

# 北京市广播电视监测中心

监测系统运行维护  
第一包：网络安全服务

## 合同书

合同编号：JCZX-YW-2024-1

招标编号：HCZB-2024-ZB0209

项目名称：监测系统运行维护

第一包：网络安全服务

甲 方：北京市广播电视监测中心

乙 方：北京华夏航通信息技术有限公司

签署日期：2024年6月7日

# 一、合同书

北京市广播电视监测中心(甲方) 监测系统运行维护(项目名称)政府采购项目中所需第一包:网络安全服务(服务名称)经华采招标集团有限公司(招标采购单位)以 HCZB-2024-ZB0209 号招标文件在国内公开招标。经评标委员会评定, 北京华夏航通信息技术有限公司(乙方)为中标人。甲、乙双方同意按照下面的条款和条件, 签署本合同。

## 1. 合同文件组成

下列文件均为本合同不可分割的组成部分, 认为是一个整体, 彼此相互解释、相互补充, 具有同等法律效力:

- 1.1 本合同书
- 1.2 中标通知书
- 1.3 投标文件(含澄清文件)
- 1.4 招标文件(含招标文件补充通知)

上述文件互为补充和解释, 如有不清或相互矛盾之处, 以所列顺序在前的为准, 但甲、乙双方有特别约定的除外。

## 2. 合同总价

本合同总价为¥601,000.00元, 大写人民币:陆拾万零壹仟元整。

价格一览表

单位: 人民币 元

序号	名称	总价
1	网络安全服务	601000.00

## 3. 服务内容

本合同服务内容: 招标文件第四部分服务要求。

## 4. 服务范围

4.1 本合同服务界定于以下范围:

项目范围包括: 招标文件第四部分服务要求。

## 5. 服务期限

服务期限: 一年(2024年7月1日至2025年6月30日)。



## **6. 付款方式**

6.1 合同签订生效后 10 个工作日内，甲方向乙方支付合同首款人民币 30.25 万元；合同期满若乙方完全履行了合同所规定的条款且无任何争议或遗留问题，经甲方验收合格后，在 10 个工作日内甲方向乙方支付合同尾款人民币 29.85 万元。

6.2 乙方户名、开户银行名称和账号为：

户 名：北京华夏航通信息技术有限公司

开户行：建行北京定慧北桥支行

帐 号：11001182900052500479

6.3 甲方每次付款前，乙方应提供符合国家相关税务规定的同等金额的增值税普通发票，否则甲方有权延迟付款且不承担违约责任。

甲方开票信息为：

户 名：北京市广播电视监测中心

税 号：1211000079755080XU

## **7. 商业秘密**

7.1 任何一方对于因签署或履行本合同而了解或接触到的对方的商业秘密及其他机密资料和信息（以下简称“保密信息”）均应保守秘密；非经对方书面同意，任何一方不得向第三方泄露、给予或转让该等保密信息；

7.2 除本合同规定之工作所需外，未经对方事先同意，不得擅自使用、复制对方的商标、标志、商业信息、技术及其他资料。

## **8. 权利义务条款**

### **甲方权利义务**

8.1 接受乙方提交的符合本合同约定条件的工作成果或者相关文件；

8.2 甲方有权向乙方提出明确的工作要求、工作目标和需求等，并审定乙方提交的委托项目工作方案和配套工作计划；

8.3 甲方有权对项目承办的筹备过程和实施过程进行监督和指导，检查监督乙方完成委托项目工作的进度，对于乙方不履行合同、不适当履行合同等行为，甲方有权要求乙方立即更正，并采取其他补救措施；



8.4 组织专家或者通过评估,对乙方提交的委托项目工作成果的质量进行评审或验收;

8.5 为保证乙方工作进行,甲方须及时向乙方提供完成委托事项所必须的技术资料和工作条件。

8.6 负责按照合同约定收集、整理与委托事项有关的项目背景资料及相关技术资料和数据并提供给乙方;

8.7 负责委托项目所涉及的、与甲方有关的外部联系和协调工作。

### **乙方权利义务**

8.8 有权接受甲方按照合同约定支付的委托报酬;

8.9 乙方发现甲方提供的技术资料、数据有明显错误和缺陷的,有权于收到上述资料后3日内书面通知甲方进行补充、修改。如逾期未提出异议的,则视为甲方提交的资料、数据符合合同约定的条件;

8.10 乙方在其经营许可的范围内,依本合同的约定向甲方提供专业的服务,并在规定的委托项目工作时间期限内完成委托项目的工作;

8.11 乙方应当遵守国家法律、法规和行业行为准则为甲方完成委托项目的工作;乙方提交的工作成果必须达到合同约定的要求,并对其完成的委托项目工作成果全面负责;

8.12 乙方应当认真按照合同要求完成委托项目工作,随时接受甲方的检查监督,并为检查监督提供便利条件;

8.13 甲方对乙方提交的委托项目工作成果提出质疑或者要求乙方答复时,乙方须在收到甲方的质疑后2个工作日内给予书面解释或者答复;

8.14 除双方另有约定外,为本项目进行调查研究、分析论证、试验测定以及到外地进行调研、收集资料所发生的费用,由乙方自行承担;乙方自行承担因履行本合同产生的各项税负;

