合同编号：　DSJ-2026-005

北京市大数据中心

服务采购合同

合同名称：2026年北京市政务信息安全监控预警服务

委托人（甲方）：北京市大数据中心

受托人（乙方）：北京安信天行科技有限公司

委托人（甲方）：北京市大数据中心

负责人：张琳

住所地：北京市通州区留庄路 3 号院

受托人（乙方）：北京安信天行科技有限公司

法定代表人：张瑞芝

住所地：北京市海淀区北四环西路 68 号 10 层 1001 号

甲、乙双方根据《中华人民共和国民法典》及相关法律法规的规定，经过友好协商，就乙方为甲方提供 2026 年北京市政务信息安全监控预警服务事宜达成如下协议，以资共同遵守。

本合同 是 ☑否 中小企业预留合同。

第一条 服务事项及内容

本合同期限内，乙方应为甲方提供如下服务：

1、应用系统技术运维服务；

2、应用系统业务运维服务；

3、硬件保修维护服务；

4、软件和数据库使用维护服务；

5、监控设备租用服务

6、与第三方合作外购数据服务。

详细服务内容及要求见**附件 1**《工作方案》。

第二条 服务质量要求及验收

1、 乙方为甲方提供的服务质量应符合国家或相关行业的标准。

2、 乙方负责建立完善的项目管理机制，保证日常维护进度及质量，建立符

合甲方系统维护、全部设备维护和项目管理文档、操作规范、配置文档和技术文档。服务期间，乙方应完成甲方制定的项目绩效目标，并且制定工作计划并执行绩效跟踪，确保年度绩效目标顺利完成。

3、 服务期间，乙方应于每月第十个工作日前定期向甲方提交上月度工作报告，报告内容包括上月完成的项目内容、系统运行情况，以及项目变更情况等。

4、 乙方在服务合同到期之后 30 天内配合甲方完成项目终验。乙方完成合同全部工作后应及时通知甲方进行最终验收。甲方组织验收合格的，甲方在验收合格报告上签字；验收不合格的，乙方应当在 10 个工作日内进行返工或调整，并重新提交甲方验收。

5、 若在下一服务年度存在运维交接情况，按照甲方要求开展运维交接工作，制定详细的交接计划方案，完成各项工作的平稳交接，包括甲方的资产状况、工作文档、业务范围，工作流程等，完成相关业务人员的培训工作。

6、 合同最终验收合格后，乙方应向甲方提交如下合同成果：

参考附件一工作方案中**验收文档要求。**

第三条 项目小组及人员要求

1、 双方各指派一名代表作为本项目负责人，项目负责人职责范围包括：项目协调、资源调配、沟通协调等。

甲方项目负责人：屈伟晨，联系方式：13911527081。

乙方项目负责人：陈青民，联系电话：13910130917。

2、 项目主要人员要求

乙方须根据项目要求安排具备相应资质和经验的专业人员从事本项目的工作，并确保项目实施队伍的稳定（项目主要人员名单详见**附件 2**）。项目实施过程中，乙方如因正当理由需要调整项目主要人员的，应当提前 30 个工作日通知甲方，获得甲方书面同意后方可更换。

第四条 服务期限

乙方为甲方提供上述服务的期限为：自合同签订之日起一年。

第五条 服务费及支付方式

1、 本合同乙方应为甲方提供以服务：

报价单位：人民币元

序号	分项名称	单价（元）	数量	合价（元）	备注/说明（此处服务内容仅为简述，具体完整服务内容详见附件1《工作方案》）
1	应用系统技术运维服务	540000	1项	540000	应用系统技术运维服务包括系统维护和故障预防处置两部分工作。
2	应用系统业务运维服务	2650000	1项	2650000	应用系统技术运维服务包括安全事件监控、监控数据分析和挖掘、移动办公拨测服务、专用协议算法解析四部分工作。
3	硬件保修维护服务	540000	1项	540000	提供安全监测设备和网络设备的维保和授权服务。
4	软件和数据库使用维护服务	960000	1项	960000	软件和数据库使用维护服务包括市政务信息安全监测预警系统应用软件的维保、安全管理与分析平台租用两部分工作。
5	监控设备租用服务	295000	1项	295000	继续租用在用的监控设备包括利亚德（TXP108 P1.2）LED 会议一体机 3 台，小鸟处理器及混合矩阵（DB-VWC2-Hpro-1823ZY，DB-HMX2-E-FR9-1112ZX）、中控系统、远程视频会议系统及监控专用终端各 1 套
6	与第三方合作外购数据服务	400000	1项	400000	与两家网络安全和数据安全权威机构合作，分别提供数据安全监测服务和网络安全监测服务。
总价（元）			6项	5385000	**人民币大写：**伍佰叁拾捌万伍仟元整

2、 本合同项下服务费总额为人民币 5,385,000 元（最终以财政预算批复金额为准），**大写：**伍佰叁拾捌万伍仟元 。前述服务费已经包含乙方完成本合同项下服务的全部费用，除前述款项外，甲方无需向乙方另行支付其他任何费用。

3、 甲方将按以下方式向乙方支付服务费：

分期支付（两次）：

第 1 次付款：本合同签署后，甲方自收到乙方提供的符合甲方要求的发票且财政资金到达甲方零余额账户并可实际使用之日起 10 个工作日内，向乙方支付（大写） 贰佰陆拾玖万玖仟贰佰元整 （￥ 2,699,200 元）；

第 2 次付款：乙方提供本合同项下的全部服务并经甲方最终验收合格，甲方自收到乙方提供的符合甲方要求的发票之日起 10 个工作日内，甲方向乙方支付（大写）贰佰陆拾捌万伍仟捌佰元整（￥ 2,685,800 元）。

乙方应在甲方付款前向甲方开具正规、合法发票，否则甲方有权暂不付款且不承担逾期付款的违约责任。因乙方原因（包括但不限于未开具发票、开具发票不符合甲方要求等）导致甲方因财政政策原因未能付款，相应责任由乙方承担。

第六条 甲方的权利义务

1、 甲方有权要求乙方按照本合同约定提供各项服务。

2、 甲方有权对乙方提供各项服务的情况进行监督和检查。

3、 甲方应按照本合同约定向乙方支付服务费。

第七条 乙方的权利义务

1、 乙方应按照本合同约定向甲方提供各项服务，确保服务质量符合法律法规、国家标准的规定及本合同约定或甲方要求；如因乙方提供服务不符合前述要求给甲方造成损失的（本协议中所指损失包括但不限于律师费、公证费、差旅费、向第三人支付的任何费用以及为减小损失、实现债权而支付的其他费用等，下文同义），乙方应予赔偿。

