监测系统运行维护项目
（第六包：网络安全服务）采购合同

合同编号： JCZX-YW-2026-6

项目编号： 11000026210200163956-XM001

第六包： 网络安全服务

甲　　方： 北京市广播电视监测中心

乙　　方： 中移建设有限公司

北京市广播电视监测中心

2026 年 6 月 1 日

监测系统运行维护项目
（第六包：网络安全服务）采购合同

甲方：北京市广播电视监测中心

地址：北京市通州区达济街5号院

法定代表人：石东正

项目联系人：路程

联系方式：010-55565332

邮箱：luchlost@163.com

乙方：中移建设有限公司

地址：北京市海淀区北蜂窝路18号(综合楼9层906、907、917)

法定代表人：孙卫东

项目联系人：王乐一

联系方式：13522867215

邮箱：wangleyi@cmtt.cmcc

一、合同书

根据《中华人民共和国民法典》《中华人民共和国招标投标法》等有关法律法规的规定，甲方监测系统运行维护项目（项目编号：11000026210200163956-XM001；项目代理编号：0686-2611BJ074408Z）中第六包：网络安全服务委托北京国际贸易有限公司在国内公开招标。经评标委员会评定，中移建设有限公司（乙方）为中标人。甲方同意乙方作为监测系统运行维护（第六包：网络安全服务）的服务商。甲乙双方经协商一致订立本合同，甲乙双方应严格遵照执行。甲、乙双方同意按照下面的条款和条件，签署本合同。

第一条　合同文件组成

下列文件均为本合同不可分割的组成部分，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：

1 本合同条款

2. 招标文件及其澄清文件

3. 投标文件及其澄清文件

4. 中标通知书

5. 形成合同的其他有关文件，包括甲乙双方就具体服务内容签订的补充合同。

第二条　合同术语定义

除非另有特别的解释或说明，在本合同中及与合同相关的，甲乙双方另行签署的其他文件（包括但不限于本合同的附件）中，下述词语均按照如下定义进行解释：

1. “甲方”系指北京市广播电视监测中心。

2. “乙方”系指根据合同规定向甲方提供服务的具有法人资格的实体；即中标人。

3. “合同”系指甲乙双方签署的，合同格式中载明的甲乙双方所达成的约定，包括构成合同的所有附件、附录和构成合同的所有文件。

4. “服务”系指乙方根据合同规定须向甲方提供的全部服务。

第三条　服务范围及时间

1. 本合同的服务范围是指乙方按照本合同附件以及监测系统运行维护（第六包：网络安全服务）公开招标文件要求为甲方提供服务。

2. 实施时间：自 2026 年 7 月 1 日起至 2027 年 6 月 30 日止。

第四条　服务权限

1. 乙方作为甲方选定的服务商，必须根据甲方要求，承担在投标文件中向甲方承诺的服务范围内的相关工作。

2. 任何情况下，未经甲方书面同意，乙方不得向第三方转让甲方在本合同中授予乙方的权限，不得超越甲方授权范围。否则甲方有权取消乙方的中标人资格。

3. 乙方不得将本项目主体业务及关键性工作、辅助性工作分包或者转委托给第三方，招标文件允许的除外。

第五条　特别承诺

乙方应保证无任何第三方就乙方向甲方提供的服务主张任何权利。如果任何第三方就乙方向甲方提供的服务主张任何权利，乙方须与第三方交涉并承担由此而产生的一切法律责任和费用，并赔偿因此给甲方造成的一切损失，以及甲方为反驳第三方的主张、向乙方主张权利所支付的各项费用，包括但不限于调查费、律师费、诉讼费等。

第六条　合同金额及付款方式

1. 本合同总价为¥1,900,000.00 元人民币，大写：壹佰玖拾万元整。

2. 服务和数量

本合同服务内容：招标文件第五部分采购需求。

分项价格一览表

单位：人民币元

序号	分项名称	单价（元）	数量	合价（元）	备注/说明
网络安全服务					
1	边界防护服务	544000	1	544000	网络边界安全防护服务，围绕网络出入口构建防护屏障，通过精细化管控与智能拦截，保障内部网络与外部系统的安全隔离与合规交互。跨越边界的访问和数据流通过防火墙提供的受控接口进行通信，实现边界防护，抵御外部风险。
2	边界隔离服务	94000	1	94000	提供物理级别的安全隔离与可控数据交互服务，确保不同安全域之间“物理断开、逻辑可控”。去除网络协议，仅做数据传输，实现网络层的物理隔离，确保业务系统安全，防御可能出现的威胁入侵行为。

3	物理机防病毒服务	78000	1	78000	针对物理服务器、工作站等终端设备，提供全周期的恶意代码（病毒、木马、勒索软件等）检测与清除服务，构建终端设备的主动防御屏障。实现对重要物理机的定期检测和病毒防护、清除，抵御病毒威胁。提供 1 个管理中心，33 个客户端和 6 台服务器端的物理机防病毒服务工具，确保最新版本病毒库并定期升级。
4	终端安全管理服务	79200	1	79200	针对所有终端设备，提供从设备接入到运行维护的全流程安全管理服务，实现终端状态可视、风险可控、合规可溯。对网络中的终端设备进行统一的管理，识别终端安全风险。构建终端风险体系并对终端风险进行终端安全管理，从而降低和避免终端安全风险事件的发生。提供 1 个管理中心，33 个管理节点授权终端安全管理服务工具；确保软件为最新版本。
5	防御支撑服务	70000	1	70000	针对攻防演练、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，辅助采购人提供工作方案并协助完成材料准备、迎检等工作；在攻防演练中建立全方位的防守体系，其中一线项目团队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，二线支撑团队提供远程专家技术支持、疑难问题处置、威胁情报共享、事件分析溯源等工作；组织专业网络安全专家，通过专业、全面的信息安全理论、信息安全实践等培训，全面提高相关人员的安全意识水平和安全技术能力，切实提高内部信息安全管理能力，保证业务系统安全稳定运行。
6	脆弱性检测服务	250000	1	250000	对网络视听新媒体综合监管平台、广播电视融合媒体智慧监管平台的服务器操作系统、数据库、中间件、网络设备、安全设备和安全管理制度等进行脆弱性检测，采用工具扫描和手工检查相结合的方式对设备漏洞进行检查，排查主机等层面存在的安全隐患，结合安全措施有效性检测，通过专业化的数据分析，提供相关脆弱性检测文档。对上述 2 系统提供 4 次脆弱性检测。
7	安全加固服务	122000	1	122000	对网络视听新媒体综合监管平台、广播电视融合媒体智慧监管平台漏洞分析识别出的不符合项和脆弱性评估识别出的风险，编制加固整改措施方案，同时对主机、网络、应用安全等方面进行加固。对上述 2 系统提供 4 次安全加固。
8	渗透测试服务	196000	1	196000	对网络视听新媒体综合监管平台、广播电视融合媒体智慧监管平台进行 SQL 注入、跨脚本、 文件上传、 跨径遍历、蛮力攻击、信息泄露、缓冲区溢

					出等安全测试，挖掘系统中的安全缺陷和漏洞。并给出安全建议，指导系统运维单位进行修复等工作。对上述 2 系统提供 4 次渗透测试。
9	安全运营服务	60000	1	60000	对网络视听新媒体综合监管平台、广播电视融合媒体智慧监管平台及监测中心网络安全相关事务提供安全运营服务。通过远程和本地相结合的方式对系统进行梳理，识别关键资产和敏感数据；实时监测网络中的流量、安全日志、安全数据，实时分析系统告警信息，及时发现系统中存在的安全威胁、潜在风险，快速定位安全事件，减少因安全事件带来的损失损害；通过在不同区域发起针对验证标靶的各类攻击动作，检验网络安全防御体系是否完整、检验运营规则的有效性以及安全设备检测能力的有效性。对网络视听新媒体综合监管平台、广播电视融合媒体智慧监管平台发生的安全事件进行分析，提出改进意见，确保系统整体安全运行。根据密码安全、数据安全、供应链安全等最新要求，协助监测中心梳理、完善相关制度，确保中心网络安全各项工作有章可依。使用智能对话分析技术，以对话方式智能分析安全情况，完成快速安全事件判断和梳理，提升安全运营整体能力。
10	等保测评服务	90000	1	90000	根据国家网络安全相关政策和要求，对网络视听新媒体综合监管平台进行等级保护测评和商用密码应用安全性评估，全面评估信息系统现有安全防护水平和相应等级安全要求之间的差距，测评内容包括技术安全测评、管理安全测评和综合测评，并出具测评报告。
11	账号统一管理服务	94940	1	94940	对现有政务云上的业务系统账号进行集中管理，实现人员一次性认证登录操作，避免账号丢失引起的安全隐患。为局内工作人员和运维人员进行账号的访问权限管理。对关键业务系统进行隐藏，减少业务系统的安全风险。为业务系统提供严格的密码管理，制定密码周期、复杂度、长度、超时锁定等规则。确保账号密码的可靠性。
现有网络安全设备软硬件维保					
1	外网防火墙	6000	1	6000	完成对网御星云 网御防火墙系统 V3.0 Power V6000（千兆）防火墙（增强级）的维保升级，对特征库进行升级。
2	WEB 应用防火墙	20000	1	20000	完成对远江盛邦 Web 应用防护系统 W1000/V6.0 WEB 应用防火墙（国际-增强级）的维保升级，对特征库进行升级。
3	内网防火墙	17000	2	34000	完成对网御星云 网御防火墙系统 V3.0 Power V6000（千兆）防火墙（增强级）的维保升级，对

					特征库进行升级。
4	综合安全审计设备	12000	1	12000	完成对网御星云 网御网络审计系统 V3.0/LA-DT 网络通讯安全审计类（增强级）的维保升级。
5	入侵检测设备	11000	1	11000	完成对网御星云 网御入侵检测系统（千兆）/V3.2 网络入侵检测系统（第三级）的维保升级，对特征库进行升级。
6	堡垒主机	9000	1	9000	完成对网御星云 网御运维安全网关系统 LA-OS/V3.0 运维安全管理产品（增强级）的维保升级。
7	日志审计设备	8000	1	8000	完成对网御星云 网御安全管理系统-日志审计 V3.0 日志分析（增强级）的维保升级。
8	安全信息采集引擎	12000	1	12000	完成对网御星云 网御入侵检测系统（千兆）/V3.2 网络入侵检测系统（第三级）的维保升级，对特征库进行升级。
9	分路器	4900	1	4900	完成对成都数维 定制开发型号的维保升级。
10	安全运营平台软件	18000	1	18000	完成对网御星云 网御安全管理系统 V3.0 安全管理平台的维保升级。
11	物理机防病毒软件	240	104	24960	完成对猎鹰安全 猎鹰终端安全管理系统 V9.0 网络版防病毒产品（一级品）的维保升级，对特征库进行升级。
12	虚拟化防病毒软件	35000	1	35000	完成对 360 终端安全管理系统 V10.0 网络版防病毒产品（增强级）的维保升级，对特征库进行升级。
13	虚拟化主机安全管理	27000	1	27000	完成对北信源 北信源内网安全管理系统 V8.1 内网主机监测（增强级）的维保升级，对特征库进行升级。
总价（元）				1900000	

