黑 龙 江 省 政 府 采 购

竞争性磋商文件

项目名称：2023年网络及安全外包运维服务

项目编号：[230101]JLZB[CS]20230001

哈尔滨峻岭招标有限公司

2023年08月

第一章 竞争性磋商邀请

哈尔滨峻岭招标有限公司受哈尔滨住房公积金管理中心委托，依据《政府采购法》及相关法规，对2023年网络及安全外包运维服务采购及服务进行国内竞争性磋商，现欢迎国内合格供应商前来参加。

一、项目名称：2023年网络及安全外包运维服务

二、项目编号：[230101]JLZB[CS]20230001

三、磋商内容

包号	货物、服务和工程名称	数量	采购需求	预算金额（元）
1	2023年网络及安全外包运维服务	1	详见采购文件	691,200.00

四、交货期限、地点：

1.交货期：

合同包1（2023年网络及安全外包运维服务）： 三年（本项目为一采叁年的项目，采购结果最多叁年沿用，合同一年一考核一续签。是否续签，由甲方视财政预算安排及乙方供应商资质条件（是否符合《政府采购法》第二十二条规定）、服务质量、服务内容、服务标准等情况确定。第一年合同自2023年12月1日至2024年11月30日止。合同期满后，经采购人有关部门审核，并且第二年或第三年项目预算不变或变动幅度不超过第一年的10%的，签订补充协议，在财政部门备案下达后可续签政府采购合同，合同标准结算方式不变；预算变动幅度超过10%的，重新开展政府采购活动。

2.交货地点：

合同包1（2023年网络及安全外包运维服务）： 招标人指定地点

五、参加竞争性磋商的供应商要求：

（一）必须具备《政府采购法》第二十二条规定的条件。

（二）参加本项目磋商的供应商，须在黑龙江省内政府采购网注册登记并经审核合格。

（三）本项目的特定资质要求：

合同包1（2023年网络及安全外包运维服务）：无

六、参与资格和竞争性磋商文件获取方式、时间及地点：

1.磋商文件获取方式：采购文件公告期为5个工作日，供应商须在公告期内凭用户名和密码，登录黑龙江省政府采购网，选择“交易执行 → 应标 → 项目投标”，在“未参与项目”列表中选择需要参与的项目，确认参与后即可获取磋商文件。获取磋商文件的供应商，方具有投标和质疑资格。逾期报名，不再受理。

2.获取磋商文件的时间：详见磋商公告。

3.获取磋商文件的地点：详见磋商公告。

七、磋商文件售价：

本次磋商文件的售价为 无 元人民币。

八、询问提起与受理：

供应商对政府采购活动有疑问或有异议的，可通过以下方式进行询问：

(一)对采购文件的询问

采购文件处项目经办人 详见磋商公告 电话：详见磋商公告

(二)对评审过程和结果的询问

递交响应文件的投标人应在评审现场以书面形式向代理机构提出。

九、质疑提起与受理：

(一)对磋商文件的质疑：已注册供应商通过政府采购网登录系统，成功下载磋商文件后，方有资格对磋商文件提出质疑。

采购文件质疑联系人： 张工

采购文件质疑联系电话： 0451-51095052

（二）对磋商过程和结果的质疑

1.提出质疑的供应商应当是参与所质疑项目采购活动的供应商；质疑供应商应当在法定期内一次性提交质疑材料；对采购过程提出质疑的，为各采购程序环节结束之日起7个工作日提出；对成交结果提出质疑的，为成交结果公告期限届满之日起7个工作日提出；

2.质疑供应商应当以书面形式向本代理机构提交《质疑函》。

磋商过程和结果质疑：详见成交公告

十、提交竞争性磋商首次响应文件截止时间及磋商时间、地点：

递交响应文件截止时间：详见磋商公告

递交响应文件地点：详见磋商公告

响应文件开启时间：详见磋商公告

响应文件开启地点：详见磋商公告

备注：所有电子响应文件应在递交响应文件截止时间前递交至黑龙江省政府采购云平台，逾期递交的响应文件，为无效投标文件，平台将拒收。

十一、发布公告的媒介

中国政府采购网（www.ccgp.gov.cn），黑龙江政府采购网（https://hljcg.hlj.gov.cn）

十二、联系信息

1.采购人信息

采购单位：哈尔滨住房公积金管理中心

采购单位联系人： 许世越

地址： 哈尔滨市道外区景阳街132号

联系方式： 13029710451

2.采购代理机构信息（如有）

名称：哈尔滨峻岭招标有限公司

地址： 黑龙江省哈尔滨市道里区抚兴街18号

联系方式： 0451-51095052

3.项目联系方式

项目联系人： 哈尔滨峻岭招标有限公司

联系方式： 0451-51095052

哈尔滨峻岭招标有限公司

2023年08月

第二章 采购人需求

一.项目概况

一、运维服务工作目标

根据对哈尔滨住房公积金管理中心（以下简称“中心”）网络信息安全工作的现状，为切合中心在信息安全建设方面的需求，在网络安全体系建设方面，通过网络安全风险评估、网络信息系统等级保护测评工作，完善现有网络运维及网络管理体系，满足国家、省市及上级业务指导部门的合规要求；在基础安全方面，通过深入开展终端、主机、网络设备、安全设备管理，进一步提升系统的网络安全防御水平；在业务安全方面，通过网络安全监测、应用安全、数据安全、安全审计等服务，提高关键业务的可靠性和可用性；在人员能力、系统保障能力提升方面，通过网络系统应急演练、应急响应、网络安全培训等服务，切实提供的安全意识和系统安全保障能力。通过落实以上四个方面的安全工作，最终将达到以下项目总体目标：

对中心突发的信息安全事件做出快速、有效的处置，需确定信息安全事件的定级准则，实施应急响应处理；防范信息系统威胁，监测可能面临自然、环境和技术故障等非人为因素的威胁，避免人员失误和恶意攻击等人为因素的威胁。判定和处置突发的信息安全事件，按信息安全事件发生的性质对信息安全事件进行处置。

1.运维服务期内无重大信息安全责任事件（重大信息安全责任事件数为0）；

2.提高信息安全技防能力，确保中心物理、主机、网络、应用、数据和外部网站等正常运行；

3.建立健全中心信息安全管理体系；

4.提高中心信息化队伍安全技术水平，提升中心整体信息安全意识。

二、运维服务工作原则

中心的安全体系服务要求遵循“面向应用，注重实效”的指导思想，紧密结合中心现有网络情况，充分保证原有系统和结构的安全可用。

1.实用性原则

中心网络安全必需保证整个防御体系的完整性，在网络及安全运维服务体系中，要求采取由专业运维团队进驻现场提供网络安全防御的技术和措施，进而保障中心的网络系统安全运行。

2.完整性原则

要求网络安全防范体系技术方案要能够随着安全技术的发展、外部环境的变化、安全目标的调整而不断升级发展。

3.动态发展原则

要求网络安全防范体系技术方案要能够随着安全技术的发展、外部环境的变化、安全目标的调整而不断升级发展。

三、运维服务内容及要求

中心业务网络是负责全市各区、县（市）内所有住房公积金管理、贷款、监管等业务的重要网络，具备高安全性、高可靠性、高连通性的要求。以哈市中心为核心，除了中心核心平台和办公网络外，还连接20多个分布在区、县（市）的分支机构、多家银行、政务内网、备份中心、网上公积金服务中心等，是中心业务唯一且重要的网络系统。其上承载多个关键和重要业务应用，且每年还不断有新的业务上线运行。

中心网络系统采用高级组网技术，全网采用动态路由和静态路由相结合的方式，全面采用标记交换技术、MSTP、XNF、双核心、冗余链路、热备等网络技术，以及边界安全隔离交互区等网络安全技术。

合同包1（2023年网络及安全外包运维服务）

1.主要商务要求

标的提供的时间	三年（本项目为一采叁年的项目，采购结果最多叁年沿用，合同一年一考核一续签。是否续签，由甲方视财政预算安排及乙方供应商资质条件（是否符合《政府采购法》第二十二条规定）、服务质量、服务内容、服务标准等情况确定。第一年合同自2023年12月1日至2024年11月30日止。合同期满后，经采购人有关部门审核，并且第二年或第三年项目预算不变或变动幅度不超过第一年的10%的，签订补充协议，在财政部门备案下达后可续签政府采购合同，合同标准结算方式不变；预算变动幅度超过10%的，重新开展政府采购活动。
标的提供的地点	招标人指定地点
投标有效期	从提交投标（响应）文件的截止之日起90日历天
付款方式	1期：支付比例50%，服务满6个月且验收合格后支付合同款的50% 2期：支付比例50%，合同期满验收合格后支付合同款的50%
验收要求	1期：按照招标技术参数标准进行验收，符合验收标准给予验收
履约保证金	不收取
合同履行期限	本项目为一采叁年的项目，采购结果最多叁年沿用，合同一年一考核
其他	

2.技术标准与要求

序号	核心产品（“△”）	品目名称	标的名称	单位	数量	分项预算单价（元）	分项预算总价（元）	面向对象情况	所属行业	招标技术要求
1		安全运维服务	2023年网络及安全外包运维服务	年	1.00	691,200.00	691,200.00	面向中小企业	软件和信息技术服务业	详见附表一

附表一：2023年网络及安全外包运维服务　是否进口：否

参数性质	序号	具体技术(参数)要求
		网络及网络安全运维管理服务 1.★服务内容包含对中心范围内所有网络安全设备（安全防护类设备、综合审计类设备、流量分析类设备）的日常巡检服务，每月定期提交网络安全巡检报告，巡检内容包含但不限于：本月网络安全整体态势情况、现网安全设备整体运行情况、高中低危告警数量及已处置数量。定期进行安全策略检查优化，根据客户业务变更需求实时对安全设备策略进行调整，在满足安全需求的同时保证业务通畅稳定运行。协助甲方制定网络安全应急预案，针对常见网络攻击、扫描、漏洞利用、WEBSHELL上传、shell反弹等攻击行为提出有效的应急处置预案。 2.★服务内容包含对现网运行安全设备的网络架构规划设计及调整,策略调整、优化，对来自互联网及内部网络的网络攻击行为进行深度分析和告警。 3.协助甲方制定网络安全应急预案，针对常见网络攻击、扫描、漏洞利用、WEBSHELL上传、shell反弹等攻击行为提出有效的应急处置预案。 4.定期对网络安全产品、态势感知进行日志分析，筛选出高危、危机的网络攻击行为，提出切实可行的处置建议。 5.负责定期对网络安全设备进行策略梳理及配置备份，及时发现冗余策略和存在逻辑错的安全策略。 6.利用技术手段实时监控网络流量中的WEB应用弱口令情况，并判断是否登陆成功，定期形成WEB应用弱口令报告提交并督促整改。 7.★每月定期提交网络安全巡检报告，巡检内容包含：安全设备软硬件健康度状态、本月网络安全整体态势情况、现网安全设备整

	1	体运行情况、高中低危告警数量及已处置数量。 8.服务内容涵盖对中心范围内整体网络框架进行日常运维管理，主要包含组网、配置备份、定期口令修改、网络设备配置调整、配置优化、网络故障排查及处置、链路监测。 9.★每月出具整体网络运行健康度巡检报告，报告内容应涵盖：中心范围内整体网络设备硬件运行健康度，网络链路质量、重要汇聚链路路径检查、重要主干链路带宽占用率检查等。 10.在服务过程中对现有网络框架不合理处提出相关改造建议方案，方案中应说明问题所在网络区域位置、问题详细描述、严重性、危害性、改造建议，改造所需时间、改造风险、改造风险管理及规避。 11.服务期内对中心整体范围内软硬件资产进行识别和统计管理，包括网络设备、办公设备、物联网设备硬件属性等信息； 12.资产底层系统识别，操作系统、软件版本、版本号等；资产对外开放的端口所对应的服务信息；资产的支撑系统包括Web服务器、Web中间件、开发语言等；资产的软件应用包括CMS、网站WAF、OA系统、CRM、邮件系统等。 13.形成软硬件资产统计清单，同时根据用户资产变更及时更新统计清单。 14.为管理层安全意识培训，提高管理层的安全意识，使被培训者了解当前网络安全态势，了解最新安全技术的发展状况，能够为网络安全建设确立目标、把握方向。 15.★对员工安全意识培训，针对员工提供安全意识培训，使被培训者通过学习了解到当前网络存在的安全风险和隐患，提升非技术人员的整体安全意识和安全防护能力。 16.对安全管理类培训，通过安全管理培训，可以提升网络安全管理的能力，降低风险事故发生的几率。通过培训了解网络安全基础知识、各种安全技术概况、常用术语及概念、了解风险评估、应急响应等安全服务的意义和安全管理的内涵。 17.对安全技术类培训，以理论学习为基础，结合专业实训，为技术人员提供坚实的网络安全基础课程。包括:恶意代码分析、Web应用安全、网络安全攻防技术渗透测试技术等。 18.培训涉及到核心网络设备维护与配置、网络安全设备维护与配置、网络线缆维护与配置等知识的综合性培训； 19.确保相关科技人员能够独立进行管理、运行、故障处理及日常测试维护等工作； 20.组织开展每年2次不限人数的网络安全知识现场学习培训，提高网络安全意识、日常办公网络安全防护、信息安全等级保护等进行了解；对《网络安全法》关于网络空间主权原则、关键信息基础设施、个人信息保护、网络使用的安全义务等内容讲解；培训学习认识网络安全防范的重要性，树立网络安全法治理念和法律红线意识，学习遵守网络安全管理有关规定，规范使用计算机网络，不泄露相关信息，提高保密意识警惕性，做好网络安全保密培训工作。 21.服务期内对中心依据国家相关法律法规要求，制定相应的网络安全管理制度，梳理信息化管理条例。 22.★派驻2名具备（中国信息安全测评中心CISP（CISE）信息安全专业人员认证或计算机技术与软件专业技术资格的网络工程师、信息安全工程师、网络规划设计师认证）专业的网络或安全维保服务工程师提供驻场服务。 23.上下班时间与用户单位保持一致，协助完成定期巡检服务、现场维护、各厂商协调、现场技术支持等工作。 24.对各项服务内容实行流程化管理，服务过程采用规范操作，确保服务质量满足用户网络安全保障要求； 25.协助完成定期巡检服务、现场维护、各厂商协调、现场技术支持等工作； 26.及时跟踪用户网络情况，对用户任何网络变化需求，完成网络配置工作，保证及时、正确、准确； 27.及时根据各个方面公布的网络漏洞、安全漏洞、主机漏洞，通过对网络上的各种设备进行配置、代码升级、系统升级等措施，消除隐患、保障安全； 28.★驻场工程师需具有网络或安全维护2年以上从业经验，具有所在委派投标单位工作一年以上的社保证明。 29.按照中心要求，每年至少2次对中心机房网络线路进行梳理、打标、规范等工作。能根据中心要求协助完成日常计算机终端维护