2、 乙方有义务配合甲方或相关单位根据工作需要，对其提供服务情况及项目服务费支出、使用情况进行的监督和检查，出现问题的应及时整改。

3、 乙方应保证为甲方提供服务的员工具备提供本合同项下服务所需的相应资质和许可，并保证乙方人员在为甲方提供服务的过程中，严格遵守甲方的各项规定、服从甲方安排。

4、 如因乙方人员原因，给甲方或第三方造成人员人身伤害或财产损失的，乙方应承担赔偿责任。

5、 未经甲方的书面许可，乙方不得以任何形式将其在本合同项下的权利义务转让给任何第三方。

6、 除双方另有约定外，为本合同相关内容进行专家咨询（验收）、调查研究、分析论证、试验测定、专利申请以及乙方到外地进行调研、收集资料所发生

的费用，均包含在本合同的项目费用中，甲方不再承担任何费用。

7、 因乙方原因造成阶段性验收或最终验收超期，导致甲方无法按照合同约定正常付款或给甲方造成损失的，乙方应承担相应赔偿责任。

8、 超出本合同约定内容或工作量 5 %以内的，乙方不再额外收取费用。

9、 自合同服务期满至下一年度服务商进入之前，乙方应继续做好合同项下各项服务直至新服务商进驻，并做好与新服务商的交接。

10、乙方应在实施阶段，接受甲方聘请第三方监理单位的管理。

11、乙方已全面知悉并保证严格遵守和履行我国网络安全法、数据安全法及个人信息保护法等法律、法规、规章及国家标准等规范性文件所规定的网络安全、数据安全及个人信息保护义务；在此前提下，乙方进一步保证不擅自留存、使用、泄露或者向他人提供任何因履行本合同而获取的任何数据，且承诺仅为履行本合同之必要目的、范围、方式而处理数据；乙方违反本条约定，一经发现，甲方有权随时解除本协议并追究乙方由此给甲方或相关方带来的全部损失和责任；甲方因此承担责任的，有权就全部损失向乙方予以追偿。

12、乙方服务人员接受甲方意识形态安全的统一管理。乙方严格执行意识形态安全管理的各项法规和甲方意识形态安全管理的各项制度，认真履行意识形态安全管理的职责，具体落实甲方外包服务人员意识形态相关管理要求，并将《意识形态安全责任书》提交甲方备案。

第八条 保密义务

1、乙方因承接本合同约定项目所知悉的该项目信息或甲方信息，以及在项目实施过程中所产生的与该项目有关的全部信息均为甲方的保密信息，乙方应对上述保密信息承担保密义务。未经甲方书面同意，乙方不得将甲方保密信息透露给任何第三方。

2、乙方应对上述保密信息予以妥善保存，并保证仅将其用于与完成本合同项下约定项目实施有关的用途或目的。在缺少相关保密条款约定时，对上述保密信息，乙方应至少采取适用于对自己核心机密进行保护的同等保护措施和审慎程度进行保密。

3、乙方保证将保密信息的披露范围严格控制在直接从事该项目工作且因工作需要有必要知悉保密信息的工作人员范围内，对乙方非从事该项目的人员一律

严格保密。

4、乙方应保证在向其工作人员披露甲方的保密信息前，认真做好员工的保密教育工作，明确告知其将知悉的为甲方的保密信息，并明确告知其需承担的保密义务及泄密所应承担的法律责任，并要求全体参与该项目的人员签署书面《保密协议》。

5、任何时间内，一经甲方提出要求，乙方应按照甲方指示在收到甲方书面通知后 5 个工作日内将含有保密信息的所有文件或其他资料归还甲方，且不得擅自复制留存。

6、非经甲方特别授权，甲方向乙方提供的任何保密信息并不包括授予乙方该保密信息包含的任何专利权、商标权、著作权、商业秘密或其它类型的知识产权。

7、乙方承担上述保密义务的期限为合同有效期间及合同终止后 5 年。

8、承担上述保密义务的责任主体为乙方（含乙方工作人员）。如乙方或乙方工作人员违反了上述保密义务，给甲方造成损失的，乙方均应向甲方承担全部责任，并赔偿因此给甲方造成的全部损失；如损失数额无法确定的，乙方同意按照人民币 54.00 万元赔偿甲方的损失。

第九条 知识产权归属

1、乙方为履行本合同或在本项目实施过程中形成的所有成果的所有知识产权（包括但不限于著作权、专利权、商标权、专有技术等权利）由甲方享有；本项目实施过程中形成的发明创造的专利申请权、非专利技术的使用权、转让权归甲方享有。

2、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、商业秘密等合法权益。否则由此产生的任何纠纷，由乙方负责解决并承担全部责任和损失；甲方因此而承担任何责任的，有权随时解除合同并就全部损失向乙方全额追偿。

第十条 违约责任及合同的解除

1、 甲乙双方均应全面履行本合同，任何一方不履行或不按约定履行均构成违约，违约方应赔偿因此给对方造成的全部损失。

2、 乙方未按照本合同约定的期限，向甲方提供服务的，每延迟 1 日，应向甲方支付本合同项下服务费总额的 0.1%违约金,累计延迟超过 30 日的，甲方有权解除本合同，乙方应返还甲方已经支付的全部款项，并向甲方支付服务费总额 10%的违约金。出现延迟不足 1 日的，按 1 日计算。

3、 乙方提供服务不符合本合同约定标准或甲方要求的，乙方应当在甲方规定的期限内进行返工、修改，并重新提交甲方验收；如乙方提供的服务经二次验收仍未通过甲方验收或乙方拒绝按照甲方要求进行返工、修改的，甲方有权解除本合同，乙方应返还甲方已经支付的全部款项，并向甲方支付服务费总额 10 %的违约金。因乙方返工等原因造成乙方提供服务迟延，应承担迟延履行的违约责任。

4、 乙方未按照本合同约定提供专业技术人员团队，或擅自更换人员的，经甲方通知后，应及时予以改正，经甲方通知后仍不改正的或上述情况累计发生 **3** 次以上的，甲方有权解除合同，如因此给甲方造成损失的，由乙方承担全部赔偿责任。

5、 乙方不接受甲方和相关审计部门对本项目进行监督检查的，或经检查发现存在违法违规情况的，按照国家和北京市有关规定处理。

6、 甲方未按本合同约定向乙方支付服务费的，每迟延一日，应向乙方支付拖欠款项 0.1 %的违约金（违约金总额不超过合同总价的 5%）。

第十一条 争议的解决

因履行合同所发生的一切争议，双方应友好协商解决，协商不成的，按下列第 （2） 种方式解决：

（1） 提交北京仲裁委员会仲裁，仲裁裁决为终局裁决；

（2） 依法向 甲方所在地 人民法院起诉。

（3）

第十二条 廉政承诺

1、合同双方承诺共同加强廉洁自律、反对商业贿赂。

2、甲方及其工作人员不得索要礼金、有价证券和贵重物品；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超标准宴请和娱乐活动。

3、乙方不得向甲方及其工作人员行贿或馈赠礼金、有价证券、贵重礼品；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超标准宴请及娱乐活动。

第十三条 其他

1、本合同自双方签字盖章之日起生效。

2、未尽事宜，经双方协商一致，签订补充协议，补充协议与本合同不一致或相冲突的内容，以补充协议为准。

3、本项目的招标文件、答疑文件、投标文件及相关承诺、协议、本合同附件等均为本合同不可分割之一部分，与本合同正文具有同等法律效力，双方均应遵照执行。如项目招标、投标文件与本合同内容存在矛盾的，按照有利于项目实施及保护甲方利益的方式理解和履行。（请列明合同附件，如没有附件请删除此条）

