产上、被哪些业务系统/源IP在访问，访问这些业务系统的是哪些用户，以及访问的次数、涉及的管控及风险；用户视角支持运维和业务两种场景的展示，呈现用户访问了哪些业务/应用、这些业务/应用/API访问了哪些资产上的哪些数据类型、访问次数、涉及的管控及风险。（提供服务工具功能截图证明，并加盖投标人公章） 9、服务工具要求支持通过大屏展示数据安全整体情况，包括：数据资产，敏感数据分类分级，敏感数据访问热度、数据安全能力概览、数据流转概览（流入和流出）、数据安全风险概览和处置。 10、服务工具要求支持资产和数据的分权分域功能，支持根据对象实体关联的组织机构和业务系统做数据权限控制，同时支持根据实体对象的创建人所属的组织机构做数据权限控制。 11、服务工具要求支持系统维护、系统配置、告警与配置、接口管理、系统日志管理功能，支持ipv4和ipv6双栈。 12、▲本服务所涉及数据安全治理工具具有中华人民共和国国家版权局计算机软件著作权登记证书。（提供有效证书复印件并加盖公章，若为授权使用的还需提供授权证明材料并加盖公章）	
			21	数据安全API接口审	1、★服务要求单服务工具配置≥500个应用接口数授权，本服务要求提供≥4套服务工具，总接入数要求≥2000个应用接口数授权。 2、服务工具要求支持HTTP协议解析，还原HTTP事件请求和返回内容。 3、服务工具要求支持新建访问域（访问域名称，单个IP或IP地址段），通过名称进行访问源区域的划分；支持对IP访问源进行流量过滤（即是否记录日志）。 4、服务工具要求支持按天、周，月，日期（时间段）配置工作时间作为风险监测规则。 5、服务工具要求内置敏感数据监测规则，包括邮箱，手机号，18位或14位身份证，16位或19位银行卡号，护照编号，组织机构代码，社会信用代码，IPv4地址，家庭地址。 6、服务工具要求支持绑定接口地址与工作时间、访问频次、敏感数据、违法信息规则，用于输出监测信息。 7、服务工具要求支持记录访问API接口/页面的日志，包括：访问源地址，被访页面/接口地址，敏感级别，被访问应用名称，目的地址，访问时间，返回数据量，并支持源数据下载操作。 8、▲服务工具要求支持记录接口访问行为，监测非工作时间段访问，监测记录包括：访问源地址，被访页面/接口地址，敏感级别，被访问应用名称，目的地址，访问时间，合规时间范围，是否合规。（提供服务工具功能截图证明，并加盖投标人公章） 9、服务工具要求支持记录一定时间规则阈值内，登录次数的行为，监测记录包括：访问源地址，被访页面/接口地址，敏感级别，被访问应用名称，目的地址，访问时间，访问频次，周期。 10、▲服务工具要求支持记录敏感信息访问监测：依据预先定义的敏感数据规则，通过数据解析去发现流量中未脱敏的信息，形成监测日志，监测记录包括：访问源地址，被访页面/接口地址，敏感级别，被访问应用名称，目的地址，访问时间，敏	

			计服务	感类型，敏感数据详情。（提供服务工具功能截图证明，并加盖投标人公章） 11、▲服务工具要求内置违法信息规则，通过数据解析去发现流量中传输的违法关键字，形成监测日志，监测记录包括：访问源地址，被访页面/接口地址，敏感级别，被访问应用名称，目的地址，访问时间，关键字类型，关键字详情。（提供服务工具功能截图证明，并加盖投标人公章） 12、服务工具要求支持被监测应用系统信息配置，包括应用系统名称、所属安全域，IP和端口，通讯协议、编码方式、负责人，并支持在应用系统创建URI接口信息，包括接口名称，URI地址，以及设置敏感级别（一般、低、中、高）。 13、服务工具要求至少支持持续发现模式和时间段模式两种工作模式设置，其中持续发现模式，代表开启API发现功能后，不间断发现流量中新增的API接口信息，在虚拟化部署方式，仅支持发现已监控应用的新增接口；时间段模式，代表启动一段时间范围内的新增的API接口发现功能。 14、服务工具要求支持基于角色的权限管理，内置普通管理员，审计管理员，系统管理员角色，可创建用户，并可按需设置应用管理，访问域管理，规则管理权限，用于区分不同管理员的权限类型。 15、▲本服务所涉及数据安全API接口审计工具具有中华人民共和国国家版权局计算机软件著作权登记证书。（提供有效证书复印件并加盖公章，若为授权使用的还需提供授权证明材料并加盖公章）	
			数据库	1、★服务要求单服务工具≥8个被审计DB服务数的授权，本服务要求提供≥6套服务工具，总接入数要求≥48个被审计DB服务数的授权。 2、服务工具要求支持对部署在vmware、KVM、Xen等虚拟化环境中的数据库进行审计，审计系统可虚拟化部署，并支持采用agent进行导流，全面适配政务云环境。 3、服务工具要求支持多种类型数据库的审计，包括但不限于：支持主流数据库Oracle、SQL-Server、DB2、Informix、Sybase、MySQL、PostgreSQL、Teradata、Cache数据库审计；支持国产数据库人大金仓、达梦、南大通用、神通、高斯等数据库的审计；支持MongoDB、redis数据库的审计；支持Hbase、hive、ES的审计； 4、服务工具要求支持对针对数据库的XSS攻击、SQL注入、CVE高危漏洞利用、口令攻击、缓冲区溢出等攻击行为进行审计。 5、服务工具要求支持访问数据库的源主机名、源主机用户、SQL操作响应时间、数据库操作成功、失败的审计。 6、服务工具要求支持用户数据库中敏感信息的自动发现，可定位敏感数据存储的服务器、库名、表名、列名，并形成针对敏感信息的审计规则。 7、服务工具要求支持对敏感信息敏感级别进行定义，各级别可对应不同风险值，方便对敏感数据泄露进行风险进行评估。 8、▲服务工具要求支持敏感信息发现功能，支持探测器和正则表达式两种方式，探测器至少包含：姓名、地名、银行卡、身份证、IP地址、密码等多种探测器（提供服务工具功能截图证明，并加盖投标人公章） 9、▲服务工具要求支持用户操作轨迹图展示，轨迹图维度可根据资源账号、源ip、	

		22	防护服务	客户端程序名、命令、表名、错误码等按需定义，可根据昨天、最近七天、最近30天以及自定义时间进行轨迹显示，可显示下一节点数量，可在某一维度中进行筛选。（提供服务工具功能截图证明，并加盖投标人公章） 10、服务工具要求支持敏感信息掩码，用户可以针对姓名、身份证号、手机号、银行卡号、住址以及自定义信息进行敏感信息掩码配置，防止敏感信息在审计系统中进行泄露。 11、服务工具要求支持敏感数据访问独立大屏展示，可直观展示各类各级别敏感数据占比、敏感数据访问量与分布、敏感数据访问用户TOP5、敏感数据访问源IPTOP5、敏感数据增删改插操作分析等内容。 12、▲服务工具要求支持基于场景的操作异常分析；可直观展现数据库异常、异常账号的访问、同账号多IP登录、上下班操作量对比异常、操作响应时间分析、用户变更、弱口令检测。（提供服务工具功能截图证明，并加盖投标人公章） 13、服务工具要求支持疑似暴力破解、疑似撞库攻击、场景的操作异常分析；行为周期与阀值可按需定义。 14、服务工具要求支持自定义报表模板，包括数据集、图表设计、数据设计等，数据设计可根据不同数据集提供不同的分析维度和指标供用户进行选择。 15、服务工具要求支持按每天、每周、每月、手动指定某一时刻生成报表，生成的报表支持邮件方式自动发送。 16、服务工具要求支持一键自检功能，可以检查系统当前运行状态，检查内容包括：系统信息、进程信息、数据库信息、授权信息、用户信息等17项内容。 17、本服务所涉及数据库防护工具具有中华人民共和国国家版权局计算机软件著作权登记证书。（提供有效证书复印件并加盖公章，若为授权使用的还需提供授权证明材料并加盖公章）
		23	数据库水印服务	1、★服务要求配置≥20个生产数据库实例授权。 2、服务工具要求支持数据水印功能，水印算法包含原地水印、不可见字符水印、伪劣水印、数据指纹。 3、服务工具要求支持数据库和文件溯源，一旦出现数据泄露可通过泄露数据样本进行溯源追责，一键高效溯源。 4、服务工具要求支持对水印任务的新建、删除、启动、停止、查询等功能。 5、服务工具要求支持水印任务管理功能，包含对任务名称、任务模式、水印算法、共享方式、水印内容、源资产、源数据库/模式、目标资产、目标数据库/模式、是否结构同步、审批人，同时在高级选项中，可以针对固定抽取最大记录数、是否处理大数据字段进行填写。 6、服务工具要求支持数据关系修改和查看，包含字段、索引、外键、SQL预览四大模块。 7、服务工具要求支持数据水印任务显示水印进度、水印状态、水印数据量（未完成/已完成）等信息。 8、服务工具要求支持任务完成后显示任务详情、任务报告、错误日志等信息。