		等桌面运维工作。
	2	网络信息安全风险评估服务 1、★针对现网运行相关网络设备、安全设备、服务器设备、操作系统、中间件、数据库等软硬件资产进行梳理统计，形成风险评估资产清单，根据资产情况单独列出重要软硬件资产清单。 2、利用人工手动、自动化、访谈等方式针对风险评估资产清单中的资产进行系统安全脆弱性发现。 3、在不影响业务稳定的前提下针对部分重要资产面临的高危风险问题进行验证。 4、★服务期内每年2次系统安全风险评估服务，出具风险评估报告，提出问题总结清单和风险处置建议。 5、要求按国家等级保护GB/22239执行标准、《GB/T 20984-2022 信息安全风险评估方法》，每年定期进行2次网络安全风险评估，并出具相应报告。 6、协助进行服务器安全加固检查主要从加固修补系统漏洞、系统帐户权限强化，加强服务器日志审核，过滤危险服务，屏蔽不必要的端口服务，优化注册表等方面来进行，并出具安全加固意见报告； 7、了解中心的信息管理系统的管理制度，以及中心的网络、系统的安全状况，确认出对中心资产会造成危害的因素，确认威胁实施的可能性，对中心资产在受到危害时，确定旗下资产根据各种对比，明确信息系统已经有的安全措施的有效性，明晰信息系统的所有安全管理需求； 8、安全技术差距分析，安全管理差距分析，系统运维差距分析，物理安全差距分析，对信息系统的现状了解详细，通过分析手机的资料和数据确认信息系统的建设是否符合该等级的安全要求； 9、从资产、脆弱性、威胁和已有安全措施等多个维度，结合风险承受能力，综合分析评价该项目各系统面临的风险，具体应包括：对信息系统所覆盖的全部资产进行识别，并合理分类；在资产识别过程中，需要详细识别核心资产的安全属性，重点识别出资产在遭受泄密、中断、损害等破坏时所遭受的影响，为资产影响分析及综合风险分析提供参考数据； 10、通过对信息系统网络架构和业务系统及流程进行威胁调查、取样等手段，识别非涉密信息系统的资产将面临的威胁源，及其威胁可能采用的威胁方法，对资产所产生的影响，并为后续威胁分析及综合风险分析提供参考数据； 11、对信息系统的服务器、存储设备、数据库、中间件、应用软件、网络和安全设备、桌面终端系统、机房物理环境、安全管理制度及流程进行脆弱性识别，采用工具扫描、手工、访谈、文档分析方法进行脆弱性识别； 12、完成针对信息系统的网络技术架构、网络设备进行评估，完成整体网络架构、网络设备安全的分析工作； 13、对安全设备配置及策略评价，如防火墙、安全审计设备等； 14、对操作系统及数据库安全策略评价，内容包括操作系统文件的完整性、补丁安装、用户权限管理、口令管理、多种操作系统间的协作性等进行评估。 15、对安全管理制度评价，对各种安全管理规章制度的齐备性及执行到位性检查评估； 16、★对资产分析、威胁分析、脆弱性分析的基础上，完成信息系统的信息系统信息安全综合风险分析。

	3	网络安全漏洞管理服务 1、★要求每月1次定期的网络安全自检、评估，服务单位需自行配备漏洞扫描系统，定期的进行网络安全检测服务，安全检测最大可能的消除安全隐患，尽可能早地发现安全漏洞并进行修补，有效的利用已有系统，优化资源，提高网络的运行效率； 2、★要求服务商通过人工、工具、手动的方式对信息系统内约1000节点的网络设备、服务器及操作系统、业务应用软件、中间件及其他资产和各种服务等进行安全漏洞识别和安全扫描，并出具漏洞发现汇总及详细报告； 3、提供主机漏洞扫描服务，结合单位信息系统的实际情况，对目标信息系统内的网络设备、操作系统、应用软件、中间件等进行漏洞扫描；利用漏洞扫描工具对基础环境进行系统漏洞扫描，出具《主机漏洞扫描报告》，并提出漏洞修复建议； 4、提供主机漏洞扫描，操作系统漏洞、网络设备漏洞、Web服务器漏洞、数据库服务器漏洞、邮件服务器漏洞、DNS漏洞等； 5、提供弱密码扫描，3389远程桌面、FTP服务器弱密码、SSH弱密码、TELNET弱密码、MSSQL、MYSQL弱密码、ORACLE弱密码、SMB弱密码、VNC弱密码等； 6、提供安装新软件、启动新服务后的检查，安装新软件和启动新服务前进行漏洞扫描检查扫描系统，保障系统安全运行； 7、网络建设和网络改造前后的安全规划评估和成效检验，从技术上和管理上加强对网络安全和信息安全的重视，形成立体防护，由被动修补变成主动的防范，最终把出现事故的概率降到最低； 8、网络安全事故后的分析调查，网络安全事故后通过网络漏洞扫描/网络评估系统分析确定网络被攻击的漏洞所在，帮助弥补漏洞，尽可能多得提供资料方便调查攻击的来源； 9、重大网络安全事件前的准备，重大网络安全事件前对网络漏洞扫描，帮助用户及时的找出网络中存在的隐患和漏洞。
		网络安全系统渗透测试服务 1、★要求服务期间提供每年对10个指定业务系统渗透测试服务；要求通过人工黑盒的测试方式，发现网络和业务系统中网络和系统存在的安全缺陷，提供渗透测试报告和改进建议。 2、★网络安全渗透测试是否可以执行计划外的命令、访问未被授权的数据、接管主机管理控制权等； 3、★渗透测试是否可以在目标系统的客户端浏览器上执行脚本，从而劫持客户端用户会话、危害网站或者将客户端用户转向恶意网站； 4、★渗透测试目标系统身份认证和密码的安全性，如用户枚举、默认、暴力破解、认证模式绕过、双因素认证安全性、记住密码和密码重置弱点、注销和浏览器缓存弱点等； 5、渗透测试目标系统的认证密码的安全强度是否足够； 6、渗透测试系统身份认证方式是否存在安全漏洞； 7、渗透测试目标系统的授权机制是否存在漏洞； 8、渗透测试目标系统是否存在绕过授权模式，是否存在越权/非授权访问漏洞、是否存在非授权提权漏洞；

	4	9、渗透测试目标系统敏感信息是否存在不安全的加密存储； 10、评估加密算法的安全轻度是否足够； 11、渗透测试目标系统的会话安全机制； 12、渗透测试攻击者是否可以假冒受害客户端执行操作； 13、渗透测试攻击者是否可以破坏会话传输的完整性和机密性； 14、渗透测试目标系统是否存在不安全的直接对象引用； 15、渗透测试目标系统是否每次都验证用户是否有权访问目标对象； 16、渗透测试攻击者是否可以操控这些引用去访问未授权数据； 17、★渗透测试目标系统的安全配置安全性，如应用程序、框架、应用程序服务器、维保服务器、数据库服务器和服务的配置是否存在安全漏洞,如：未更改默认账户/密码、未使用的网页、未安装补丁的漏洞、为被保护的文件和目录、未禁用或杀出多余的端口/服务/网页/账户/权限等； 18、渗透测试攻击者利用错误的安全配置是否可以访问目标系统未授权的数据或功能； 19、渗透测试系统是否限制URL访问权限； 20、渗透测试系统重定向或转发链接是否经过验证； 21、渗透测试攻击者是否利用不安全的转发绕过访问控制； 22、渗透测试系统在业务逻辑层面是否存在安全漏洞； 23、渗透测试攻击者是否可以利用缓冲区溢出漏洞进行非授权访问、获取控制权、破坏可用性等威胁操作； 24、渗透测试系统的可用性是否易被攻击和影响； 25、渗透测试系统的页面是否已经或可以被攻击者篡改； 26、渗透测试目标系统是否已经或可以被挂暗链； 27、渗透测试系统是否已经或可以被挂马； 28、渗透测试攻击者是否可以获取目标系统的后台管理路径，甚至后台管理权限； 29、渗透测试攻击者是否可以非法上传文件； 30、渗透测试是否通过渗透获取目标系统，并通过渗透进一步扩散到内网； 31、实施人员不得将渗透测试中有关用户的信息泄露给第三方； 32、渗透测试方应说明进行渗透测试的详细工作流程和具体实施步骤； 33、渗透测试方应能说明进行渗透测试所依照的相关渗透测试标准、漏洞库、软件缺陷等； 34、渗透测试方应能说明进行渗透测试所采用的工具，如商业评估工具、开源评估工具、自开发工具/脚本、源代码安全测试工具等；

		35、渗透测试方应说明进行渗透测试前，用户应进行的准备工作，包括网络接入环境、办公场所准备、所需材料准备、所需信息准备、所需人员配合等； 36、渗透测试方应说明进行渗透测试各项工作时，可能对目标系统产生的影响，尤其是可能造成目标系统性能下降、数据完整性和机密性破坏的影响；
5	网络安全及重大时期应急响应保障服务	★测试结束后需出具完整的渗透测试报告，并提出改进意见。 1、协助采购单位对应用服务瘫痪、网络阻塞、DDOS攻击问题、服务器劫持、系统异常宕机、恶意入侵、黑客攻击、病毒爆发、内网安全问题进行应急处置；协助用户降低影响，并在应急处理完毕后提供事件应急响应报告，说明事件原因、处理过程及处理结果，提供此事件的安全分析建议。 2、★协助采购单位分析、处置网络安全事件（事故）、信息安全事件（事故）、实施应急处理计划，协助采购单位验证恢复后的系统是否运行正常，并确认与原有系统配置保持一致； 3、协助对发生异常的系统进行分析，判断是否真正发生了安全事件， 协助采购单位共同确定应急处理方案，并协助落实； 4、★应急响应方式：现场响应，发生应急响应事件时，需安排不少于2名经验丰富的服务工程师提供现场服务，工程师需24小时待命，随时配合用户服务，当已有的工程师力量无法满足现场需要时，服务商需无条件协调相关具有服务技术实力力量的厂商、供应商等资源保障用户单位的系统正常使用； 5、本地支持：接到采购单位紧急服务请求，支持人员在最短时间内赶赴客户现场，协助客户分析事件可能的原因，解决各类安全事件； 6、远程支持；通过电话、QQ远程协助、远程临时接入等非现场的活动，协助客户分析事件可能的原因，解决各类安全事件。 7、特定时期护网与重要时期需确保网络安全监测处置平台设备长期、稳定的工作，最大限度降低系统的运行故障及网络安全系统设备的使用； 8、★每年进行2次网络或网络安全应急演练，要求应急演练模拟真实可能发生的风险隐患，协调中心业务相关的软件、网络、容灾备份等各方服务人员，应急演练结束后要根据演练结果和发现的问题，出具应急演练总结报告。 9、★特定时期需保障3名以上网络安全工程师全天候现场驻守服务，维护工程师需每日对网络安全监测处置平台设备、WAF、全流量分析设备、蜜罐等配套的安全软件系统进行巡检，对各类安全设备及流量监测设备产生的攻击日志进行实时分析和预警，排除安全隐患； 10、对网络梳理服务，配合网络管理中心梳理互利网暴露面网络架构及资产，同时配合各分公司对相关的网络拓扑、网络架构、安全现状进行梳理，明确网管中心及各分公司网络及拓扑架构的模式，详细了解网络各出口的作用，掌握互联网暴露面安全风险状况； 11、配合网管及各分公司梳理防火墙防护策略，整理冗余策略、杜绝对外暴露运维服务端口； 12、对网络架构梳理，通过人工与设备相结合的方式，利用全流量分析系统中互联关系管理功能对网管中心安全资产访问关系进行梳理，从而得到各资产的访问拓扑图，从而识别各资产属性，统计互联网出口数量和情况及互利网业务情况。 13、对于梳理出来的隐患及问题结合网管中心及各分公司的本地需求网络，满足上级单位迎检规范、符合等保测评要求，针对信息安全提出相应整改建议，配合用户进行安全隐患问题排查解决； 14、★对防火墙策略梳理，通过全流量分析系统或人工梳理的方式协助管理员优化防火墙的配置策略；