8.15 乙方在履行合同期间使用的由甲方提供或者支付费用的设备设施,属于甲方的财产,乙方在完成委托项目并向甲方提交工作成果时,应当将设备设施归还给甲方。

8.16 未经甲方书面同意,乙方不得将承办项目全部或者部分承办任务转委托其他第三方机构或组织承担。



## **9. 违约责任**

9.1 甲、乙双方应正当行使权利，履行义务，保证本合同的顺利履行；

9.2 乙方没有充分、及时履行义务的，应当承担违约责任；给甲方造成损失的，应赔偿甲方由此所遭受的直接和间接经济损失。

9.3 由于乙方的过错造成其提供的服务不能满足合同中规定的要求，则甲方应以书面形式通知乙方予以改进。乙方自接到书面通知之日起 15 日予以改进或向甲方提出书面异议。否则，甲方有权要求乙方支付违约金，违约金的金额为服务费总额的 10%，并赔偿由此给甲方带来的相关损失。由于乙方的过错造成其不能按时完成服务的，每逾期 1 个工作日，乙方向甲方支付违约金，违约金的金额为服务费总额的 1%。上述两项违约金的金额可以叠加。如违约金总额超过服务费总额的 30%，甲方有权解除合同，乙方应向甲方返还已支付合同费用，违约金不足以弥补甲方损失的，乙方赔偿由此给甲方带来的所有损失。

9.4 因乙方原因致使甲方遭受第三方追诉的，乙方应赔偿由此给甲方造成的损失。

## **10. 免责规定**

10.1 若双方因地震、火灾、水灾等自然灾害，战争等不可抗力原因或国家政策调整致使本合同无法履行的，双方应协商解决，互不承担责任；

10.2 若免责条件结束后，本合同内容仍能继续履行，本合同继续有效。

## **11. 乙方的保证**

乙方保证在履行本合同过程中提供的服务不侵犯任何第三方的合法权益或引起任何第三方的指控或行政机关的处罚，因乙方过错导致任何第三方向甲方主张侵权或赔偿或行政处罚，因此而发生的一切费用、赔偿金及罚金由乙方承担。同时乙方需提供全力支持，防止因上述侵权或可能的侵权给甲方造成的损失，包括但不限于提供甲方继续使用本合同项下的服务而需取得的第三方授权、修改本合同项下服务使其至少在功能上可以替代原服务、提供功能上相等的使甲方可以达到本合同目的的其他服务，并由乙方承担因此而产生的所有的费用。

乙方在提供服务过程中，应严格遵守甲方的规章制度。乙方员工在实施过程中由于自身原因发生安全事故，造成甲方、第三方、乙方人员自身的财产、人身



损害等，由乙方负责解决并承担相关责任。

## **12. 培训**

合同期间，乙方应根据甲方工作需要，免费为甲方提供与合同相关的业务培训。

## **13. 验收**

合同期满后，乙方完全履行了合同所规定的条款，且无任何争议或遗留问题，按照甲方的项目验收要求进行验收，验收相关费用由乙方承担。

## **14. 合同执行**

14.1 甲乙双方签订、变更、中止或者终止政府采购合同的相关条款应遵守《中华人民共和国政府采购法》第五章政府采购合同的规定；

14.2 本合同其效力、解释、履行和争议的解决，适用于中华人民共和国法律，属中华人民共和国法律管辖；

14.3 双方合同执行中如有争议，应友好协商解决，协商不成按照中华人民共和国有关法律提交甲方所在地有管辖权人民法院解决。

## **15. 廉政承诺**

15.1 合同双方承诺共同加强廉洁自律、反对商业贿赂。

15.2 甲方及其工作人员不得收受可能影响正常执行公务的礼品、礼金、消费卡和有价证券、股权、其他金融产品等财物，不得收受其他明显超出正常礼尚往来的财物；不得在乙方报销应由本单位或个人支付的费用；不得以参与项目实施为名，接受乙方从该项目中支取的劳务报酬；不得参加乙方安排的可能影响公正执行公务的宴请或者旅游、健身、娱乐等活动。

15.3 乙方不得向甲方及其工作人员馈赠可能影响公正执行公务的礼品、礼金、消费卡和有价证券、股权、其他金融产品等财物，不得馈赠其他明显超出正常礼尚往来的财物；不得为其报销应由甲方单位或个人支付的费用；不得向甲方工作人员支付劳务报酬；不得安排甲方工作人员参加可能影响公正执行公务的宴请或者旅游、健身、娱乐等活动。

15.4 乙方的股东、董事、监事、高层管理人员、合作项目负责人及工作人

员为甲方员工的亲友或与甲方有密切关系的，应在合作前，以书面方式全面、如实告知。

## 16. 合同生效和其它

16.1 本合同经双方法定代表人或授权代表人签字、盖章之日起生效；

16.2 合同一式陆份。甲方执肆份，乙方执贰份，具有同等法律效力。

甲方：北京市广播电视监测中心

名称：

(印章)



授权代表(签字)：

钱富奎

地 址：北京市通州区达济街

5号院

邮政编码：101117

电 话：55565330

联 系 人：殷悦

开户银行：北京银行潞城支行

账 号：20000003326820112001009

乙 方：北京华夏航通信息技术有限

名称：

(印章)



授权代表(签字)：

耿馥焜

地 址：北京市门头沟区石龙经济

开发区永安路20号3号

B1-6298室

邮政编码：100142

电 话：010-62885567

联 系 人：耿馥焜

开户银行：建行北京定慧北桥支行

账 号：11001182900052500479



## 二、中标通知书

# 中标通知书

**北京华夏航通信息技术有限公司：**

兹通知，贵单位在我公司组织的监测系统运行维护（第1包：网络安全服务）（项目代理编号：HCZB-2024-ZB0209）公开招标采购中，经评标委员会评定，报请北京市广播电视监测中心确认，同意贵单位为本包的中标单位。