3. 本合同的付款方式为：

合同签订生效后 10 个工作日内，甲方向乙方支付合同首款，即人民币 958000 元（大写：玖拾伍万捌仟元整）；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，即人民币 942000 元（大写：玖拾肆万贰仟元整）。

因相应财政资金未能及时到账而导致的延期支付，不应视为甲方违约，付款时间相应顺延。

4. 甲方付款前，乙方应先向甲方提供等额正式发票，乙方未按本合同约定向甲方提供发票的，甲方有权拒绝支付委托报酬，并不视为甲方违约。乙方提供发票等行为须符合甲方执行的相关财政规定。

甲方开票信息为：

户名：北京市广播电视监测中心

税号：1211000079755080XU

乙方户名、开户银行名称和账号为：

户名：中移建设有限公司

开户行：中国建设银行北京金融街支行

帐号：11001070800059000531

5.甲方支付的合同款已经包含了乙方为完成项目所需的全部费用，除合同另有明文规定外，甲方不再承担该项目其他任何费用，亦不再向乙方支付其他任何费用。

6.与该项目相关的所有费用支出，均需符合相关要求，乙方需配合甲方相关检查、延伸审计，提供相关合同、凭据、票据、支出凭证、签收单等材料。

第七条　甲、乙双方的责任、权利及义务

（一）甲方的责任、权利及义务

1.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；

2.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；

3.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；

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；

5.为保证乙方工作顺利进行，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。

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；

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。

（二）乙方的责任、权利和义务

1.乙方按照甲方要求，完成甲方指定服务内容。

2.乙方保证具有签订与履行本合同的能力和具备相应资质，保证承办的工作人

员具有履行本合同义务的相应能力和资质，保证提供的服务合法且不侵犯任何第三方合法权益。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。

3. 乙方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。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。

4. 有权接受甲方按照合同约定支付的委托报酬。

5. 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。

6. 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。

7. 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. 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。

9. 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；乙方自行负担因履行本合同产生的各项税负。

10. 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。

11. 合同期间，乙方应根据甲方工作需要，为甲方提供与合同相关的业务培训。

第八条　合同执行

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。

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。

第九条　税费

1. 根据国家现行税法规定，应当对甲方征收的与本合同有关的一切税费均由甲方负担。

2. 根据国家现行税法规定，应当对乙方征收的与本合同有关的一切税费均由乙方负担。

3. 在中国境外发生的与本合同执行有关的一切税费均由乙方负担。

第十条　项目验收

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。

第十一条　保密条款

双方承诺，对因履行本合同所知悉对方尚未进入公知领域的信息承担保密义务，未经双方书面同意不得向本合同以外任何其他方泄露，或用于本合同以外的任何其他目的。

第十二条　知识产权

1. 双方合作期间产生的知识产权归甲方单独所有，乙方不得擅自使用或转让给第三方。

2. 乙方提供的相关产品应是自行开发的或具备合法、合规授权，满足知识产权方面的有关规定和要求。

3. 乙方保证向甲方提供的服务成果是其独立实施完成，不存在任何侵犯第三方专利权、商标权、著作权等合法权益。如因乙方提供的服务成果侵犯任何第三方的合法权益，导致该第三方追究甲方责任的，乙方应负责解决并赔偿因此给甲方造成的全部损失。

4. 双方确定，甲方有权利用乙方按照本合同约定提供的研究开发成果，进行后续改进。由此产生的具有实质性或创造性技术进步特征的新的技术成果及其权利归属，由甲方享有。

第十三条　廉政承诺条款

1. 合同双方承诺共同加强廉洁自律、反对商业贿赂。

2. 甲方及其工作人员严格遵守《北京市政商交往负面清单》和《北京市广播电视局政商交往正负面清单》等相关廉洁纪律规定。

3. 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。

4. 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。

5. 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。

第十四条　违约责任

1. 甲乙双方违反本合同约定，违约方应当按《中华人民共和国民法典》的规定，承担违约责任。

2. 乙方未按本合同及附件约定完成边界防护、边界隔离、病毒防护、终端安全管理、防御支撑、脆弱性检测、安全加固、渗透测试、安全运营、等级保护测评、商用密码应用安全性评估、账号统一管理、网络安全设备维保、工具特征库和病毒库升级、授权更新、巡检、培训演练、技术服务报告或项目审计报告等工作的，甲方有权要求乙方限期整改。乙方逾期整改的，每延迟一日按合同总价的万分之五向甲方支付违约金；整改后仍不符合本合同及附件要求的，乙方应继续整改，并按合同总价 10%向甲方支付违约金。

3. 乙方未按本合同及附件约定在 2 小时内响应软硬件设备故障，或者未按一般故障 24 小时内修复、严重故障 72 小时内修复等要求处理故障的，每逾期满 24 小时按合同总价的万分之五向甲方支付违约金，不足 24 小时按 24 小时计算；因此影响网络安全防护、系统稳定运行或安全播出重保工作的，乙方还应赔偿甲方因此遭受的损失。

4. 乙方提交的脆弱性检测、安全加固、渗透测试、安全运营、等级保护测评、商用密码应用安全性评估、巡检报告或技术服务报告不真实、不完整，或者遗漏应当发现的重大风险、漏洞、配置缺陷或安全事件线索的，甲方有权要求乙方重新检测、补充报告并采取补救措施；乙方拒不补救或补救后仍不符合要求的，应按合同总价 10%向甲方支付违约金。

5. 乙方未经甲方书面同意，将网络安全监测、漏洞分析、应急处置等主体业务及关键性工作分包或转委托第三方的，甲方有权要求乙方限期改正；乙方拒不改正或因此影响服务质量、造成安全风险或损失的，甲方有权解除合同，乙方应承担违约责任并赔偿甲方损失。

6. 乙方发生本条约定的违约行为，经甲方书面催告后仍未改正，或者违约行为持续超过 30 日，或者违约行为已经导致甲方合同目的不能实现的，甲方有权解除本合同。合同解除的，乙方应向甲方返还已支付合同费用，并向甲方支付相当于合同总价 30%的违约金；违约金不足以弥补甲方损失的，乙方还应对不足部分承担赔偿责任。

7. 乙方违反本合同其他条款的，应支付合同总金额 10%的违约金，违约金不足以弥补甲方损失的，需另行补足。

第十五条　合同解除

1. 如果乙方破产、解散、清算、停业、濒临破产、受到行政处罚或因其他原因无力履行本合同时，甲方可在任何时候以书面通知乙方解除本合同。自甲方向乙方发出解除本合同的书面通知到达乙方时，本合同即告解除。

2. 本合同解除后，根据合同履行情况，甲方可以要求乙方恢复原状、采取补救措施，并有权要求赔偿损失。

第十六条　不可抗力

1. 本合同所称不可抗力是指不能预见、不能避免并不能克服的客观情况，包括但不限于战争、严重火灾、水灾、台风和地震、法规政策的变更以及其他双方书面同意属于不可抗力的情形。

2. 受不可抗力影响的一方应在不可抗力发生后，以最快的方式在最短的时间内通知另一方，并在不可抗力发生后 10 日内，将有关部门出具的证明文件直接送达或邮寄另一方。

3. 当不可抗力事件发生时，执行合同的期限可相应延长，不视为任何一方违

约。如果延长期限后合同仍不能履行的，双方均有权终止本合同。若合同终止，双方互不承担违约责任。但因一方迟延履行导致不可抗力的，不能免除责任。

第十七条　通知与送达

1. 本合同项下的通知、函件及其他书面文件，应以书面形式送达对方。送达方式包括当面递交、邮政特快专递（EMS）或电子邮箱、短信等电子方式。当面递交的，以签收之日为送达日；以邮政特快专递方式送达的，以寄出之日起第三个工作日视为送达日；以电子方式送达的，以发送成功的时间为送达日；受送达方拒绝签收或无法联系的，以邮件退回之日视为送达日。

2. 双方以本合同首部载明的地址，联系人、联系人电话、邮箱以及为有效送达地址。一方变更送达地址或联系方式的，应在变更后五个工作日内书面通知另一方；未履行通知义务的，按照原地址送达即视为有效送达。

3. 因本合同产生争议进入诉讼程序的，双方确认本合同首部载明的联络信息同时作为司法文书送达地址。一方未依本条第 2 款通知变更地址，致使人民法院的法律文书无法实际送达的，以向原地址邮寄之日即视为送达之日。

第十八条　争议的解决

1. 本合同依中华人民共和国现行法律法规（不包括香港和澳门特别行政区及台湾地区的法律法规）签署并据其解释。

2. 在执行本合同过程中，双方如若发生争议，应先协商解决，协商达成一致意见，须以书面形式并加盖公章确认方可有效；协商不成时，任何一方均有权将争议提交至甲方所在地有管辖权的人民法院解决。

第十九条　附则

1. 本合同经双方法定代表人或授权代表签字加盖公章或合同专用章后生效。签字日期不一致的，以最后签字日期为本合同生效日期。双方在加盖有效印章时务必加盖骑缝章。

2. 本合同一式陆份，以中文书写，甲方执肆份，乙方执贰份，具有同等法律效力。

3. 如需修改或补充本合同内容，经协商，双方应签署书面修改或补充合同，并将其作为本合同的组成部分。

（以下为签字盖章页）

甲方（盖章）：北京市广播电视监测中心

法定代表人或授权代表：

（签字）

签署日期：2026 年 6 月 1 日

地址：北京市通州区达济街 5 号院

邮政编码：101117

联系人：路程

电话：010-55565332

开户银行：北京银行潞城支行

账号：20000003326820112001009

乙方（盖章）：中移建设有限公司

法定代表人或授权代表：

（签字）

签署日期：2026 年 6 月 1 日

地址：北京市海淀区北蜂窝路 18 号（综合楼 9 层 906、907、917）

邮政编码：100038

联系人：王乐一

电话：13522867215

开户银行：中国建设银行北京金融街支行

账号：11001070800059000531

二、中标通知书

中标通知书

中移建设有限公司：

在我公司组织的监测系统运行维护（第六包：网络安全服务）（招标编号：11000026210200163956-XM001-6、0686-2611BJ074408Z/6）公开招标中，经评标委员会评审后，确定贵公司为中标单位，中标金额为人民币1,900,000.00元。