		15、在特定时期护网与重要时期按保障安全需求，协调各网络安全厂商资源，通过临时借调相应设备、临时搭建网络安全平台、聘请专业的网络安全工程师配合我单位进行相关安全保障工作； 16、★对信息系统、VPN、无线网络、运维管理系统等账号进行梳理，清理无用账号，减少管理员账号数量，限定管理员登录地址，做到账户和权限清晰，全面消除弱密码； 17、组织信息系统开发、运维等合作公司，对开发和运维人员掌握的网络和系统相关文档、资料进行归类和清理。对信息系统后台管理页面进行排查梳理，禁止通过互联网直接访问后台管理页面； 18、★对网络攻击行为进行技术分析，对网络攻击造成的影响进行评估，根据应急处置情况研究相应对策。根据网络攻击影响评估结果，提出下达网络链路中断和恢复以及业务系统等停用和恢复指令的意见 。
	6	网络及网络安全设备软硬件维护维修服务 1、硬件维保包含的内容及在设备维保工作规范，包含对硬件设备的故障排查、配件更换、定期巡检、定期培训等相关要求技术规范； 2、★要求中标单位提供对 “维保设备清单”中的所有设备进行硬件免费维护、软件免费升级服务， 对“维保设备清单”中的设备提供免费无偿维修服务；当设备发生非人为故障需要更换配件时，需由中标单位提供配件免费更换，以保证系统的正常、稳定运行； 3、提供网络及网络安全设备备机响应，在网络安全设备出现故障时，按故障设备的性能标准，提供相应的备机进行临时替换，将故障设备进行返修，在返修期内，备机能代替故障设备，保障整体网络的稳定运行。 建立系统设备的配置档案和升级、维修、维护档案，定期提交系统维护及管理报告。
	7	运维服务工作要求 1.服务期间，需为中心运行的网络系统提供网络优化、网络配置及备份、网络改造扩展时的技术发展规划和设计、网络及安全设备硬件维护、软件免费升级、特征库更新、无偿修理/更换等工作。 2.要求提供2名工程师驻中心现场提供服务，驻场工程师要求具有网络或安全维护二年以上从业经验，需具有中国信息安全测评中心CISP（CISE）信息安全专业人员认证或计算机技术与软件专业技术资格的网络工程师、信息安全工程师、网络规划设计师认证，驻场服务工作日时间、上下班时间与中心工作人员一致，按照中心标准考核出勤方式，出勤率不低于98%，出差费用自理，承诺提供到我单位的驻场服务工程师要求与投标文件中列明的工程师一致，需提供该工程师所在供应商任职1年以上社保缴费记录及认证证明。 3.提供中心网络及安全运维服务，包括网络及安全设备运维服务、网络及安全架构设计优化及调整、安装调试、故障处理、技术支持、定期巡检、移机、桌面运维等技术服务，并能根据中心要求协助完成日常计算机终端维护等工作。每年至少开展2次网络安全应急演练，负责异地灾备、应急处置、设备特征库、网络安全软件定期升级等工作，提供市中心、9区9县、银行延伸网点等20多个分支机构的网络及安全设备硬件、网络配置、安全配置方面的故障、升级、完善、优化等具体工作。
	8	网络安全设备软件升级服务 1、对现有的网络安全设备攻击规则库升级；应用识别规则库升级；URL库升级；信誉库升级；病毒库升级服务；软件特征库升级服务周期不少于一年； 2、★主要升级服务设备：抗Ddos系统、远程安全评估系统、上网行为管理系统、内网入侵检测系统、网站威胁检测及预警系统软件及特征库升级服务，需对以上网络安全设备规则库定期升级，对网络安全漏洞补丁通告及维护；随着客户单位的网络及网络安全设备增加，服务商需配合用户扩充相应的规则库升级工作。

	9	设备巡检、预警、排错服务要求 1、定期巡检，需由驻场工程师、专业级技术人员执行，对每日服务工作形成工作日志，对中心网络管理平台巡检周期为每周1次，对中心全网设备巡检周期为每月1次；对20多个分支机构主干网络每个月巡检1次；每月底前向中心提出正式文本并加盖公章的书面巡检报告。 2、错误修正，对发现的中心网络系统内存在的风险安全隐患与安全漏洞，提供技术解决方案报用户单位审批，第一时间安排网络安全专业人员处理，24小时内解决风险隐患。 3、网络配置，定期检测中心网络运行情况，处理任何网络变化需求，完成网络配置工作，保障网络运行稳定无故障。及时根据各个信息渠道公布的网络漏洞、安全漏洞、主机漏洞，对网络上的各种设备进行策略配置调整、特征库升级、系统升级等措施，提前预防隐患、保障安全。 4、硬件维修，需对中心《网络及安全相关设备维保清单》中所有设备提供维护及技术支持，提供软件升级服务，要求免费提供损坏设备维修工作，对损坏配件或备件进行免费更换，无法立即修复的设备需提供同等规格备机保障系统的正常、稳定运行。 5、技术培训，要求对中心相关信息系统主管人员、操作人员、科技人员、系统管理人员等进行系统化、实用化的培训，要求培训内容涉及到核心网络设备维护与配置、网络安全设备维护与配置、网络线缆维护与配置、国家网络安全相关法律法规等知识的综合性培训，以确保相关技术人员能够独立进行管理、运行、故障处理及日常测试维护等工作。
	10	网站安全检测服务 1、★网站远程安全监测平台具备：漏洞扫描发现、违规内容监测、网站连通性监测、网站挂马监测、网站解析速度、网站黑链监测、内容变更监测、报表管理和事件通知管理模块； 2、服务要求：提供7x24小时的安全事件监测验证和安全事件通告下发，具备远程漏洞扫描及高危漏洞人工验证服务； 3、要求监测系统为Saas服务，直接通过账号进行管理； 4、★对发现网站存在的SQL注入、XSS跨站脚本、目录遍历、文件包含、备份文件、敏感文件等漏洞，检测内容覆盖WASC分类的多种Web应用漏洞和OWASP TOP10网站漏洞进行管理；定期跟踪漏洞的修复情况从而使网站的漏洞得以快速修复，降低网站被入侵的风险。利用POC对目标网页进行WEB漏扫，发现SQL注入漏洞、命令注入、CRLF注入、LDAP注入、XSS跨站脚本漏洞、路径遍历漏洞、URL跳转漏洞、文件包含漏洞、应用程序漏洞、文件上传漏洞、等安全漏洞问题，对mysql、redis、ftp、ssh等弱口令进行监测； 5、具备针对常见漏洞进行程序自动化验证，并可将自动验证漏洞生成安全告警； 6、具备针对行业漏洞情报进行同步预警，展示最新漏洞情报关联的资产信息； 7、使用模拟浏览器、爬虫UA等多种技术发现网站黑链，具备图片暗链的检测，具备全站对于潜藏在页面深处的第三方黄赌毒广告类链接进行监测并告警，可定位源代码黑链的位置和内容，黑词样本数5700+。具备配置监测频率，具备任务并发量配置，具备用户自定义黑词； 8、系统具备海量词库及人工识别功能，通过先进机器学习手段，提供敏感词发现的技术手段，具备全站安全监测，可定位敏感词位置和内容。涉及敏感词样本5000+，具备配置监测频率，具备任务并发量配置，具备用户自定义敏感词，具备网页附件内容检测； 9、★WEB站点服务可用性监测。具备华北、华东、华南、海外机房20个检测节点，电信、联通和移动都具备监测

		点；具备网站故障原因定位，不限于：响应连接被重置、连接超时、http状态码、连接被拒绝等；可用性监测配置。可支持get/head/post三种方式对HTTP/HTTPS服务进行监控，监控频率支持自定义。支持添加域名时识别IP协议栈情况，并且根据识别结果分别配置IPv4和IPv6的监测节点，具备自定义监测节点，在高级配置中，设置异常节点阈值和超时阈值； 10、系统具备DNS监测，包括华北、华东、华南、海外机房20个监测节点，确保电信、联通和移动都具备监测点；具备记录更改监测，网站A记录解析更变时可进行告警，告警支持短信/邮件方式； 11、系统对站点首页及重点页面内容变更监测：页面发生变更即产生告警，变更类型包括外链、黑词、Body标签为空、HTML之外内容； 12、采用特征分析技术对网站进行木马检测分析，实现快速、准确的发现和定位网页木马，确保用户在第一时间发现感染的木马并及时消除。对木马威胁进行报警、通知、处置管理； 13、★系统具备资产管理功能，包括但不限于自动获取备案信息：网站备案号，网站名称，网站首页地址，审核日期等；注册信息包括但不限于：注册商，域名服务器，责任人姓名，责任人邮箱，责任人电话；安全告警统计：各类型告警数量统计，网站IP地址列表展示，网站DNS列表展示等； 14、系统支持自动添加网站责任人信息、自定义通知转发对象功能；支持查看被通知的基本信息、安全告警列表。具备对处理过程的展示，并可跟踪告警通知处理的全过程，可对相关人的处理行为进行记录； 15、具备日报、周报、月报、季报的生成；具备自定义周期性报告内容，包括自定义报告覆盖的资产、告警类型等； 提供云端7x24小时告警人工运营服务，并提供问题处置建议和咨询；具有重大活动运营支撑服务。
	11	运维服务时间要求 1、服务级别为每周7天X 8小时,其余时间发生故障时，工程师需要在1小时内到达故障现场。 2、市级中心设备修复时间为1小时以内。 3、市区内网点设备修复时间为2小时内。 4、县市网点设备修复时间为5小时内。 5、配置类软故障修复时间为40分钟内。 6、非设备和配置类故障，应在故障定位后10分钟内通知相关方来解决。 7、故障定位时间为20分钟以内，并立即告知中心主管人员，立即提供准确的解决方案。 8、驻场技术人员不能立即解决需要供应商再派技术人员的，需在1小时内到达现场，到达后40分钟内解决。 9、网络设备等软、硬件出现问题，均由供应商负责恢复至故障前状态。对未能按规定时间修复的，供应商应提供合理的经济赔偿和承担聘请第三方技术人员的费用。 10、制定应急预案，协助节假日值班等，配合中心进行各类应急演练。在发生大规模网络故障、病毒爆发、黑客入侵等安全事件时，供应商应配合中心进行安全防护工作，包含攻击溯源，问题处理，样本提取分析等，投标书提供《网络故障应急响应预案》，列出详细故障应急保障计划，并在每次安全事件后提供安全事件分析报告。 11、供应商在合同签订后应组织项目人员，对所维保的设备进行一次现场全面健康性检查，及时发现故障隐患，并提交相关检查报告及整改建议。
		信息安全态势感知管理平台服务

	信息安全态势感知管理平台服务
12	1、功能包含：日志采集，安全事件管理，日志存储，日志查询，统计报表管理，知识库管理等； 2、★服务单位需提供本项服务的软硬件支撑保障，硬件系统需满足配备≥2*CPU（10核），≥128G内存，≥256G SSD系统盘，≥4*4TB SATA硬盘，≥2个千兆电口，≥4个接口扩展槽位，含交流冗余电源模块； 3、★要求平台服务具备接入现有入侵防御系统日志并进行统一分析展现的功能，可以通过日志分析，展现出攻击链条，并可以在平台中查看日志尽心溯源，接入数量不少于20台； 4、要求平台具备接入现有WEB应用防火墙日志并进行统一分析展现的功能，可以通过日志分析，展现出web攻击的态势，对攻击地址进行top排行，接入数量不少于2台； 5、要求平台服务具备接入现有防火墙流量日志并进行统一分析展现的功能，接入数量不少于20台； 6、要求平台服务具备日志威胁分析，平均处理能力（每秒日志解析能力EPS）≥1000EPS； 7、★要求平台服务平台应具备内置≥600+设备日志解析规则查看以及筛选，包括但不限于网络设备（防火墙、交换机、网关）、安全设备（入侵检测设备、WEB攻击防护设备、APT检测设备、防火墙、网络审计、流量探针等）、终端主机日志、数据库等； 8、要求平台服务具备针对采集日志配置数据清洗规则以过滤无业务价值数据； 9、要求平台服务具备界面化配置规范化规则采集第三方日志实现异构日志格式归一化。解析规则支持正则表达式等前置过滤方式及json、kv、csv、正则表达式类型的解析规则，具备界面划取字段配置、多级解析提取嵌套字段、配置规范化规则对解析提取的字段进行字段类型、名称、取值规范化； 10、要求平台服务具备规则分析能力，应支持不少于300种内置分析识别规则并具备内置规则的升级，具备用户自定义规则，用户自定义规则可以支持导入导出； 11、要求平台服务具备对失陷资产进行判定并提供失陷资产的判定依据，包括但不限于失陷资产概要信息、攻击结果、攻击链分布阶段、失陷资产的攻击过程及过程判定依据如攻击特征、流量上下文、关联的告警日志及流量日志以及pcap包下载，并可快速扩展该失陷资产的全部攻击事件以及该失陷资产攻击者发起的攻击、该失陷资产的同类型威胁事件； 12、要求平台服务具备简易模式和专家模式的两种自定义规则，可支持用户在选择日志类型、设置常见日志类型字段过滤条件之后，即可新建或编辑规则，从而生成事件。具备行为分析、多源关联分析、机器学习等多种分析模式，同时可按需自定义生成的事件模版信息如威胁等级、攻击链阶段、事件类型、攻击意图等； 13、要求平台服务具备基于资产维度的风险资产视角分析，支持展示失陷主机、高风险主机、低风险主机，支持总数/今日新增数/已处置数，支持风险资产组Top5/Top10展示，支持今天/近7天/近30天的数据展示切换，支持资产列表展示，支持主机IP、主机名等多种条件进行查询，查询结果支持导出为Excel文件，支持自定义列表中展示的列，支持资产列表中跳转到一键响应/加入白名单/变更状态/详情，支持基于资产组/业务视图/组织架构进行风险资产统计分析。支持攻击者视角/被攻击者视角的攻击情况展示，支持资产名称、资产IP、所属资产组、所属业务视图、所属组织机构、攻击链阶段等资产信息展示，支持基于攻击时间轴的溯源，基于关键时点展示安全事件及详细信息，支持该资产相关的安全事件列表，支持攻击关系图，展示遭受外部攻击、遭受内部横向攻击、发起内部横向攻击、发起外连攻击的可视化关系图，支持处置建议和处置历史； 14、要求平台服务具备外连威胁分析，支持后门外连等分页面统计分析，支持发起外连资产Top5、发起外连资产组Top5，支持外连目标Top5、外连地区Top5，支持威胁类型分布和外连威胁趋势图，支持发起者和外连目标不同视