中标单位：北京华夏航通信息技术有限公司

中标金额：人民币小写：601000.00元

人民币大写：陆拾万零壹仟元整

请贵单位自本通知书发出之日起三十日内，与采购人办理签订合同事宜。

特此通知。



华采招标集团有限公司  
地址：北京市丰台区广安路9号国投财富广场6号楼1601室  
电话：010-63509799

传真：010-63509799 转 808  
电子邮箱：hczb104@163.com



### 三、投标方案

(一) 采购需求偏离表

序号	招标文件条 目号(页码)	招标文件要求	响应内容	偏离 情况	说明
1.	第五章 采 购需求；第 一包 网络 安全服务 采购需求； 一、概述(第 11 页)	北京市广播电视监测中心广播电视融合媒体智慧监管平台建设于2024年，公共广播信号监测系统建设于2013年，目前均已投入运行，为充分保障监管平台网络安全，本包采购相应的网络安全服务，确保监测系统安全稳定、可靠、不间断运行。 ★说明：各项服务内容中所有人员、工具设备及耗材费用由中标人承担。	应答：完全满足 我公司在充分理解该项目的概述情况下，完成对该项目的建设。 北京市广播电视监测中心广播电视融合媒体智慧监管平台建设于2024年，公共广播信号监测系统建设于2013年，目前均已投入运行，为充分保障监管平台网络安全，本包采购相应的网络安全服务，确保监测系统安全稳定、可靠、不间断运行。 各项服务内容中所有人员、工具设备及耗材费用由我公司承担。	无 偏离	无
2.	第五章 采 购需求；第 一包 网络 安全服务 采购需求； 二、服务内 容(第11 页)	根据《信息安全技术 网络安全等级保护定级指南》(GB/T 22240-2020)，广播电视融合媒体智慧监管平台和公共广播信号监测系统定级为等保二级。根据网络安全法、《信息安全技术网络安全等级保护基本要求》(GB/T22239-2019)，等保二级系统应具有边界防护、入侵防范、安全加固服务等安全防护功能。	应答：完全满足 我公司将按照项目招标要求完成项目的服务内容。 根据《信息安全技术 网络安全等级保护定级指南》(GB/T 22240-2020)，广播电视融合媒体智慧监管平台和公共广播信号监测系统定级为等保二级。根据网络安全法、《信息安全技术网络安全等级保护基本要求》(GB/T22239-2019)，等保二级系统应具有边界防护、入侵防范、安全加固服务等安全防护功能。	无 偏离	无



<p>第五章 采购需求；第一包 网络安全服务采购需求；</p> <p>二、服务内容；</p> <p>（一）网络安全服务内容（第11-12页）</p>	<p>根据监测中心业务系统网络实际情况和网络安全防护要求，网络安全服务内容表 1 网络安全服务内容</p>	<p>应答：完全满足</p> <p>我公司将根据监测中心业务系统网络实际情况和网络安全防护要求，完成项目服务内容。网络安全服务内容见表 1。</p>	<p>表 1 网络安全服务内容</p>	<table border="1"> <thead> <tr> <th>序号</th> <th>名称</th> <th>内容</th> <th>备注</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>边界防护</td> <td>在可视指挥调度前端与中心平台边界部署 1 台防火墙，实现访问控制功能，抵御外部风险，及时更新升级特征库（入侵防御、防病毒、上网行为等）使之保持最新版本。</td> <td>我公司将在可视指挥调度前端与中心平台边界部署 1 台防火墙，实现访问控制功能，抵御外部风险，及时更新升级特征库（入侵防御、防病毒、上网行为等）使之保持最新版本。</td> </tr> <tr> <td>2</td> <td>物理机防病毒</td> <td>在各区融媒体中心共享终端、广播电视台/鼎视/歌华/移动电视信息共享终端、值班服务器防病毒软件，实现对重要物理机的定期检测和病毒防护。</td> <td>我公司将在各区融媒体中心信息共享终端、广播电视台/鼎视/歌华/移动电视信息共享终端、值班服务器部署防病毒软件，实现对重要物理机的定期检测和病毒防护。</td> </tr> <tr> <td>3</td> <td>终端安全管理</td> <td>对各区融媒体中心共享终端、广播电视台/鼎视/歌华/移动电视信息统一管理，管理设备端口、记录操作行为、识别安全风险</td> <td>我公司将对各区融媒体中心信息共享终端、广播电视台/鼎视/歌华/移动电视信息统一管理，</td> </tr> <tr> <td>4</td> <td>防御</td> <td>1.对公共广播信号监</td> <td></td> </tr> </tbody> </table>	序号	名称	内容	备注	1	边界防护	在可视指挥调度前端与中心平台边界部署 1 台防火墙，实现访问控制功能，抵御外部风险，及时更新升级特征库（入侵防御、防病毒、上网行为等）使之保持最新版本。	我公司将在可视指挥调度前端与中心平台边界部署 1 台防火墙，实现访问控制功能，抵御外部风险，及时更新升级特征库（入侵防御、防病毒、上网行为等）使之保持最新版本。	2	物理机防病毒	在各区融媒体中心共享终端、广播电视台/鼎视/歌华/移动电视信息共享终端、值班服务器防病毒软件，实现对重要物理机的定期检测和病毒防护。	我公司将在各区融媒体中心信息共享终端、广播电视台/鼎视/歌华/移动电视信息共享终端、值班服务器部署防病毒软件，实现对重要物理机的定期检测和病毒防护。	3	终端安全管理	对各区融媒体中心共享终端、广播电视台/鼎视/歌华/移动电视信息统一管理，管理设备端口、记录操作行为、识别安全风险	我公司将对各区融媒体中心信息共享终端、广播电视台/鼎视/歌华/移动电视信息统一管理，	4	防御	1.对公共广播信号监	
序号	名称	内容	备注																					
1	边界防护	在可视指挥调度前端与中心平台边界部署 1 台防火墙，实现访问控制功能，抵御外部风险，及时更新升级特征库（入侵防御、防病毒、上网行为等）使之保持最新版本。	我公司将在可视指挥调度前端与中心平台边界部署 1 台防火墙，实现访问控制功能，抵御外部风险，及时更新升级特征库（入侵防御、防病毒、上网行为等）使之保持最新版本。																					
2	物理机防病毒	在各区融媒体中心共享终端、广播电视台/鼎视/歌华/移动电视信息共享终端、值班服务器防病毒软件，实现对重要物理机的定期检测和病毒防护。	我公司将在各区融媒体中心信息共享终端、广播电视台/鼎视/歌华/移动电视信息共享终端、值班服务器部署防病毒软件，实现对重要物理机的定期检测和病毒防护。																					
3	终端安全管理	对各区融媒体中心共享终端、广播电视台/鼎视/歌华/移动电视信息统一管理，管理设备端口、记录操作行为、识别安全风险	我公司将对各区融媒体中心信息共享终端、广播电视台/鼎视/歌华/移动电视信息统一管理，																					
4	防御	1.对公共广播信号监																						
3.				无偏离																				