请贵公司接此中标通知后按规定与买方签订采购合同。

特此通知。

北京国际贸易有限公司

二〇二六年五月十九日

三、招标文件

（主要内容）

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2024年6月投入运行，2026年7月进入运维期，网络视听新媒体综合监管平台（升级改造项目）2026年投入运行，两大平台均为北京市安全播出指挥专网的重要组成部分。该指挥专网为北京市广播电视局核心关键网络，涉及与应急广播、指挥调度、各区融媒体中心、政务云的多类网络交互边界。本包采购相应的网络安全服务，以充分保障北京市安全播出指挥专网整体网络安全，确保各业务系统稳定可靠、不间断运行。

★说明：各项服务内容中所有软硬件维护升级、策略配置、授权更新以及人员、工具设备、耗材费用由中标人承担。投标人须出具承诺函，格式自拟、加盖公章。

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定级为等保二级，网络视听新媒体综合监管平台定级为等保三级。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)，上述两个平台需具备对应等保等级要求的安全防护功能。

（一）网络安全服务内容

根据等保2.0二级防护要求，对广播电视融合媒体智慧监管平台进行安全防护，对系统预警信息发布与可视指挥调度业务进行边界防护，对安全播出共享信息终端进行物理机防病毒软件、终端安全管理。

根据等保2.0三级防护要求，对网络视听新媒体综合监管平台进行安全防护，对系统与国家广播电视总局的三个部门业务系统对接提供边界防护，对系统与北京广播电视台广播端、电视端安全信息对接提供隔离防护，对网络视听监管、网络舆情监管等业务自系统账号进行统一管理，为局内工作人员和运维人员进行访问权限管理，减少业务系统的安全风险。

对上述平台，监测中心各业务系统进行防御支撑服务、脆弱性检测服务、安全加固服务、渗透测试服务、安全运营服务。对网络视听新媒体综合监管平台进行等保测评和商用密码应用安全性评估等。

（1）网络安全服务需求清单如下：

序号	名称	内容
1	边界防护服务	网络边界安全防护服务，围绕网络出入口构建防护屏障，通过精细化管控与智能拦截，保障内部网络与外部系统的安全隔离与合规交互。跨越边界的访问和数据流通过防火墙提供的受控接口进行通信，实现边界防护，抵御外部风险。
2	边界隔离服务	提供物理级别的安全隔离与可控数据交互服务，确保不同安全域之间“物理断开、逻辑可控”。去除网络协议，仅做数据传输，实现网络层的物理隔离，确保业务系统安全，防御可能出现的威胁入侵行为。
3	物理机防病毒服务	针对物理服务器、工作站等终端设备，提供全周期的恶意代码（病毒、木马、勒索软件等）检测与清除服务，构建终端设备的主动防御屏障。实现对重要物理机的定期检测和病毒防护、清除，抵御病毒威胁。
4	终端安全管理服务	针对所有终端设备，提供从设备接入到运行维护的全流程安全管理服务，实现终端状态可视、风险可控、合规可溯。对网络中的终端设备进行统一的管理，识别终端安全风险。构建终端风险体系并对终端风险进行终端安全管理，从而降低和避免终端安全风险事件的发生。
5	防御支撑服务	针对攻防演练、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，辅助采购人提供工作方案并协助完成材料准备、迎检等工作；在攻防演练中建立全方位的防守体系，其中一线项目团队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，二线支撑团队提供远程专家技术支持、疑难问题处置、威胁情报共享、事件分析溯源等工作；组织专业网络安全专家，通过专业、全面的信息安全理论、信息安全实践等培训，全面提高相关人员的安全意识水平和安全技术能力，切实提高内部信息安全管理能力，保证业务系统安全稳定运行。
6	脆弱性检测服务	对网络视听新媒体综合监管平台、广播电视融合媒体智慧监管平台的服务器操作系统、数据库、中间件、网络设备、安全设

		备和安全管理制度等进行脆弱性检测，采用工具扫描和手工检查相结合的方式对设备漏洞进行检查，排查主机等层面存在的安全隐患，结合安全措施有效性检测，通过专业化的数据分析，提供相关脆弱性检测文档。对上述 2 系统提供 4 次脆弱性检测。
7	安全加固服务	对网络视听新媒体综合监管平台、广播电视融合媒体智慧监管平台漏洞分析识别出的不符合项和脆弱性评估识别出的风险，编制加固整改措施方案，同时对主机、网络、应用安全等方面进行加固。对上述 2 系统提供 4 次安全加固。
8	渗透测试服务	对网络视听新媒体综合监管平台、广播电视融合媒体智慧监管平台进行 SQL 注入、跨脚本、 文件上传、 跨径遍历、蛮力攻击、信息泄露、缓冲区溢出等安全测试，挖掘系统中的安全缺陷和漏洞。并给出安全建议，指导系统运维单位进行修复等工作。对上述 2 系统提供 4 次渗透测试。
9	安全运营服务	对网络视听新媒体综合监管平台、广播电视融合媒体智慧监管平台及监测中心网络安全相关事务提供安全运营服务。通过远程和本地相结合的方式对系统进行梳理，识别关键资产和敏感数据；实时监测网络中的流量、安全日志、安全数据，实时分析系统告警信息，及时发现系统中存在的安全威胁、潜在风险，快速定位安全事件，减少因安全事件带来的损失损害；通过在不同区域发起针对验证标靶的各类攻击动作，检验网络安全防御体系是否完整、检验运营规则的有效性以及安全设备检测能力的有效性。对网络视听新媒体综合监管平台、广播电视融合媒体智慧监管平台发生的安全事件进行分析，提出改进意见，确保系统整体安全运行。根据密码安全、数据安全、供应链安全等最新要求，协助监测中心梳理、完善相关制度，确保中心网络安全各项工作有章可依。使用智能对话分析技术，以对话方式智能分析安全情况，完成快速安全事件判断和梳理，提升安全运营整体能力。
10	等保测评	根据国家网络安全相关政策和要求，对网络视听新媒体综合监

	服务	管平台进行等级保护测评和商用密码应用安全性评估，全面评估信息系统现有安全防护水平和相应等级安全要求之间的差距，测评内容包括技术安全测评、管理安全测评和综合测评，并出具测评报告。
11	账号统一管理服务	对现有政务云上的业务系统账号进行集中管理，实现人员一次性认证登录操作，避免账号丢失引起的安全隐患。为局内工作人员和运维人员进行账号的访问权限管理。对关键业务系统进行隐藏，减少业务系统的安全风险。为业务系统提供严格的密码管理，制定密码周期、复杂度、长度、超时锁定等规则。确保账号密码的可靠性。

表 1

（2）对现有网络安全设备软硬件维保。待维保设备清单如下：

序号	设备名称	品牌、规格、型号	数量
1	外网防火墙	网御星云 网御防火墙系统 V3.0 Power V6000（千兆）防火墙（增强级）（需对特征库进行升级）	1 台
2	WEB 应用防火墙	远江盛邦 Web 应用防护系统 W1000/V6.0 WEB 应用防火墙（国际-增强级）（需对特征库进行升级）	1 台
3	内网防火墙	网御星云 网御防火墙系统 V3.0 Power V6000（千兆）防火墙（增强级）（需对特征库进行升级）	2 台
4	综合安全审计设备	网御星云 网御网络审计系统 V3.0/LA-DT 网络通讯安全审计类（增强级）	1 台
5	入侵检测设备	网御星云 网御入侵检测系统（千兆）/V3.2 网络入侵检测系统（第三级）（需对特征库进行升级）	1 台
6	堡垒主机	网御星云 网御运维安全网关系统 LA-OS/V3.0 运维安全管理产品（增强级）	1 台
7	日志审计设备	网御星云 网御安全管理系统-日志审计 V3.0 日志分析（增强级）	1 台
8	安全信息采集引擎	网御星云 网御入侵检测系统（千兆）/V3.2 网络入侵检测系统（第三级）（需对特征库进行升级）	1 台
9	分路器	成都数维 定制开发型号	1 台

序号	设备名称	品牌、规格、型号	数量
10	安全运营平台软件	网御星云 网御安全管理系统 V3.0 安全管理平台	1套
11	物理机防病毒软件	猎鹰安全 猎鹰终端安全管理系统 V9.0 网络版防病毒产品（一级品）（需对特征库进行升级）	104套
12	虚拟化防病毒软件	360 终端安全管理系统 V10.0 网络版防病毒产品（增强级）（需对特征库进行升级）	1套
13	虚拟化主机安全管理	北信源 北信源内网安全管理系统 V8.1 内网主机监测（增强级）（需对特征库进行升级）	1套

表2

投标人须对上述安全服务和维保项作出分项报价。

（二）网络安全服务工具

根据监测中心业务特点、网络性能实际情况和网络安全等保二级、三级要求，投标人使用的网络安全服务工具（含软硬件）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。
	≥6个10/100/1000BASE-T端口、≥4个千兆SFP光纤插槽并配齐光模块、≥2个高速USB2.0接口，可接移动存储进行日志存储。
	吞吐量≥3.0Gbps，最大并发连接数≥200万。
	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。
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	具备中国网络安全审查技术与认证中心颁发的《网络关键设备和网络安全专用产品安全认证证书》。

2. 边界隔离工具

功能规格	性能配置要求
系统要求	采用“2+1”系统架构，即由两个主机系统和一个隔离交换模块组成；隔离交换模块基于专用芯片实现，保证数据在搬移的时间内，内、外网隔离卡与内、外网系统为断开状态。
	≥6 个 10/100/1000BASE-T 端口、≥2 个千兆 SFP 光纤插槽并配齐光模块。≥4 个高速 USB2.0 接口。
	吞吐量≥400Mbps，最大并发连接数≥6 万，延时＜1ms。
系统管理	内、外网主机分别具备三系统，即系统 A、系统 B 和备份系统。支持在 WEB 界面上配置启动顺序，在 A 系统发生故障时，可以切换到 B 系统；支