序号	附件名称
1	工作方案
2	项目主要人员名单

4、本合同一式 陆 份，甲方执 叁 份，乙方执 叁 份，具有同等法律效力。

（以下无正文）

甲方（盖章）：北京市大数据中心

签署人：

签订日期： 2026.2.26

乙方（盖章）：北京安信天行科技有限公司

签署人：

签订日期： 2026.2.26

开户行：北京银行双清苑支行

开户名称：北京安信天行科技有限公司

账号：01090327800120102315974

附件 1

工作方案

一、工作内容

（一）应用系统技术运维服务

1. 系统维护服务

（1）乙方负责对监测预警系统基础软硬件进行日常运维，包括配置管理、补丁升级、病毒木马查杀、数据备份/恢复等日常运行维护工作，填写编制相关运行维护记录，确保相关数据不被损坏或丢失，保障监测预警系统安全稳定的运行和监测工作的连续性。确保系统可用性达到 99.9%

（2）乙方负责对系统设备和状态进行日常巡检，包括每日对监测预警系统相关设备和服务器等的关键安全指标进行检查，每月对监测预警系统相关的设备和服务器等的主要运行、安全指标进行检查，并提交每日报告和每月报告。

（3）每年进行一次对监测预警系统设备和状态的年度巡检，对所有监测节点的全部设备进行实地巡检，对监测预警系统相关的设备和服务器等的运行、安全指标进行全面检查，深入查找安全隐患，并提交年度巡检报告。

2. 故障预防处置服务

（1）根据监测预警系统运行实际需要，乙方负责对政务云上部署的操作系统、数据库等软件和应用部分及各监测节点所有设备的故障处置，确保故障修复率≥96%。实时解决故障问题，解决不了的，乙方协调设备厂商及派工程师赶赴现场进行处置，其中单次故障影响时间小于 2 小时，简单故障排除时间小于 48 小时（因重大活动保障等原因导致无法赴现场进行设备调整的情况除外），复杂故障需延长排除时间的（或特殊情况下故障暂时不能排除的），向大数据中心说明并征得大数据中心同意。系统故障及时处置率 100%。

（2）乙方负责定期总结系统工作状况，在用户现场进行技术总结，对系统存在的潜在安全或故障隐患进行分析并提出相应的解决方案加以排除，并科学分析现有系统资源使用情况并提供总结报告。

（二）应用系统业务运维服务

1.安全事件监控服务

乙方负责对政务外网、政务云、重要政务网站（不少于1200个）和重要信息系统节点、互联网出口等进行监测值守，对网络攻击、恶意程序、数据泄露与异常访问、系统中断和访问异常、安全漏洞等做到早发现、快处置。

（1）乙方派遣专业技术人员完成7*24小时值守工作。

（2）乙方负责对监测数据进行值守发现、验证确认、深度发掘，确保年度发现安全问题≥1000起，发现高风险和中风险安全问题（即一般（中）以上的安全事件及中危以上的安全漏洞）的比例合计不低于60%，且通知完成度达到100%。

（3）乙方负责对发现的问题及时通知到事发单位并确保对方知悉，按规定进行安全事件跟踪及上报。

（4）乙方负责对事件可能产生的外延影响进行深度挖掘，对受害系统进行跟踪处置。

（5）乙方负责安全问题的跟踪处置工作，包括但不限于完成安全问题的通报、处置、跟踪工作，对未能及时闭环的事件问题报告至甲方负责人，根据大数据中心要求协助责任单位进行问题处置。

（6）对重大活动和重要信息系统有针对性监测值守保障。

（7）乙方负责将安全问题监测、分析和处置过程形成经验文档，对大数据中心开展政务信息安全监测工作提出建议。

■ 重要信息系统监测范围：（包括但不限于以下系统）

序号	系统名称	监测指标
1	统一用户空间系统	1.安全事件发现率≥99%【乙方监测发现网络攻击事件数÷网络攻击事件发现总数×100%】 2.系统流量异常和中断发现率≥99%【乙方发现的系统流量异常和中断事件数
2	统一申办受理平台	
3	数字化运营管理系统	
4	政务服务导办系统	
5	政务办事知识库系统	
6	统一电子档案系统	
7	市政务服务局门户网站	

8	北京市网上政务服务大厅	÷（乙方发现+外部通知的系统流量异常和服务中断事件总数）× 100%】 3. 一般（高）以上网络安全事件完成通报和报告时间不超过 10 分钟 4. 安全问题通知率 100% 5. 安全事件告警处置率 100% 6. 安全事件闭环率 100%
9	VR 实景引导体验系统	
10	政务服务业务分析与管理系统	
11	北京市政务服务事项管理系统	
12	北京市“互联网+监管”系统	
13	北京市政务服务中心综合受理平台	
14	政务服务数据资源管理平台	
15	统一行政审批管理平台	
16	政务服务便民自助平台	
17	政务服务安全管理平台	
18	政务服务运维管理平台	
19	知识库	
20	北京市首贷服务中心综合业务系统	
21	北京市 12345 市民热线核心受理平台	
22	北京 12345 平台	
23	12345 接诉即办智能知识库	
24	首都之窗门户网站	
25	“京办”系统	
26	“京通”系统（微信端）	
27	“京通”系统（支付宝端）	
28	“京通”系统（百度端）	
29	“京智”系统	
30	北京市公务员电子邮箱系统	
31	公共数据开放平台	
32	自然人统一身份认证平台子系统	
33	法人网上统一认证管理平台子系统	
34	移动公共服务平台支付平台子系统	
35	北京市电子签章系统	
36	大数据平台门户	

37	北京市电子证照系统	
38	北京市区块链先进算力实验平台-企业认证平台	
39	北京市感知管理服务平台	
40	政府投资信息化项目全流程管理系统升级改造项目	
41	北京市政务地理空间共享服务平台	
42	资源接入与分发系统	
43	北京市级政务云综合监管平台	
44	区块链先进算力平台-互联网基础运行环境	
45	区块链先进算力平台-政务外网网基础运行环境	
46	北京市区块链先进算力实验平台-公共服务区块链支撑平台	
47	城市码服务平台	
48	“京策”平台	
49	财务系统	
50	北京市投资项目在线审批监管平台	
51	北京市中介服务网上交易平台	
52	北京市政务服务监督检查和效能促进平台	
53	北京市大数据中心蓝光介质备份试点系统	

2.监测数据分析和挖掘服务

乙方通过监测数据深度分析与挖掘，发现监测预警系统未直接告警的安全访问、安全事件及安全态势。

（1）监测数据分析和挖掘，乙方派遣专业技术人员依托监测预警系统对报警数据进行分析和挖掘工作，对监测日志、报警数据进行深层次分析，挖掘安全隐患、判断隐患威胁的严重程度，并对报警情况的分析结果归类整理。

（2）按照大数据中心要求，乙方负责定期（周、月、年）对监测报警数据进行汇总、分析、整理，并按照要求完成事件简报、周、月、年度分析报告（包括且不限于重保时期的监测报告等），报告中对监测数据进行分类统计、历史对比、危害程度分析判断和评估，对发生的重点问题提出其成因、危害程度、发展趋势和解决建议等说明。

（3）乙方负责及时跟踪最新漏洞及恶意攻击爆发情况，根据大数据中心要求，不定期开展安全隐患专项排查工作，并对排查结果进行分析整理，形成报告。全年专项安全隐患排查工作 4 次。