			支撑服务	<p>测系统、广播电视融合媒体智慧监管平台发生的安全事故进行分析，给出解决方案，减少损失和负面影响，确保系统整体安全运行。</p> <p>2. 协助监测中心建立全方位的业务系统防守体系，负责攻击演练期间现场值守、设备监控预警、威胁检测分析与事件快速处置等工作及远程技术支持、疑难问题处置、威胁情报共享、事件分析溯源等工作。</p> <p>3. 针对上级单位下达的网络安全保障、安全风险自查和网络安全落实情况检查工作并提供工作方案并协助监测中心完成材料准备、现场迎检等工作。</p> <p>4. 协助做好防御技术培训，针对防御技巧、防御策略、防御工具使用、防御技术原理等，</p>		4	防御支撑服务	<p>管理设备端口、记录操作行为、识别安全风险</p> <p>1. 我公司将对公共广播信号监测系统、广播电视融合媒体智慧监管平台发生的安全事故进行分析，给出解决方案，减少损失和负面影响，确保系统整体安全运行。</p> <p>2. 我公司将协助监测中心建立全方位的业务系统防守体系，负责攻击演练期间现场值守、设备监控预警、威胁检测分析与事件快速处置等工作及远程技术支持、疑难问题处置、威胁情报共享、事件分析溯源等工作。</p> <p>3. 我公司将针对上级单位下达的网络安全保障、安全风险自查和网络安全落实情况检查工作并提供工作方案并协助监测中心完成材料准备、现场迎检等工作。</p>			
--	--	--	------	---	--	---	--------	---	--	--	--







			<p>系统现状调研,根据调研结果编制测评申请书,在测评现场提供技术支持,根据测评结果协助整改并提供复测咨询等。</p> <p>根据国家网络安全相关政策和要求,组织有资质的第三方机构对公共广播信号监测系统等进行等级保护测评,包括技术安全测评、管理安全测评和综合测评,并出具测评报告。</p>	<p>9</p> <p>等保测评服务</p>	<p>8</p> <p>辅助测评服务</p>	<p>9</p> <p>等保测评服务</p>	<p>给出安全建议。每年开展2轮。</p> <p>我公司将针对网络安全等级保护测评提供咨询服务,协助通过等级保护测评,咨询服务内容包括系统现状调研,根据调研结果编制测评申请书,在测评现场提供技术支持,根据测评结果协助整改并提供复测咨询等。</p> <p>根据国家网络安全相关政策和要求,我公司将组织有资质的第三方机构对公共广播信号监测系统等进行等级保护测评,包括技术安全测评、管理安全测评和综合测评,并出具测评报告。</p>			<p>4.</p> <p>第五章 采购需求; 第一包 网络安全服务采购需求; 二、服务内容; (二)</p>	<p>根据监测中心广播电视监测业务特点、网络性能实际情况和网络安全服务工具(含软件)功能性能配置应满足以下要求。</p>	<p>应答: 完全满足</p> <p>我公司将根据监测中心广播电视监测业务特点、网络性能实际情况和网络安全服务工具(含软件)功能性能配置全部满足以下招标要求。</p>	<p>无偏 离</p>	<p>无</p>
--	--	--	--	------------------------	------------------------	------------------------	--	--	--	--	--	---	-----------------	----------



	网络安全服务工具（第12页）				
5.		采用专用架构平台和专用安全操作系统，无通用操作系统漏洞；硬件和软件为最新版本。	应答：完全满足 我公司将提供边界防护工具。采用专用架构平台和专用安全操作系统，无通用操作系统漏洞；硬件和软件为最新版本。	无偏离	无
6.	第五章 采购需求；第一包 网络安全服务	不少于 6 个 10/100/1000BASE-T 端口、4 个千兆 SFP 光纤插槽、2 个高速 USB2.0 接口，可接移动存储进行日志存储。	应答：完全满足 我公司将提供边界防护工具。6 个 10/100/1000BASE-T 端口、4 个千兆 SFP 光纤插槽、2 个高速 USB2.0 接口，可接移动存储进行日志存储。	无偏离	无
7.	二、服务内	系统要求 吞吐量大于 3.0Gbps，最大并发连接数大于 200 万。	应答：完全满足 我公司将提供边界防护工具。吞吐量 4.0Gbps，最大并发连接数 300 万。	无偏离	无
8.	容；（二）网络安全服务工具；1. 边界防护工具（第12-13页）	配置 IPSec VPN 和 SSL VPN 模块（大于 200 个并发用户），以及 IPS 模块、AV 模块和上网行为管理模块。	应答：完全满足 我公司将提供边界防护工具。配置 IPSec VPN 和 SSL VPN 模块（200 个并发用户），以及 IPS 模块、AV 模块和上网行为管理模块。	无偏离	无
9.		基于状态检测的动态包过滤	应答：完全满足 我公司将提供边界防护工具。基于状态检测的动态包过滤	无偏离	无
10.	访问控制	支持基于用户、用户组的访问控制，用户认证支持 Radius、LDAP、Windows AD 域等方式，内置认证服务器，支持双因子认证。	应答：完全满足 我公司将提供边界防护工具。支持基于用户、用户组的访问控制，用户认证支持 Radius、LDAP、Windows AD 域等方式，内置认证服务器，支持双因子认证。	无偏离	无