功能规格	性能配置要求
	持将当前运行系统备份。
访问控制	支持基于动态密码+本地密码的双因子认证方式。
文件交换	支持 NFS、CIFS（SAMBA）、FTP、SFTP 等文件系统；FTP 文件交换支持 SSL 加密。
	支持文件格式特征过滤；并能提供具备图形化界面的文件类型判断工具以帮助用户识别不常见文件类型。
	支持单任务文件统计及查询，可展示任务号、文件数、文件大小、文件名称、发送时间等信息，并根据结果进行查询。
数据库同步	支持同种数据库间（同构）和不同种数据库间（异构）的同步。
	支持病毒检测；支持达梦、人大金仓、Gbase、神通数据库、博阳、瀚高等主流国产数据库。
安全传输	支持 IPv4、IPv6 双协议栈接入。
	支持 HTTP/HTTPS/FTP/SMTP/POP3 等应用协议。
	支持任务策略命中数统计展示。
攻击防护	持抗攻击功能，能够识别和防御抗地址欺骗攻击、抗源路由攻击、抗 Smurf 攻击、抗 LAND 攻击、抗 Winnuke 攻击、抗 Queso 扫描、抗 SYN/FIN 扫描、抗 Null 扫描、抗圣诞树攻击、抗死亡之 PING 扫描、抗 fraggle 攻击、抗 TearDrop 攻击、抗 SYN Flood、抗 UDP Flood、抗 ICMP Flood 等。
系统管理	支持 HTTPS 的 Web 方式管理，实现了远程管理信息加密传输。
	内/外网主机系统分别具有独立管理接口，而不是采用低安全的管理方式，如通过业务口管理或通过内网唯一管理接口完成全部管理等。
日志审计与状态监控	支持 SNMP v1、v2、v3 版本，并支持 trap 方式。
	支持中文日志显示，并能实现内外网主机日志同步。
产品资质	具备中国网络安全审查技术与市场监管大数据中心颁发的《网络关键设备和网络安全专用产品安全认证证书》。

3. 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，33 个客户端和 6 台服务器端，最新版本病毒库并定期升级。

4. 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，33 个管理节点授权；软件为最新版本。

三、服务要求

1. 维护要求

（1）升级“二、服务内容（二）网络安全服务工具”中“1. 边界防护工具、2. 边界隔离工具、3. 物理机防病毒软件工具、4. 终端安全管理工具”中的特征库、病毒库，对系统的网络安全、数据安全情况进行检查和安全隐患处置，对工具授权进行更新。前述工具产权归投标人所有。

（2）软硬件设备发生故障的，2 小时内响应。严重故障 72 小时内修复；一般故障，24 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 1 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网络视听新媒体综合监管平台实际情况，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. 项目需求分析

投标人应根据采购人实际开展的各类监测监管业务、系统组成编制《项目需求分析》，内容应包括业务总体认识、需求理解、重点难点分析等。

3. 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，并在各安全

播出重保期前提供专项巡检。

4. 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。

5. 服务团队要求

（1）服务团队不少于 5 人，应包含项目负责人 1 人，团队成员不少于 4 人。整个团队应相对固定，人员具有 CISP 资质证书并具有专业 2 年以上（含）网络安全运维经验。

（2）★提供不少于 1 人的 5×8 小时现场应急响应和技术服务保障，做好系统状态检查、参数门限调整、系统巡检、故障应急处理等相关工作，确保系统稳定可靠运行。**投标人须出具承诺函，格式自拟、加盖公章。**

6. 备件要求

对于提供网络安全服务所需的软硬件和待维护软硬件设备，其中关键、核心设备应提供备件，存放于中标方指定地点，提供备品备件清单。

7. 其他要求

（1）必要时中标人负责联系协调设备原厂进行技术支持，相关费用由中标人负责。

（2）巡检维护、应急抢修产生的交通食宿费用由中标人负责。

（3）项目结束后提供项目审计报告。

四、服务期限

签订合同后 12 个月。

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。

六、采购标的所属行业

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。

七、验收

1.验收时间：合同期满后，中标人完全履行了合同所规定的条款，且无任何争议或遗留问题，采购人按照项目验收要求进行验收。

2.验收要求：

2.1 中标人提供的服务符合招标文件和合同条款要求。

2.2 服务期期满。

2.3 中标人提交的相关验收材料符合采购人要求。

四、投标文件

（主要内容）

一、合同条款偏离表

序号	招标文件条目号（页码）	招标文件要求	投标文件内容	偏离情况	说明
对本项目合同条款的偏离情况（应进行选择，未选择**投标无效**）： ☑**无偏离**（如无偏离，仅选择无偏离即可；无偏离即为对合同条款中的所有要求，均视作供应商已对之理解和响应。） ☐**有偏离**（如有偏离，则应在本表中对负偏离项逐一列明，否则**投标无效**；对合同条款中的所有要求，除本表列明的偏离外，均视作供应商已对之理解和响应。）					

二、采购需求偏离表

针对本招标文件《采购需求》中条款的偏离情况（应进行选择，未选择响应无效）：
☑无偏离（如无偏离，仅在此处勾选无偏离即可。无偏离即为对采购需求条款中的所有要求，均视作投标人已对之理解和响应。）

□有偏离（如有偏离，则应在此处进行勾选，同时在下表中对偏离项逐一列明，否则投标无效。对采购需求条款中的所有要求，除本表列明的偏离外，均视作投标人已对之理解和响应。）

序号	招标文件条目号(页码)	招标文件要求	投标响应内容	偏离情况	说明
	第五章 采购需求；第六包网络安全服务；一、概述（第16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2024年6月投入运行，2026年7月进入运维期，网络视听新媒体综合监管平台（升级改造项目）2026年投入运行，两大平台均为北京市安全播出指挥专网的重要组成部分。该指挥专网为北京市广播电视局核心关键网络，涉及与应急广播、指挥调度、各区融媒体中心、政务云的多类网络交互边界。本包采购相应的网络安全服务，以充分保障北京市安全播出指挥专网整体网络安全，确保各业务系统稳定可靠、不间断运行。 ★说明：各项服务内容中所有软硬件维护升级、策略配置、授权更新以及人员、工具设备、耗材费用由中标人承担。投标人须出具承诺函，格式自拟、加盖公章。	应答：完全满足 我公司将对该项目的项目概述进行全面且充分的了解，完成对该项目所要求的建设内容。 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2024年6月投入运行，2026年7月进入运维期，网络视听新媒体综合监管平台（升级改造项目）2026年投入运行，两大平台均为北京市安全播出指挥专网的重要组成部分。该指挥专网为北京市广播电视局核心关键网络，涉及与应急广播、指挥调度、各区融媒体中心、政务云的多类网络交互边界。本包采购相应的网络安全服务，以充分保障北京市安全播出指挥专网整体网络安全，确保各业务系统稳定可靠、不间断运行。 各项服务内容中所有软硬件维护升级、策略配置、授权更新以及人员、工具设备、耗材费用由我公司承担。我公司将出具承诺函，并加盖公章。承诺函详见“33、10-13招标文件要求提供或投标人认为应附的其他材料”中“10.3.4.1服务承诺函1”	无偏离	无
	第五章 采购需求；第六包	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	应答：完全满足 我公司将根据该项目招标要求，完成项目中所有的网	无偏离	无

	网络安全服务；二、服务内容（第16页）	管平台定级为等保二级，网络视听新媒体综合监管平台定级为等保三级。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)，上述两个平台需具备对应等保等级要求的安全防护功能。	络安全服务内容。 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定级为等保二级，网络视听新媒体综合监管平台定级为等保三级。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)，上述两个平台需具备对应等保等级要求的安全防护功能。		
	第五章 采购需求；第六包网络安全服务；二、服务内容；（一）网络安全服务内容（第16-17页）	根据等保2.0二级防护要求，对广播电视融合媒体智慧监管平台进行安全防护，对系统预警信息发布与可视指挥调度业务进行边界防护，对安全播出共享信息终端进行物理机防病毒软件、终端安全管理。 根据等保2.0三级防护要求，对网络视听新媒体综合监管平台进行安全防护，对系统与国家广播电视总局的三个部门业务系统对接提供边界防护，对系统与北京广播电视台广播端、电视端安全信息对接提供隔离防护，对网络视听监管、网络舆情监管等业务自系统账号进行统一管理，为局内工作人员和运维人员进行访问权限管理，减少业务系统的安全风险。 对上述平台，监测中心各业务系统进行防御支撑服务、脆弱性检测服务、安全加固服务、渗透测试服务、安全运营服务。对网络视听新媒体综合监管平台进行等保测评和商用密码应用安全性评估等。	应答：完全满足 我公司将根据等保2.0二级防护要求，对广播电视融合媒体智慧监管平台进行安全防护，对系统预警信息发布与可视指挥调度业务进行边界防护，对安全播出共享信息终端进行物理机防病毒软件、终端安全管理。 我公司将根据等保2.0三级防护要求，对网络视听新媒体综合监管平台进行安全防护，对系统与国家广播电视总局的三个部门业务系统对接提供边界防护，对系统与北京广播电视台广播端、电视端安全信息对接提供隔离防护，对网络视听监管、网络舆情监管等业务自系统账号进行统一管理，为局内工作人员和运维人员进行访问权限管理，减少业务系统的安全风险。 我公司将对上述平台，监测中心各业务系统进行防御支撑服务、脆弱性检测服务、安全加固服务、渗透测试服务、安全运营服务。对网络视听新媒体综合监管平台进行等保测评和商用密码应用安全性评估等。	无偏离	无
	第五章 采购需求；第六包网络安全服务；二、服务内容；（一）网络安全服务内容；（1）网	网络安全服务需求清单如下： 序号 名称 内容 1 边界防护服务 网络边界安全防护服务，围绕网络出入口构建防护屏障，通过精细化管控与智能拦截，保障内部网络与外部系统	应答：完全满足 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，完成该项目中要求的网络安全服务内容。 序号 名称 内容 1 边界防护服务 网络边界安全防护服务，围绕网络出入口构建防护屏	无偏离	无

	络安全服务需求清单（第17-19页）			的安全隔离与合规交互。跨越边界的访问和数据流通过防火墙提供的受控接口进行通信，实现边界防护，抵御外部风险。			障，通过精细化管控与智能拦截，保障内部网络与外部系统的安全隔离与合规交互。跨越边界的访问和数据流通过防火墙提供的受控接口进行通信，实现边界防护，抵御外部风险。		
		2	边界隔离服务	提供物理级别的安全隔离与可控数据交互服务，确保不同安全域之间“物理断开、逻辑可控”。去除网络协议，仅做数据传输，实现网络层的物理隔离，确保业务系统安全，防御可能出现的威胁入侵行为。	2	边界隔离服务	提供物理级别的安全隔离与可控数据交互服务，确保不同安全域之间“物理断开、逻辑可控”。去除网络协议，仅做数据传输，实现网络层的物理隔离，确保业务系统安全，防御可能出现的威胁入侵行为。		
		3	物理机防病毒服务	针对物理服务器、工作站等终端设备，提供全周期的恶意代码（病毒、木马、勒索软件等）检测与清除服务，构建终端设备的主动防御屏障。实现对重要物理机的定期检测和病毒防护、清除，抵御病毒威胁。	3	物理机防病毒服务	针对物理服务器、工作站等终端设备，提供全周期的恶意代码（病毒、木马、勒索软件等）检测与清除服务，构建终端设备的主动防御屏障。实现对重要物理机的定期检测和病毒防护、清除，抵御病毒威胁。提供1个管理中心，33个客户端和6台服务器端的物理机防病毒服务工具，确保最新版本病毒库并定期升级。		
		4	终端安全管理服务	针对所有终端设备，提供从设备接入到运行维护的全流程安全管理服务，实现终端状态可视、风险可控、合规可溯。对网络中的终端设备进行统一的管理，识	4	终端安全管理服务	针对所有终端设备，提供从设备接入到运行维护的全流程安全管理服务，实现终端状态可视、风险可控、合规可溯。对网络中的终端设备		