3. 移动办公拨测服务

为加强移动政务 APP 及重要信息系统专项监测，乙方负责对甲方目标系统开展实时拨测服务，并满足如下功能要求：

（1）详细功能要求

类别	要求项	详细要求
监测节点	拨测点	在本地部署节点和公有云端手机节点进行拨测。拨测点支持 4G/WIFI/网线。
	覆盖范围	监测点覆盖北京，能够覆盖移动、电信、联通等三大运营商的 IPV4 及 IPV6 网络。
	拨测周期	支持灵活、可配置的定时与周期性探测任务。
	通知报告	提供实时监控仪表盘与多通道告警通知。具备强大的数据统计、分析与定期报告生成能力。
	PC 拨测节点	提供软硬一体化监控节点，支持自部署方式。
	APP 拨测节点	提供真实手机监测点，非 PC 模拟器，覆盖 iOS、Android 和鸿蒙系统。
拨测能力	支持应用类型	监测点支持对 APP、网站、h5、微信小程序、微信公众号、支付宝小程序进行拨测。
	脚本录制	支持通过云端任意一个节点，即可对测试对象进行脚本录制。
	持续监控	支持常态化拨测，达到 5 分钟级的任务监控，能够设置白天及夜间自定义的监测频率。

类别	要求项	详细要求
	小程序即时监测	具备对微信小程序或支付宝小程序进行监控，监控关键业务的可用性和性能问题、并获取操作过程中的网络请求等数据，支持后期分析。
	报告服务	系统中所展现的图表支持添加到报表池，支持生成自动报告，并可在生成的报告中进行编辑，并支持以 PDF 方式导出便于后续查阅。
	告警服务	告警维度设置支持可用性、耗时、崩溃等维度。
		告警对象设置支持指定任一任务或任务中某一步骤设置告警。
		告警方式支持：短信、邮件、微信、钉钉、webhook。
		告警恢复后能触发恢复通知。
		告警信息区分普通及严重级别，不同级别的告警支持通过短信、邮件等方式发送至对应级别的人员。
		可以对网络错误和网络性能告警，支持指定域名或 url。
	支持灵活的拨测配置能力	拨测任务配置支持选择城市、机型、OS 版本、运营商、网络类型。支持指定时间、频率、次数。可直观显示任务已执行次数。
	竞品分析能力	支持自定义的对比分析：包括任务、业务步骤维度。
	启动过程分析能力	当 app 启动慢时，对 app 启动过程做深层次分析，细化到函数级别，并结合网络瀑布图，帮助研发进行根因分析。
	IPv6 分析能力	具备针对应用端 IPv6 的监测和统计能力。
	异常定位能力	根据异常场景，提供崩溃日志和异常原因分析。
		具有定位卡顿步骤、异常节点 URL 等信息的能力。
		支持基于任务、步骤的耗时异常原因定位和分析能力。
		支持按照域名、主机、接入方式、运营商、ipv4/ipv6、http/网络错误类型等维度进行分析。
		支持提供单独步骤的网络瀑布图分析。
		支持采集网络请中的请求头、响应头、（文

类别	要求项	详细要求
		本型）响应体。
		支持提供拨测任务期间的 app 自身日志，供研发分析。
	群控测试	支持通过中央控制系统进行即时性操作，达到同时操控多台智能手机，可在一个界面上同时看到每台设备的执行情况。
	自定义网络探测	支持自定义配置 ICMP-Ping 或 TCP-Ping，在任务执行的同时，对指定 ULR 进行主动探测，验证网络连通性问题。

（2）详细非功能要求

类别	要求项	详细要求
授权	真机 APP 拨测时长	APP 拨测时长至少满足 200000 分钟。
	软硬一体机（PC 拨测节点）	不少于 2 台，内置配套拨测软件，根据实际需求进行调整。
培训	管理员培训	涵盖系统管理、节点部署、用户权限管理等
	操作员培训	涵盖脚本录制、任务配置、告警设置、数据查看等日常操作。
	培训材料	提供完整的培训材料。
技术支持	支持力度	提供 7x24 小时的在线技术支持服务，对于系统故障类问题在 2 小时内响应并提供解决方案。
	支持渠道	提供专属的技术支持渠道。
数据报告	报告周期	每月（通常为次月前 5 个工作日内）向甲方提供一份月度拨测数据总结报告。
	报告内容	报告内容包括：月度任务执行概况、业务可用性与性能趋势分析、主要告警事件回顾、优化建议等。

4. 专用协议算法解析服务

遵循流量分析、算法构建和验证评估的核心逻辑，分三个核心阶段开展服务工作，确保各环节衔接顺畅、成果可控：

（1）政务网络加密流量特征深度分析：以“精准提取特征、支撑模型构建”

为核心目标，从四大维度开展加密流量特征分析工作：

■握手流程特征解析：系统剖析政务网络主流加密协议的握手交互机制，重点分析 TLS 协议（1-RTT/2-RTT 模式）、IPSec/IKE 协议（IKEv2 四消息协商流程）、OpenVPN 隧道协议的完整握手流程，提取握手阶段的交互时序、消息类型、参数协商等核心特征；

■流统计特征提取：基于政务网络加密流量的传输规律，精准计算核心流统计指标，包括数据包长度的均值、方差、偏度、峰度等分布特征，数据包到达间隔（IAT）的时序分布特征，以及流持续时间、数据吞吐量等传输特征，通过统计分析区分自动化攻击行为与正常人类操作产生的流量差异；

■元数据指纹分析：聚焦加密协议握手阶段的明文元数据，重点解析 TLS 协议 Client Hello 消息中的核心参数（含协议版本、加密套件选型、扩展字段类型），提取并分析 JA3 指纹等关键指纹信息，建立政务网络正常加密流量的指纹基线；

■证书相关特征梳理：针对加密通信中的证书交互环节，分析证书链长度、证书签名算法（RSA/SM2 等）、证书有效期等明文暴露信息，挖掘异常加密通信中证书使用的共性特征。

（2）基于流量统计特征的异常检测模型构建：基于流量统计特征建立异常检测构建工作，包含：

■算法选型论证：结合政务网络加密流量“高并发、多协议、特征维度复杂”的特点，选用 XGBoost（eXtreme Gradient Boosting）算法构建异常检测模型。该算法具备优秀的稀疏数据处理能力与直方图优化特性，可有效适配政务网络多场景加密流量的特征分析需求，提升模型检测效率与精准度；

■特征工程与模型设计：基于前期提取的加密流量多维度特征，采用 CICFlowMeter 工具完成流级统计特征的标准化处理，构建适配 XGBoost 算法的特征集；合理设置基学习器数量、树深度等核心参数，通过正则化处理防止模型过拟合，确保模型仅依赖流量统计特征开展检测，不涉及流量载荷解密，保障政务数据安全合规。

（3）算法模型验证与效果评估：以“验证模型可行性、评估检测效果”为核心，开展模型验证分析工作：

■数据集选型与验证设计：采用公开权威的 CIC-DDoS-2019 数据集开展验证工作，该数据集包含多种 DDoS 攻击场景，可有效模拟政务外网的混合攻击环境；将数据集按科学比例划分为训练集、验证集与测试集，确保验证结果客观可信；

■多维度效果评估：围绕指南要求的“较高检出率”核心指标，开展模型效果评估，重点分析模型对各类目标威胁的检出率、误报率等关键指标；同时开展特征重要性分析，筛选对检测结果贡献度最高的 Top 5 核心特征，开展精简特征集的模型训练与测试，验证模型的高效性与稳定性；

■验证结论梳理：系统总结模型验证过程与结果，形成模型可行性分析报告，明确模型在政务网络加密流量异常检测中的适用场景与应用效果。

（三）硬件保修维护服务

（1）乙方负责提供安全监测设备和网络设备的维保和授权服务，包括设备维修服务、远程技术支持、现场服务、设备故障应急响应服务，提供相关设备的规则库升级或版本升级服务，设备维保清单如下：