		24	终端数据防泄漏服务	1、★服务要求配置≥100个客户端组件授权。 2、服务工具要求支持主流Windows操作系统。 3、▲服务工具要求支持定义敏感文档关键字，当检测到终端内文档中包含有大量敏感关键字时可将其视为敏感文件。（提供服务工具功能截图证明，并加盖投标人公章） 4、服务工具要求支持支持定义文件指纹，对文件进行敏感评估，当某文档被视为敏感文件后，即使修改其部分内容，也可立即识别出来，避免因为检测md5码而出现敏感漏洞。 5、服务工具要求支持终端敏感信息发现功能，支持全盘文件索引功能，开启功能后自动建立索引，后期所有文件变动、新增都增量更新索引。 6、▲服务工具要求支持全盘或指定位置检查是否存在敏感文件及文件敏感等级等信息，无需周期性扫描检查，支持记录敏感文件创建时间和最后修改时间。（提供服务工具功能截图证明，并加盖投标人公章） 7、服务工具要求支持基于客户端的敏感信息防防漏功能，支持敏感文件扫描、文件拷贝、剪切板、QQ、邮件、WEB、FTP以及自定义应用程序等方式外发的管控与审计。 8、服务工具要求支持屏幕水印功能，水印内容支持显示终端特征信息，支持自定义文字和图片。 9、服务工具要求支持点阵式屏幕水印功能，点阵信息支持自定义边长、间距、颜色、透明度等信息，通过对点阵水印信息解析可支持对录屏、截屏、拍照等行为获取到的图片信息进行溯源追踪。 10、服务工具要求支持对终端接入的移动存储设备提供认证、授权和审计，确保终端使用认证通过的移动储存设备，对数据进行授权共享，彻底杜绝通过移动存储设备的数据非法外泄。 11、▲服务工具要求支持对移动存储认证模式至少要支持专用目录加密和全盘加密二种认证模式，支持USB2.0及USB3.0的移动存储设备及大容量移动硬盘。（提供服务工具功能截图证明，并加盖投标人公章） 12、▲本服务所涉及数据防泄漏工具具有中华人民共和国国家版权局计算机软件著作权登记证书。（提供有效证书复印件并加盖公章，若为授权使用的还需提供授权证明材料并加盖公章）
				1、★服务要求配置≥20个生产数据库实例授权。 2、服务工具要求支持Oracle、DB2、Informix、SQLServer、MySQL、Sybase、Postgresql、Gbase、达梦（DM）等主流数据库的脱敏、同时支持Nosql数据库MongoDB和大数据Hadoop Hive等类似数据库，并支持TXT、CSV、DEL等文件的脱敏。 3、服务工具要求支持自定义敏感信息发现规则，发现规则支持基于正则表达式、关键字匹配和字段名匹配三种方式；支持自定义混合敏感数据发现规则。 4、服务工具要求内置中文姓名脱敏规则、中文地址脱敏规则、身份证脱敏规则、组织机构名称脱敏规则、电子邮件脱敏规则、IPV4地址脱敏规则、IPV6地址脱敏规则、URL地址脱敏规则、电话号码脱敏规则、手机号码脱敏规则、银行卡号脱敏规则、工商注册号脱敏规则、组织机构代码脱敏规则、税务登记号脱敏规则、统一信

		25	数据静态脱敏服务	用代码脱敏规则、军官证号码脱敏规则、车牌号脱敏规则、中国护照脱敏规则、港澳居民来往内地通行证脱敏规则、外国人永久居住证脱敏规则、邮政编码脱敏规则、随机替换规则、置空规则、日期随机脱敏规则、数值随机脱敏规则。 5、▲服务工具要求支持自定义脱敏规则，可以基于长度、分隔符进行拆分成任意数量的数据分段，每个数据分段均可以自由配置脱敏算法，由各分段的不同算法，组合成脱敏规则。（提供服务工具功能截图证明，并加盖投标人公章） 6、服务工具要求支持多种脱敏模式，包括但不限于：支持数据库脱敏到数据、支持文本文件脱敏到文本文件、支持文本文件脱敏到数据库、支持各类数据库之间的异构脱敏，无需操作人员进行任何额外操作，全自动化将字段类型进行映射和转换。支持对自动映射和转换的字段类型进行手动修改和支持增量脱敏。 7、▲服务工具要求支持在脱敏配置中，可以通过配置SQL语句，实现数据表部分数据抽取脱敏，即可以实现抽取行数限定，也可以实现抽取部分字段的限定。（提供服务工具功能截图证明，并加盖投标人公章） 8、服务工具要求支持保证脱敏前后的数据特征不变，脱敏后数据保持原业务属性，如中文姓名脱敏后的数据为中文姓名、手机号脱敏后的数据也为手机号、身份证号码脱敏后的数据也为身份号码等，且保证脱敏后的数据通过校验。 9、▲服务工具要求具备复杂数据处理能力，能脱敏在一个单元格内由多段敏感数据组合的数据，例如：姓名/手机号码这种复杂数据的脱敏。（提供服务工具功能截图证明，并加盖投标人公章） 10、服务工具要求内置大量敏感字段识别规则，可以自动发现以下敏感字段：中文姓名、中文地址、身份证、组织机构名称、电子邮件、IPV4地址、IPV6地址、URL地址、电话号码、手机号码、银行卡号、工商注册号、组织机构代码、税务登记号、统一信用代码、军官证号码、车牌号、中国护照、港澳居民来往内地通行证、外国人永久居住证、邮政编码、证件号码混合、姓名和组织机构名称混合。 11、服务工具要求支持数据库和文件脱敏模板，用户创建任务，上传模板即可完成敏感数据确认、脱敏算法选择等，便于快捷对数据库和文件进行脱敏。 12、服务工具要求具备审批模块,系统中操作员可以创建脱敏任务,但需要管理员审批后脱敏任务才可执行。 13、服务工具要求支持数据不落地脱敏，脱敏系统不留存脱敏前后的数据。 14、服务工具要求支持针对不同用户配置不同权限，对用户可设置数据源对应关系，分配不同的数据源给不同的用户。用户无法对未授权的数据源执行脱敏任务。 15、▲本服务所涉及数据静态脱敏工具具有中华人民共和国国家版权局计算机软件著作权登记证书。（提供有效证书复印件并加盖公章，若为授权使用的还需提供授权证明材料并加盖公章）	
				1、★接入服务器主机（含虚拟机）数量≥1000个 2、资源兼容性 支持多种资源的特权账号管理，支持资源分类管理，支持资源组管理； 支持Windows、Unix、Linux等主机系统； 支持华为、H3C等网络设备及安全设备； 支持MySQL 、Oracle、PostgreSQL、MSSQL、MongoDB等数据库；	