角的列表展示，支持资产IP、资产名、资产组等多种条件进行查询，查询结果支持导出为Excel文件，支持自定义列表中展示的列；

15、★要求平台服务具备主机、应用等弱口令访问行为的检测，弱密码应加密展示且需要管理员的二次独立认证授权后方可查阅明文弱口令。同时支持批量导出弱口令帐号能力以便于弱口令帐号的分发整改；

16、要求平台服务支持多维度资产管理，进行多维度资产视图分析，系统至少内置五种视图：资产组视图、业务系统视图、组织结构视图、地理位置视图、行业视图；

17、具备HTTPS协议的选择可以选择SSL/TLS协议版本，可选SSLv3、TLS1.0、TLS1.1、TLS1.2；

18、具备HTTPS站点SSL算法自动探测功能。探测时可以设置指定站点及端口，可以显示探测结果；

19、要求平台服务具备纵深防御体系可视化，边界防御、内网防御、安管中心动态展示安全建设运营效果，运营效率数字量化，响应手段可视化，包括但不限于处置效率统计、风险资产、安全事件、安全漏洞、设备联动的处置状态分布、处理历史列表展示等，支持大屏下钻；

20、要求平台服务具备对威胁、失陷主机、漏洞等事件进行统一运维处理，提供统一入口；

21、要求平台服务具备对各类运维事件进行运维处置，包括但不限于提交研判人员进行分析、忽略、误报、处置、优先处理、加入白名单、生成报告、联动封堵设备封堵处置、邮件通报、工单通报等；

22、要求平台服务具备将威胁、漏洞、失陷资产等事件以工单的形式通知用户进行工单处理，支持邮件通知；

23、要求平台服务具备工单数据的权限管理，所有的运维人员都可查看平台所有工单，可通过责任人是自己来查看自己的工单；仅支持对责任人是自己账号的工单进行操作；

24、要求平台服务具备自动报表，支持日报、周报、月报、季报、半年报、年报，支持按时自动生成报表，支持报表订阅，支持日历模式和列表模式可切换，支持基于报表类型、报表模板、报表名称、生成时间段的查询，查找指定的报表；

25、要求平台服务支持自动通知，支持通知策略新建，支持通知策略查询、编辑、删除、启动、禁用，支持邮件、短信、钉钉、企业微信的通知方式，支持风险资产、安全事件、漏洞、工单、报表的通知内容，可根据需要设置具体内容，支持实时通知和周期通知，周期通知支持设置间隔时间和发送通知时间，支持通知历史可查询；　要求提供服务期内安全系统模型升级服务及维保服务。

运维服务备品备件要求

为保障中心网络系统发生故障时能够快速返应和处理，要求供应商在哈尔滨本地有备件库，内部存放与维保范围内相关设备同档次产品作为备件，关键设备或部件在用户现场存放（如路由器、防火墙、交换机、入侵防御、漏洞扫描系统等）。

1、备用设备的整机和配件性能要求等于或高于运行的设备。

2、提供《备机备件方案》要求设计详细、合理。

3、需存放置在中心现场的备品备件设备清单如下。

13

序号	备品名称	配置描述	数量
1	防火墙系统	≥1*RJ45 串口，≥1*RJ45 管理口，≥2*USB 接口，≥6*GE 电口（Bypass）网络层吞吐≥8G，应用吞吐≥4G。	1 台
2	Web 应用防火墙系统	≥2*USB 接口，≥1*RJ45 管理口，≥1*RJ45 串口，≥6*GE 电口（Bypass），≥1 个接口扩展槽位,网络层吞吐≥8G，应用吞吐≥4G，最大并发 TCP 会话数≥150000，每秒新增 TCP 会话数≥10，000cps。	1 台
3	交换机	≥24 个 10/100/1000Base-T 以太网端口,≥4 个 100/1000 SFP，≥4 个万兆 SFP+，≥2 个 QSFP+堆叠口交换容量≥600Gbps/6Tbps，包转发率≥220Mpps。	2 台
4	路由器	交换容量≥640Gbps，≥3*GE（2* GE combo 光口），模块插槽≥10 个，包转发能力≥20Mpps。	2 台
5	漏洞扫描系统	1*RJ45 串口，1*GE 管理口，6 个 10M/100M/1000M 自适应以太网电口扫描口，标准配置提供 1 路授权扫描端口，最大扫描速度≥600IP/H，并发扫描数≥30 个 IP 地址，最大并发任务数≥5，支持多路扫描。	1 套
6	入侵防御系统	≥2*USB 接口，≥1*RJ45 串口，≥1*RJ45 管理口，≥6*GE（Bypass）接口，≥1 个接口扩展槽位，≥1TSATA 硬盘，三层吞吐量≥8Gbps,应用层吞吐量≥4Gbps,最大并发连接≥150万，每秒新建会话数≥4 万。	1 台

14

运维服务维保周期要求

一年服务期满，根据中心工作需要选择是否续签维保合同至下一年度。如合同续签，合同金额与第一年中标价格相同。供应商在维保期内如果没有按照招标文件要求履行维保服务，中心有权随时解除服务合同，重新招标。维保服务合同最多可以续签三年。

	15	**抗DDOS攻击流量防御服务** 1、支持对网络层的SYN Flood、UDP Flood等DDoS攻击进行实时监控并防范； 2、支持对多种业务类型（如TCP/UDP/HTTP/HTTPS）进行DDoS攻击防护； 3、单个服务可同时提供电信、联通和BGP多链路的大流量DDoS攻击防护； 4、支持CC防御能力，单位时间内IP数量不做限制，最高可提供100万QPS的防御能力。支持验证码、js、源限速、ip+cookie限速等方式的CC防御； 5、抗拒绝服务系统可以查看第三方清洗资源被压制IP开始压制时间、结束压制时间，已经压制时间使用情况； 6、支持攻击溯源； 7、支持WAF防护，如web漏洞XSS、SQL注入等web攻击防御； 8、单个服务可同时对≥50个网站业务或非网站业务提供电信、联通和BGP链路提供大流量DDoS攻击防护； 9、★DDoS防御能力可根据实际需要进行动态提升，最高可防御攻击峰值达300G的DDoS攻击流量； 10、对总清洗流量不做限制； 11、可提供DDoS防御，CC防御和WAF防御相关的三份报表； ★服务期内每年≥4次抗DDoS攻击清洗服务，其中20G清洗峰值≥3次，100G清洗峰值≥1次。
		特征库升级的服务要求 1、软件更新服务 服务名称 | 服务方式 | 服务内容 | 服务效果 特征库升级 | 提供特征库补丁和规则下载现场服务 | 提供最新产品特征库补丁和产品规则文件下载，许可证补发支持 | 产品特征库最新规则和补丁在线可用，产品许可证损坏和丢失后可于 1 工作日内提供 • 对中心网络安全设备更新服务包括产品服务期内系统的规则库升级、补丁升级、软件版本升级和产品许可证的补发支持。 • 对中心特征库更新服务期内，要求对网络安全设备软件的最新补丁及规则库升级，提供相应软件补丁和规则库的更新。 • 具有特征库的产品保修服务包括产品保修服务期内产品的维修服务，提供替换备用机的服务。 2、远程支持服务

服务名称	服务方式	服务内容	服务效果
远程支持	提供现场、网站、电话、传真、邮件等途径	产品应用情况及使用问题的解决、相关售后文档的提供，产品应用情况通告。	解决用户单位使用产品的问题，同时通过KB、FAQ等方式提供适合网络情况的产品应用方案。

16

- 要求供应商须努力解决问题，对于不能马上解决的问题，需提供二线或三线工程师寻求其它解决办法并主动答复。
- 要求供应商提供远程支持服务包括远程受理和解决中心问题、资料提供和其他应用咨询等内容。

3、中心待升级特征库设备及软件内容清单（包含且不限于以下清单列表）

序号	设备名称	品牌	数量	单位	服务内容
1	外联区抗 ddos 系统	绿盟	1	套/年	硬件保修、特征库升级、软件升级、远程支持
2	远程安全评估系统	绿盟	1	套/年	
3	上网行为管理系统	网御	1	套/年	
4	内网入侵检测系统	铱讯	1	套/年	
5	网站威胁检测及预警系统	谷兰	1	套/年	
6	内网终端安全管理系统	金山	1	套/年	
7	数据库审计	铱迅	1	套/年	
8	日志审计	圣博润	1	套/年	

网络及网络安全设备维护要求

1.此清单设备为目前中心使用的网络及网络安全产品，随着中心工作需要随时对设备进行调整、更新换代、新增的相关设备均包含在本项目服务范围中，运维服务期间需为中心运行的网络系统提供网络优化、网络技术发展规划设计、网络扩展时的技术规划和设计，要求中标单位提供对 “网络及安全相关设备维保清单”中的所有设备进行硬件免费维护、软件免费升级服务，对“硬件维保设备清单”中的设备提供免费无偿维修服务；当设备发生非人为故障需要更换配件时，需由供应商提供配件免费更换。

2.在质保期范围内设备的技术故障由中心协调相关单位或原厂按合同要求进行技术服务支持工作。

3.要求投标时提供针对中心和分支机构的设备软件、硬件、网络配置、安全配置方面的故障、升级、完善、优化等具体《服务工作方案》，有《售后服务承诺》，服务流程要求清晰完整，需列出详细服务具体内容，服务响应时间，有整套、严密、可行的应急管理措施、应急预案、保障服务、可顺利完成服务要求。

网络及安全相关设备维保清单（包含且不限于以下清单列表）：

序号	类别	品牌	数量	设备型号
1	路由器	H3C	2 台	H3C 6608
2	交换机	H3C	2 台	H3C S10508-V
3	路由器	华为	2 台	AR3260
4	交换机	华为	2 台	S5720-56C-EI
5	交换机	华为	2 台	S5720-36PC-EI
6	交换机	华为	2 台	S5720-36PC-EI
7	交换机	H3C	2 台	H3C S5500
8	交换机	H3C	2 台	H3C S5500
9	交换机	华为	2 台	S5720-28P-SI-AC
10	交换机	华为	1 台	S5720-28P-SI-AC

序号	类别	品牌	数量	设备型号
11	交换机	华为	1 台	S5720-28P-SI-AC
12	交换机	思科	1 台	Cisco3560 v2
13	交换机	TP-LINK	1 台	TL-SG1024T
14	交换机	博达	1 台	BDCOMS3524
15	交换机	H3C	1 台	S1024R
16	交换机	华为	1 台	S1700
17	交换机	思科	1 台	Cisco 3750G
18	交换机	华为	1 台	S5720-28P-LI-AC
19	交换机	H3C	1 台	Cisco 3560
20	交换机	TP-LINK	1 台	TL-SG1016T
21	路由器	H3C	1 台	H3C MSR 26-30
22	路由器	华为	1 台	AR28-31
23	交换机	华为	1 台	S1700-24-AC
24	交换机	思科	2 台	Cisco 3750
25	交换机	思科	1 台	Cisco 2950
26	交换机	H3C	1 台	H3C S1024R
27	交换机	华为	1 台	S5720S-28P-SI-AC
28	交换机	思科	1 台	Cisco 3750
29	交换机	思科	1 台	Cisco 2950
30	交换机	思科	1 台	Cisco 3560
31	交换机	思科	1 台	Cisco 2950
32	交换机	TP-LINK	2 台	TL-SG1024T

17

序号	类别	品牌	数量	设备型号
33	交换机	华为	1 台	华为 S1700
34	交换机	H3C	2 台	H3C S1024R
35	交换机	H3C	1 台	H3C S1024R
36	路由器	H3C	19 台	H3C 36-60
37	路由器	华为	1 台	AR2220E-S
38	路由器	华为	2 台	USG6000 USG6620-AC
39	防火墙	绿盟	2 台	NX3-G4000L
40	防火墙	绿盟	1 台	NF NX3-G4000L
41	防火墙	绿盟	1 台	NF NX3-G4000L
42	防火墙	绿盟	1 台	NF NX3-G4000L
43	入侵防御	绿盟	2 台	NIPS NX3-N1000A-C
44	入侵防御	绿盟	2 台	NIPS NX3-N2000A-C
45	防毒墙	金山	2 台	VGM-3000X
46	安全堡垒机	绿盟	1 台	NX3-H1000C-C
47	日志审计	启明星辰	1 台	TSOC-SA2100
48	防火墙	绿盟	1 台	NFNX3-G4000M-NDE-01
49	防火墙	绿盟	2 台	NF NX3-G2000H
50	WEB 防火墙	绿盟	1 台	NX3-P1000B-C-NDE-01
51	防火墙	绿盟	2 台	NF NX3-G4000H
52	网络隔离系统	启明星辰	1 台	GAP-6000-5610BD
53	数据库审计	铱迅	1 台	YXLink DBA-6000
54	日志审计	圣博润	1 台	V2 LAS-P2000