			别终端安全风险。构建终端风险体系并对终端风险进行终端安全管理，从而降低和避免终端安全风险事件的发生。			进行统一的管理，识别终端安全风险。构建终端风险体系并对终端风险进行终端安全管理，从而降低和避免终端安全风险事件的发生。提供1个管理中心，33个管理节点授权终端安全管理服务工具；确保软件为最新版本。		
		5	防御支撑服务	针对攻防演练、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，辅助采购人提供工作方案并协助完成材料准备、迎检等工作；在攻防演练中建立全方位的防守体系，其中一线项目团队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，二线支撑团队提供远程专家技术支持、疑难问题处置、威胁情报共享、事件分析溯源等工作；组织专业网络安全专家，通过专业、全面的信息安全理论、信息安全实践等培训，全面提高相关人员的安全意识水平和安全技术能力，切实提高内部信息安全管理能力，保证业务系统安全稳定运行。	5	防御支撑服务	针对攻防演练、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，辅助采购人提供工作方案并协助完成材料准备、迎检等工作；在攻防演练中建立全方位的防守体系，其中一线项目团队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，二线支撑团队提供远程专家技术支持、疑难问题处置、威胁情报共享、事件分析溯源等工作；组织专业网络安全专家，通过专业、全面的信息安全理论、信息安全实践等培训，全面提高相关人员的安全意识水平和安全技术能力，切实提高内部信息安全管理能力，保证业务系统安全稳定运行。		
					6	脆弱性检测	对网络视听新媒体综合监管		

		6	脆弱性检测服务	对网络视听新媒体综合监管平台、广播电视融合媒体智慧监管平台的服务器操作系统、数据库、中间件、网络设备、安全设备和安全管理制度等进行脆弱性检测，采用工具扫描和手工检查相结合的方式对设备漏洞进行检查，排查主机等层面存在的安全隐患，结合安全措施有效性检测，通过专业化的数据分析，提供相关脆弱性检测文档。对上述2系统提供4次脆弱性检测。				
		7	安全加固服务	对网络视听新媒体综合监管平台、广播电视融合媒体智慧监管平台漏洞分析识别出的不符合项和脆弱性评估识别出的风险，编制加固整改措施方案，同时对主机、网络、应用安全等方面进行加固。对上述2系统提供4次安全加固。				
		8	渗透测试服务	对网络视听新媒体综合监管平台、广播电视融合媒体智慧监管平台进行SQL注入、跨脚本、				

		9	安全运营服务	文件上传、跨径遍历、蛮力攻击、信息泄露、缓冲区溢出等安全测试，挖掘系统中的安全缺陷和漏洞。并给出安全建议，指导系统运维单位进行修复等工作。对上述2系统提供4次渗透测试。 对网络视听新媒体综合监管平台、广播电视融合媒体智慧监管平台及监测中心网络安全相关事务提供安全运营服务。通过远程和本地相结合的方式对系统进行梳理，识别关键资产和敏感数据；实时监测网络中的流量、安全日志、安全数据，实时分析系统告警信息，及时发现系统中存在的安全威胁、潜在风险，快速定位安全事件，减少因安全事件带来的损失损害；通过在不同区域发起针对验证标靶的各类攻击动作，检验网络安全防御体系是否完整、检验运营规则的有效性以及安全设备检测能力的有效性。对网络视听	9	安全运营服务	渗透测试。 对网络视听新媒体综合监管平台、广播电视融合媒体智慧监管平台及监测中心网络安全相关事务提供安全运营服务。通过远程和本地相结合的方式对系统进行梳理，识别关键资产和敏感数据；实时监测网络中的流量、安全日志、安全数据，实时分析系统告警信息，及时发现系统中存在的安全威胁、潜在风险，快速定位安全事件，减少因安全事件带来的损失损害；通过在不同区域发起针对验证标靶的各类攻击动作，检验网络安全防御体系是否完整、检验运营规则的有效性以及安全设备检测能力的有效性。对网络视听新媒体综合监管平台、广播电视融合媒体智慧监管平台发生的安全事件进行分析，提出改进意见，确保系统整体安全运行。根据密码安全、数据安全、供应链安全等最新要求，协助监测中心梳理、完善相关制度，确保中心网络安全各项工作有章可依。使用智能对话分析技术，以对话方式智能分析安全情况，完成快速安全事		

				新媒体综合监管平台、广播电视融合媒体智慧监管平台发生的安全事件进行分析，提出改进意见，确保系统整体安全运行。根据密码安全、数据安全、供应链安全等最新要求，协助监测中心梳理、完善相关制度，确保中心网络安全各项工作有章可依。使用智能对话分析技术，以对话方式智能分析安全情况，完成快速安全事件判断和梳理，提升安全运营整体能力。			件判断和梳理，提升安全运营整体能力。		
		10	等保测评服务	根据国家网络安全相关政策和要求，对网络视听新媒体综合监管平台进行等级保护测评和商用密码应用安全性评估，全面评估信息系统现有安全防护水平和相应等级安全要求之间的差距，测评内容包括技术安全测评、管理安全测评和综合测评，并出具测评报告。	10	等保测评服务	根据国家网络安全相关政策和要求，对网络视听新媒体综合监管平台进行等级保护测评和商用密码应用安全性评估，全面评估信息系统现有安全防护水平和相应等级安全要求之间的差距，测评内容包括技术安全测评、管理安全测评和综合测评，并出具测评报告。		
		11	账号统一管理服务	对现有政务云上的业务系统账号进行集中管理，实现人员一次性认	11	账号统一管理服务	对现有政务云上的业务系统账号进行集中管理，实现人员一次性认证登录操作，避免账号丢失引起的安全隐患。为局内工作人员和运维人员进行账号的访问权限管理。对关键业务系统进行隐藏，减少业务系统的安全风险。为业务系统提供严格的密码管理，制定密码周期、复杂度、长度、超时锁定等规则。确保账号密码的可靠性。		
					表 1				

		证登录操作，避免账号丢失引起的安全隐患。为局内工作人员和运维人员进行账号的访问权限管理。对关键业务系统进行隐藏，减少业务系统的安全风险。为业务系统提供严格的密码管理，制定密码周期、复杂度、长度、超时锁定等规则。确保账号密码的可靠性。 表 1			
	第五章 采购需求；第六包网络安全服务；二、服务内容；（一）网络安全服务内容；（1）对现有网络安全设备软硬件维保。待维保设备清单（第19-20页）	对现有网络安全设备软硬件维保。待维保设备清单如下： 序号 设备名称 品牌、规格、型号 数量 1 外网防火墙 网御星云 网御防火墙系统 V3.0 Power V6000（千兆）防火墙（增强级）（需对特征库进行升级） 1台 2 WEB 应用防火墙 远江盛邦 Web 应用防护系统 W1000/V6.0 WEB 应用防火墙（国际-增强级）（需对特征库进行升级） 1台 3 内网防火墙 网御星云 网御防火墙系统 V3.0 Power V6000（千兆）防火墙（增强级） 2台	应答：完全满足 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，完成该项目中要求的现有网络安全设备软硬件维保内容，完成设备的维保升级，具体维保设备清单如下： 序号 设备名称 品牌、规格、型号 数量 1 外网防火墙 网御星云 网御防火墙系统 V3.0 Power V6000（千兆）防火墙（增强级）（对特征库进行升级） 1台 2 WEB 应用防火墙 远江盛邦 Web 应用防护系统 W1000/V6.0 WEB 应用防火墙（国际-增强级）（对特征库进行升级） 1台 3 内网防火墙 网御星云 网御防火墙系统 V3.0 Power V6000（千兆）防火 2台	无偏离	无

				（需对特征库进行升级）					墙（增强级）（对特征库进行升级）		
		4	综合安全审计设备	网御星云 网御网络审计系统 V3.0/LA-DT 网络通讯安全审计类（增强级）	1台	4	综合安全审计设备	网御星云 网御网络审计系统 V3.0/LA-DT 网络通讯安全审计类（增强级）	1台		
		5	入侵检测设备	网御星云 网御入侵检测系统（千兆）/V3.2 网络入侵检测系统（第三级）（需对特征库进行升级）	1台	5	入侵检测设备	网御星云 网御入侵检测系统（千兆）/V3.2 网络入侵检测系统（第三级）（对特征库进行升级）	1台		
		6	堡垒主机	网御星云 网御运维安全网关系统 LA-OS/V3.0 运维安全管理产品（增强级）	1台	6	堡垒主机	网御星云 网御运维安全网关系统 LA-OS/V3.0 运维安全管理产品（增强级）	1台		
		7	日志审计设备	网御星云 网御安全管理系统-日志审计 V3.0 日志分析（增强级）	1台	7	日志审计设备	网御星云 网御安全管理系统-日志审计 V3.0 日志分析（增强级）	1台		
		8	安全信息采集引擎	网御星云 网御入侵检测系统（千兆）/V3.2 网络入侵检测系统（第三级）（需对特征库进行升级）	1台	8	安全信息采集引擎	网御星云 网御入侵检测系统（千兆）/V3.2 网络入侵检测系统（第三级）（对特征库进行升级）	1台		
		9	分路器	成都数维 定制开发型号	1台	9	分路器	成都数维 定制开发型号	1台		
		10	安全运营平台软件	网御星云 网御安全管理系统 V3.0 安全管理平台	1套	10	安全运营平台软件	网御星云 网御安全管理系统 V3.0 安全管理平台	1套		
						11	物理机防病毒软件	猎鹰安全 猎鹰终端安全管理系统 V9.0 网络版防病毒产品（一	104套		