				支持C/S、B/S业务系统。 3、协议兼容性 支持对Telnet、SSH、VNC、X11、SFTP、RDP、HTTP/HTTPS等协议运维控制及操作审计。 4、运维工具兼容性 支持各种运维客户端工具，如SecureCRT、XShell、PUTTY、Remote Desktop、WinSCP客户端； 支持WEB运维；支持应用发布方式加载客户端工具运维。 5、认证方式兼容性 支持多种认证方式，支持静态口令、LDAP认证、AD认证、OTP认证及其他认证方式的扩展，支持与IAM系统进行集成，由IAM系统提供用户管理供给及认证能力集成。 6、用户管理 支持页面同时添加多个用户。支持用户的导入导出。 7、机构管理 支持按照机构管理用户和资产数据。 8、三员管理模式 支持管理员、安全员、审计员、普通用户角色间权限进行互斥规则，每个用户只能具备一个三员身份，防止权限交叉引发安全漏洞。 9、用户密码策略 设置支持对用户密码策略进行设置，包括长度，复杂度，相关度和错误次数锁定等信息的设置。 10、资源自定义分组分类管理 支持自定义多级资源树，对资产进行分类管理，快速定位各类资源。 11、资产批量操作 支持页面同时添加和编辑多条资产信息，高效完成资源登记。 12、资产管理分配 支持指定资源负责人，并支持负责人之间数据隔离，资产负责人可自主接管资产或将资产管理权进行移交。 13、字符集设置 支持资产账号登记时，设置字符集。 14、认证模式设置 支持对资产访问时的认证模式设置，包括SSO认证，二次认证等。适配资产自身多因素认证场景。 15、凭证托管设置 支持对资产账号登记时进行凭证托管或只托不管设置，对已托管的账号凭证，为管理员提供账号凭证集中管理视图。 16、管理模式设置 支持资产登记时设置管理模式，适配管理账号不能直连的场景，包括直连模式，sudo模式，su模式。 17、资产批量导入/导出	

		26	特权安全防护服务	支持对资产信息以文件的方式导入/导出。 18、资产账号批量操作 支持页面登记和编辑资产账号时，同时操作多个账号。 19、资产密码覆盖 支持资产账号登记时，强制覆盖密码。根据密码策略自动生成密码并覆盖。 20、资产账号发现 支持手动和自动发现资产账号，并提供待处理账号页面展示。 资产账号批量导入/导出 支持对资产账号信息以文件的方式导入/导出。 21、密码重置管理 支持资产账号密码重置。 支持批量对多个账号同时进行重置。 支持批量重置时，为每个账号生成不同的密码。 支持批量重置时，为所有账号指定同一密码。 22、支持定期自动重置。 支持根据不同资源类型，账号级别定义不同密码复杂度策略和重置周期。 23、密码邮件管理 支持以密码邮件的方式备份资产密码。该功能需用户进行二次身份认证。 24、密码验证 支持定期自动验证密码有效性，及时发现密码异常账号。 密码历史 支持密码历史查看功能，展示资产账号使用过的密码历史。该功能需用户进行二次身份认证。 25、资产访问权限管理 支持对资产访问协议级授权，授权用户仅允许使用指定协议访问资产账号。 支持临时授权，仅允许在指定时间范围内访问。 支持设置授权命令策略，限制用户仅能执行或不能执行指定命令。 支持设置时间策略，限制用户仅能在指定时间周期范围内访问。 支持设置IP策略，限制用户仅能在指定IP段内进行资产访问。 支持设置应用命令策略，限制用户范围应用类资产时，进行精准菜单和按钮权限控制。 26、数据库运维命令阻断 支持数据库运维过程中敏感操作的命令阻断。通过策略配置运维命令黑名单，确保在运维过程中敏感操作不被执行。 27、数据库运维防绕行 支持禁止数据库运维操作中，调用工具连接功能访问其他业务数据库。防止用户通过平台绕行访问非授权资源。 28、资产凭证权限管理 支持对资产账号的密码或密钥检出权限进行授权。 支持用户检出凭证后，账号锁定限制，明确资产账号责任人。 支持一次一密场景，密码，密钥检入或到期后自动重置密码或轮换密钥。	

					29、认证管理审计 支持对用户认证，账号认证，运维认证多维度认证情况进行审计记录。 授权情况审计 支持对访问权限，凭证权限授权情况进行审计日志记录。 30、数据库运维命令审计 支持数据库运维过程中的SQL命令记录和日志审计。 在线监控审计 支持对资产访问会话过程在线监控。实时查看资产访问操作画面。 会话回放审计 支持对资产访问过程全流程图形回放审计，查看已结束会话的操作画面 行为操作审计 支持对资产访问过程中的操作行为进行完整记录和回放。 31、运维统计分析 支持通过资源类型、操作类型按照时间对凭证进行分析； 运维信息分时段进行统计、按协议分时段进行统计； 通过资源主类型、类型、协议三个维度按照时间对资源进行分析 ▲32、服务工具具有中华人民共和国国家版权局颁发的《计算机软件著作权登记证书》（提供有效证书复印件并加盖公章，若为授权使用的还需提供授权证明材料并加盖公章）。

27	网络安全体系建设专家咨询服务	**★1、服务频次** 1年，每年2次。 **★2、服务范围** 锦江区智慧蓉城。 **3、服务内容** （1）网络安全管理体系服务建设：参考《信息技术安全技术信息安全管理体系要求》（GB/T22080-2016）、《信息技术 安全技术信息安全管理实用规则》（GB/T22081-2016）以及《信息安全技术 网络安全等级保护基本要求》（GBT22239-2019）提出安全风险管理和控制的相关要求，制定标准化的信息安全管理制度，构建可持续的安全管理能力。 （2）网络安全技术体系规划咨询：根据服务对象的信息安全战略目标和安全现状与需求总结，遵循国家及行业法规政策要求，参照国内外最佳实践模型，采用科学的信息安全规划方法论，构建符合服务对象未来发展的信息安全总体架构，并通过业务和项目约束关系分析关键实施计划和路径，用以指导信息安全建设方向，满足法律、管理与业务发展需要。 （3）组织架构及队伍服务建设：落实信息安全保障体系必须要切实抓好安全支撑队伍建设，健全安全人才保障机制。安全支撑队伍要有明确分工。管理队伍和建设、运行技术服务队伍可以分设，明确人员和职责分工，分别行使管理、建设和运行技术服务的责任。 **4、服务方式** 网络安全体系建设专家咨询服务采用现场人工服务的方式开展，由中标人安排网络安全专家（高级专业技术职称）现场开展。 **★5、服务交付** 网络安全体系咨询报告； 网络安全体系规划方案； 网络安全体系人员方案。

		28	网络安全培训服务	**★1、服务范围** 锦江区智慧蓉城。 **★2、服务频次** 1年，每年1次。 **3、服务内容** （1）网络安全意识培训：是以提高参训人员的安全意识，了解当前信息安全技术的发展状况，了解信息安全常用术语及概念，增强技术防护的实践能力为目标。安全意识培训面向普通使用者，可以分批分次进行，每次进行1-2门课，历时0、5-1天。这样进行的培训不会影响参训人员日常工作，可以灵活安排进行，以求最大范围覆盖需要人群，提升党政机关人员的个人安全意识。 （2）网络安全技能培训：是以帮助参训人员进一步了解信息安全技术的最新发展动态，掌握常见安全设备和技术的基础知识，掌握信息安全体系架构的设计方法，掌握安全行业的法律法规和相关的标准，掌握信息安全管理体系的建立方法为目标。面向系统开发、管理和维护人员，以及信息化建设的主管，可设置一定的技术专题，组织持续1-2天的半脱产学习，以满足不同基础的参训人员在某一安全领域内的具体培训需求。这样进行的培训针对性强、内容丰富、贴近参训人员具体需求，可以很好地提升相关人员的安全技能和安全管理水平。 （3）网络安全知识培训：帮助参训人员补充网络安全知识、加强日常工作中网络安全防范，从国内外网络安全形势、国内网络安全法律法规、常见的网络攻击及防范方法等几个方面系统地介绍网络安全知识，并结合日常工作和生活中真实案例进行讲解，分析问题发生的原因及造成的危害，并提出具体应对措施。 （4）配合采购人完成上级单位检查。 （5）配合采购人完成上级单位年度、季度考核要求。 **4、服务方式** 网络安全培训服务采用现场人工服务的方式开展，由中标人安排网络安全专家（高级专业技术职称）现场开展。 **★5、服务交付** 网络安全培训材料； 网络安全培训考试； 网络安全人员评估。
				本项目提供3名人力驻场服务，其中数据安全驻场人员2名，网络安全驻场人员1名，驻场人员将全程服务于本项目，驻场人员需要符合以下标准： 一、网络安全1名驻场人员 1、拥有网络安全领域专业证书； 2、具备本科或以上学历； 3、熟悉owasp top10 漏洞及其形成原理； 4、熟悉常见操作系统(如Windows、linux)的安全配置和维护; 5、熟悉常见网络设备(如交换机、路由器)和网络安全设备(如防火墙、WAFIPS)的基本使用和配置，以及告警分析研判; 6、掌握各类渗透测试工具，具有漏洞挖掘能力；