序号	类别	品牌	数量	设备型号
55	上网行为管理	网域	1 台	AC5000-Q
56	运维审计	铱迅	1 台	Yxlink OAS-2000Z
57	入侵防御系统	铱迅	1 台	YXLink IPS-D6000
58	网络安全态势感知管理平台	绿盟	1 套	V3.0R00F04
59	网络综合运维管理平台	北塔	1 套	北塔 3.0.4
60	运维 VPN 系统	深信服	1 台	VPN-1000 V7.0
61	准入管理系统	盈高	2 台	MSEP500 CAR-1011C-SHYG01
62	防火墙	绿盟	1 台	NF NX3-G2000M
63	防火墙	绿盟	1 台	NF NX3-G2000M
64	防火墙	深信服	2 台	AF-2000-B2150-BU
65	入侵防御	深信服	2 台	NIPS-2000-B2150-BU
66	防火墙	深信服	1 台	AF-2000-B2150-PM
67	入侵防御	深信服	1 台	NIPS-1000-FA40-PM
68	抗 DDOS	绿盟	1 台	ADSNX5-6025E-C-NDE-01
69	漏洞扫描	绿盟	1 台	NX3-G2000M
70	网站内容检测系统	谷兰	1 台	GoodLan-SCM-500
71	应急联动处置系统	谷兰	1 台	GoodLan-Linkage-2280
72	网站威胁检测系统与预警系统	谷兰	1 台	GoodLan-TMC-M3000
73	杀毒软件	金山	2 套	终端安全管理系统 v9

	18	网络及网络安全运维管理服务 1.对中心范围内所有网络及安全设备（安全防护类设备、综合审计类设备、流量分析类设备）的日常巡检服务，每月定期提交网络及安全巡检报告，巡检内容包含但不限于：本月网络安全整体态势情况、现网安全设备整体运行情况、高中低危告警数量及以处置数量。定期进行安全策略检查优化，根据客户业务变更需求实时对安全设备策略进行调整，在满足安全需求的同时保证业务通畅稳定运行。协助甲方制定网络安全应急预案，针对常见网络攻击、扫描、漏洞利用、WEBSHELL上传、shell反弹等攻击行为提出有效的应急处置预案。 2.对中心范围内整体网络框架进行日常运维管理，主要包含组网、配置备份、定期口令修改、网络设备配置调整、配置优化、网络架构规划设计及调整、网络故障排查及处置、链路监测。每月出具整体网络运行健康度巡检报告，报告内容应涵盖：中心范围内整体网络设备硬件运行健康度，网络链路质量、重要汇聚链路路径检查、重要主干链路带宽占用率检查等。 3.服务期内对中心整体范围内软硬件资产进行识别和统计管理，包括网络设备、办公设备、物联网设备硬件属性等信息；资产底层系统识别，操作系统、软件版本、版本号等；资产对外开放的端口所对应的服务信息；资产的支撑系统包括Web服务器、Web中间件、开发语言等；资产的软件应用包括CMS、网站WAF、OA系统、CRM、邮件系统等。 4.对相关系统主管人员、操作人员、科技人员、系统管理人员等进行系统化、一体化的培训，培训涉及到核心网络设备维护与配置、网络安全设备维护与配置综合性培训，以确保相关技术人员能够独立进行管理、运行、故障处理及日常测试维护等工作。 5.服务期内对中心依据国家相关法律法规要求，制定相应的网络安全管理制度，梳理信息化管理条例。 6.派驻2名具备（中国信息安全测评中心CISP（CISE）信息安全专业人员认证或计算机技术与软件专业技术资格的网络工程师、信息安全工程师、网络规划设计师认证）专业的网络或安全维保服务工程师提供驻场服务，上下班时间与用户单位保持一至，协助完成定期巡检服务、现场维护、各厂商协调、现场技术支持等工作。 7.按照中心要求，每年至少2次对中心机房网络线路进行梳理、打标、规范等工作。能根据中心要求协助完成日常计算机终端维护等桌面运维工作。
	19	网络信息安全风险评估服务 1.结合《信息安全技术网络安全等级保护基本要求》.GB/T22239、《GB/T 20984-2022 信息安全风险评估方法》及所属行业相关要求开展信息安全风险评估工作，出具信息资产清单、重要资产面临威胁及脆弱性评估、信息安全风险评估报告、信息安全风险控制清单、风险处置策略及建议等。服务期内每年2次系统安全风险评估服务。
	20	网络安全漏洞管理服务 1.对信息系统、登录入口、数据库、中间件、服务器中的系统漏洞、弱口令、应用漏洞基于漏洞数据库分析，通过系统扫描手段对指定的信息系统的安全脆弱性进行检测，发现可利用漏洞安全问题，针对漏洞提供安全加固或安全修复建议，输出漏洞报告，对修复后的漏洞进行跟踪复测。服务期内每月1次系统漏洞扫描服务。
	21	网络安全系统渗透测试服务 1.以攻击者视角模拟黑客所使用的攻击手段对目标系统进行模拟入侵，充分挖掘和暴露系统的弱点，发现和挖掘系统中存在的安全缺陷，暴露系统中存在的安全隐患和问题，提供系统渗透测试报告和改进措施建议，服务期内提供每年10次对业务系统、网站系统、管理系统网络安全渗透测试服务。

	22	网络安全重大时期及应急响应保障服务 1.中心在遇到突发安全事件，如黑客入侵、病毒蠕虫、信息窃取、拒绝服务等攻击时，安全专家提供现场应急处理技术支持，判断事件类型、攻击来源、收集证据、协助客户降低影响，并在应急处理完毕后提供事件应急响应报告，说明事件原因、处理过程及处置结果，提供此事件的安全分析建议。 2.每年进行2次网络或网络安全应急演练，要求应急演练模拟真实可能发生的风险隐患，协调中心业务相关的软件、网络、容灾备份等各方服务人员，应急演练结束后要根据演练结果和发现的问题，出具应急演练总结报告。 3.特定时期护网与重要时期需确保网络安全监测处置平台设备长期、有效、稳定的工作，最大限度降低系统的运行故障及网络安全系统设备的使用，特定时期需保障3名以上网络安全工程师全天候现场驻守服务，维护工程师需每日对网络安全监测处置平台设备、WAF、全流量分析设备等配套的安全系统进行巡检，排除故障发生隐患，最大限度降低设备的故障发生率。对各类安全设备及流量监测设备产生的攻击日志进行实时分析和预警，在特定时期护网与重要时期按保障安全需求，协调各网络安全厂商资源，通过临时借调相应设备、临时搭建网络安全平台、聘请专业的网络安全工程师配合我单位进行相关安全保障工作。
	23	网络及网络安全设备软硬件维护维修服务 1.要求中标单位提供对“维保设备清单”中的所有设备进行免费维护、软件免费升级服务，对“维保设备清单”中的设备提供免费无偿维修服务；当设备发生非人为故障需要更换配件时，需由中标单位提供配件免费更换，以保证系统的正常、稳定运行；服务期内需对用户单位网络及网络安全有关设备提供硬件维护及技术支持服务，包含：设备硬件运行状态、策略配置情况、授权情况进行检查，记录检查结果；提供硬件技术维修服务，以保证系统的正常、稳定运行。
	24	网络安全设备软件升级服务 1.对网络安全设备攻击规则库升级；应用识别规则库升级；URL库升级；信誉库升级；病毒库升级服务；包含抗ddos系统、远程安全评估系统、上网行为管理系统、内网入侵检测系统、网站威胁检测及预警系统软件及特征库升级服务，需对以上网络安全设备规则库定期升级，对网络安全漏洞补丁通告及维护；
	25	网站安全检测服务 1.要求提供网站安全在线监测SaaS服务，提供7*24小时的网站安全监测服务，及时发现网站存在的漏洞风险以及被篡改、挂马等安全问题。一旦发现网站存在安全风险状况，要求第一时间通知用户，并提供专业的安全解决建议，服务期内每月1次出具网站安全检测综合评估报告。
	26	信息安全态势感知管理平台服务 要求对中心网络流量信息进行深度还原、存储、查询和分析，及时掌握所有业务信息系统相关网络安全威胁风险和隐患，及时检测漏洞、网络攻击、病毒木马等情况，及时发现网络安全事件线索，及时通报预警重大网络安全威胁，调查、防范和打击网络攻击等恶意行为，保障中心网络所有业务信息系统的网络安全稳定运行。
	27	**抗DDOS攻击流量防御服务** 1.提供抗D-DDoS攻击流量清洗防御服务，对大流量DDoS攻击防御、CC攻击防御提供防护能力，提供智能攻击识别引擎，保障中心的业务系统不中断稳定运行。
说明	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投标无效。	

第三章 投标人须知

一.前附表

序号	条款名称	内容及要求
1	计划编号	哈财采备[2023]02133号
2	项目编号	[230101]JLZB[CS]20230001
3	项目名称	2023年网络及安全外包运维服务
4	包组情况	共1包
5	是否专门面向中小企业采购	采购包1：面向中小企业，采购包专门预留
6	采购资金预算金额	691,200.00
7	采购方式	竞争性磋商
8	开标方式	不见面开标
9	评标方式	现场网上评标
10	评标办法	合同包1（2023年网络及安全外包运维服务）：综合评分法
11	现场踏勘	否
12	保证金缴纳截止时间（同递交投标文件截止时间）	详见采购公告
13	电子响应文件递交	电子响应文件在响应截止时间前递交至黑龙江省项目采购电子交易系统
14	响应有效期	从提交投标（响应）文件的截止之日起90日历天
15	投标文件要求	（1）加密的电子响应文件 1 份（需在投标截止时间前上传至“黑龙江省项目采购电子交易系统”）。 （2）若现场无法使用系统进行电子开评标的，投标供应商须开标现场递交非加密电子版响应文件U盘（或光盘）0份。 （3）纸质响应文件正本 0 份，纸质响应文件副本 0 份。
16	中标候选人推荐家数	采购包1： 3家
17	中标供应商确定	采购人授权磋商小组按照评审原则直接确定中标（成交）人。
18	备选方案	不允许
19	联合体投标	包1： 不接受
20	代理服务费收取方式	向中标/成交供应商收取

21	投标保证金	本项目允许投标供应商按照相关法律法规自主选择以支票、汇票、本票或者金融机构、担保机构出具的保函等非现金形式缴纳保证金。 2023年网络及安全外包运维服务：保证金人民币：5,000.00元整。 开户单位：哈尔滨峻岭招标有限公司 开户银行：中国建设银行股份有限公司哈尔滨安发支行 银行账号：23001867136050501611 特别提示： 1、响应供应商应认真核对账户信息，将响应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。响应保证金到账（保函提交）的截止时间与响应截止时间一致，逾期不交者，响应文件将作无效处理。 2、响应供应商在转账或电汇的凭证上应按照以下格式注明，以便核对：“（项目编号：***、包组：***）的响应保证金”。

22	电子招投标	各投标人应当在投标截止时间前上传加密的电子投标文件至“黑龙江省政府采购网”未在投标截止时间前上传电子投标文件的，视为自动放弃投标。投标人因系统或网络问题无法上传电子投标文件时，请在工作时间及时拨打联系电话4009985566按5转1号键。 不见面开标（远程开标）： 1．项目采用不见面开标（网上开标），如在开标过程中出现意外情况导致无法继续进行电子开标时，将会由开标负责人视情况来决定是否允许投标人导入非加密电子投标文件继续开标。本项目采用电子评标（网上评标），只对通过开标环节验证的电子投标文件进行评审。 2．电子投标文件是指通过投标客户端编制，在电子投标文件中，涉及“加盖公章”的内容应使用单位电子公章完成。加密后，成功上传至黑龙江省政府采购网的最终版指定格式电子投标文件。 3．使用投标客户端，经过编制、签章，在生成加密投标文件时，会同时生成非加密投标文件，投标人请自行留存。 4．投标人的法定代表人或其授权代表应当按照本招标公告载明的时间和模式等要求参加开标，在开标时间前30分钟，应当提前登录开标系统进行签到，填写联系人姓名与联系号码。 5．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。（请各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。具体环境要求详见操作手册） 6．开标时出现下列情况的，将视为逾期送达或者未按照招标文件要求密封的投标文件，采购人、采购代理机构应当视为投标无效处理。 （1） 投标人未按招标文件要求参加远程开标会的； （2） 投标人未在规定时间内完成电子投标文件在线解密； （3） 经检查数字证书无效的投标文件； （4） 投标人自身原因造成电子投标文件未能解密的。 7．供应商必须保证在规定时间内完成已投项目的电子响应文件解密，并在规定时间内进行签章确认，未在规定时间内签章的，视同接受开标结果。
23	电子响应文件签字、盖章要求	应按照第六章“响应文件格式与要求”，使用CA进行签字、盖章。 说明：若涉及到授权委托人签字的可将文件签字页先进行签字、扫描后导入加密电子响应文件或签字处使用电脑打字输入。
24	其他	
25	项目兼投兼中规则	兼投兼中：-
26	报价区间	各合同包报价不超过预算总价
27	报价形式	合同包1（2023年网络及安全外包运维服务）:总价