		11 物理机防病毒软件 猎鹰安全 猎鹰终端安全管理系统 V9.0 网络版防病毒产品（一级品）（需对特征库进行升级） 104 套 12 虚拟化防病毒软件 360 终端安全管理系统 V10.0 网络版防病毒产品（增强级）（需对特征库进行升级） 1 套 13 虚拟化主机安全管理 北信源 北信源内网安全管理系统 V8.1 内网主机监测（增强级）（需对特征库进行升级） 1 套 表 2 投标人须对上述安全服务和维保项作出分项报价。		级品）（对特征库进行升级） 12 虚拟化防病毒软件 360 终端安全管理系统 V10.0 网络版防病毒产品（增强级）（对特征库进行升级） 1 套 13 虚拟化主机安全管理 北信源 北信源内网安全管理系统 V8.1 内网主机监测（增强级）（对特征库进行升级） 1 套 表 2 我公司将对上述安全服务和维保项作出分项报价，具体报价详见“4 投标分项报价表”		
	第五章 采购需求；第六包网络安全服务；二、服务内容；（二）网络安全服务工具（第 20 页）	根据监测中心业务特点、网络性能实际情况和网络安全等保二级、三级要求，投标人使用的网络安全服务工具（含软硬件）功能性能配置应满足以下要求。		应答：完全满足 我公司将根据监测中心业务特点、网络性能实际情况和网络安全等保二级、三级要求，我公司使用的网络安全服务工具（含软硬件）功能性能配置应满足以下要求。	无偏离	无	
	第五章 采购需求；第六包网络安全服务；二、服务内容；（二）	功能规格	性能配置要求	边界防护工具性能配置	无偏离	无	
		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。	应答：完全满足 我公司将提供符合该项目要求的边界防护工具。 采用专用架构平台和专用安全操作系统，无通用操作			

	网络安全服务工具；1.边界防护工具（第20-22页）			系统漏洞：硬件和软件为最新版本。		
			≥6个10/100/1000BASE-T端口、≥4个千兆SFP光纤插槽并配齐光模块、≥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 我公司将提供符合该项目要求的边界防护工具。 6个10/100/1000BASE-T端口、4个千兆SFP光纤插槽并配齐光模块、2个高速USB2.0接口，可接移动存储进行日志存储。	无偏离	无
			吞吐量≥3.0Gbps，最大并发连接数≥200万。	应答：完全满足 我公司将提供符合该项目要求的边界防护工具。 吞吐量：3.0Gbps，最大并发连接数：200万。	无偏离	无
			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。	应答：完全满足 我公司将提供符合该项目要求的边界防护工具。 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
		访问控制	基于状态检测的动态包过滤。	应答：完全满足 我公司将提供符合该项目要求的边界防护工具。 基于状态检测的动态包过滤。	无偏离	无
			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 我公司将提供符合该项目要求的边界防护工具。 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
			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。	应答：完全满足 我公司将提供符合该项目要求的边界防护工具。 支持同一主机源会话、目的会话分别管理和限制，支持设定网段内并发连接限制。	无偏离	无
			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 我公司将提供符合该项目要求的边界防护工具。 支持应用层访问控制，包括P2P软件、网游软件等	无偏离	无
			支持一体化安全策略配置，实现用户认证、IPS、AV、URL过	应答：完全满足 我公司将提供符合该项目要求的边界防护工具。	无偏离	无

			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。	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。	应答：完全满足 我公司将提供符合该项目要求的边界防护工具。 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。	无偏离	无
		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 我公司将提供符合该项目要求的边界防护工具。 支持透明、路由、混合三种工作模式。	无偏离	无
			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 我公司将提供符合该项目要求的边界防护工具。 支持静态路由，动态路由（OSPF、RIP 等），VLAN 间路由，组播路由等。	无偏离	无
		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。	应答：完全满足 我公司将提供符合该项目要求的边界防护工具。 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。	无偏离	无
		主动防御	能主动屏蔽恶意地址。	应答：完全满足 我公司将提供符合该项目要求的边界防护工具。 能主动屏蔽恶意地址。	无偏离	无
			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 我公司将提供符合该项目要求的边界防护工具。 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。	无偏离	无
		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 我公司将提供符合该项目要求的边界防护工具。 支持数字证书和电子钥匙方式，支持 SNMP 管理，与	无偏离	无

				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。	应答：完全满足 我公司将提供符合该项目要求的边界防护工具。 支持日志中文化，可显示配置命令日志的操作人。	无偏离	无
		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 我公司将提供符合该项目要求的边界防护工具。 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。	无偏离	无
			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 我公司将提供符合该项目要求的边界防护工具。 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。	无偏离	无
		产品资质	具备中国网络安全审查技术与认证中心颁发的《网络关键设备和网络安全专用产品安全认证证书》。	应答：完全满足 我公司将提供符合该项目要求的边界防护工具。 具备中国网络安全审查技术与认证中心颁发的《网络关键设备和网络安全专用产品安全认证证书》。具体证书详见“33、10-13 招标文件要求提供或投标人认为应附的其他材料”中的“10.3.1.1 边界防护工具”部分	无偏离	无
	第五章 采购需求；第六包 网络安全服务；二、服务内容；（二）网络安全服务工具；2.边界隔离工具（第 22-24 页）	功能规格	性能配置要求	边界隔离工具性能配置	无偏离	无
		系统要求	采用“2+1”系统架构，即由两个主机系统和一个隔离交换模块组成；隔离交换模块基于专用芯片实现，保证数据在搬移的时间内，内、外网隔离卡与内、外网系统为断开状态。	应答：完全满足 我公司将提供符合该项目要求的边界隔离工具。 采用“2+1”系统架构，即由两个主机系统和一个隔离交换模块组成；隔离交换模块基于专用芯片实现，保证数据在搬移的时间内，内、外网隔离卡与内、外网系统为断开状态。		
			≥ 6 个 10/100/1000BASE-T 端口、≥2 个千兆 SFP 光纤插槽并配齐光模块。≥4 个高速 USB2.0 接口。	应答：完全满足 我公司将提供符合该项目要求的边界隔离工具。 6 个 10/100/1000BASE-T 端口、2 个千兆 SFP 光纤插槽并配齐光模块。4 个高速 USB2.0 接口。	无偏离	无

			吞吐量≥400Mbps，最大并发连接数≥6万，延时＜1ms。	应答：完全满足 我公司将提供符合该项目要求的边界隔离工具。 吞吐量：400Mbps，最大并发连接数：6万，延时＜1ms。	无偏离	无
		系统管理	内、外网主机分别具备三系统，即系统A、系统B和备份系统。支持在WEB界面上配置启动顺序，在A系统发生故障时，可以切换到B系统；支持将当前运行系统备份。	应答：完全满足 我公司将提供符合该项目要求的边界隔离工具。 内、外网主机分别具备三系统，即系统A、系统B和备份系统。支持在WEB界面上配置启动顺序，在A系统发生故障时，可以切换到B系统；支持将当前运行系统备份。	无偏离	无
		访问控制	支持基于动态密码+本地密码的双因子认证方式。	应答：完全满足 我公司将提供符合该项目要求的边界隔离工具。 支持基于动态密码+本地密码的双因子认证方式。	无偏离	无
		文件交换	支持NFS、CIFS（SAMBA）、FTP、SFTP等文件系统；FTP文件交换支持SSL加密。	应答：完全满足 我公司将提供符合该项目要求的边界隔离工具。 支持NFS、CIFS（SAMBA）、FTP、SFTP等文件系统；FTP文件交换支持SSL加密。	无偏离	无
			支持文件格式特征过滤；并能提供具备图形化界面的文件类型判断工具以帮助用户识别不常见文件类型。	应答：完全满足 我公司将提供符合该项目要求的边界隔离工具。 支持文件格式特征过滤；并能提供具备图形化界面的文件类型判断工具以帮助用户识别不常见文件类型。	无偏离	无
			支持单任务文件统计及查询，可展示任务号、文件数、文件大小、文件名称、发送时间等信息，并根据结果进行查询。	应答：完全满足 我公司将提供符合该项目要求的边界隔离工具。 支持单任务文件统计及查询，可展示任务号、文件数、文件大小、文件名称、发送时间等信息，并根据结果进行查询。	无偏离	无
		数据库同步	支持同种数据库间（同构）和不同种数据库间（异构）的同步。	应答：完全满足 我公司将提供符合该项目要求的边界隔离工具。 支持同种数据库间（同构）和不同种数据库间（异构）的同步。	无偏离	无

			支持病毒检测；支持达梦、人大金仓、Gbase、神通数据库、博阳、瀚高等主流国产数据库。	应答：完全满足 我公司将提供符合该项目要求的边界隔离工具。 支持病毒检测；支持达梦、人大金仓、Gbase、神通数据库、博阳、瀚高等主流国产数据库。	无偏离	无
		安全传输	支持 IPv4、IPv6 双协议栈接入。	应答：完全满足 我公司将提供符合该项目要求的边界隔离工具。 支持 IPv4、IPv6 双协议栈接入。	无偏离	无
			支持 HTTP/HTTPS/FTP/SMTP/POP3 等应用协议。	应答：完全满足 我公司将提供符合该项目要求的边界隔离工具。 支持 HTTP/HTTPS/FTP/SMTP/POP3 等应用协议。	无偏离	无
			支持任务策略命中数统计展示。	应答：完全满足 我公司将提供符合该项目要求的边界隔离工具。 支持任务策略命中数统计展示。	无偏离	无
		攻击防护	持抗攻击功能，能够识别和防御抗地址欺骗攻击、抗源路由攻击、抗 Smurf 攻击、抗 LAND 攻击、抗 Winnuke 攻击、抗 Queso 扫描、抗 SYN/FIN 扫描、抗 Null 扫描、抗圣诞树攻击、抗死亡之 PING 扫描、抗 fraggle 攻击、抗 TearDrop 攻击、抗 SYN Flood、抗 UDP Flood、抗 ICMP Flood 等。	应答：完全满足 我公司将提供符合该项目要求的边界隔离工具。 支持抗攻击功能，能够识别和防御抗地址欺骗攻击、抗源路由攻击、抗 Smurf 攻击、抗 LAND 攻击、抗 Winnuke 攻击、抗 Queso 扫描、抗 SYN/FIN 扫描、抗 Null 扫描、抗圣诞树攻击、抗死亡之 PING 扫描、抗 fraggle 攻击、抗 TearDrop 攻击、抗 SYN Flood、抗 UDP Flood、抗 ICMP Flood 等。	无偏离	无
		系统管理	支持 HTTPS 的 Web 方式管理，实现了远程管理信息加密传输。	应答：完全满足 我公司将提供符合该项目要求的边界隔离工具。 支持 HTTPS 的 Web 方式管理，实现了远程管理信息加密传输。	无偏离	无
			内/外网主机系统分别具有独立管理接口，而不是采用低安全的管理方式，如通过业务口管理或通过内网唯一管理接口完成全部管理等。	应答：完全满足 我公司将提供符合该项目要求的边界隔离工具。 内/外网主机系统分别具有独立管理接口，而不是采用低安全的管理方式，如通过业务口管理或通过内网唯一管理接口完成全部管理等。	无偏离	无