11.			支持同一主机源会话、目的会话分别管理和限制，支持设定网段内并连接限制。	应答：完全满足 我公司将提供边界防护工具。支持同一主机源会话、目的会话分别管理和限制，支持设定网段内并连接限制。	无	无
12.			支持应用层访问控制，包括 P2P 软件、网游软件等	应答：完全满足 我公司将提供边界防护工具。支持应用层访问控制，包括 P2P 软件、网游软件等	无	无
13.			支持一体化安全策略配置，实现用户认证、IPS、AV、URL 过滤、协议控制、流量控制、并发、新建限制、垃圾邮件过滤、审计等功能。	应答：完全满足 我公司将提供边界防护工具。支持一体化安全策略配置，实现用户认证、IPS、AV、URL 过滤、协议控制、流量控制、并发、新建限制、垃圾邮件过滤、审计等功能。	无	无
14.	安全防护 模板		支持主要防护功能的统一模版设置，模版分为高、中、低三个级别防护强度，可单击选择切换或通过外置按键一键切换。	应答：完全满足 我公司将提供边界防护工具。支持主要防护功能的统一模版设置，模版分为高、中、低三个级别防护强度，可单击选择切换或通过外置按键一键切换。	无	无
15.	网络适应性		支持透明、路由、混合三种工作模式。	应答：完全满足 我公司将提供边界防护工具。支持透明、路由、混合三种工作模式。	无	无
16.			支持静态路由，动态路由（OSPF、RIP 等），VLAN 间路由，组播路由等。	应答：完全满足 我公司将提供边界防护工具。支持静态路由，动态路由（OSPF、RIP 等），VLAN 间路由，组播路由等。	无	无
17.	IPv6/IPv4 双协议栈		支持 IPv6 地址、地址组配置。支持 IPv6 安全控制策略，能针对 IPv6 的目的/源地址、目的/源服务端口、	应答：完全满足 我公司将提供边界防护工具。支持 IPv6 地址、地址组配置。支持 IPv6 安全控	无	无



18.		服务、扩展头属性等进行安全访问规则设置。	制策略，能针对 IPV6 的目的/源地址、目的/源服务端口、服务、扩展头属性等进行安全访问规则设置。			
19.	主动防御	能主动屏蔽恶意地址。 具有主动防御功能，对服务器、主机进行后门、服务探测、文件共享、系统补丁、IE 漏洞等进行主动式扫描。	应答：完全满足 我公司将提供边界防护工具。 能主动屏蔽恶意地址。 应答：完全满足 我公司将提供边界防护工具。 具有主动防御功能，对服务器、主机进行后门、服务探测、文件共享、系统补丁、IE 漏洞等进行主动式扫描。	无	无	无
20.	管理配置	支持数字证书和电子钥匙方式，支持 SNMP 管理，与通用网络管理平台兼容。	应答：完全满足 我公司将提供边界防护工具。 支持数字证书和电子钥匙方式，支持 SNMP 管理，与通用网络管理平台兼容。	无	无	无
21.		支持日志中文化，可显示配置命令日志的操作人。	应答：完全满足 我公司将提供边界防护工具。 支持日志中文化，可显示配置命令日志的操作人。	无	无	无
22.	高可用性	具有链路备份、链路聚合功能，可以在多个网络出口之间自动切换。	应答：完全满足 我公司将提供边界防护工具。 具有链路备份、链路聚合功能，可以在多个网络出口之间自动切换。	无	无	无
23.		支持与原有设备（Power V 防火墙）双机热备和负载均衡，切换时间小于 1 秒。	应答：完全满足 我公司将提供边界防护工具。 支持与原有设备（Power V 防火墙）双机热备和负载均衡，切换时间小于 1 秒。	无	无	无



24.			产品资质	具备公安部颁发的《计算机信息系统安全专用产品销售许可证》。	应答：完全满足 我公司将提供边界防护工具。 具备公安部颁发的《计算机信息系统安全专用产品销售许可证》。	无	无
25.				具备中国信息安全产品认证中心颁发的《中国信息安全产品认证证书》。	应答：完全满足 我公司将提供边界防护工具。 具备中国信息安全产品认证中心颁发的《中国信息安全产品认证证书》。	无	无
26.		第五章 采购需求；第一包 网络安全服务	产品配置	不少于 1 个管理中心，18 个客户端和 6 台服务器端，最新版本病毒库并定期升级。	应答：完全满足 我公司将提供物理机防病毒软件工具。 1 个管理中心，18 个客户端和 6 台服务器端，最新版本病毒库并定期升级。	无	无
27.		采购需求；二、服务内容；（二）网络安全服务工具；2. 物理机防病毒软件工具（第 14 页）	产品资质	具有公安部颁发的《计算机信息系统安全专用产品销售许可证》。	应答：完全满足 我公司将提供物理机防病毒软件工具。 具有公安部颁发的《计算机信息系统安全专用产品销售许可证》。	无	无
28.		第五章 采购需求；第一包 网络安全服务	产品配置	不少于 1 个管理中心，18 个管理节点授权；软件为最新版本。	应答：完全满足 我公司将提供终端安全管理工具。 1 个管理中心，18 个管理节点授权；软件为最新版本。	无	无
29.		采购需求；二、服务内容；（二）网络安全服务	产品资质	具有公安部颁发的《计算机信息系统安全专用产品销售许可证》。	应答：完全满足 我公司将提供终端安全管理工具。 具有公安部颁发的《计算机信息系统安全专用产品销售许可证》。	无	无