序号	设备种类	设备名称	设备型号	数量	备注
1	安全监测设备	天诚蜜罐诱捕系统	蜜罐诱捕监测系统	8 台	/
2	安全监测设备	天融信防火墙设备	NGFW4000-UF	4 台	/
3	安全监测设备	东软下一代防火墙	NetEye	9 台	/
4	安全监测设备	启明星辰防火墙	天清汉马	4 台	/
5	安全监测设备	建恒信安堡垒机	堡垒机	1 台	/
6	网络设备	交换机	华为 S5700-28C-EI 、S5700-24TP-SI-AC 、S2326TP-SI 等网络设备提供备机备件服务、设备维修服务、远程技术支持、现场服务	48 台	/
7	网络设备	分流器	奇策科技 /EX30-56LA 56*10GE 万兆网络分流	4 台	

序号	设备种类	设备名称	设备型号	数量	备注
			器/EX30-56LA 等分流器提供备机备件服务、设备维修服务、远程技术支持、现场服务		
8	服务器	服务器	曙光 A620R-H、航天联志 Aisino 26081R 等各类服务器提供备机备件服务、设备维修服务、远程技术支持、现场服务	82 台	/

（2）乙方具有稳定可靠的备品备件供应来源、完善的备品备件保障体系，包括但不限于安全设备、网络设备、服务器、监控终端等。其中安全监测设备的备件服务，确保备用设备更换不影响监测业务运转，根据各类设备的规模、部署范围、保有量情况进行备件准备，若无法提供原厂备件服务的，应提供相应的备用方案，以确保监测预警系统的正常运转。

为避免因设备故障引起网络故障，从而导致业务中断，为大数据中心提供产品备品备件服务，安全产品整机或零部件故障或损坏，且短时间内无法修复时，则提供备用机，保证业务连续性。确保提供的监测预警系统备品备件，能够与监测预警系统现有设备和网络环境兼容，并满足监测预警系统业务需求和正常运行需要的备品备件。

（四）软件和数据库使用维护服务

1.软件维保服务

乙方负责提供市政务信息安全监测预警系统相关应用软件的维保服务，包括远程技术支持、现场服务、软件优化服务、系统故障应急响应服务，各项软件等要求在到期前解决维保延续问题，维保清单如下：

序号	软件名称	详细描述	数量	备注
1	监测预警系统维保	监控预警平台涉及的技术监控、资产管理、报表分析、网站监控、安全咨询分析、工作流、知识库、策略管理、系统管理、安全监控展示、安全认证等功能模块提供故障排查、BUG 修复、系统调优等相关工作，同时提供 7*24 小时的故障排除和服务工作。提供网站监测定制化及监测设备维修拓展相关服务。	1 套	/

序号	软件名称	详细描述	数量	备注
		监控预警系统涉及的监控报告生成、信息安全咨询发布、整体监控状况展示等功能模块提供故障排查、BUG 修复、系统调优等相关工作，同时提供 7*24 小时的故障排除和服务工作。	1 套	/
		提供 NetEye SOC 专用扩展采集引擎的技术支持服务，包括对新晋设备未知日志数据的识别和支持，节点变更对采集引擎的部署及调试。	1 套	/

（1）远程技术支持服务

针对应用软件，乙方提供 7×24 小时远程技术支持服务，通过专属服务热线、远程协助平台，及时响应各类咨询与故障申报，协助甲方排查系统运行异常、配置参数调整、日志分析等问题。

（2）现场技术服务

当远程支持无法定位或解决问题时，乙方启动现场服务响应机制，安排专业技术人员赶赴现场，针对系统软件的复杂故障、硬件联动异常、现场环境适配等问题开展深度排查与修复。定期开展全面的现场巡检，对系统部署环境、软件运行状态、数据交互链路进行全方位检查，输出优化建议。

（3）软件优化服务

乙方基于业务需求变化，持续提供软件优化服务。包括对系统性能进行调优，通过算法优化、资源分配调整提升监测分析效率。根据政策要求与业务新增场景，优化系统功能模块。定期对软件进行兼容性维护，确保与现有硬件平台、操作系统及关联业务系统的稳定协同。

（4）系统故障应急响应服务

乙方建立完善的系统故障应急处置体系，针对软件崩溃、数据异常、监测功能失效等突发场景，一旦发生故障，应急技术团队将立即启动响应流程，通过“远程排查—现场支撑—数据恢复—功能验证”的闭环操作，确保系统在最短时间内恢复正常运行；能够模拟各类极端故障场景，检验预案有效性并优化处置流程，最大限度降低故障对政务安全监测业务的影响。

2. 安全管理与分析平台租用服务

（1）提供基础安全分析及平台使用：乙方所提供的平台具备更专业的关联

分析及深度检测能力。

■采用自研的安全事件关联分析引擎，实现多源日志关联分析能力，实时对范式化后的日志流进行关联分析、具备自适应学习能力。

■对我中心下辖288家组织机构近25万政务信息资产进行接入，建立分权用户角色，能为我中心的网络安全提供更为全面的监测预警能力。

■基于大数据分析技术，对网内海量安全数据进行分析挖掘，可发现WEB攻击、恶意文件、钓鱼邮件、失陷主机等深度安全威胁，在告警分析时提供详细的取证信息，为分析处置提供可靠的数据支撑，有效提高大数据中心的监测预警及分析研判能力。

■全年完成安全分析报告数量12份。

（2）持续优化服务要求：乙方通过研发团队持续性针对我中心进行定制化优化服务。

■针对大数据中心现有安全设备、其他方安全设备和测试设备的告警日志的采集回传数据结构化统一和采集；

■对不同品牌厂商报警、日志等数据的字段进行有效的聚合清洗和降噪，相比2025年无效告警占比有降低，有效减少重复或无效告警数量；

■定制化提供综合态势、外部威胁等多块态势感知大屏，实现安全可视化。

（3）专业分析支撑服务要求：乙方通过专业安全团队基于平台，在重保期、专项保障期、重大安全事件发生时提供支持服务，包括样本分析、安全情报数据分析、攻击者分析研判支撑对一线无法判断的恶意文件样本、攻击组织，攻击者特征及范围进行定性分析等，为重要时期网络安全提供保障。

（4）利用AI算法和技术，对告警进行自动研判。通过各类告警的综合分析，自动筛选出有效告警，减少人工干预，提高威胁发现的准确性和效率。借助AI的数据分析能力，实现有效告警与其他告警的智能关联。通过对不同来源数据的整合和分析，挖掘出隐藏在数据背后的安全威胁。通过引导式事件调查，帮助更全面地分析安全事件，实现对安全事件的快速响应和详细报告。

（五）监控设备租用服务

乙方对大数据中心在用的监控设备提供上述设备或不低于上述设备同等性能的监控设备租用服务。按照大数据中心的时间安排将所有设备安装部署至指定

位置。费用由乙方承担。

监控设备包括：

■利亚德（TXP108 P1.2）LED 会议一体机 3 台；

■小鸟处理器及混合矩阵（DB-VWC2-Hpro-1823ZY，DB-HMX2-E-FR9-1112ZX）、中控系统、远程视频会议系统及监控专用终端各 1 套。

（1）部署实施：严格按照需求提供符合技术参数的设备，若原厂设备供应存在缺口，第一时间提供同等性能的替代设备方案并征得大数据中心确认。在收到具体部署时间节点后，将组织专业技术团队完成设备的运输与系统联调，针对 LED 会议一体机进行显示效果校准，对小鸟处理器及混合矩阵完成信号传输链路测试，确保中控系统与各设备的联动控制功能正常，远程视频会议系统可实现稳定的跨区域音视频交互，监控专用终端覆盖目标区域并满足画质与存储要求。