7、熟悉常见的web安全问题，熟悉Python、shell等脚本编写。

二、数据安全2名驻场人员

1、拥有数据安全领域专业证书；

2、具备本科或以上学历；

3、熟悉国内外安全法律法规，对网络安全法、数据安全法、个人信息保护法等法律法规；

4、熟悉数据安全标准规范，熟悉数据全生命周期管控措施及数据保护技术；

5、熟悉主流的网络安全产品（防火墙、入侵监测、日志审计、堡垒机等）及数据安全产品（数据库审计、数据脱敏、数据防泄漏、数据库水印等）工作原理及使用方法；

6、具备数据安全管理体系相关管理制度、规范流程的编写经验；

7、具备数据安全风险监测、通告预警、应急响应等数据安全风险管理服务经验。

对于驻场人员在入场服务前需要提交人员简历，并通过项目管理人员面试通过后方可入场服务。

三、驻场服务内容要求如下：

1、全年网络安全工作计划制定服务：基于国家信息安全相关法律法规及实施标准，结合采购人实际情况以及用户具体需求，制定全年网络安全工作计划，并在相应时间点落实计划。服务期内提供每年1次服务。

★2、服务交付物：《年度工作计划表》

3、安全管理体系咨询服务：依照国际或国家信息安全管理体系相关标准，基于业务风险方法，通过定义范围和方针、业务分析、风险评估、设计、实施等步骤，面向客户建立、实施、运行、监控、评审、保持和改进信息安全的体系。服务期内提供每年1次服务。

★4、服务交付物：《安全建设方案》

5、风险评估服务：运用科学的方法和手段，系统地识别、分析网络与信息系统所面临的威胁及其存在的脆弱性，评估安全事件一旦发生可能造成的危害程度，提出有针对性的抵御威胁的防护对策和整改措施。服务期内提供每年1次服务。

支持对采购人及其他相关单位提供该服务。

服务范围：对采购人指定业务系统进行风险评估

★6、服务交付物：《系统风险评估报告》

7、资产梳理服务：主动发现网络环境内资产主机，发现和梳理出的资产，形成资产视图。支持对采购人及其他相关单位提供该服务。服务期内提供每季度1次服务。

支持对采购人及其他相关单位提供该服务。

★8、服务交付物：《资产表》

9、安全监测服务：技术服务人员根据相应的安全监测类设备，分析设备告警日志，及时发现威胁，为用户网络环境提供安全监测服务。

支持对采购人及其他相关单位提供该服务。

★10、服务交付物：《网络安全态势总结报告》

11、业务系统漏洞扫描服务：在授权范围内，使用专业检测工具，基于漏洞数据库，通过自动化检测结合人工分析的手段对指定信息系统的安全脆弱性进行快速检

				测，发现可利用漏洞。服务期内提供每季度1次服务。 支持对采购人及其他相关单位提供该服务。 服务范围：漏洞扫描的范围是采购人指定相关业务系统。 服务内容：本项目漏洞扫描内容将围绕系统层、应用层、网络层进行展开，通过使用工具或检测设备等方式，针对不同层面的安全漏洞及威胁进行测试，漏洞扫描内容包含但不限于配置管理、安全基本检测、访问权限控制、身份鉴别、会话管理、输入验证、错误处理等内容，并且对所发现的漏洞进行验证。 ★12、服务交付物：《业务系统漏洞扫描报告》 **13、服务器漏洞扫描服务：**在授权范围内，使用专业检测工具，基于漏洞数据库，通过自动化检测结合人工分析的手段对指定信息系统的安全脆弱性进行快速检测，发现可利用漏洞。服务期内提供每季度1次服务。 支持对采购人及其他相关单位提供该服务。 服务范围：漏洞扫描的范围是采购人指定相关服务器。 服务内容：本项目漏洞扫描内容将围绕系统层、应用层、网络层进行展开，通过使用工具或检测设备等方式，针对不同层面的安全漏洞及威胁进行测试，漏洞扫描内容包含但不限于配置管理、安全基本检测、访问权限控制、身份鉴别、会话管理、输入验证、错误处理等内容，并且对所发现的漏洞进行验证。 ★14、服务交付物：《服务器漏洞扫描报告》 **15、弱口令扫描服务：**在授权范围内，使用专业检测工具，基于弱口令字典，通过自动化的手段对指定服务器和业务系统的口令脆弱性进行快速检测，发现弱口令。服务期内提供每季度1次服务。 支持对采购人及其他相关单位提供该服务。 服务范围：弱口令扫描的范围是采购人指定相关业务系统、服务器及数据库。 ★16、服务交付物：《弱口令扫描结果表》 **17、基线核查服务：**结合国家等级保护、国家技术标准及行业安全基线标准等要求，配合自动化安全检查工具、脚本程序或人工检查checklist对目标范围内的操作系统、网络设备、数据库、中间件等多类设备及系统进行高效、准确的安全配置检测及加固建议。服务期内提供每季度1次服务。 支持对采购人及其他相关单位提供该服务。 ★18、服务交付物：《基线核查报告》 **19、渗透测试服务：**从攻击者角度对目标网络、系统、主机、应用等安全性进行深入的非破坏性的探测，发现系统中的薄弱环节，让用户清晰了解目前网络的脆弱性、可能造成的影响，以便采取必要的防范措施。服务器内每季度提供1次渗透测试服务。	
			29	人力驻场服务	服务范围：本项目渗透测试的范围是采购人指定相关业务系统。 服务内容：本项目渗透测试内容将围绕系统层、应用层、网络层进行展开，通过使用工具、人工或检测设备等方式，针对不同层面的安全漏洞及威胁进行测试，渗透测试内容包含但不限于配置管理、安全基本检测、访问权限控制、身份鉴别、会话管理、输入验证、错误处理等内容，并且对所发现的漏洞进行验证。 ★20、服务交付物：《渗透测试报告》 **21、主机安全巡检服务：**服务工程师到现场进行安全维护服务，服务期内提供每	

季度1次安全巡检服务，对客户网络及重要主机进行分析，主要包括主机的配置检查，对主机的运行状态、安全策略等进行安全配置核查；主机配置核查，对主机资源、身份鉴别、默认配置、共享设置、补丁管理、日志等进行安全配置核查；主机木马查杀，采用智能木马检测技术，可高效、准确识别服务器或终端电脑中存在的恶意程序，使安全管理员能够第一时间获知安全隐患，避免不法分子利用肉鸡进行大规模的安全攻击。

★22、服务交付物：《主机安全巡检表》

23、网络设备安全巡检服务：服务工程师到现场进行安全维护服务，服务期内提供每季度1次安全巡检服务，对客户网络设备进行分析，主要包括网络设备的配置检查，对网络设备的运行状态、安全策略等进行安全配置核查

★24、服务交付物：《网络设备安全巡检表》

25、安全设备安全巡检服务：服务工程师到现场进行安全维护服务，服务期内提供每季度1次安全巡检服务，对客户安全设备进行分析，主要包括安全设备的配置检查，对安全设备的运行状态、安全策略、漏洞库等进行安全配置核查；

★26、服务交付物：《安全设备安全巡检表》

27、应急演练服务：根据业务系统实际运行情况，分析其可能面临的风险，根据可能发生的安全事件定制化编写详尽的应急预案，并根据应急预案，每年组织完成一次应急演练。

支持对采购人及其他相关单位提供该服务。

★28、服务交付物：《应急预案》、《应急演练报告》、《应急演练方案》

29、网络安全技术演练服务 – 攻击队：此项服务通过实战对抗，检验当前体系的防御能力和缺陷。仅派出攻击队进行检测。服务期间每年提供1次服务。

支持对采购人及其他相关单位提供该服务。

服务范围：此项服务要求参与攻击队技术人员严格按照国家相关法律法规，在规定的攻击时间内对授权范围内的目标开展红队实战攻击行为。

服务内容：本项目网络安全技术演练（攻击队）内容将围绕系统层、应用层、网络层进行展开，通过使用工具、人工或检测设备等方式，针对不同层面的安全漏洞及威胁进行测试。

★30、服务交付物：《红队实战攻击报告》

31、网络安全技术演练服务 - 防守队：防守人员根据告警、日志、流量等信息，对攻击队的攻击行为进行分析、溯源，并还原攻击场景。支持对采购人及其他相关单位提供该服务。服务期间提供每年1次服务，防守人员不少于2名。