二.说明

1.委托

授权代表如果不是法定代表人/单位负责人，须持有《法定代表人/单位负责人授权书》（统一格式）。

2.费用

无论磋商过程中的作法和结果如何，参加磋商的供应商须自行承担所有与参加磋商有关的全部费用。

三.响应文件

1.响应文件计量单位

响应文件中所使用的计量单位，除有特殊要求外，应采用国家法定计量单位，报价最小单位为人民币元。

2.响应文件的组成

响应文件应按照磋商文件第六章“响应文件格式”进行编写（可以增加附页），作为响应文件的组成部分。

（二）资格证明及其他文件包括：

★1、供应商具有独立承担民事责任的能力

注：①供应商若为企业法人：提供“统一社会信用代码营业执照”；未换证的提供“营业执照、税务登记证、组织机构代码证或三证合一的营业执照”；②若为事业法人：提供“统一社会信用代码法人登记证书”；未换证的提交“事业法人登记证书、组织机构代码证”；③若为其他组织：提供“对应主管部门颁发的准许执业证明文件或营业执照”；④若为个体工商户：提交“统一社会信用代码的营业执照”或“营业执照、税务登记证”；⑤若为自然人：提供“身份证明材料”。以上均提供复印件。

★2、法定代表人/单位负责人签字并加盖公章的法定代表人/单位负责人授权书。

注：供应商为法人单位时提供“法定代表人授权书”，供应商为其他组织时提供“单位负责人授权书”，供应商为自然人时提供“自然人身份证明材料”。

★3、法定代表人/单位负责人身份证正反两面复印件及投标代表身份证明身份证正反两面复印件。**供应商为大学生创办的小微企业还应提供法定代表人的学生证或毕业证或国外学历学位认证书复印件**。

（三）报价书附件的编制及编目

1、报价书附件由供应商自行编制，规格幅面应与正文一致，附于正文之后，与正文页码统一编目编码装订。

2、报价书附件必须包含以下内容：

（1）产品主要技术参数明细表及报价表；

（2）技术服务和售后服务的内容及措施。

3、报价书附件可以包含以下内容：

（1）产品详细说明书。包括：产品主要技术数据和性能的详细描述或提供产品样本；

（2）产品制造、验收标准；

（3）详细的交货清单；

（4）特殊工具及备件清单；

（5）供应商推荐的供选择的配套货物表；

（6）提供报价所有辅助性材料或资料。

3.报价

（一）所有价格均以人民币报价，所报价格为送达用户指定地点安装、调试、培训完毕价格.

（二）磋商报价分两次，即初始报价，供应商递交的响应文件中的报价及磋商结束后的最后报价，且将做为最终的成交价格。

（三）具备初始报价，方有资格做第二次报价。

（四）最低报价不能作为成交的唯一保证。

（五）如仅发起一轮报价实质性响应供应商未按规定要求和时间递交最后报价，将以该供应商提交的首轮报价作为其最后报价，如发起多轮报价实质性响应供应商未按规定要求和时间递交最后报价，将以该供应商提交的最后一轮报价作为其最后报价。

（六）供应商应注意本文件的技术规格中指出的工艺、材料和设备型号仅起说明作用，并没有任何限制性。供应商在报价中可以选用替代标准或型号，但这些替代要实质上满足或超过本文件的要求。

4.响应文件的签署及规定

（一）组成响应文件的各项资料均应遵守本条规定。

（二）响应文件应按规范格式编制，按要求签字、加盖公章。

（三）响应文件装订成册、编制页码且页码连续。

（四）响应文件的正本必须用不退色的墨水填写或打印，注明“正本”字样，副本可以用复印件。正本 0 份，副本 0 份

（五）响应文件不得涂改和增删，如有修改错漏处，必须由磋商代表签字并加盖公章。

（六）响应文件因字迹潦草或表达不清所引起的后果由供应商自行负责。

（七）法定代表人/单位负责人授权书应由法定代表人/单位负责人签字并加盖公章。

5.响应文件存在下列任意一条的，则响应文件无效：

（一）任意一条不满足磋商文件★号条款要求的；

（二）单项产品五条及以上不满足非★号条款要求的；

（三）供应商所提报的技术参数没有如实填写，没有与“竞争性磋商文件技术要求”一一对应，只简单填写“响应或完全响应”的以及未逐条填写应答的；

（四）供应商提报的技术参数中没有明确品牌、型号、规格、配置等；

（五）单项商品报价超单项预算的；

（六）响应产品中如要求安装软件，应提供正版软件，否则响应无效；台式计算机、便携式计算机必须预装正版操作系统，该系统须有唯一的正版序列号与之对应，一个正版序列号只能对应一台计算机，否则响应无效；

（七）政府采购执行节能产品政府强制采购和优先采购政策。如采购人所采购产品为政府强制采购的节能产品，供应商所投产品的品牌及型号必须为清单中有效期内产品并提供证明文件，否则其响应将作为无效响应被拒绝；

（八）信息安全产品，供应商所响应产品应为经国家认证的信息安全产品，并提供由中国信息安全认证中心按国家标准认证颁发的有效认证证书，否则响应无效。

注：本项目评审条款中有特殊情形的，以评审条款中的规定为准。

6.供应商出现下列情况之一的，响应文件无效：

（一）非★条款有重大偏离经磋商小组专家认定无法满足竞争性磋商文件需求的；

（二）未按竞争性磋商文件规定要求签字、盖章的；

（三）响应文件中提供虚假材料的；（提供虚假材料进行报价、应答的，还将移交财政部门依法处理）；

（四）提交的技术参数与所提供的技术证明文件不一致的；

（五）所报项目在实际运行中，其使用成本过高、使用条件苛刻的需经磋商小组确定后不能被采购人接受的；

（六）法定代表人/单位负责人授权书无法定代表人/单位负责人签字或没有加盖公章的；

（七）参加政府采购活动前三年内，在经营活动中有重大违法记录的；

（八）供应商对采购人、代理机构、磋商小组及其工作人员施加影响，有碍公平、公正的；

（九）单位负责人为同一人或者存在直接控股、管理关系的不同供应商参与本项目同一合同项下的投标的，其相关投标将被认定为投标无效；

（十）属于串通投标，或者依法被视为串通投标的；

（十一）磋商小组认为，排在前面的入围候选供应商的报价明显不合理或者低于成本，有可能影响服务质量和不能诚信履约的，应当要求该供应商作出书面说明并提供相关证明材料，否则，磋商小组可以取消该供应商的成交候选资格，按顺序由排在后面的成交候选供应商递补；

（十二）按有关法律、法规、规章规定属于响应无效的；

（十三）磋商小组在磋商过程中，应以供应商提供的响应文件为磋商依据，不得接受响应文件以外的任何形式的文件资

料。

7.供应商禁止行为

（一）供应商在提交响应文件截止时间后撤回响应文件；

（二）成交人在磋商结果产生后放弃成交；

（二）成交人在规定的时限内不签订政府采购合同。

8.竞争性磋商文件质疑提起与受理

供应商在参加黑龙江省政府采购代理机构组织的政府采购活动中，认为采购文件使自己的权益受到损害的，可依法提出质疑；

（一）潜在供应商已依法获取采购文件，且满足参加采购活动基本条件的，可以对该文件提出质疑；对采购文件提出质疑的，应当在首次获取采购文件之日起7个工作日内提出；

（二）提出质疑的供应商应当在规定的时限内，以书面形式一次性地向代理机构递交质疑函和必要的证明材料。

（三）有下列情形之一的，政府采购代理机构不予受理：

1、按照“谁主张、谁举证”的原则，应由质疑供应商提供质疑事项的相关证据、依据和其他有关材料，未能提供的；

2、未按照补正期限进行补正或者补正后仍不符合规定的；

3、未在质疑有效期限内提出的；

4、同一质疑供应商一次性提出质疑后又提出新质疑的；

（四）有下列情形之一的，质疑不成立：

1、质疑事项缺乏事实依据的；

2、质疑供应商捏造事实或者提供虚假材料的；

3、质疑供应商以非法手段取得证明材料的。

（五）对虚假和恶意质疑的处理。

代理机构将对虚假和恶意质疑的供应商进行网上公示，推送省级信用平台；报省政府采购监督管理部门依法处理，记入政府采购不良记录；限制参与政府采购活动；

有下列情形之一的，属于虚假和恶意质疑：

1、主观臆造、无事实依据进行质疑的；

2、捏造事实或提供虚假材料进行质疑的；

3、恶意攻击、歪曲事实进行质疑的；

4、以非法手段取得证明材料的。

第四章 磋商及评审方法

一.磋商评审要求

1、评审方法

综合评分法，响应文件满足磋商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供应商为成交候选人的评审方法。（最低报价不是成交的唯一依据。）

2、评审原则

2.1 评审活动遵循公平、公正、科学和择优的原则，以磋商文件和响应文件为评审的基本依据，并按照磋商文件规定的评审方法和评审标准进行评审。

2.2 具体评审事项由磋商小组负责，并按磋商文件的规定办法进行评审。

3、磋商小组

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

3.2 磋商小组成员有下列情形之一的，应当回避：

（1）参加采购活动前三年内,与供应商存在劳动关系,或者担任过供应商的董事、监事,或者是供应商的控股股东或实际控制人；

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

（3）与供应商有其他可能影响政府采购活动公平、公正进行的关系。

3.3 磋商小组负责具体评审事务，并独立履行下列职责：

（1）审查、评价响应文件是否符合磋商文件的商务、技术等实质性要求；

（2）要求供应商对响应文件有关事项作出澄清或者说明，与供应商进行分别磋商；

（3）对响应文件进行比较和评价；

（4）确定成交候选人名单，以及根据采购人委托直接确定成交供应商；

（5）向采购人、采购代理机构或者有关部门报告评审中发现的违法行为；

（6）法律法规规定的其他职责。

4、澄清

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

4.1 磋商小组不接受供应商主动提出的澄清、说明或更正。

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

5、有下列情形之一的，视为供应商串通投标：

（1）不同供应商的响应文件由同一单位或者个人编制；（不同供应商响应文件上传的项目内部识别码一致）；

（2）不同供应商委托同一单位或者个人办理投标事宜；

（3）不同供应商的响应文件载明的项目管理成员或者联系人员为同一人；

（4）不同供应商的响应文件异常一致或者投标报价呈规律性差异；

（5）不同供应商的响应文件相互混装；

（6）不同供应商的投标保证金为从同一单位或个人的账户转出；

说明：在项目评审时被认定为串通投标的供应商不得参加该合同项下的采购活动

6、有下列情形之一的，属于恶意串通投标：

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

（2）供应商按照采购人或者采购代理机构的授意撤换、修改投标文件或者响应文件；

（3）供应商之间协商报价、技术方案等投标文件或者响应文件的实质性内容；

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

（5）供应商之间事先约定由某一特定供应商成交、成交；

（6）供应商之间商定部分供应商放弃参加政府采购活动或者放弃成交、成交；

（7）供应商与采购人或者采购代理机构之间、供应商相互之间，为谋求特定供应商成交、成交或者排斥其他供应商的其他串通行为。

7、投标无效的情形

详见资格性审查、符合性审查和磋商文件其他投标无效条款。

8、废标（终止）的情形

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

（1）因情况变化，不再符合规定的竞争性磋商采购方式适用情形的；

（2）出现影响采购公正的违法、违规行为的；

（3）在采购过程中符合磋商要求的供应商或者报价未超过采购预算的供应商不足3家的，但经财政部门批准的情形除外；

（4）法律、法规以及磋商文件规定其他情形。

9、定标

磋商小组按照磋商文件确定的评审方法、步骤、标准，对响应文件进行评审。评审结束后，对供应商的评审名次进行排序，确定成交供应商或者推荐成交候选人。

二.政府采购政策落实

1.节能、环保要求

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，具体按照本采购文件相关要求执行。

2.对小型、微型企业、监狱企业或残疾人福利性单位给予价格扣除

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：（监狱企业、残疾人福利性单位视同为小、微企业）。

合同包1（2023年网络及安全外包运维服务）

序号	情形	适用对象	价格扣除比例	计算公式
注：（1）上述评标价仅用于计算价格评分，成交金额以实际投标价为准。（2）组成联合体的大中型企业和其他自然人、法人或者其他组织，与小型、微型企业之间不得存在投资关系。				

价格扣除相关要求：

（1）所称小型和微型企业应当同时符合以下条件：

①符合中小企业划分标准；

②提供本企业制造的货物、承担的工程或者服务，或者提供其他中小企业制造的货物。本项所称货物不包括使用大型企业注册商标的货物；

中小企业划分标准，是指国务院有关部门根据企业从业人员、营业收入、资产总额等指标制定的中小企业划型标准。

小型、微型企业提供中型企业制造的货物的，视同为中型企业。

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

①在货物采购项目中，货物由中小企业制造，即货物由中小企业生产且使用该中小企业商号或者注册商标；

②在工程采购项目中，工程由中小企业承建，即工程施工单位为中小企业；

③在服务采购项目中，服务由中小企业承接，即提供服务的人员为中小企业依照《中华人民共和国劳动合同法》订立劳动合同的从业人员。

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

以联合体形式参加政府采购活动，联合体各方均为中小企业的，联合体视同中小企业。其中，联合体各方均为小微企业的，联合体视同小微企业。

（3）供应商属于小微企业的应填写《中小企业声明函》；监狱企业须供应商提供由监狱管理局、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；残疾人福利性单位应填写《残疾人福利性单位声明函》，否则不认定价格扣除。

说明：供应商应当认真填写声明函，若有虚假将追究其责任。供应商可通过“国家企业信用信息公示系统”（http://www.gsxt.gov.cn/index.html），点击“小微企业名录”（http://xwqy.gsxt.gov.cn/）对供应商和核心设备制造商进行搜索、查询，自行核实是否属于小微企业。