	<p>务工具； 3. 终端安全管理工具（第14页）</p>				
<p>30.</p>	<p>第五章 采购需求：第一包 网络安全服务采购需求；三、服务要求；1.维护要求（第14页）</p>	<p>(1) 免费升级特征库、病毒库，网络安全情况检查和安全隐患排除、故障设备处理、数据检查维护等。  (2) 设备故障为软件故障的，2小时内修复。硬件故障的，严重故障，4小时内修复；一般故障，2小时内修复。  (3) 每次服务完成后应提交技术服务报告，主要包括网络运行状态、数据库及系统日志情况、设备性能、故障现象及处理、软件运行等内容。  (4) 广播电视安全播出重要保障期（春节、两会、五一、十一等）期间，安排技术人员值守服务，处置突发事件，保障系统正常运行。  (5) 服务期为监测中心技术人员提供2次网络安全技术培训。  (6) 配合监测中心做好网络安全应急演练有关工作，根据广播电视融合媒体智慧监管平台和公共广播信号监测系统实际情况，提供应急演练服务，包含应急预案制定、应急演练操作等；模拟突发事件的处理过程，推演应急演练全流程。  (7) 配合监测中心做好网络安全检查有关工作。</p>	<p>应对：完全满足  (1) 我公司将负责免费升级特征库、病毒库，网络安全情况检查和安全隐患排除、故障设备处理、数据检查维护等。  (2) 设备故障为软件故障的，我公司将在2小时内修复。硬件故障的，严重故障，我公司将在4小时内修复；一般故障，我公司将在2小时内修复。  (3) 每次服务完成后我公司项目服务人员将提交技术服务报告，主要包括网络运行状态、数据库及系统日志情况、设备性能、故障现象及处理、软件运行等内容。  (4) 广播电视安全播出重要保障期（春节、两会、五一、十一等）期间，我公司将安排技术人员值守服务，处置突发事件，保障系统正常运行。  (5) 服务期我公司将为监测中心技术人员提供2次网络安全技术培训。  (6) 我公司将配合监测中心做好网络安全应急演练有关工作，根据广播电视融合媒体智慧监管平台和公共广播信号监测系统实际情况，提供应急演练服务，包含应急预案制定、应急演练操作等；模拟突发事件的处理过程，推演应急演练全流程。</p>	<p>无</p>	



			(7) 我公司将配合监测中心做好网络安全检查工作。			
31.	第五章 采购需求：第一包 网络安全服务 三、服务要求；2.巡检要求（第14-15页）	投标人应提供详细具体的巡检方案，每月对网络安全设备进行巡检，各安全播出重保期前提供专项巡检。	应对：完全满足 我公司将提供详细具体的巡检方案，每月对网络安全设备进行巡检，各安全播出重保期前提供专项巡检。	无偏离	无	
32.	第五章 采购需求：第一包 网络安全服务 三、服务要求；3.服务方案和应急预案（第15页）	应提供详细具体、可行、有针对性的服务方案和应急预案。	应对：完全满足 我公司将提供详细具体、可行、有针对性的服务方案和应急预案。	无偏离	无	
33.	第五章 采购需求：第一包 网络安全服务 三、服务要求；4.服务	(1) 团队成员应相对固定，并具有专业2年以上（含）网络安全运维经验。 (2) 安全服务人员应具有 CISP 资质证书。	应对：完全满足 (1) 我公司服务团队成员将确保固定，并具有专业2年以上（含）网络安全运维经验。 (2) 我公司安全服务人员具有 CISP 资质证书。	无偏离	无	



34.	团队要求 (第 15 页) 第五章 采购需求; 第一包 网络安全服务 采购需求; 三、服务要求; 5. 备件要求 (第 15 页)	应有设备备件, 存放于中标方。	应对: 完全满足 公司将对服务设备足备件, 存放于我公司。	无 无 无
35.	第五章 采购需求; 第一包 网络安全服务 采购需求; 四、服务期限 (第 15 页)	2024 年 7 月 1 日至 2025 年 6 月 30 日。	应对: 完全满足 我公司将严格按照项目规定的服务期限完成项目内容, 具体项目服务期限为: 2024 年 7 月 1 日至 2025 年 6 月 30 日。	无 无 无
36.	第五章 采购需求; 第一包 网络安全服务 采购需求; 五、廉政要求 (第 15 页)	投标人和采购人承诺共同加强廉洁自律、反对商业贿赂。 1. 投标人不向采购人工作人员行贿或馈赠礼金、有价证券、贵重礼品; 2. 投标人不报销应由采购人或工作人员支付的费用; 3. 投标人不向采购人工作人员支付劳务报酬; 不安排采购人工作人员参加宴请及娱乐活动。	应对: 完全满足 我公司和采购人承诺共同加强廉洁自律、反对商业贿赂。 1. 我公司不向采购人工作人员行贿或馈赠礼金、有价证券、贵重礼品; 2. 我公司不报销应由采购人或工作人员支付的费用; 3. 我公司不向采购人工作人员支付劳务报酬; 不安排采购人工作人员参加宴请及娱乐活动。	无 无 无