（2）运维与故障保障：服务周期内建立常态化运维机制，按用户实际要求开展现场巡检，对设备运行状态、散热环境、信号链路进行全面检查，形成巡检报告并同步优化建议；提供 7×24 小时远程技术支持，针对设备卡顿、信号中断等常见问题进行实时排查与远程修复；若出现硬件故障，提供备用设备临时替换，在用户要求时间内完成故障设备的维修或更换，确保业务场景不中断。

（3）技术支持与操作培训：为大数据中心提供设备操作专项培训，涵盖 LED 一体机画面切换、混合矩阵信号调度、中控系统场景预设、远程会议系统发起与管理等内容，确保相关人员熟练掌握设备使用技能；同时建立专属服务对接群，实时响应使用疑问、功能优化需求，定期收集用户反馈并迭代设备配置，提升系统与业务场景的适配性。

（六）与第三方合作外购数据服务

1.数据安全监测服务

（1）数据安全态势服务：通过互联网上暴露的数据，对北京市政务数据整体情况、安全风险进行实时监测，分析研判整体政务数据安全态势，每月提供《北京市政务数据安全态势报告》。

（2）重大数据安全事件通报服务：对发现的涉及北京市政务数据的安全风险及事件，第一时间通报，并根据要求协助处置。事件通报覆盖范围为北京市政务数据，所有数据安全事件在发生后及时通报。

（3）重要政务数据安全外围监测服务：委托权威机构利用其自身的数据安全事件监测能力和技术手段，对指定的北京市政务数据进行 7*24 小时保护性监测。安排日常监测值守，提供安全监测服务，全年及时通报监测期间发现的攻击面暴露、数据泄露、个人信息泄露、数据安全隐患等安全事件不少于 50 个，按月提交上月度监测报告，并于服务期满后将本年度工作情况进行汇总编制年度工作报告。

（4）敏感时期数据安全保障服务：在“春节”、“两会”、“五一”、“国庆”等重大节日、重要社会及政治活动期间，以及重大政治事件敏感时期，提供人员值守服务，及时通报敏感期间发现的攻击面暴露、数据泄露、个人信息泄露、数据安全隐患等安全事件，并于敏感时期结束后提交专项报告。

（5）技术培训服务：为大数据中心相关人员提供 2 次数据安全相关观摩或培训，邀请参与权威机构组织举办的重要数据安全会议、应急演练等活动。

2. 网络安全监测服务

（1）网络安全态势服务：按照大数据中心要求对北京市面临的网络安全形势做出分析研判，每月及时向大数据中心提交北京市网络安全态势信息报告。

（2）重大网络安全事件通报服务：充分利用厂商、合作单位等信息渠道，及时向大数据中心通报重要信息安全预警信息，事件通报覆盖范围为大数据中心监控业务范围内所有政务网站，所有网络安全事件在发生后应及时通报。

（3）重要政务网站外围监测服务：委托权威机构利用其自身的网络安全事件监测能力和技术手段，协助大数据中心对北京市重要政务网站提供安全监测服务。安排日常监测值守，提供安全监测服务，及时通报监测期间发现的网站服务中断、网站篡改、网站挂马、网站漏洞、安全隐患等安全事件，要求发现安全事件数量不少于 50 个，并于每月提交上月月度监测报告，并于服务期满后将本年度工作情况进行汇总编制年度工作报告。

（4）敏感时期网络安全保障服务：在“春节”、“两会”、“五一”、“国庆”等重大节日、重要活动期间，根据大数据中心要求提供 7×24 小时外围监测，及时通报敏感期间发现的网站服务中断、网站篡改、网站挂马、网站漏洞、安全隐患等安全事件，并于敏感时期结束 5 个工作日内提交专项报告。

二、工作要求

（一）项目管理要求

建立完善、高效的项目管理体系，是项目按期优质完成的根本保证。乙方建立独立的项目监督机构，对工程实施的全过程进行监督和检查，及时纠正工程中出现的各种差错，保证项目按期优质完成。在服务过程中严格按照相关安全标准，形成相关实施文档模板和质量记录文档。

（二）项目团队要求

（1）乙方提供和配备不少于 13 人（不含项目经理）的驻场运维服务团队，确保 7*24 小时提供监测服务，并提供驻场服务（工作日 5*8 小时期间 7 人驻场，每周工作日 5*8 小时外所有时间 1 人驻场，重大活动保障期间根据大数据中心需求调整驻场人数），驻场人员至少有两人具备 CISP 或 NISP（二级及以上）证书，团队配备能够胜任监测预警系统运行维护的各项工作高级别专业技术人员，同时团队具备运维、值守、信息安全咨询、应急等所需的技术能力和从业经验。

团队人员设置及岗位职责和服务要求

序号	岗位名称	岗位人数	人员要求	服务要求
1	系统运维	2	具有2年以上信息系统运维经验人员	1.负责监测预警系统及监测节点各类设备配置管理、软硬件升级、病毒木马查杀、数据备份/恢复、维保、授权等服务 2.负责监控系统及各监测节点的各类设备的巡检、日常运行维护保障，同时定期对监控系统设备和状态进行巡检，并做好巡检记录、巡检报告和日志分析报告。
2	故障处置	1	具有2年以上信息系统运维经验人员	1. 负责对监测预警系统及监测节点各类设备的故障进行现场处置以及技术咨询、总结等工作，无法解决的，协调设备厂商及投标人派工程师赶赴现场进行处置 2. 单次故障响应时间小于 2 小时，故障排除时间小于 48 小时。
3	监测值守	7	至少有5名及以上人员具有2年以上监测值守经验人员	1.开展7*24小时北京市政务信息安全监控预警及驻场值守服务，负责威胁报警的监测、分析，并协助中心完成事件的通报、跟踪、处置工作。 2.对典型事件及分析过程进行梳理，根据中心要求将安全问题监测、分析和处置过程形成经验文档。

序号	岗位名称	岗位人数	人员要求	服务要求
4	监测数据分析和挖掘	3	至少有2名及以上人员具有2年以上数据分析和挖掘经验人员	1.负责派专人定期（周、月、年）对监控报警数据进行汇总、分析、整理，按照中心要求完成事件简报、周、月、年度分析报告，报告中对监控数据进行分类统计、历史对比、危害程度分析判断和评估，对发生的重点事件提出其成因、危害程度、发展趋势和解决建议等说明。 2.研判北京市政务信息安全态势，针对安全监测预警系统的运行管理，梳理相关工作流程，根据中心要求编写监控设备操作手册、事件分析处置作业指导书及相关文档

（2）乙方指派1人为项目经理，具备5年及以上相关工作经验，具备信息系统项目管理师证书（高级），负责项目统筹、计划、实施进度、质量等关键工作，以及项目团队的日常管理，维保、备品备件申购等项目统筹协调工作。