（4）提供供应商的《中小企业声明函》、《残疾人福利性单位声明函》（格式后附，不可修改），未提供、未盖章或填写内容与相关材料不符的不予价格扣除。

（5）报价供应商为大学生创办的小微企业的，对其法定代表人身份及企业性质进行核查，请报价供应商提供（A）、（B）、（C）的登录名和密码：

（A）法定代表人为在校大学生的，学生证复印件与《企业法人营业执照》上的法人代表名称应一致。查询路径：中国高等教育学生信息网(学信网)http：//www.chsi.com.cn/。

（B）法定代表人为大学毕业生的，毕业证复印件与《企业法人营业执照》上的法人代表名称应一致。查询路径：中国高等教育学生信息网(学信网)http：//www.chsi.com.cn/。

（C）法定代表人为留学回国人员的，国外学历学位认证书复印件与《企业法人营业执照》上的法人代表名称应一致。查询路径：教育部留学服务中心-国（境）外学历学位认证系统http：//renzheng.cscse.edu.cn/Login.aspx。

（D）企业法定代表人必须为在校大学生、毕业五年内大学生（含留学回国），同时大学生必须为控股股东。控股情况查询：全国企业信用信息公示系统http：//gsxt.saic.gov.cn/。

（E）各项查询结果需打印并由磋商小组签字。

三.评审程序

1.资格性审查和符合性审查

资格性审查。磋商小组依据法律法规和竞争性磋商文件规定，对响应文件中的资格证明等进行审查，以确定供应商是否具备入围资格。如供应商不具备入围资格，应书面告知未入围的供应原因并要求其签字确认收到告知书。（详见后附表一资格性审查表）

符合性审查。依据磋商文件的规定，从响应文件的有效性、完整性和对磋商文件的响应程度进行审查，以确定是否对磋商文件的实质性要求作出响应。（详见后附表二符合性审查表）

资格性审查和符合性审查中凡有其中任意一项未通过的，评审结果为未通过，未通过资格性审查、符合性审查的投标单位按无效投标处理。

2.磋商

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

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

对磋商文件作出的实质性变动是磋商文件的有效组成部分，磋商小组应当及时、同时通知所有参加磋商的供应商

供应商应当按照磋商文件的变动情况和磋商小组的要求进行最终报价或重新提交响应文件，并由其法定代表人或授权代表

签字或者加盖公章。由授权代表签字的，应当附法定代表人授权书。供应商为自然人的，应当由本人签字并附身份证明。

3.最后报价

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

已提交响应文件的供应商，在提交最后报价之前，可以根据磋商情况退出磋商。

4.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。

5.综合评分（详见后附表三详细表）

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

6.汇总、排序

评审结果按评审后总得分由高到低顺序排列。评审得分相同的，按照最后报价由低到高的顺序推荐。评审得分且最后报价相同的，按照技术指标优劣顺序推荐，以上均相同的由采购人确定。

四.确定成交供应商

（一）磋商小组依据磋商方法和原则确定成交供应商，并将成交结果通知所有参加磋商的未成交供应商。

（二）如供应商对成交结果有异议，请当场以书面形式提出，由磋商小组以书面形式进行回复，其他任何形式的回复无效。

（三）成交公告和成交通知书

代理机构负责发布成交公告，同时向成交供应商发出《成交通知书》，《成交通知书》是《合同》的一个组成部分。

（四）排名第一的成交候选人不与采购人签订合同的，采购人可直接上报哈尔滨市财政部门。

五.合同的签订

（一）成交供应商应按《成交通知书》规定的时间、地点与采购人签订政府采购合同。

（二）竞争性磋商文件、成交供应商的响应文件、磋商过程中的有关澄清和承诺文件均是政府采购合同的必要组成部分，与合同具有同等法律效力。

（三）采购人不得向成交供应商提出任何不合理的要求，作为签订合同的条件，不得与成交供应商订立违背合同实质性内容的协议。

（四）合同由采购人通过黑龙江省政府采购网上传哈尔滨市财政部门备案。

（五）采购人负责合同的审核、签订、履约及验收工作，哈尔滨市财政部门负责对合同签订、合同履约及验收进行监督检查。

六.履约金

合同包1（2023年网络及安全外包运维服务）： 本合同包不收取

七.付款及验收

合同包1（2023年网络及安全外包运维服务）

付款方式	1期: 50%，服务满6个月且验收合格后支付合同款的50% 2期: 50%，合同期满验收合格后支付合同款的50%
验收要求	1期: 按照招标技术参数标准进行验收，符合验收标准给予验收

表一资格性审查表：

合同包1（2023年网络及安全外包运维服务）

具有独立承担民事责任的能力	在中华人民共和国境内注册的法人或其他组织或自然人，投标时提交有效的营业执照（或事业法人登记证或身份证等相关证明）副本复印件或提供加盖供应商公章的《黑龙江省政府采购供应商资格承诺函》。
有依法缴纳税收和社会保障资金的良好记录	提供投标截止日前6个月内任意1个月依法缴纳税收和社会保障资金的相关材料或提供加盖供应商公章的《黑龙江省政府采购供应商资格承诺函》。如依法免税或不需要缴纳社会保障资金的，提供相应证明材料。
具有良好的商业信誉和健全的财务会计制度	供应商必须具有良好的商业信誉和健全的财务会计制度（提供2022年度财务状况报告或基本开户行出具的资信证明或提供加盖供应商公章的《黑龙江省政府采购供应商资格承诺函》）。
履行合同所必须的设备和专业技术能力	提供加盖供应商公章的《黑龙江省政府采购供应商资格承诺函》。
参加采购活动前3年内，在经营活动中没有重大违法记录	提供加盖供应商公章的《黑龙江省政府采购供应商资格承诺函》。 重大违法记录，是指供应商因违法经营受到刑事处罚或者责令停产停业、 吊销许可证或者执照、较大数额罚款等行政处罚。（较大数额罚款按照发出行政处罚决定书部 门所在省级政府，或实行垂直领导的国务院有关行政主管部门制定的较大数额罚款标准，或罚 款决定之前需要举行听证会的金额标准来认定）
信用记录	供应商未被列入“信用中国”网站(www.creditchina.gov.cn)“记录失信被执行人或重大税收违法案件当事人名单或政府采购严重违法失信行为”记录名单；不处于中国政府采购网(www.ccgp.gov.cn)“政府采购严重违法失信行为信息记录”中的禁止参加政府采购活动期间。（以采购代理机构于投标（响应）截止时间当天在“信用中国”网站（www.creditchina.gov.cn）及中国政府采购网（http://www.ccgp.gov.cn/）查询结果为准，如相关失信记录已失效，供应商需提供相关证明资料），或提供加盖供应商公章的《黑龙江省政府采购供应商资格承诺函》
供应商必须符合法律、行政法规规定的其他条件	单位负责人为同一人或者存在直接控股、管理关系的不同供应商，不得同时参加本采购项目（包组）投标。 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，不得再参与本项目投标， 提供加盖供应商公章的《黑龙江省政府采购供应商资格承诺函》
促进中小企业发展	采购包整体专门面向中小企业

表二符合性审查表：

合同包1（2023年网络及安全外包运维服务）

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。
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；投标承诺书。
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“法定代表人（或授权代表）签字或盖章、单位盖章”。
联合体投标	符合关于联合体投标的相关规定。

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。
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。

表三详细评审表：

2023年网络及安全外包运维服务

评审因素	评审标准	
分值构成	技术部分66.0分 商务部分14.0分 报价得分20.0分	
技术部分	技术响应 (16.0分)	所有服务需求、技术指标全部满足招标文件要求得16分。有一项负偏离扣4分，超过4项负偏离，响应无效。带星号为实质性条款，若有任何一条负偏离或不满足则导致投标无效
	运维服务方案 (10.0分)	针对本项目制定相关的运维服务方案，方案应包含服务工作方案、设备巡检服务方案、运维售后服务方案、设备维修维护方案、运维质量保证方案、本地备机备件解决方案、重要时期服务保障方案、运维安全与保密解决方案、运维人员日常管理制度，运维技术培训方案等内容，每提供一项得1分，此项最多得10分，每有一处具有缺陷（缺陷是指：存在不适用项目实际情况的情形、凭空编造、内容前后不一致、前后逻辑错误、涉及的规范及标准错误、地点区域错误、内容缺失、不符合采购需求）的扣1分，扣完为止，没有或与本项目不相关的不得分。
	运行维护方案 (10.0分)	针对本项目制定相关的运行维护方案，方案应包含网络安全服务分析、网络安全技术措施、网络安全防护措施、网络系统测试方案、网络系统维护方案等内容，每提供一项得2分，此项最多得10分，每有一处具有缺陷（缺陷是指：存在不适用项目实际情况的情形、凭空编造、内容前后不一致、前后逻辑错误、涉及的规范及标准错误、地点区域错误、内容缺失、不符合采购需求）的扣1分，扣完为止，没有或与本项目不相关的不得分。
	关键技术服务解决方案 (5.0分)	针对本项目制定相关的关键技术服务解决方案，方案应包含系统升级、架构调整、数据迁移、系统崩溃、电源掉电等内容，每提供一项得1分，此项最多得5分，每有一处具有缺陷（缺陷是指：存在不适用项目实际情况的情形、凭空编造、内容前后不一致、前后逻辑错误、涉及的规范及标准错误、地点区域错误、内容缺失、不符合采购需求）的扣1分，扣完为止，没有或与本项目不相关的不得分。
	应急预案方案 (5.0分)	针对本项目制定相关的应急预案方案，方案应包含应急响应突发事件分类、处理应急响应突发工作职责、预防与预警机制、应急响应处置预案、后期处置及应急保障等内容，每提供一项得1分，此项最多得5分，每有一处具有缺陷（缺陷是指：存在不适用项目实际情况的情形、凭空编造、内容前后不一致、前后逻辑错误、涉及的规范及标准错误、地点区域错误、内容缺失、不符合采购需求）的扣1分，扣完为止，没有或与本项目不相关的不得分。

	应急演练方案 (5.0分)	针对本项目制定相关的应急演练方案，方案应包含应急演练组织机构、应急演练方案、应急演练准备工作、应急演练处置工作、应急演练总结报告等内容，每提供一项得1分，此项最多得5分，每有一处具有缺陷（缺陷是指：存在不适用项目实际情况的情形、凭空编造、内容前后不一致、前后逻辑错误、涉及的规范及标准错误、地点区域错误、内容缺失、不符合采购需求）的扣1分，扣完为止，没有或与本项目不相关的不得分。
	应急响应能力 (5.0分)	在应急响应服务过程中提供应急响应处置系统（工具）的得5分；不提供的不得分。投标时需提供应急响应处置系统（工具）的软件著作权证书并加盖投标人公章，相关系统（工具）采购发票或合同。
	安全评估检查能力 (5.0分)	在安全评估或安全检查服务中提供安全评估检查系统（工具）的得5分；不提供的不得分。投标时需提供安全评估检查系统（工具）的软件著作权证书并加盖投标人公章，相关系统（工具）采购发票或合同。
	项目人员配备 (5.0分)	供应商针对本项目所配备的服务人员需具备中国信息安全测评中心的注册信息安全工程师认证证书（CISP-CISE）、注册信息安全管理人员认证证书（CISP-CISO），或者计算机技术与软件专业技术资格的网络工程师、信息安全工程师、网络规划设计师认证证书（至少为以上任一种）。每有一人满足的得2.5分，本项最高得5分；不满足的不得分。投标时需提供服务人员身份证明，相关资质证书原件或加盖投标单位公章的相关资质证书扫描件或证书网站有效期内的截图证明。
商务部分	服务承诺 (3.0分) ）	1、售后服务承诺（承诺满足招标人要求的服务具体内容、服务相应时间）； 2、备品备件承诺（承诺按照相关清单的类型和数量要求在招标人处存放关键设备，在当地有备件库）； 3、人员配备承诺（承诺驻场人员经验、资质、任职时间满足招标人要求，实际驻场人员与投标文件所列人员一致，并提供社保缴费记录等）。以上全部内容无少项、漏项，得3分，每缺一项扣1分。
	服务能力 (8.0分)	1、供应商需具备国家互联网应急中心（CNCERT）颁发的网络安全应急服务支撑单位证书。评标时提供资质证明文件原件或加盖投标单位公章的扫描件得4分，不提供不得分。 2、供应商需具备中国信息安全测评中心颁发的国家信息安全测评信息安全服务资质证书（风险评估二级及以上）。评标时提供资质证明文件原件或加盖投标单位公章的扫描件得4分，不提供不得分。
	业绩方面 (3.0分)	提供供应商近三年内，项目金额在50万及以上的同类服务项目。投标时提供业绩证明材料，至少包括合同首页、含有项目名称的页面、合同主要内容及签章页，认定时间以合同签订时间为准。每提供1个得1分，本项最高得3分。
投标报价	投标报价得分 (20.0分)	投标报价得分＝（评标基准价/投标报价）×价格分值【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。

第五章 主要合同条款及合同格式

合同编号：

《黑龙江省政府采购合同》（试行）文本

一般货物类

采购单位(甲 方)　　采购计划号
供 应 商(乙 方)　　招 标 编 号
签 定 地 点　　签 订 时 间

根据《中华人民共和国政府采购法》、《中华人民共和国民法典》等法律、法规规定，按照招投标文件规定条款和中标投标人承诺，甲乙双方签订本合同。

第一条 合同标的

1、供货一览表

序号	产品名称	商标品牌	规格型号	生产厂家	数量及单位	单价（元）	金额（元）
1							
2							
3							
4							
5							
人民币合计金额（大写）				（小写）			