37.	<p>第五章 采购需求：第一包 网络安全服务采购需求；六、采购标的的所属行业（第 15 页）</p>	<p>本项目采购标的属于《工业和信息化部、国家统计局、国家发展和改革委员会、财政部关于印发中小企业划型标准规定的通知》（工信部联企业[2011]300号）中的（十二）软件和信息技术服务业。</p>	<p>应答：完全满足          本项目采购标的属于《工业和信息化部、国家统计局、国家发展和改革委员会、财政部关于印发中小企业划型标准规定的通知》（工信部联企业[2011]300号）中的（十二）软件和信息技术服务业。</p>	无偏离	无
-----	--	--	---	-----	---



## **(二) 服务承诺**

北京华夏航通信息技术有限公司为监测系统运行维护（第一包 网络安全服务）提供如下服务承诺：

**各项服务内容中所有人员、工具设备及耗材费用由中标人承担。**

**满足本项目中的所有服务要求：**

### **1.维护要求**

(1) 免费升级特征库、病毒库，网络安全情况检查和安全隐患排查、故障设备处理、数据检查维护等。

(2) 设备故障为软件故障的，2小时内修复。硬件故障的，严重故障，4小时内修复；一般故障，2小时内修复。

(3) 每次服务完成后应提交技术服务报告，主要包括网络运行状态、数据库及系统日志情况、设备性能、故障现象及处理、软件运行等内容。

(4) 广播电视安全播出重要保障期（春节、两会、五一、十一等）期间，安排技术人员值守服务,处置突发事件，保障系统正常稳定运行。

(5) 服务期为监测中心技术人员提供2次网络安全技术培训。

(6) 配合监测中心做好网络安全应急演练有关工作，根据广播电视融合媒体智慧监管平台和公共广播信号监测系统实际情况，提供应急演练服务，包含应急预案制定、应急演练操作等；模拟突发事件的处理过程，推演应急处理全流程。

(7) 配合监测中心做好网络安全检查有关工作。

### **2.巡检要求**

我公司提供详细具体的巡检方案，每月对网络安全设备进行巡检，各安全播出重保期前提供专项巡检。

### **3.服务方案和应急预案**

我公司提供详细具体、可行、有针对性的服务方案和应急预案。

### **4.服务团队要求**

(1) 我公司团队成员确保固定，并具有专业2年以上（含）网络安全运维经验。

(2) 我公司安全服务人员具有CISP资质证书。

### **5.备件要求**

服务设备备足备件，存放于我公司。

**满足本项目服务期限要求：**

2024年7月1日至2025年6月30日。

**(三) 其他内容详见投标文件。**



## 四、招标要求

### 第一包 网络安全服务 采购需求

**注：**招标文件带有“★”号条款为实质性条款，不满足要求为**无效投标**。

#### 一、概述

北京市广播电视监测中心广播电视融合媒体智慧监管平台建设于2024年，公共广播信号监测系统建设于2013年，目前均已投入运行，为充分保障监管平台网络安全，本包采购相应的网络安全服务，确保监测系统安全稳定、可靠、不间断运行。

**★说明：**各项服务内容中所有人员、工具设备及耗材费用由中标人承担。

#### 二、服务内容

根据《信息安全技术 网络安全等级保护定级指南》(GB/T 22240-2020)，广播电视融合媒体智慧监管平台和公共广播信号监测系统定级为等保二级。根据网络安全法、《信息安全技术网络安全等级保护基本要求》(GB/T22239-2019)，等保二级系统应具有边界防护、入侵防范、安全加固服务等安全防护功能。

##### (一) 网络安全服务内容

根据监测中心业务系统网络实际情况和网络安全防护要求，网络安全服务内容见表1。

表1 网络安全服务内容

序号	名称	内容	备注
1	边界防护	在可视指挥调度前端与中心平台边界部署1台防火墙，实现访问控制等功能，抵御外部风险，及时更新升级特征库（入侵防御、防病毒、上网行为等）使之保持最新版本。	
2	物理机防病毒	在各区融媒体中心信息共享终端、广播电视台/鼎视/歌华/移动电视信息共享终端、监测值班服务器部署防病毒软件，实现对重要物理机的定期检测和病毒防护。	
3	终端安全管理	对各区融媒体中心信息共享终端、广播电视台/鼎视/歌华/移动电视信息共享终端进行统一的管理，管理设备端口、记录操作行为、识别安全风险	



4	防御支撑服务	<p>1. 对公共广播信号监测系统、广播电视融合媒体智慧监管平台发生的安全事故进行分析，给出解决方案，减少损失和负面影响，确保系统整体安全运行。</p> <p>2. 协助监测中心建立全方位的业务系统防守体系，负责攻击演练期间现场值守、设备监控预警、威胁检测分析与事件快速处置等工作及远程技术支持、疑难问题处置、威胁情报共享、事件分析溯源等工作。</p> <p>3. 针对上级单位下达的网络安全保障、安全风险自查和网络安全落实情况检查等工作任务提供工作方案并协助监测中心完成材料准备、现场迎检等工作。</p> <p>4. 协助做好防御技术培训，针对防御技巧、防御策略、防御工具使用、防御技术原理等，提升监测中心整体技术人员的安全防御能力。</p>
5	脆弱性检测服务	对公共广播信号监测系统等业务系统的操作系统、数据库、中间件、网络设备、安全设备和安全管理制度等进行2轮脆弱性检测，及时发现安全隐患，提供脆弱性检测文档。
6	安全加固服务	对公共广播信号监测系统等业务系统进行安全加固。每年开展2轮。根据《信息安全技术网络安全等级保护基本要求》完善相关制度。
7	渗透测试服务	对公共广播信号监测系统等业务系统进行渗透测试，挖掘出正常业务流程中的安全缺陷和漏洞。并给出安全建议。每年开展2轮。
8	辅助测评服务	针对网络安全等级保护测评提供咨询服务，协助通过等级保护测评，咨询服务内容包括系统现状调研，根据调研结果编制测评申请书，在测评现场提供技术支持，根据测评结果协助整改并提供复测咨询等。
9	等保测评服务	根据国家网络安全相关政策和要求，组织有资质的第三方机构对公共广播信号监测系统进行等级保护测评，包括技术安全测评、管理安全测评和综合测评，并出具测评报告。