（3）乙方制定完善的人员稳定性保障方案及人员流动应急预案，如需进行人员调整提前1个月向大数据中心提出申请并征得大数据中心同意，且在调整前完成工作交接和培训上岗，以保障在服务期内的技术人员稳定性及项目交付质量。

（4）乙方组建故障处置外围保障小组，开展故障预防、技术咨询等工作，保障突发情况下监测预警系统的人员综合技术保障能力。

（三）技术支持要求

乙方拥有一支稳定的服务保障队伍，并具有较强的技术保障实力，遇到突发情况时能够及时解决问题，具有完善的技术支持服务体系，可提供如下技术支持服务：

1）针对用户在安全运维过程中提出的技术问题提供解答；

2）具备电话、E-Mail和Internet网站等多种技术支持方式；

3）提供“7×24”小时技术支持，针对出现的突发故障或问题，在10分钟内给予响应，2小时到现场，4小时内予以解决；

4）提供远程支持、现场支持多种方式排除系统出现的各类安全问题，并协助进行解决。

（四）保密要求

乙方对项目实施中涉及到的相关数据、资料、文档等具有保密的义务，并按

照相应保密规定执行。

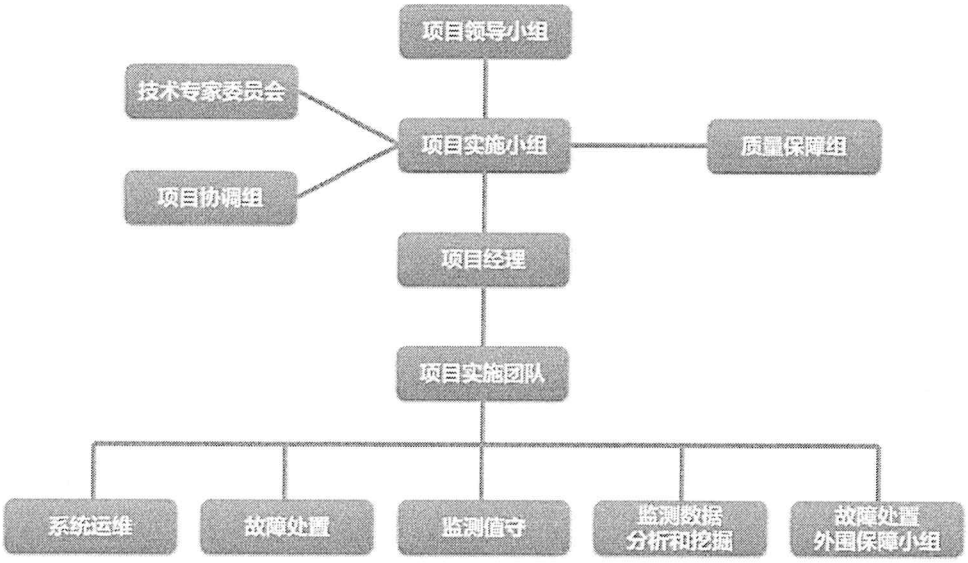
乙方严格遵守合同规定，执行有关保密的法律法规，选派具有良好职业道德的人员参与和从事本项目工作，教育相关人员恪守职业道德，乙方服从大数据中心的管理，严格遵守大数据中心的保密规定和工作制度，并承担相应的保密责任。

乙方所有参与本项目的技术人员，都必须与大数据中心签订《保密承诺书》。乙方负责对《保密承诺书》归档保管，并接受大数据中心检查，对承诺履行情况负有监督责任，一旦发现违反承诺情况，要及时向大数据中心报告。

三、工作组织

为了保证本项目的顺利实施，确保运维服务项目质量并达到预期目标，乙方将加强管理和协调合作，使工作和责任更加清晰明确，针对本项目建立分工明确，职责清楚，层次分明同时又能协调配合的科学项目管理组织和架构。

根据本项目具体情况，项目管理是在项目经理负责制的基础上，采用多任务并行机制，实施流程优化等方法，对系统运维、信息安全维护、安全服务、网络信任体系维护以及产品维护等方面工作所涉及的工作和人员，以及服务申请、服务实施、服务成果提交、服务确认等各个阶段的活动进行整体考虑，结成相应的服务小组，提高工作的并行度，并做到规范落实、组织落实、计划落实、资金落实。下图给出了该项目的组织结构示意图：



项目组织结构图

项目各小组职责分工如下：

项目领导小组：乙方与大数据中心双方各指定负责人作为项目主管，并加入

乙方销售代表，共同组成项目领导小组。大数据中心项目主管负责对乙方的服务工作进行总体监督、对运维驻场人员和技术支持人员进行工作安排、考核，对乙方服务工作进行评价和反馈；乙方的项目主管负责对安全保障服务和系统运行维护支持工作的总体管理，包括安全保障服务、运维服务和技术支持工作制度的建立、执行、运维服务人员的工作调派、考核、运维服务工作的总结及整改等，是乙方服务的第一责任人和接口人；我公司销售代表负责商务总协调。

技术专家委员会：由乙方相关技术高层管理人员、资深技术专家和外协单位（如测评中心、国密办和科研院校等）信息安全技术专家组成。主要负责指导、审核服务技术方案、服务工作规范以及服务方法，并对服务过程中的技术难题提供指导、支持。

项目协调组：负责对本项目的整体协调和进度控制，服务工作中如遇到重大问题组织各方面力量进行支持、处理。

项目经理：由乙方委派具备安全服务资质和相关丰富经验，项目综合能力优秀的管理人员担任，负责项目整体工作的具体制定、开展，率领各项目小组规范执行各项工作。项目经理具备 5 年以上相关工作经验，具备信息系统项目管理师证书（高级），负责项目统筹、计划、实施进度、质量等关键工作，以及项目团队的日常管理，维保、备品备件申购等项目统筹协调工作。具体职责如下：

- 主持项目现场实施工作；
- 主持服务管理体系编制工作；
- 主持安全服务方案的编制工作；
- 主持项目进度计划和实施方案的编制工作；
- 负责项目的协调与调度、管理工作；
- 负责项目质量的控制和保证；
- 负责协调、组织产品维护、维修、测试以及其他任务的组织执行；
- 负责项目文档计划、管理和审核；
- 组织服务成果的检查、交付与确认。

质量控制组：协助项目经理制定质量工作计划，并监督项目质量执行过程以确保项目按时保质完成；负责对项目实施全过程的质量活动进行跟踪、监督、检查和及时纠正。

项目实施团队：配备了不少于 13 人（不含项目经理）的驻场运维服务团队，确保 7*24 小时提供监测服务，并提供驻场服务（工作日 5*8 小时期间 7 人驻场，每周工作日 5*8 小时外所有时间 1 人驻场，重大活动保障期间根据大数据中心需求调整驻场人数），驻场人员至少有两人具备 CISP 或 NISP（二级及以上）证书，团队配备可以胜任监测预警系统运行维护的各项工作高级别专业技术人员，同时团队具备运维、值守、信息安全咨询、应急等所需的技术能力和从业经验。另外还为本项目组建故障处置外围保障小组，开展故障预防、技术咨询等工作，保障突发情况下监测预警系统的人员综合技术保障能力。

项目实施团队在项目经理带领下，负责项目的具体实施工作，按照项目所包含的不同任务，分成系统运维组、故障处置组、监测值守组和监测数据分析和挖掘组、故障处置外围保障小组。各小组职责如下：