★32、服务交付物：《网络安全攻防演练防守方案》、《网络安全攻防演练防守总结报告》

33、安全事件应急服务：提供日常应急响应服务和特殊时期响应服务，1年不超过5人天（含），服务方式包括7*24小时应急响应，远程技术支持，现场技术支持。在收到紧急突发安全事件通知后，及时进行安全响应，并根据事件类别进行判断。紧急事件响应进行处理指导，技术人员在约定时间内赶到现场。根据事件表现情况对问题进行分析、处理，第一时间恢复系统运行。清除或修正导致问题的隐患，处理完毕后出具安全事件分析处理报告。

				★34、服务交付物：《安全事件分析处理报告》 **35、安全加固服务：**根据用户提供的安全加固需求，对安全问题进行确认、分析、提出安全加固建议，并协助安全运维人员进行加固部署，对已加固系统进行验证服务，服务期内提供安全加固服务。 加固范围应覆盖网络设备、操作系统和应用系统。 **36、安全意识培训服务：**通过安全培训，提高智慧蓉城相关工作人员的安全意识和安全技能，使之能够符合相关信息安全工作岗位的能力要求，全面提高整体的信息安全水平。 支持对采购人及其他相关单位提供该服务。 培训对象包括管理人员、技术人员。培训目的：参加培训人员掌握主流的安全事件发展趋势、国内外相关安全标准。 ★37、为指导运维人员日常安全工作，提升安全意识，掌握安全防护能力，服务期内提供每年1次安全意识培训，培训时间不少于2小时。 ★38、服务交付物：《安全意识培训PPT》 **39、安全技能培训服务：**为解决日常运维中遇到的各类安全问题，结合用户应用系统、安全风险及安全管理人员情况，提供安全培训服务。 培训对象包括管理人员、技术人员。培训目的：参加培训人员掌握主流的安全事件发展趋势、攻防技术原理、安全加固方法、国内外相关安全标准。 支持对采购人及其他相关单位提供该服务。 ★40、为指导运维人员日常安全工作，提升安全意识，掌握安全防护能力，服务期内提供每年1次安全技能培训，培训时间不少于2小时。 ★41、服务交付物：《安全技能培训PPT》 **42、应急处置培训服务：**通过安全培训，提高智慧蓉城相关工作人员的应急处置能力，使之能够符合相关信息安全工作岗位的能力要求，全面提高整体的信息安全水平。 支持对采购人及其他相关单位提供该服务。 ★43、为指导运维人员日常安全工作，提升安全意识，掌握安全防护能力，服务期内提供每年1次应急处置培训，培训时间不少于2小时。 ★44、服务交付物：《应急处置培训PPT》 **45、重要时期保障服务：**在重大活动、敏感时期、HW行动期间，根据智慧蓉城项目实际需求，派驻人员配合进行相应值班、检查、分析、监控、加固等保障支持服务。此项服务要求相关技术人员以现场的方式配合用户进行保障值守工作，并在值守过程中为用户提供检查、分析、监控、加固等保障支持服务 支持对采购人及其他相关单位提供该服务。 ★46、服务交付物：《重保报告》 **47、安全管理工作制度建设服务：**安全管理制度建设是网络安全建设中的重要组成部分，根据《网络安全等级保护》制度要求，结合采购人实际管理情况，出具符合《网络安全保护》要求的相关管理制度，并对现有的管理制度进行优化，并对缺少的管理制度进行补充。 ★48、服务交付物：《网络安全管理制度》 **四、其他要求：**	

				★1、渗透测试服务不允许破坏用户数据，对发现的安全隐患进行保密，不允许泄露； 2、服务响应时间，驻场服务人员2小时内到达现场，非工作时间内4小时内到达现

（三）服务时间：

本服务期限为1年，投标人需在签订合同后15天内完成工具类服务的部署上线。

（四）人员配置要求

投标人负责为本项目配备服务团队（包含项目经理1名、驻场人员共计不少于 3 人并自行配备专业技术服务团队，并自行根据项目实施内容组建服务规划团队、信息安全保障团队、网络技术服务团队、质量保障团队），项目经理为固定联络人员，项目经理、技术总监具有类似项目的实施经验，自备通讯工具（手机）24小时畅通，项目经理负责团队整体工作安排、与采购人衔接等内容。非取得采购人的许可，项目经理、技术总监不得随意变更。

（五）设施设备要求

本项目所需设施设备及耗材由投标人根据项目情况自行配备，当出现设施设备数量或者能力无法满足本项目实际使用需求时，投标人应及时补充或更换设备，以保障项目的顺利实施。

（六）服务部署要求

本项目所涉及工具类服务支持无缝迁移到信创云环境，所有产品支持信创产品的接入，涉及电脑终端类工具服务支持信创电脑终端环境部署。

3.2.3人员配置要求

采购包1：

详见“3.2.2服务要求”。

3.2.4设施设备配置要求

采购包1：

详见“3.2.2服务要求”。

3.2.5其他要求

采购包1：

无。

3.3商务要求

3.3.1服务期限

采购包1：

自合同签订之日起365日

3.3.2服务地点

采购包1：

成都市锦江区，采购人指定地点。

3.3.3考核（验收）标准和方法

采购包1：

采购人将按照本项目采购文件、中标人投标文件、合同约定的考核内容与《财政部关于进一步加强政府采购需求和履约验收管理的指导意见》(财库〔2016〕205号)等有关法律法规的规定进行考核验收。

3.3.4支付方式

采购包1：

分期付款

3.3.5.支付约定

采购包1： 付款条件说明： 合同签订后，在收到中标人提供的真实有效、合法、等额的发票，采购人审签完成后 ，达到付款条件起 15 日内，支付合同总金额的 60.00%。

采购包1： 付款条件说明： 合同签订服务满6个月后，在收到中标人提供的真实有效、合法、等额的发票，采购人审签完成后 ，达到付款条件起 15 日内，支付合同总金额的 20.00%。

采购包1： 付款条件说明： 服务期满后，在收到中标人提供的真实有效、合法、等额的发票，采购人审签完成后 ，达到付款条件起 15 日内，支付合同总金额的 20.00%。

3.3.6违约责任与解决争议的方法

采购包1：

1、双方必须遵守合同并执行合同中的各项规定，保证合同的正常履行。 2、因采购人原因逾期支付合同款的，除应及时付合同款外，应向中标人支付欠款总额万分之一/天的违约金； 3、中标人不能按时完成服务内容而违约的，除应及时完成服务内容外，应向采购人支付合同金额百分之一/天的违约金；未能按时完工超过10天，采购人有权立即终止本项目，中标人则应按合同总价的百分之十的合同总价向采购人支付赔偿金，并须全额退还采购人已经付给中标人的合同款。 4、中标人支付的违约金不足以弥补采购人损失的，还应按采购人损失尚未弥补的部分，支付赔偿金给采购人。 5、如因中标人工作人员在履行职务过程中的疏忽、失职、过错等故意或者过失原因给采购人造成损失或侵害，包括但不限于采购人本身的财产损失、由此而导致的采购人对任何第三方的法律责任等，中标人对此均应承担全部的赔偿责任。 6、合同履行期间,若双方发生争议，可协商或由有关部门调解解决，协商或调解不成的，由当事人向采购人项目所在地人民法院提起诉讼。

3.4其他要求

★（一）投标人对服务团队人员服务过程中的人身及财产安全负责，本项目实施过程中的所有安全责任（含事故）均有中标人自行全权负责，采购人不承担任何责任。（提供承诺函加盖投标人公章） ★（二）投标人应承诺为本项目提供的所有服务均符合现行国家相关标准、行业标准、地方标准或者其他标准、规范。（提供承诺函加盖投标人公章） ★（三）知识产权：投标人应承诺在本项目中提供或使用的任何产品和服务（包括部分提供或使用）时，不会产生因第三方提出侵犯其专利权、商标权或其它知识产权而引起的法律和经济纠纷，如因专利权、商标权或其它知识产权而引起法律和经济纠纷，由投标人承担所有相关责任。（提供承诺函加盖投标人公章） （四）投标人负责对其拟投入的人员进行培训（含保密培训）。 （四）投标人自行根据招标文件内容编制项目实施方案，包括：业务现状分析、服务需求分析、服务方案、服务考核方案、服务保障方案。 （五）投标人自行根据招标文件内容编制服务质量保障措施，包括：服务管理制度、质量保障措施。