## (二) 网络安全服务工具

根据监测中心广播电视监测业务特点、网络性能实际情况和网络安全等保二级要求，投标人使用的网络安全服务工具（含软件）功能性能配置应满足以下要求。

### 1. 边界防护工具

功能规格	性能配置要求
系统要求	采用专用架构平台和专用安全操作系统，无通用操作系统漏洞；硬件



	和软件为最新版本。
	不少于 6 个 10/100/1000BASE-T 端口、4 个千兆 SFP 光纤插槽、2 个高速 USB2.0 接口，可接移动存储进行日志存储。
	吞吐量大于 3.0Gbps，最大并发连接数大于 200 万。
	配置 IPSec VPN 和 SSL VPN 模块（大于 200 个并发用户），以及 IPS 模块、AV 模块和上网行为管理模块。
访问控制	基于状态检测的动态包过滤
	支持基于用户、用户组的访问控制，用户认证支持 Radius、LDAP、Windows AD 域等方式，内置认证服务器，支持双因子认证。
	支持同一主机源会话、目的会话分别管理和限制，支持设定网段内并发连接限制。
	支持应用层访问控制，包括 P2P 软件、网游软件等
	支持一体化安全策略配置，实现用户认证、IPS、AV、URL 过滤、协议控制、流量控制、并发、新建限制、垃圾邮件过滤、审计等功能。
安全防护模板	支持主要防护功能的统一模版设置，模版分为高、中、低三个级别防护强度，可单击选择切换或通过外置按键一键切换。
网络适应性	支持透明、路由、混合三种工作模式。
	支持静态路由，动态路由（OSPF、RIP 等），VLAN 间路由，组播路由等。
IPv6/IPv4 双协议栈	支持 IPv6 地址、地址组配置。支持 IPv6 安全控制策略，能针对 IPV6 的目的/源地址、目的/源服务端口、服务、扩展头属性等进行安全访问规则设置。
主动防御	能主动屏蔽恶意地址。
	具有主动防御功能，对服务器、主机进行后门、服务探测、文件共享、系统补丁、IE 漏洞等进行主动式扫描。
管理配置	支持数字证书和电子钥匙方式，支持 SNMP 管理，与通用网络管理平台兼容。
	支持日志中文化，可显示配置命令日志的操作人。
高可用性	具有链路备份、链路聚合功能，可以在多个网络出口之间自动切换。



	支持与原有设备（Power V 防火墙）双机热备和负载均衡，切换时间小于 1 秒。
产品资质	具备公安部颁发的《计算机信息系统安全专用产品销售许可证》。
	具备中国信息安全产品认证中心颁发的《中国信息安全产品认证证书》。

## 2. 物理机防病毒软件工具

功能规格	性能配置要求
产品配置	不少于 1 个管理中心，18 个客户端和 6 台服务器端，最新版本病毒库并定期升级。
产品资质	具有公安部颁发的《计算机信息系统安全专用产品销售许可证》。

## 3. 终端安全管理工具

功能规格	性能配置要求
产品配置	不少于 1 个管理中心，18 个管理节点授权；软件为最新版本。
产品资质	具有公安部颁发的《计算机信息系统安全专用产品销售许可证》。

## 三、服务要求

### 1. 维护要求

(1) 免费升级特征库、病毒库，网络安全情况检查和安全隐患排查、故障设备处理、数据检查维护等。

(2) 设备故障为软件故障的，2 小时内修复。硬件故障的，严重故障，4 小时内修复；一般故障，2 小时内修复。

(3) 每次服务完成后应提交技术服务报告，主要包括网络运行状态、数据库及系统日志情况、设备性能、故障现象及处理、软件运行等内容。

(4) 广播电视安全播出重要保障期（春节、两会、五一、十一等）期间，安排技术人员值守服务,处置突发事件，保障系统正常稳定运行。

(5) 服务期为监测中心技术人员提供 2 次网络安全技术培训。



(6) 配合监测中心做好网络安全应急演练有关工作，根据广播电视融合媒体智慧监管平台和公共广播信号监测系统实际情况，提供应急演练服务，包含应急预案制定、应急演练操作等；模拟突发事件的处理过程，推演应急处理全流程。

(7) 配合监测中心做好网络安全检查有关工作。

## **2.巡检要求**

投标人应提供详细具体的巡检方案，每月对网络安全设备进行巡检，各安全播出重保期前提供专项巡检。

## **3.服务方案和应急预案**

应提供详细具体、可行、有针对性的服务方案和应急预案。

## **4.服务团队要求**

(1) 团队成员应相对固定，并具有专业2年以上（含）网络安全运维经验。

(2) 安全服务人员应具有CISP资质证书。

## **5.备件要求**

应有设备备件，存放于中标方。

## **四、服务期限**

2024年7月1日至2025年6月30日。

## **五、廉政要求**

投标人和采购人承诺共同加强廉洁自律、反对商业贿赂。

1. 投标人不向采购人工作人员行贿或馈赠礼金、有价证券、贵重礼品；
2. 投标人不报销应由采购人或工作人员支付的费用；
3. 投标人不向采购人工作人员支付劳务报酬；不安排采购人工作人员参加宴请及娱乐活动。