- 系统运维组：负责监测预警系统及监测节点各类设备配置管理、软硬件升级、病毒木马查杀、数据备份/恢复、维保、授权等服务；负责监控系统及各监测节点的各类设备的巡检、日常运行维护保障，同时定期对监控系统设备和状态进行巡检，并做好巡检记录、巡检报告和日志分析报告。
- 故障处置组：负责对监测预警系统及监测节点各类设备的故障进行现场处置以及技术咨询、总结等工作，无法解决的，协调设备厂商及派工程师赶赴现场进行处置。单次故障响应时间小于 2 小时，故障排除时间小于 48 小时。
- 监测值守组：开展 7*24 小时北京市政务信息安全监控预警及驻场值守服务，负责威胁报警的监测、分析，并协助中心完成事件的通报、跟踪、处置工作。对典型事件及分析过程进行梳理，根据大数据中心要求将安全问题监测、分析和处置过程形成经验文档。
- 监测数据分析和挖掘组：负责派专人定期（周、月、年）对监控报警数据进行汇总、分析、整理，按照大数据中心要求完成事件简报、周、月、年度分析报告，报告中对监控数据进行分类统计、历史对比、危害程度分析判断和评估，对发生的重点事件提出其成因、危害程度、发展趋势和解决建议等说明。研判北京市政务信息安全态势，针对安全监测预警

系统的运行管理，梳理相关工作流程，根据大数据中心要求编写监控设备操作手册、事件分析处置作业指导书及相关文档

- 故障处置外围保障小组：开展故障预防、技术咨询等工作，保障突发情况下监测预警系统的人员综合技术保障能力。

四、计划安排

为保证本项目的顺利实施，根据用户的实际情况，编制项目实施进度计划。乙方将此次项目任务加以分解，并确定每一阶段任务的详细计划进度，以指导和保证项目组按照项目进度要求完成项目所包括的服务任务。

实施进度计划通过科学应用启动、实施、收尾、验收、售后技术支持和服务等项目管理过程，规范地完成项目的需求分析及实施进度计划的确定。

（1）准备阶段

签订合同及编制项目实施方案：中标后开始，10 个工作日内完成。

（2）实施阶段

开展应用系统技术运维服务、应用系统业务运维服务、硬件保修维护服务、软件和数据库使用维护服务、监控设备租用服务、与第三方合作外购数据服务：中标后开始，服务周期 1 年。

（3）总结验收阶段

进行项目总结和项目成果文档交接，并完成项目验收：服务期结束后 30 天内完成。

五、验收标准及要求

（一）验收要求

乙方根据招标文件中项目目标、项目要求及项目验收等内容在投标时提供完整的项目实施方案，在中标后与甲方就方案内容细节进行沟通协商，确保方案符合甲方项目需求。

乙方在服务合同到期之后 30 天内配合甲方完成项目终验。

乙方提供纸质和电子版的项目验收文档。

验收标准：按照招标文件和合同约定标准验收。

（二）验收文档要求

服务名称		成果文档
应用系统技术运维服务	系统维护服务	《北京市政务信息安全监测预警系统设备配置变更记录》（按需） 《北京市政务网络和信息系统安全监测节点现场巡检报告》（1 份） 《北京市政务信息安全监测预警系统运维日报》（每日 1 份） 《北京市政务信息安全监测预警系统运维周报》（每周 1 份） 《北京市政务信息安全监测预警系统运维月报》（每月 1 份）
	故障预防处置服务	《北京市政务信息安全监测预警系统故障处置记录》（按需）
应用系统业务运维服务	安全事件监控服务	《北京市政务信息安全监测预警系统安全问题通知单》（按需） 《北京市政务信息安全监测值班记录》（每日 1 份）
	监测数据分析和挖掘服务	《北京市政务信息安全监测预警系统监测数据分析周报》（每周 1 份） 《北京市政务信息安全监测预警系统监测数据分析月报》（每月 1 份） 《北京市政务信息安全监测预警系统监测数据分析年报》（1 份） 《北京市政务信息安全隐患专项排查报告》（4 份）
	移动办公拨测服务	《移动办公拨测系统月度拨测数据总结报告》（每月 1 份） 《移动办公拨测服务年度总结报告》（1 份）
	专用协议算法解析服务	《政务网络典型加密流量及其威胁识别验证方法研究报告》（1 份）

硬件保修维护服务		《备品备件更换预案》（1 份） 《备品备件检查记录》（按需）
软件和数据库使用维护服务	软件维保服务	《北京市政务信息安全监测预警系统软件维护报告》（1 份） 《北京市政务信息安全监测预警系统软件故障处置记录表》（按需） 《北京市政务信息安全监测预警系统软件配置变更记录表》（按需）
	安全管理与分析平台租用服务	《安全分析报告》（每月 1 份） 《安全管理与分析平台服务总结报告》（1 份）
监控设备租用服务		\
与第三方合作外购数据服务	数据安全监测服务	《北京市政务数据安全态势报告》（每月 1 份） 《北京市政务数据重大数据安全事件通报》（按需） 《北京市重要政务数据安全外围监测工作月报》（每月 1 份） 《北京市重要政务数据安全外围监测工作年报》（1 份，其中攻击面暴露、数据泄露、个人信息泄露、数据安全隐患等安全事件不少于 50 个） 《敏感时期数据安全保障专项报告》（按需） 数据安全相关技术培训邀请函（2 份） 《数据安全监测服务年度工作总结报告》（1 份）
	网络安全监测服务	《北京市政务网络安全态势报告》（每月 1 份）

		《北京市政务重大网络安全事件通报》（按需） 《北京市重要政务网站外围监测工作月报》（每月 1 份） 《北京市重要政务网站外围监测工作年报》（1 份，其中网站服务中断、网站篡改、网站挂马、网站漏洞、安全隐患等安全事件数量不少于 50 个） 《敏感时期网络安全保障专项报告》（按需） 《网络安全漏洞》（周报、月报及专项报告） 《网络安全监测服务年度工作总结报告》（1 份）

附件 2 项目主要人员名单

序号	姓名	性别	年龄	学历	职称	职务	项目角色	承担工作
1	陈青民	男	43	硕士	高级	中心总监	项目经理	项目管理
2	李嘉诚	男	33	本科	无	安全工程师	驻场人员	监测值守
3	王浩	男	30	本科	无	安全工程师	驻场人员	监测值守
4	李响	男	29	本科	无	安全工程师	驻场人员	监测值守
5	张宇航	男	27	专科	无	安全工程师	驻场人员	监测值守
6	张斌	男	27	本科	无	安全工程师	驻场人员	监测值守
7	史鑫	男	32	本科	无	安全工程师	驻场人员	监测值守
8	胡锦徽	男	27	本科	无	安全工程师	驻场人员	监测值守
9	陈京生	男	27	本科	无	安全工程师	驻场人员	数据分析
10	张书滔	男	29	专科	无	安全工程师	驻场人员	数据分析
11	贾云鹏	男	27	本科	无	安全工程师	驻场人员	数据分析
12	全文杰	男	25	本科	无	安全工程师	驻场人员	系统运维
13	张强强	男	26	本科	无	安全工程师	驻场人员	系统运维
14	史杰	男	26	本科	无	安全工程师	驻场人员	故障处置
15	梁晨	男	44	本科	无	安全工程师	二线支持	外围保障
16	董策	男	42	本科	无	安全工程师	二线支持	外围保障