		日志审计与状态监控	支持 SNMP v1、v2、v3 版本，并支持 trap 方式。	应答：完全满足 我公司将提供符合该项目要求的边界隔离工具。 支持 SNMP v1、v2、v3 版本，并支持 trap 方式。	无偏离	无
			支持中文日志显示，并能实现内外网主机日志同步。	应答：完全满足 我公司将提供符合该项目要求的边界隔离工具。 支持中文日志显示，并能实现内外网主机日志同步。	无偏离	无
		产品资质	具备中国网络安全审查技术与市场监管大数据中心颁发的《网络关键设备和网络安全专用产品安全认证证书》。	应答：完全满足 我公司将提供符合该项目要求的边界隔离工具。 具备中国网络安全审查技术与市场监管大数据中心颁发的《网络关键设备和网络安全专用产品安全认证证书》。具体证书详见“33、10-13 招标文件要求提供或投标人认为应附的其他材料”中的“10.3.1.2 边界隔离工具”部分。	无偏离	无
	第五章 采购需求；第六包网络安全服务；二、服务内容；（二）网络安全服务工具；3. 物理机防病毒软件工具（第 24 页）	功能规格	性能配置要求	物理机防病毒软件工具性能配置	无偏离	无
		产品配置	不少于 1 个管理中心，33 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 我公司将提供符合该项目要求的物理机防病毒软件工具。 1 个管理中心，33 个客户端和 6 台服务器端，最新版本病毒库并定期升级。		
	第五章 采购需求；第六包网络安全服务；二、服务内容；（二）网络安全服务工具；4.终端安全管理工具（第 24 页）	功能规格	性能配置要求	终端安全管理工具性能配置	无偏离	无
		产品配置	不少于 1 个管理中心，33 个管理节点授权；软件为最新版本。	应答：完全满足 我公司将提供符合该项目要求的终端安全管理工具。 1 个管理中心，33 个管理节点授权；软件为最新版本。		

	第五章 采购需求；第六包网络安全服务；三、服务要求；1.维护要求（第24-25页）	（1）升级“二、服务内容（二）网络安全服务工具”中“1.边界防护工具、2.边界隔离工具、3. 物理机防病毒软件工具、4.终端安全管理工具”中的特征库、病毒库，对系统的网络安全、数据安全情况进行检查和安全隐患处置，对工具授权进行更新。前述工具产权归投标人所有。	应答：完全满足 （1）我公司将负责升级“二、服务内容（二）网络安全服务工具”中“1.边界防护工具、2.边界隔离工具、3. 物理机防病毒软件工具、4.终端安全管理工具”中的特征库、病毒库，对系统的网络安全、数据安全情况进行检查和安全隐患处置，对工具授权进行更新。前述工具产权归我公司所有。	无偏离	无
		（2）软硬件设备发生故障的，2小时内响应。严重故障72小时内修复；一般故障，24小时内修复。	应答：完全满足 （2）软硬件设备发生故障的我公司将在2小时内响应。严重故障72小时内修复；一般故障，24小时内修复。	无偏离	无
		（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。	应答：完全满足 （3）我公司在每次服务完成后提交技术服务报告，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。	无偏离	无
		（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。	应答：完全满足 （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。	无偏离	无
		（5）服务期为监测中心技术人员提供1次网络安全技术培训。	应答：完全满足 （5）我公司在服务期内为监测中心技术人员提供1次网络安全技术培训。	无偏离	无
		（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网络视听新媒体综合监管平台实际情况，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。	应答：完全满足 （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网络视听新媒体综合监管平台实际情况，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。	无偏离	无
		（7）配合监测中心做好网络安全检查有关工作。	应答：完全满足 （7）我公司将配合监测中心做好网络安全检查有关工作。	无偏离	无

	第五章 采购需求；第六包网络安全服务；三、服务要求；2.项目需求分析（第25页）	投标人应根据采购人实际开展的各类监测监管业务、系统组成编制《项目需求分析》，内容应包括业务总体认识、需求理解、重点难点分析等。	应答：完全满足 我公司将根据北京市广播电视监测中心实际开展的各类监测监管业务、系统组成编制《项目需求分析》，内容应包括业务总体认识、需求理解、重点难点分析等。	无偏离	无
	第五章 采购需求；第六包网络安全服务；三、服务要求；3.巡检要求（第25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，并在各安全播出重保期前提供专项巡检。	应答：完全满足 我公司将根据项目情况和北京市广播电视监测中心的系统运行情况，提供详细具体的巡检方案，每月对网络安全设备进行巡检，并在各安全播出重保期前提供专项巡检。	无偏离	无
	第五章 采购需求；第六包网络安全服务；三、服务要求；4.服务方案和应急预案（第25页）	应提供详细具体、可行、有针对性的服务方案和应急预案。	应答：完全满足 我公司将根据项目情况和北京市广播电视监测中心的系统运行情况，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
	第五章 采购需求；第六包网络安全服务；三、服务要求；5.服务团队要求（第25页）	（1）服务团队不少于5人，应包含项目负责人1人，团队成员不少于4人。整个团队应相对固定，人员具有CISP资质证书并具有专业2年以上（含）网络安全运维经验。	应答：完全满足 （1）我公司服务团队具有5人，包含项目负责人1人，团队成员4人。整个团队确保固定，所有人员均具有CISP资质证书并具有专业2年以上（含）网络安全运维经验。	无偏离	无
		（2）★提供不少于1人的5×8小时现场应急响应和技术服务保障，做好系统状态检查、参数门限调整、系统巡检、故障应急处理等相关工作，确保系统稳定可靠运行。投标人须出具承诺函，格式自拟、加盖公章。	应答：完全满足 （2）我公司将提供1人的5×8小时现场应急响应和技术服务保障，做好系统状态检查、参数门限调整、系统巡检、故障应急处理等相关工作，确保系统稳定可靠运行。我公司将出具承诺函，并加盖公章。承诺函	无偏离	无

			详见“33、10-13 招标文件要求提供或投标人认为应附的其他材料”中“10.3.5.2 服务承诺函 2”		
	第五章 采购需求：第六包网络安全服务；三、服务要求；6.备件要求（第 25-26 页）	对于提供网络安全服务所需的软硬件和待维护软硬件设备，其中关键、核心设备应提供备件，存放于中标方指定地点，提供备品备件清单。	应答：完全满足 对于提供网络安全服务所需的软硬件和待维护软硬件设备，其中关键、核心设备我公司将提供备件，存放于指定地点，我公司将提供备品备件清单。备品备件清单详见“30、10-11 备品备件”	无偏离	无
	第五章 采购需求：第六包网络安全服务；三、服务要求；7.其他要求（第 26 页）	（1）必要时中标人负责联系协调设备原厂进行技术支持，相关费用由中标人负责。	应答：完全满足 （1）必要时我公司负责联系协调设备原厂进行技术支持，相关费用由我公司负责。	无偏离	无
		（2）巡检维护、应急抢修产生的交通食宿费用由中标人负责。	应答：完全满足 （2）巡检维护、应急抢修产生的交通食宿费用由我公司负责。	无偏离	无
		（3）项目结束后提供项目审计报告。	应答：完全满足 （3）项目结束后我公司将提供项目审计报告。	无偏离	无
	第五章 采购需求；第六包网络安全服务；四、服务期限（第 26 页）	签订合同后 12 个月。	应答：完全满足 我公司将严格按照项目的要求，签订合同后 12 个月的服务期限。	无偏离	无
	第五章 采购需求；第六包网络安全服务；五、廉政要求（第 26 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。	应答：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	无偏离	无

			排采购人工作人员参加宴请及娱乐活动。		
	第五章 采购需求；第六包网络安全服务；六、采购标的所属行业（第 26 页）	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。	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。	无偏离	无
	第五章 采购需求；第六包网络安全服务；七、验收（第 26-27 页）	1.验收时间：合同期满后，中标人完全履行了合同所规定的条款，且无任何争议或遗留问题，采购人按照项目验收要求进行验收。 2.验收要求： 2.1 中标人提供的服务符合招标文件和合同条款要求。 2.2 服务期期满。 2.3 中标人提交的相关验收材料符合采购人要求。	应答：完全满足 1.验收时间：合同期满后，我公司完全履行了合同所规定的条款，且无任何争议或遗留问题，采购人按照项目验收要求进行验收。 2.验收要求： 2.1 我公司提供的服务符合招标文件和合同条款要求。 2.2 服务期期满。 2.3 我公司提交的相关验收材料符合采购人要求。	无偏离	无

三、服务承诺

服务承诺函 1

尊敬的北京市广播电视监测中心/北京国际贸易有限公司：

中移建设有限公司为监测系统运行维护（第六包 网络安全服务）提供如下服务承诺：

★各项服务内容中所有软硬件维护升级、策略配置、授权更新以及人员、工具设备、耗材费用由我公司承担。

投标人名称：中移建设有限公司

日期：2026年05月11日

服务承诺函 2

尊敬的北京市广播电视监测中心/北京国际贸易有限公司：

中移建设有限公司为监测系统运行维护（第六包 网络安全服务）提供如下服务承诺：

★我公司提供1人（李宁，具备CISP资质证书）的5×8小时现场应急响应和技术服务保障，做好系统状态检查、参数门限调整、系统巡检、故障应急处理等相关工作，确保系统稳定可靠运行。

投标人名称：中移建设有限公司

日期：2026年05月11日

服务承诺函 3

尊敬的北京市广播电视监测中心/北京国际贸易有限公司：

中移建设有限公司为监测系统运行维护（第六包 网络安全服务）提供如下服务承诺：

满足本项目中的所有服务要求：

1. 满足本项目维护要求

（1）我公司将负责升级“二、服务内容（二）网络安全服务工具”中“1.边界防护工具、2.边界隔离工具、3. 物理机防病毒软件工具、4.终端安全管理工具”中的特征库、病毒库，对系统的网络安全、数据安全情况进行检查和安全隐患处置，对工具授权进行更新。前述工具产权归我公司所有。

（2）软硬件设备发生故障的我公司将在2小时内响应。严重故障72小时内修复；一般故障，24小时内修复。

（3）我公司在每次服务完成后提交技术服务报告，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）我公司在服务期内为监测中心技术人员提供1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网络视听新媒体综合监管平台实际情况，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）我公司将配合监测中心做好网络安全检查有关工作。