第四章 资格审查

资格审查由成都市锦江区人民政府办公室组建的资格审查小组依据法律法规和招标文件的规定，对投标文件中的资格证明等进行审查，以确定投标人是否具备投标资格，并出具资格审查报告。

4.1一般资格审查

采购包1：

序号	资格审查要求概况	评审点具体描述	关联格式
1	具有独立承担民事责任的能力。	提供营业执照复印件（正本或副本）或法人证书复印件（正本或副本）或执业许可证明。【供应商为自然人的仅提供身份证复印件。】并进行电子签章。	营业执照或法人证书或执业许可证 投标文件封面 投标（响应）函 投标人应提交的相关资格证明材料
2	具有良好的商业信誉	供应商需在项目电子化交易系统中按要求填写《投标（响应）函》完成承诺并进行电子签章。	投标（响应）函
3	具有健全的财务会计制度。	供应商需在项目电子化交易系统中按要求填写《投标（响应）函》完成承诺并进行电子签章。	投标（响应）函
4	具有履行合同所必需的设备和专业技术能力。	供应商需在项目电子化交易系统中按要求填写《投标（响应）函》完成承诺并进行电子签章。	投标（响应）函
5	有依法缴纳税收和社会保障资金的良好记录。	供应商需在项目电子化交易系统中按要求填写《投标（响应）函》完成承诺并进行电子签章。	投标（响应）函
6	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。	供应商需在项目电子化交易系统中按要求填写《投标（响应）函》完成承诺并进行电子签章。	投标（响应）函
7	不存在与单位负责人为同一人或者存在直接控股、管理关系的其他供应商参与同一合同项下的政府采购活动的行为。	供应商需在项目电子化交易系统中按要求填写《投标（响应）函》完成承诺并进行电子签章。	投标（响应）函
8	不属于为本项目提供整体设计、规范编制或者项目管理、监理、检测等服务的供应商。	供应商需在项目电子化交易系统中按要求填写《投标（响应）函》完成承诺并进行电子签章。	投标（响应）函

4.2特殊资格审查

采购包1：

序号	资格审查要求概况	评审点具体描述	关联格式

无

4.3落实政府采购政策资格审查

采购包1：

序号	资格审查要求概况	评审点具体描述	关联格式
无			

第五章 评标办法

5.1 总则

一、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》《政府采购货物和服务招标投标管理办法》等法律规章，结合采购项目特点制定本评标办法。

二、评标工作由代理机构负责组织，具体评标事务由采购人或代理机构依法组建的评标委员会负责。评标委员会由采购人代表和评审专家组成。

三、评标工作应遵循公平、公正、科学及择优的原则，并以相同的评标程序和标准对待所有的投标人。

四、本项目采取电子评审，通过项目电子化交易系统完成评审工作。评标委员会成员、采购人、代理机构和投标人应当按照本招标文件规定和项目电子化交易系统操作要求开展或者参加评标活动。

五、评标过程中的书面材料往来均通过项目电子化交易系统传递，投标人通过互认的证书及签章加盖其电子印章后生效。出现无法在线签章的特殊情况，评标委员会成员可以线下签署评标报告，由代理机构对原件扫描后以附件形式上传。

六、评标过程应当独立、保密，任何单位和个人不得非法干预评标活动。投标人非法干预评标活动的，其投标文件将作无效处理；代理机构、采购人及其工作人员、采购人监督人员非法干预评标活动的，将依法追究其责任。

5.2评标委员会

一、本项目评标委员会成员人数应当为五人以上单数，其中评审专家不得少于成员总数的三分之二。评审专家是采取随机方式在采购一体化平台的专家库系统（以下简称专家库系统）抽取。技术复杂、专业性较强的采购项目，评审专家中应当包含1名法律专家。

二、评标委员会成员应当满足并适应电子化采购评审的工作需要，使用已身份认证并具备签章功能的证书，登录项目电子化交易系统进入项目评审功能模块确认身份、签到、推荐评标委员会组长。采购人代表可以使用采购人代表专用签章确认评审意见。

三、评标委员会成员获取解密后的投标文件，开展评标活动。出现应当回避的情形时，评标委员会成员应当主动回避；代理机构按规定申请补充抽取评审专家；无法及时补充抽取的，采购人或者代理机构应当封存供应商投标文件，按规定重新组建评标委员会，解封投标文件后，开展评标活动。

四、评标委员会按照招标文件规定的评标程序、评标方法和标准进行评标，并独立履行下列职责：

（一）熟悉和理解招标文件；

(二)审查供应商投标文件等是否满足招标文件要求，并作出评价；

(三)根据需要要求采购组织单位对招标文件作出解释；根据需要要求供应商对投标文件有关事项作出 澄清、说明或者更正；

(四)推荐中标候选供应商，或者受采购人委托确定中标供应商；

(五)起草评标报告并进行签署；

(六)向采购组织单位、财政部门或者其他监督部门报告非法干预评审工作的行为；

(七)法律、法规和规章规定的其他职责。

5.3评标方法

采购包1：综合评分法

5.4评标程序

5.4.1熟悉和理解招标文件和停止评标

一、评标委员会正式评审前，应当对招标文件进行熟悉和理解，内容主要包括招标文件中供应商资格资质性要求、采购项

目技术、服务和商务要求、评审方法和标准以及可能涉及签订政府采购合同的内容等。

二、本招标文件有下列情形之一的，评标委员会应当停止评标：

（一）招标文件的规定存在歧义、重大缺陷的；

（二）招标文件明显以不合理条件对供应商实行差别待遇或者歧视待遇的；

（三）采购项目属于国家规定的优先、强制采购范围，但是招标文件未依法体现优先、强制采购相关规定的；

（四）采购项目属于政府采购促进中小企业发展的范围，但是招标文件未依法体现促进中小企业发展相关规定的；

（五）招标文件规定的评标方法是综合评分法、最低评标价法之外的评标方法，或者虽然名称为综合评分法、最低评标价法，但实际上不符合国家规定；

（六）招标文件将投标人的资格条件列为评分因素的；

（七）招标文件有违反国家其他有关强制性规定的情形。

出现上述应当停止评标情形的，评标委员会应当通过项目电子化交易系统向采购组织单位提交相关说明材料，说明停止评审的情形和具体理由。除上述情形外，评标委员会不得以任何方式和理由停止评标。

出现上述应当停止评标情形的，采购组织单位应当通过项目电子化交易系统书面告知参加采购活动的供应商，并说明具体原因，同时在四川政府采购网公告。采购组织单位认为评标委员会不应当停止评标的，可以书面报告采购项目同级财政部门依法处理，并提供相关证明材料。

5.4.2符合性审查

评标委员会依据本招标文件的实质性要求，对符合资格的投标文件进行审查，以确定其是否满足本招标文件的实质性要求。本项目符合性审查事项，必须以本招标文件的明确规定的实质性要求作为依据。

在符合性审查过程中，如果出现评标委员会成员意见不一致的情况，按照少数服从多数的原则确定，但不得违背政府采购基本原则和招标文件规定。

符合性审查标准见下表（按以下顺序审查）：

采购包1：

序号	符合审查要求概况	评审点具体描述	关联格式
1	不正当竞争预防措施（实质性要求）	在评标过程中，评标委员会认为投标人投标报价明显低于其他通过符合性审查投标人的投标报价，有可能影响产品质量或者不能诚信履约的，评标委员会应当要求其在合理的时间内通过项目电子化交易系统进行书面说明，必要时提交相关证明材料。投标人提交的书面说明，应当加盖投标人电子章，在评标委员会要求的时间内通过项目电子化交易系统进行提交，否则视为不能证明其投标报价合理性。投标人不能证明其投标报价合理性的，评标委员会应当将其投标文件作为无效投标处理。	开标一览表 分项报价表
2	投标文件的计量单位、报价货币、投标有效期	计量单位、报价货币、投标有效期均符合招标文件的要求。	开标一览表 分项报价表 投标（响应）函
3	投标报价	（1）报价唯一；（2）未超过招标文件规定的最高限价；（3）投标报价应包含本次招标要求的所有服务的费用；	开标一览表 分项报价表