2、合同合计金额包括货物价款，备件、专用工具、安装、调试、检验、技术培训及技术资料和包装、运输等全部费用。如招投标文件对其另有规定的，从其规定。

第二条 质量保证

1、乙方所提供的货物型号、技术规格、技术参数等质量必须与招投标文件和承诺相一致。乙方提供的节能和环保产品必须是列入政府采购清单的产品。

2、乙方所提供的货物必须是全新、未使用的原装产品，且在正常安装、使用和保养条件下，其使用寿命期内各项指标均达到质量要求。

第三条 权利保证

乙方应保证所提供货物在使用时不会侵犯任何第三方的专利权、商标权、工业设计权或其他权利。

第四条 包装和运输

1、乙方提供的货物均应按招投标文件要求的包装材料、包装标准、包装方式进行包装，每一包装单元内应附详细的装箱单和质量合格证。

2、货物的运输方式：　　。

3、乙方负责货物运输，货物运输合理损耗及计算方法：　　。

第五条 交付和验收

1、交货时间：　　地点：　　。

2、乙方提供不符合招投标文件和本合同规定的货物，甲方有权拒绝接受。

3、乙方应将所提供货物的装箱清单、用户手册、原厂保修卡、随机资料、工具和备品、备件等交付给甲方，如有缺失应及时补齐，否则视为逾期交货。

4、甲方应当在到货（安装、调试完）后7个工作日内进行验收，逾期不验收的，乙方可视同验收合格。验收合格后由甲乙双方签署货物验收单并加盖采购单位公章，甲乙双方各执一份。

5、政府代理机构组织的验收项目，其验收时间以该项目验收方案确定的验收时间为准，验收结果以该项目验收报告结论为准。在验收过程中发现乙方有违约问题，可暂缓资金结算，待违约问题解决后，方可办理资金结算事宜。

6、甲方对验收有异议的，在验收后5个工作日内以书面形式向乙方提出，乙方应自收到甲方书面异议后　　日内及时予以解决。

第六条 安装和培训

1、甲方应提供必要安装条件（如场地、电源、水源等）。

2、乙方负责甲方有关人员的培训。培训时间、地点：　　。

第七条 售后服务

1、乙方应按照国家有关法律法规和“三包”规定以及招投标文件和本合同所附的《服务承诺》，为甲方提供售后服务。

2、货物保修起止时间：　　。

3、乙方提供的服务承诺和售后服务及保修期责任等其它具体约定事项。（见合同附件）

第八条 付款方式和期限

1、资金性质：　　。

2、付款方式：财政性资金按财政国库集中支付规定程序办理；自筹资金：　　。付款期限为甲方对货物验收合格后7个工作日内付款。

第九条 履约、质量保证金

1、乙方在签订本合同之日，按本合同合计金额 5%比例提交履约保证金。节能、环保产品提交履约保证金按本合同合计金额 2.5%比例提交，待货物验收合格无异议后5个工作日内无息返还。

2、乙方应在货物验收合格无异议后5个工作日内按本合同合计金额　　比例向甲方提交质量保障金，质量保证期过后5个工作日内无息返还。

第十条 合同的变更、终止与转让

1、除《中华人民共和国政府采购法》第50条规定的情形外，本合同一经签订，甲乙双方不得擅自变更、中止或终止。

2、乙方不得擅自转让（无进口资格的投标人委托进口货物除外）其应履行的合同义务。

第十一条 违约责任

1、乙方所提供的货物规格、技术标准、材料等质量不合格的，应及时更换，更换不及时的按逾期交货处罚；因质量问题甲方不同意接收的或特殊情况甲方同意接收的，乙方应向甲方支付违约货款额 5%违约金并赔偿甲方经济损失。

2、乙方提供的货物如侵犯了第三方合法权益而引发的任何纠纷或诉讼，均由乙方负责交涉并承担全部责任。

3、因包装、运输引起的货物损坏，按质量不合格处罚。

4、甲方无故延期接收货物、乙方逾期交货的，每天向对方偿付违约货款额3‰违约金，但违约金累计不得超过违约货款额5%，超过　　天对方有权解除合同，违约方承担因此给对方造成经济损失；甲方延期付货款的，每天向乙方偿付延期货款额3‰滞纳金，但滞纳金累计不得超过延期货款额5%。

5、乙方未按本合同和投标文件中规定的服务承诺提供售后服务的，乙方应按本合同合计金额 5%向甲方支付违约金。

6、乙方提供的货物在质量保证期内，因设计、工艺或材料的缺陷和其它质量原因造成的问题，由乙方负责，费用从质量保证金中扣除，不足另补。

7、其它违约行为按违约货款额5%收取违约金并赔偿经济损失。

第十二条 合同争议解决

1、因货物质量问题发生争议的，应邀请国家认可的质量检测机构对货物质量进行鉴定。货物符合标准的，鉴定费由甲方承担；货物不符合标准的，鉴定费由乙方承担。

2、因履行本合同引起的或与本合同有关的争议，甲乙双方应首先通过友好协商解决，如果协商不能解决，可向仲裁委员会申请仲裁或向人民法院提起诉讼。

3、诉讼期间，本合同继续履行。

第十三条 签订本合同依据

1、政府采购招标文件；

2、乙方提供的投标文件；

3、投标承诺书；

4、中标或成交通知书。

第十四条 本合同一式四份，政府采购办、政府代理机构各一份，甲乙双方各一份（可根据需要另增加）。

本合同甲乙双方签字公章后生效，自签订之日起七个工作日内，采购人应当将合同副本报同级政府采购监督管理部门备案。

甲方（章） 年　　月　　日	乙方（章） 年　　月　　日
单位地址：	单位地址：
法定代表人：	法定代表人：
委托代理人：	委托代理人：
电话：	电话：
电子邮箱：	电子邮箱：
开户银行：	开户银行：
账号：	账号：
邮政编码：	邮政编码：
采购办审核（章） 经办人： 年　　月　　日	

合同附件

一般货物类

1、投标人承诺具体事项：
2、售后服务具体事项：
3、保修期责任：
4、其他具体事项：

甲方（章） 年　月　日	乙方（章） 年　月　日

注：售后服务事项填不下时可另加附页

黑龙江省政府采购合同使用说明

（一般货物类）

《政府采购合同》是对招投标文件中货物和服务要约事项的细化和补充，所签订的合同不得对招标文件和中标投标人投标文件作实质性修改；招标过程中有关项目标的性状的重要澄清和承诺事项必须在合同相应条款中予以明确表达。采购人和中标投标人不得提出任何不合理的要求作为签订合同的条件；不得私下订立背离招标文件实质性内容的协议。

一、本合同适用范围

家用电器、电子产品、教学仪器设备、医疗仪器设备、广播电视仪器设备、体育器材、音响乐器、药品、服装、印刷设备和印刷品等政府采购项目（协议供货除外）适用于本合同。

二、填写说明

（一）合同标题：地市县使用时可在“黑龙江省”后再加所在地名称或将“黑龙江省”删除加所在地名称。

（二）本合同划线部分所需填写内容，除以下条款特殊要求外，按招投标文件要求填写，如招投标文件没有明确，按甲乙双方商定意见填写。

（三）第一条合同标的：按表中各项目要求填写，内容填写不下时可另加附页。

（四）第四条包装和运输：货物运输方式包括；汽车、火车、轮船等。

（五）货物交付和验收：时间按合同签订（或生效）后多少日（或工作日）或直接填X年X月X日前交货。

（六）第八条付款方式和期限：资金性质按财政性资金（预算内资金、预算外资金）和自筹资金填写。

三、有关要求

（一）各单位现使用的专业合同可作为本合同附件，但专业合同各条款必须符合招投标文件和本合同各条款要求，如发生矛盾以本合同为准。

（二）协议供货合同应使用原文本。

（三）甲乙双方对本合同各条款均不能改动，只能在划线位置填写，如有改动视同无效合同。

（四）本合同统一用A4纸打印。

（五）本合同为试行文本，采购人和中标投标人在使用过程中如发现不当之处，请及时提出建议，以便修正。

本合同各条款由黑龙江省政府采购办公室负责解释。

电话：0451—53679987　　0451—82833586

第六章 响应文件格式与要求

《响应文件格式》是参加竞争性磋商供应商的部分响应文件格式，请参照这些格式编制响应文件。

一、响应文件封面格式

政 府 采 购
响 应 文 件

项目名称：2023年网络及安全外包运维服务

项目编号：[230101]JLZB[CS]20230001

供应商全称：（公章）

授权代表：

电话：

磋商日期：

二、首轮报价表

注：采用电子招投标的项目无需编制该表格，投标供应商应在投标客户端【报价部分】进行填写，投标客户端软件将自动根据供应商填写信息在线生成开标一览表（首轮报价表、报价一览表）或分项报价表，若在投标文件中出现非系统生成的开标一览表（首轮报价表、报价一览表）或分项报价表，且与投标客户端生成的开标一览表（首轮报价表、 报价一览表）或分项报价表信息内容不一致，以投标客户端生成的内容为准。

三、分项报价表

注：采用电子招投标的项目无需编制该表格，投标供应商应在投标客户端【报价部分】进行填写，投标客户端软件将自动根据供应商填写信息在线生成开标一览表（首轮报价表、报价一览表）或分项报价表，若在投标文件中出现非系统生成的开标一览表（首轮报价表、报价一览表）或分项报价表，且与投标客户端生成的开标一览表（首轮报价表、 报价一览表）或分项报价表信息内容不一致，以投标客户端生成的内容为准。

四、技术偏离及详细配置明细表

项目名称：2023年网络及安全外包运维服务

项目编号：[230101]JLZB[CS]20230001

（第　包）

序号	服务名称	磋商文件的服务需求	响应文件响应情况	偏离情况

供应商全称：

日期：　　年　　月　　日

五、技术服务和售后服务的内容及措施

供应商全称：

六、法定代表人/单位负责人授权书

：

（报价单位全称）法定代表人/单位负责人　　授权　　（授权代表姓名）为响应供应商代表，参加贵处组织的　　项目（项目编号）竞争性磋商，全权处理本活动中的一切事宜。

法定代表人/单位负责人签字：

供应商全称（公章）：

日　期：

附：

授权代表姓名：　　授权代表：（签字）

职　　务：

详细通讯地址：

邮 政 编 码：

传　　真：

电　　话：

七、法定代表人/单位负责人和授权代表身份证明

（法定代表人/单位负责人身份证正反面复印件）

（授权代表身份证正反面复印件）

供应商全称：

八、小微企业声明函

注：响应供应商及响应产品是小微企业的提供，否则无需提供

中小企业声明函（货物）

本公司（联合体）郑重声明，根据《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）的规定，本公司（联合体）参加（单位名称）的（项目名称）采购活动，提供的货物全部由符合政策要求的中小企业制造。相关企业（含联合体中的中小企业、签订分包意向协议的中小企业）的具体情况如下：

1.（标的名称），属于（采购文件中明确的所属行业）行业；制造商为（企业名称），从业人员　　人，营业收入为　　万元，资产总额为　　万元，属于（中型企业、小型企业、微型企业）；

2.（标的名称），属于（采购文件中明确的所属行业）行业；制造商为（企业名称），从业人员　　人，营业收入为　　万元，资产总额为　　万元，属于（中型企业、小型企业、微型企业）；

……

以上企业，不属于大企业的分支机构，不存在控股股东为大企业的情形，也不存在与大企业的负责人为同一人的情形。

本企业对上述声明内容的真实性负责。如有虚假，将依法承担相应责任。

企业名称（盖章）：

日期：　　年　　月　　日

从业人员、营业收入、资产总额填报上一年度数据，无上一年度数据的新成立企业可不填报

中小企业声明函（工程、服务）

本公司（联合体）郑重声明，根据《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）的规定，本公司（联合体）参加（单位名称）的（项目名称）采购活动，工程的施工单位全部为符合政策要求的中小企业（或者：服务全部由符合政策要求的中小企业承接）。相关企业（含联合体中的中小企业、签订分包意向协议的中小企业）的具体情况如下：

1.（标的名称），属于（采购文件中明确的所属行业）；承建（承接）企业为（企业名称），从业人员　　人，营业收入为　　万元，资产总额为　　万元，属于（中型企业、小型企业、微型企业）；

2.（标的名称），属于（采购文件中明确的所属行业）；承建（承接）企业为（企业名称），从业人员　　人，营业收入为　　万元，资产总额为　　万元，属于（中型企业、小型企业、微型企业）；

……

以上企业，不属于大企业的分支机构，不存在控股股东为大企业的情形，也不存在与大企业的负责人为同一人的情形。

本企业对上述声明内容的真实性负责。如有虚假，将依法承担相应责任。

企业名称（盖章）：

日期：　　年　　月　　日

从业人员、营业收入、资产总额填报上一年度数据，无上一年度数据的新成立企业可不填报

九、残疾人福利性单位声明函

本单位郑重声明，根据《财政部 民政部 中国残疾人联合会关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141号）的规定，本单位为符合条件的残疾人福利性单位，且本单位参加　　单位的　　目采购活动提供本单位制造的货物（由本单位承担工程/提供服务），或者提供其他残疾人福利性单位制造的货物（不包括使用非残疾人福利性单位注册商标的货物）。

本单位对上述声明的真实性负责。如有虚假，将依法承担相应责任。

残疾人福利性单位（盖章）：

日期：　　年　　月　　日

十、投标人关联单位的说明

说明：投标人应当如实披露与本单位存在下列关联关系的单位名称：

（1）与投标人单位负责人为同一人的其他单位；

（2）与投标人存在直接控股、管理关系的其他单位。