2.满足本项目需求分析

我公司将根据北京市广播电视监测中心实际开展的各类监测监管业务、系统组成编制《项目需求分析》，内容应包括业务总体认识、需求理解、重点难点分析等。

3. 满足本项目巡检要求

我公司将根据项目情况和北京市广播电视监测中心的系统运行情况，提供详细具体的巡检方案，每月对网络安全设备进行巡检，并在各安全播出重保期前提供专项巡检。

4. 满足本项目服务方案和应急预案要求

我公司将根据项目情况和北京市广播电视监测中心的实践系统运行情况，提供详细具体、可行、有针对性的服务方案和应急预案。

5. 满足本项目服务团队要求

（1）我公司服务团队具有5人，包含项目负责人1人，团队成员4人。整个团队确保固定，所有人员均具有CISP资质证书并具有专业2年以上（含）网络安全运维经验。

（2）我公司将提供1人（高莹蓓，具备CISP资质证书）的5×8小时现场应急响应和技术服务保障，做好系统状态检查、参数门限调整、系统巡检、故障应急处理等相关工作，确保系统稳定可靠运行。

6. 满足本项目备件要求

对于提供网络安全服务所需的软硬件和待维护软硬件设备，其中关键、核心设备我公司将提供备件，存放于指定地点，我公司将提供备品备件清单。具体备品备件清单如下：

序号	备品备件名称	备品备件规格	数量
1.	边界防护工具	标准机架式设备，冗余电源；标准配置6个10/100/1000BASE-T端口、4个千兆SFP光纤插槽并配齐光模块、2个高速USB2.0接口，可接移动存储进行日志存储。吞吐量:3.0Gbps，最大并发连接数:200万。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。	按需
2.	边界隔离工具	标准机架式设备，冗余电源，标准配置6个10/100/1000BASE-T端口、2个千兆SFP光纤插槽并配齐光模块。4个高速USB2.0接口。吞吐量400Mbps，最大并发连接数6万，延时＜1ms。	按需
3.	物理机防病毒软件工具	能够对已知、未知病毒、木马、恶意程序等进行检测、清除。具备系统文件监控能力，能够监控计算机系统所有活跃文件的安全性。杀毒软件管理端须具备集中管理全网各类型终端能力，终端类型包括各版本的windows，linux，以及主流国产操作系统等。	按需
4.	终端安全管理工具	支持资产大屏、威胁大屏、运维大屏、数据安全大屏等多维度的大屏信息呈现，以不同维度展示资产细节、威胁告警、敏感信息。支持系统、应用、中间件、数据库等类型的漏洞检测。支持基于白名单或者黑名单形式，对配置端口进行管控。支持基于接口类型与包括移动硬盘/U盘、光驱、鼠标、键盘、手机/平板、蓝牙等设备类型进行精细化管控。	按需

7. 满足本项目其他要求

（1）必要时我公司负责联系协调设备原厂进行技术支持，相关费用由我公司负责。

（2）巡检维护、应急抢修产生的交通食宿费用由我公司负责。

（3）项目结束后我公司将提供项目审计报告。

8. 满足本项目服务期限要求：

我公司将严格按照项目的要求，提供12个月的项目服务期限。

9. 满足本项目廉政要求：

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。

10. 满足本项目验收要求：

1.验收时间：合同期满后，我公司完全履行了合同所规定的条款，且无任何争议或遗留问题，招标人按照项目验收要求进行验收。

2.验收：

2.1 我公司提供的服务符合招标文件和合同条款要求。

2.2 服务期期满。

2.3 我公司将提交的相关验收材料符合招标人要求。

投标人名称：中移建设有限公司

日期：2026年05月11日

四、其他内容详见投标文件。

五、乙方相应资质文件。

1.营业执照

2. 信息安全管理体系认证证书

信息安全管理体系认证证书

证书号： 099320ISR1

兹证明

中移建设有限公司

注册地址：北京市海淀区北蜂窝路 18 号（综合楼 9 层 906、907、917）

审核地址：北京市西城区广宁伯街 2 号

统一社会信用代码：911101087481059966

建立的信息安全管理体系符合标准：

ISO/IEC 27001:2022

通过认证范围

计算机应用软件研发及系统集成；通信网络系统维护

所涉及的信息安全管理活动

（适用性声明版本：B/0）

上一周期证书到期日：2024 年 5 月 27 日

发证日期：2024 年 6 月 26 日　有效期至：2027 年 5 月 27 日

证书的有效性需经 EWC 通过定期的监督审核确认保持；在一个监督周期后，本证书必须与 EWC 签发的《监督审核合格通知书》合并使用方可有效。查询证书有效状态请登陆www.ewqcc.org；

本证书信息可在国家认证认可监督管理委员会官方网(www.cnca.gov.cn)上查询。

EWC 授权人：

中国认可
国际互认
管理体系
MANAGEMENT SYSTEM
CNAS C039-M

北京埃尔维质量认证中心
北京市西城区车公庄大街甲4号

3. 信息安全服务资质认证证书

信息安全服务资质认证证书

证书编号：CCRC-2022-ISV-SI-3485

兹证明

中移建设有限公司

统一社会信用代码：91110108748105996 6

信息系统安全集成服务资质符合

CCRC-ISV-C01:2025《信息安全服务规范》

CCRC-ISV-R01:2025《信息安全服务资质认证实施规则》

三级服务资质要求

注册地址：北京市海淀区北蜂窝路 18 号（综合楼 9 层 906、907、917）

办公地址：北京市海淀区北蜂窝路 18 号 1 号楼 7 层、8 层

发证日期：2025 年 9 月 30 日　　**有效期至**：2028 年 9 月 29 日

首次颁证日期：2022 年 9 月 30 日

证书有效期内本证书的有效性依据发证机构的定期监督获得保持。

中国认可 产品 PRODUCT CNAS C066-P

陈建良

Signed: Chen Jianliang

中国网络安全审查认证和市场监管大数据中心 1101021013249

证书可通过扫描二维码或网站查询 The certificate can be verified through scanning the QR code or the website. cx.cnca.cn or www.isccc.gov.cn

中国网络安全审查认证和市场监管大数据中心

CHINA CYBERSECURITY REVIEW, CERTIFICATION AND MARKET REGULATION BIG DATA CENTER

中国 · 北京 · 朝阳区惠新里241号 100029

No.241 Huixinli Street, Chaoyang District, Beijing, 100029 China

4. 信息系统建设和服务能力等级证书

CS

信息系统建设和服务能力

等 级 证 书

经评估，中移建设有限公司 符合《信息系统建设和服务 能力评估体系 能力要求》，能力达到良好级(CS3)，特发此证书。

评估依据：《信息系统建设和服务 能力评估体系 能力要求》（T/CFEII 0001-2019）

证书编号：CS3-1100-000596　　发证日期：2025-10-31

查询平台：http://www.cs-cas.cn/　　有效日期：2029-12-31 止

中国电子信息行业联合会

5. 质量管理体系认证证书

质量管理体系认证证书

证书号：023224Q

兹证明

中移建设有限公司

注册地址：北京市海淀区北蜂窝路 18 号（综合楼 9 层 906、907、917）

审核地址：北京市西城区广宁伯街 2 号

统一社会信用代码：911101087481059966

建立的质量管理体系符合标准：

GB/T 19001-2016/ISO 9001:2015

通过认证范围

安全技术防范系统设计、安装、施工、维护，

通信网络维护，数据中心基础设施维护

颁证日期：2024 年 8 月 23 日　有效期至：2027 年 8 月 22 日

证书的有效性需经 EWC 通过定期的监督审核确认保持；在一个监督周期后，本证书必须与 EWC 签发的《监督审核合格通知书》合并使用方可有效。查询证书有效状态请登陆www.ewqcc.org；

本证书信息可在国家认证认可监督管理委员会官方网(www.cnca.gov.cn)上查询。

EWC 授权人：徐清

中国认可
国际互认
管理体系
MANAGEMENT SYSTEM
CNAS C039-M

北京埃尔维质量认证中心　北京市西城区车公庄大街甲4号

6. 环境管理体系认证证书

环境管理体系认证证书

证书号： 023224E

兹证明

中移建设有限公司

注册地址：北京市海淀区北蜂窝路 18 号（综合楼 9 层 906、907、917）

审核地址：北京市西城区广宁伯街 2 号

统一社会信用代码：91110108748105996G

建立的环境管理体系符合标准：

GB/T 24001-2016/ISO 14001:2015

通过认证范围

资质范围内通信工程施工、电子与智能化工程施工、
市政公用工程施工、建筑工程施工、机电工程施工、
安全技术防范系统设计、安装、施工、维护，通信网络维护，
数据中心基础设施维护所涉及的环境管理活动

颁证日期：2024 年 8 月 23 日　　有效期至：2027 年 8 月 22 日

证书的有效性需经 EWC 通过定期的监督审核确认保持；在一个监督周期后，本证书必须与 EWC 签发的《监督审核合格通知书》合并使用方可有效。查询证书有效状态请登陆www.ewqcc.org；

本证书信息可在国家认证认可监督管理委员会官方网(www.cnca.gov.cn)上查询。

EWC 授权人：

中国认可
国际互认
管理体系
MANAGEMENT SYSTEM
CNAS C039-M

北京埃尔维质量认证中心　北京市西城区车公庄大街甲4号

7. 职业健康安全管理体系认证证书

职业健康安全管理体系认证证书

证书号：023224S

兹证明

中移建设有限公司

注册地址：北京市海淀区北蜂窝路 18 号（综合楼 9 层 906、907、917）

审核地址：北京市西城区广宁伯街 2 号

统一社会信用代码：91110108748105996G

建立的职业健康安全管理体系符合标准：

GB/T 45001-2020/ISO 45001:2018

通过认证范围

资质范围内通信工程施工、电子与智能化工程施工、
市政公用工程施工、建筑工程施工、机电工程施工、
安全技术防范系统设计、安装、施工、维护，通信网络维护，
数据中心基础设施维护所涉及的职业健康安全管理活动

颁证日期：2024 年 8 月 23 日　有效期至：2027 年 8 月 22 日

证书的有效性需经 EWC 通过定期的监督审核确认保持；在一个监督周期后，本证书必须与 EWC 签发的《监督审核合格通知书》合并使用方可有效。查询证书有效状态请登陆www.ewqcc.org；

本证书信息可在国家认证认可监督管理委员会官方网(www.cnca.gov.cn)上查询。

EWC 授权人：

中国认可
国际互认
管理体系
MANAGEMENT SYSTEM
CNAS C039-M

北京埃尔维质量认证中心　北京市西城区车公庄大街甲4号