4	招标文件第3章打★号的技术、商务和其他要求	投标文件均实质性响应招标文件第3章中加★号的要求。	服务偏离表 开标一览表 分项报价表 “★”号项内容承诺函与证明材料 其他材料 商务应答表 投标（响应）函
5	不属于禁止参加投标或投标无效的投标人	1.根据招标文件的要求不属于禁止参加投标或投标无效的投标人； 2.评标委员会未发现或者未知晓投标人存在属于国家相关法律法规规定的禁止参加投标或投标无效的投标人。	营业执照或法人证书或执业许可证 投标文件封面

以上实质性要求全部响应并满足采购需求的，则通过符合性审查；如有任意一项未响应或不满足采购需求的，则按无效投标文件处理。如果评标委员会认为投标人有任意一项不通过的，应在符合性审查表中载明不通过的具体原因。

5.4.3解释、澄清有关问题

一、评标过程中，评标委员会认为招标文件有关事项表述不明确或需要说明的，可以提请代理机构书面解释。代理机构的解释不得改变招标文件的原义或者影响公平、公正，解释事项如果涉及投标人权益的以有利于投标人的原则进行解释。

二、对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，评标委员会应当要求投标人作出必要的澄清、说明或更正，并给予投标人必要的反馈时间。投标人应当按评标委员会的要求进行澄清、说明或者更正。投标人的澄清、说明或者更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。澄清、说明或者更正不影响投标文件的效力，有效的澄清、说明或者更正材料是投标文件的组成部分。

三、投标人的澄清、说明或者更正需进行电子签章，应当不超出投标文件的范围、不实质性改变投标文件的内容、不影响投标人的公平竞争、不导致投标文件从不响应招标文件变为响应招标文件的条件。下列内容不得澄清：

（一）投标人投标文件中不响应招标文件规定的技术参数指标和商务应答；

（二）投标人投标文件中未提供的证明其是否符合招标文件资格、符合性规定要求的相关材料。

（三）投标人投标文件中的材料因印刷、影印等不清晰而难以辨认的。

四、投标文件报价出现下列情况的，按以下原则处理：

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

（二）大写金额和小写金额不一致的，以大写金额为准，但大写金额出现文字错误，导致金额无法判断的除外；

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

（四）总价金额与按单价汇总金额不一致的，以单价金额计算结果为准。

同时出现两种以上不一致的，按照前款规定的顺序修正。修正后的报价经投标人确认后产生约束力，投标人不确认的，其投标无效。

五、对不同语言文本投标文件的解释发生异议的，以中文文本为准。

六、代理机构宣布评标结束前，投标人应通过项目电子化交易系统随时关注评标消息提示，及时响应评标委员会发出的澄清、说明或更正要求。投标人未能及时响应的，自行承担不利后果。

评标委员会应当积极履行澄清、说明或者更正的职责，不得滥用权力。

5.4.4比较与评价

评标委员会应当按照招标文件规定的评标细则及标准，对符合性检查合格的投标文件进行商务和技术评估，综合比较和评价。

5.4.5复核

评分汇总结束后，评标委员会应当进行复核，对拟推荐为中标候选供应商、报价最低、投标文件被认定为无效等进行重点复核。

评标结果汇总完成后，评标委员会拟出具评标报告前，代理机构应当组织不少于2名工作人员，在采购监督人员的监督之下，依据有关的法律制度和招标文件对评标结果进行复核，出具复核报告。

评标结果汇总完成后，除下列情形外，任何人不得修改评标结果：

（一）分值汇总计算错误的；

（二）分项评分超出评分标准范围的；

（三）评标委员会成员对客观评审因素评分不一致的；

（四）经评标委员会认定评分畸高、畸低的。

评标报告签署前，经复核发现存在以上情形之一的，评标委员会应当当场修改评标结果，并在评标报告中记载；评标报告签署后，采购人或者代理机构发现存在以上情形之一的，应当组织原评标委员会进行重新评审，重新评审改变评标结果的，书面报告本级财政部门。

5.4.6确定中标候选人名单

采购包1： 确定3家供应商为成交候选人。 确定3家供应商为中标候选人。

（综合评分法适用）按投标人综合得分从高到低顺序排列，确定中标候选人。综合得分相同的，按投标报价由低到高顺序排列；得分且投标报价相同的，按投标人提供的优先采购产品认证证书数量由多到少顺序排列；得分且投标报价且提供的优先采购产品认证证书数量相同的并列。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。

（最低评标价法适用）按投标人投标报价从低到高顺序排列，确定中标候选人。投标报价相同的，按投标人提供的优先采购产品认证证书数量由多到少顺序排列；投标报价且提供的优先采购产品认证证书数量相同的并列。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。

5.4.7编写评标报告

评标报告是评标委员会根据全体评标成员签字的评标记录和评标结果编写的报告，其主要内容包括：

一、招标公告刊登的媒体名称、开标日期和地点；

二、投标人名单和评标委员会成员名单；

三、评标方法和标准；

四、开标记录和评标情况及说明，包括投标无效投标人名单及原因；

五、评标结果，确定的中标候选人名单或者经采购人委托直接确定的中标人；

六、其他需要说明的情况，包括评标过程中投标人根据评标委员会要求进行的澄清、说明或者更正，评标委员会成员的更换等；

七、报价最高的投标人为中标候选人的，评标委员会应当对其报价的合理性予以特别说明。

评标委员会成员应当在评标报告中签字或加盖电子签章确认，对评标过程和结果有不同意见的，应当在评标报告中写明并说明理由。签字但未写明不同意见或者未说明理由的，视同无意见。拒不签字或加盖电子签章又未另行说明其不同意见和理由的，视同同意评标结果。

5.5评标争议处理规则

评标委员会在评标过程中，对于符合性审查、对投标人文件作无效投标处理及其他需要共同认定的事项存在争议的，应当以少数服从多数的原则作出结论，但不得违背法律法规和招标文件规定。持不同意见的评标委员会成员应当在评标报告上签署不同意见及理由，否则视为同意评标报告。持不同意见的评标委员会成员认为认定过程和结果不符合法律法规或者招标文件规定的，应当及时向采购人或代理机构书面反映。采购人或代理机构收到书面反映后，应当书面报告采购项目同级财政部门依法处理。

5.6评标细则及标准

一、评标委员会只对通过资格审查的投标文件，根据招标文件的要求采用相同的评标程序、评分办法及标准进行评价和比

较。

二、评标委员会成员应依据招标文件规定的评分标准和方法独立评审。

5.6.1评分办法

（综合评分法适用）采用综合评分法的，由评标委员会各成员对通过资格检查和符合性审查的投标人的投标文件进行独立评审。

投标报价得分=（评标基准价 / 投标报价）×100

评标总得分=F1×A1+F2×A2+……+Fn×An

F1、F2……Fn分别为各项评审因素的得分；

A1、A2、……An 分别为各项评审因素所占的权重（A1+A2+……+An=1）。

评标过程中，不得去掉报价中的最高报价和最低报价。

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。

5.6.2评分标准

采购包1：

评审因素		评审标准			
分值构成		详细评审90.00分 报价得分10.00分			
评审因素分类	评审项	详细描述	分值	客观/主观	关联格式
	服务响应 （共同评审因素）	投标人提供的投标文件完全满足招标文件第三章中“服务工具要求”的得28分，其中： 1、带“★”号条款为实质性要求，若不满足视为无效投标。 2、带“▲”号条款（共45项）作为重要指标，“▲”项技术条款响应得分=（满足“▲”项技术条款的数量÷“▲”项技术条款的总数量）×18分。 3、无符号条款（共214项）作为一般指标要求，无符号技术条款响应得分=（满足无符号技术条款的数量÷无符号技术条款的总数量）×10.7分。 注：1.以阿拉伯数字1、2、3为单独1项进行计分； 2.文件要求提供证明材料的应当按照要求对应提供，未明确要求的投标人应在服务偏离表中应答或响应或提供承诺函进行承诺。	28.70	客观	本项目的技术方案、项目实施方案 服务偏离表 商务应答表 其他材料

详细评审	服务方案 （技术类评审因素）	根据投标人针对本项目提供的项目实施方案，包括：①业务现状分析、②服务需求分析、③服务方案、④服务考核方案、⑤服务保障方案。完整提供上述内容的得30分；每有一项缺失扣6分，每有一项存在缺陷扣3分，本项分值扣完为止。注：上述“缺陷”是指项目名称描述错误；实际方案存在相互矛盾；照搬其他项目方案而存在与本项目执行无关的内容；只有简单复制粘贴需求内容而无描述；语言文字错误；表述内容存在歧义；不满足采购需求中非实质性要求的情形。	30.00	主观	本项目的技术方案、项目实施方案 其他材料 商务应答表
	服务人员配置 （共同评审因素）	1、拟投入本项目项目经理（1人）：其具有系统架构设计师[计算机技术与软件专业技术资格(高级)]、系统分析师[计算机技术与软件专业技术资格(高级)]、信息系统项目管理师[计算机技术与软件专业技术资格(高级)]证书的，项目经理每拥有一个证书得 2 分，最多得 6 分。 2、专业技术服务团队（14分，不含项目经理） ①拟投入服务规划团队：成员具有系统分析师[计算机技术与软件专业技术资格(高级)]证书的,每有 1 名成员得 2 分，本项最多得 4 分。 ②拟投入信息安全保障团队：成员具有注册信息安全管理人员证书(CISP)的得2分，本项最多得6分。 ③拟投入网络技术服务团队：成员具有高级网络信息安全工程师证书的得 2 分，本项最多得2分 ④拟投入质量保障团队：有1名成员具有高级软件测试工程师证书得 2分；本项最多得 2 分。 注：①提供人员配置清单；②提供人员证书复印件并加盖投标人公章；③专业技术服务团队同一人员不重复计分。	20.00	客观	本项目的技术方案、项目实施方案 其他材料

	业绩 （共同评审因素 ）	投标人自2020年1月1日（含）以来具有类似履约经验的，得1.3分。 注：①提供合同（协议）或中标（成交）通知书复印件并加盖公章；②合同（协议）以签订时间为准，中标（成交）通知书以发出时间为准；③类似项目是指网络安全类项目。	1.30	客观	其他材料
	服务质量保障措施 （技术类评审因素）	根据投标人针对本项目提供的服务质量保障措施进行评分，包括：①服务管理制度、②质量保障措施。完整提供上述内容的得10分；每有一项缺失扣5分，每有一项存在缺陷扣2.5分，本项分值扣完为止。注：上述“缺陷”是指项目名称描述错误；实际方案存在相互矛盾；照搬其他项目方案而存在与本项目执行无关的内容；只有简单复制粘贴需求内容而无描述；语言文字错误；表述内容存在歧义；不满足采购需求中非实质性要求的情形。	10.00	主观	本项目的技术方案、项目实施方案 其他材料
价格分	价格分	价格分应当采用低价优先法计算，即满足招标文件要求且投标价格最低的投标报价为评标基准价，其价格分为满分。其他投标人的价格分统一按照下列公式计算： 投标报价得分=(评标基准价／投标报价)×10	10.00	客观	开标一览表 分项报价表

价格扣除

序号	情形	适用对象	比例	说明	关联格式

1	小型、微型企业，监狱企业，残疾人福利性单位	投标人或联合体成员均为小型、微型企业	10.00%	对符合《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）规定的小微企业报价给予10%的扣除，用扣除后的价格参加评审。承接本项目的供应商符合相应条件时，给予10%的价格扣除;监狱企业与残疾人福利性单位视同小型、微型企业，享受同等价格扣除，当企业属性重复时，不重复价格扣除。	开标一览表 分项报价表 中小企业声明函 残疾人福利性单位声明函 监狱企业的证明文件

说明：

1、评分的取值按四舍五入法，保留小数点后两位；

2、评分标准中要求提供的证明材料须清晰可辨。

（最低评标价法适用）采用最低评标价法的，投标文件满足招标文件全部实质性要求，且投标报价最低的投标人为中标候选人。采用最低评标价法评标时，除了算术修正和落实政府采购政策需进行的价格扣除外，不能对投标人的投标价格进行任何调整。

5.7废标

本次政府采购活动中，出现下列情形之一的，予以废标：

一、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三家的；

二、出现影响采购公正的违法、违规行为的；

三、投标人的报价均超过了采购预算，采购人不能支付的；

四、因重大变故，采购任务取消的；

废标后，代理机构将在四川政府采购网上公告。对于评标过程中废标的采购项目，评标委员会应当对招标文件是否存在倾向性和歧视性、是否存在不合理条款进行论证，并出具书面论证意见。

5.8定标

5.8.1 定标原则

采购人在评标报告确定的中标候选人名单中按顺序确定1名中标人。中标候选人并列的，由采购人采取随机抽取的方式确定中标人。

5.8.2定标程序

一、评标委员会在项目电子化交易系统中编制评标情况，生成评标报告。

二、代理机构在评标结束之日起2个工作日内将评标报告送采购人。

三、采购人在收到评标报告后5个工作日内，按照评标报告中推荐的中标候选人顺序确定中标供应商。逾期未确认的，又不能说明合法理由的，视同按评标报告推荐的顺序确定排名第一的中标候选人为中标供应商。

四、根据确定的中标供应商，代理机构在四川政府采购网上发布中标结果公告，通过项目电子化交易系统向中标供应商发出中标通知书。

5.9评审专家在政府采购活动中承担以下义务

（一）遵守评审工作纪律；

（二）按照客观、公正、审慎的原则，根据采购文件规定的评审程序、评审方法和评审标准进行独立评审；

（三）不得泄露评审文件、评审情况和在评审过程中获悉的商业秘密；

（四）及时向监督管理部门报告评审过程中的违法违规情况，包括采购组织单位向评审专家作出倾向性、误导性的解释或者说明情况，供应商行贿、提供虚假材料或者串通情况，其他非法干预评审情况等；

（五）发现采购文件内容违反国家有关强制性规定或者存在歧义、重大缺陷导致评审工作无法进行时，停止评审并通过项目电子化交易系统向采购组织单位书面说明情况，说明停止评审的情形和具体理由；

（六）配合答复处理供应商的询问、质疑和投诉等事项；

（七）法律、法规和规章规定的其他义务。

5.10评审专家在政府采购活动中应当遵守以下工作纪律

（一）遵行《中华人民共和国政府采购法》第十二条和《中华人民共和国政府采购法实施条例》第九条及财政部关于回避的规定。

（二）评标前，应当将通讯工具或者相关电子设备交由采购组织单位统一保管。

（三）评标过程中，不得与外界联系，因发生不可预见情况，确实需要与外界联系的， 应当在监督人员监督之下办理。

（四）评标过程中，不得干预或者影响正常评标工作，不得发表倾向性、引导性意见， 不得修改或细化招标文件确定的评标程序、评标方法、评审因素和评审标准，不得接受供应商主动提出的澄清和解释，不得征询采购人代表的意见，不得协商评分，不得违反规定的评审格式评分和撰写评标意见，不得拒绝对自己的评标意见签字确认。

（五）在评审过程中和评审结束后，不得记录、复制或带走任何评审资料，除因履行本规程第十三条第（六）项规定的义务外，不得向外界透露评审内容。

（六）服从评审现场采购组织单位的现场秩序管理，接受评审现场监督人员的合法监督。

（七）遵守有关廉洁自律规定，不得私下接触供应商，不得收受供应商及有关业务单位和个人的财物或好处，不得接受采购组织单位的请托。

第6章投标文件格式

6.1投标文件封面格式

采购包1：

分册名称：投标响应文件分册

详见附件：投标文件封面

详见附件：投标（响应）函

详见附件：中小企业声明函

详见附件：残疾人福利性单位声明函

详见附件：监狱企业的证明文件

详见附件：投标人应提交的相关资格证明材料

详见附件：商务应答表

详见附件：开标一览表

详见附件：分项报价表

详见附件：本项目的技术方案、项目实施方案

详见附件：营业执照或法人证书或执业许可证

详见附件：其他材料

详见附件：“★”号项内容承诺函与证明材料

详见附件：服务偏离表

第7章 拟签订采购合同文本

详见附件：合同主要条款.pdf