合同编号：BJIP02026-030506-010

网络安全咨询及技术保障服务
项目委托协议书

项目名称：政务云租用及网络安全运维项目安全运维服务采购项目

项目委托方（甲方）：中关村知识产权促进中心

项目承担方（乙方）：北京禹宏信安科技有限公司

委托时间: 2026 年 5 月

项目名称		政务云租用及网络安全运维项目安全运维服务采购项目		
合同名称		网络安全咨询及技术保障服务项目委托协议书		
合同金额		¥933000.00 元（人民币大写）玖拾叁万叁仟元整		
甲方	单位名称	中关村知识产权促进中心		
	负责人（签章）	[illegible]	职务	[illegible]
	项目联系人	孙绍炜	手机	18603338868
	地址及邮编	北京市丰台区西三环南路 1 号；100161		
	电话	010-89156523		
	传真	010-89156523		
	电子邮箱	cujinzhongxin@zscqj.beijing.gov.cn		
乙方	单位名称	北京禹宏信安科技有限公司		
	负责人（手签）	[illegible]	职务	法定代表人
	项目联系人	雷雪	电话	18210129596
	地址及邮编	北京市朝阳区小营路 17 号一幢四层 408 室；100101		
	电话及传真	010-88116617		
	电子邮箱	leixue@chaosec.com		
	开户名	北京禹宏信安科技有限公司		
	开户银行	招商银行股份有限公司北京自贸试验区商务中心区支行		
	帐号	110912038910901		

（单位公章）
2026 年 5 月 21 日

（单位公章）
2026 年 5 月 21 日

为提高北京市知识产权局网络安全管理与技术保障水平，做好各类网络安全工作。甲方委托乙方实施政务云租用及网络安全运维项目安全运维服务采购项目(网络安全咨询及技术保障服务)（以下简称“本项目”）。甲、乙双方经协商，就下列条款达成一致，并承诺予以严格遵守。

一、委托工作期限

本项目实施的委托工作期限为【2026】年【6】月【1】日至【2027】年【5】月【31】日。

二、委托工作内容、成果和合作模式

（一）项目委托工作内容

1. 基础信息安全运维服务

（1）安全咨询服务

安全咨询服务，对现有的信息系统的主机操作系统、数据库、管理账号等安全策略配置提供安全咨询，对配置存在的安全缺陷指导相应的业务支撑单位完成修复工作；对现有网络安全管理体系进行持续更新，对局安全管理制度，进行修订完善，确保管理体系符合等保及监管要求；对北京市知识产权局网络安全涉及所有信息系统资产进行梳理，编制风险隐患台账，跟踪安全整改进度，提供技术咨询；针对网络安全态势、重要系统漏洞等安全预警通告或安全整改通知，及时向北京市知识产权局告知相关危害、影响范围及应对方案；在各系统信创改造建设整改过程中提供安全咨询，结合网络安全法律法规、监管通知、网络安全等级保护、数据安全风险管理等方面相关要求

提出安全建议。

（2）安全巡检

根据甲方要求，采用人工检查和工具扫描相结合的方式，登录信息系统相关主机，对操作系统的账户、端口及进程异常情况进行人工分析，对信息系统文件进行后门排查分析，协助清理后门。

（3）办公终端安全运维

提供非涉密终端涉密检查技术支持，主要包括检查软件准备及人工现场检查配合等；如检查发现安全风险，配合进行整改后结果复查，对初测复测检查结果进行数据汇总与分析。每年按甲方要求的时间段提供相关服务(终端数量不少于100台)。

终端防病毒控制中心巡检，协助运维管理终端防病毒控制中心，包括策略配置、规则库更新等；定期对终端防病毒控制中心病毒查杀情况等安全告警进行巡检及分析，发现安全风险提供安全整改建议及整改后复查。

（4）渗透测试

在甲方的授权和监督下，利用已掌握的漏洞信息，针对甲方指定的业务信息系统（不少于3个）开展非破坏性的模拟黑客攻击测试，发现漏洞反馈整改建议简报，修复后配合进行复测，以确认漏洞是否被完全修复（包括初测及复测），最终出具完整渗透测试报告，报告中需详细记录测试过程。

2.安全保障服务

（1）应急响应及重点保障

根据监管要求，在春节、两会、五一、国庆等重要时期，提供7×24远程值守保障服务，对互联网开放信息系统运行情况进行实时监控，及时发现潜在的安全隐患或突发安全事件。及时响应信息系统的突发安全事件，将事件的损失降到最低，协助清除安全事件对业务系统产生的影响，恢复业务系统的运行，并开展相应的事后分析。

（2）特殊时期护网攻防演练

在监管机构护网攻击前，组织攻击队伍（至少4人）对北京市知识产权局面向互联网的业务系统，通过远程的网络攻击技术，以拿到预定核心目标主机权限或数据库权限为目标，模拟黑客入侵和攻击方法对真实环境系统进行非破坏性攻击测试，全面高效地发现信息系统不同层面的薄弱环节，将发现的安全风险进行分析提供安全整改建议，并组织复测，最终结果形成攻防演练总结报告。

（3）安全自查整改服务

根据监管单位要求，制定网络安全检查方案及检查表单，对局机关、促进中心、保护中心及公共服务中心安全管理制度制定及落实情况，安全技术防护措施落实情况进行全面的安全检查（包括对办公终端的漏洞扫描），总结反馈发现的安全风险，提交安全整改建议报告。

（4）源代码审计服务

使用专业工具和人工对指定信息系统源代码依据最佳安全实践，挖掘存在的安全漏洞及系统严重BUG，有效提升代码质

量以及信息系统的网络安全防护能力。满足合规性 GB/T 28448-2019《信息安全技术 网络安全等级保护测评要求》中“应核查是否具有软件安全测试报告和代码审计报告，明确软件存在的安全问题及可能存在的恶意代码”要求。

（5）网络安全培训

依据落实网络安全责任制要求，协助组织开展安全培训工作。根据网络安全、数据安全与等级保护测评等相关法律法规，结合日常工作开展中存在的安全风险及隐患，协助开展有关日常安全意识或网络安全技术技能等维度的安全培训（不少于 4 次）。

3. 等级保护测评服务

依照国家《GB/T 22239-2019 信息安全技术 网络等级保护基本要求》中三级的要求，提供网络安全等级保护技术方面的测评和管理方面的测评，根据差距分析的结果给出整改建议，提供整改咨询。由专业的测评机构，依照国家《信息安全技术 网络安全等级保护基本要求》中三级的要求，进行回归测评，出具符合公安要求的测评报告。

4. 信息系统数据安全风险评估服务

对指定信息系统依照数据安全合规性评估规范流程开展评估，评估团队开展合规性评估，包括正当必要性评估、基础性安全评估和数据全生命周期安全评估，研判合规性评估结果，对数据处理活动的安全风险进行分析研判，并及时开展风险处置，确保安全风险可控。

（二）合作模式

甲方提出项目目标、任务要求、工作进度和质量要求，进行项目协调，参加项目工作计划制定、实施过程和业务讨论，组织项目评估和验收评审，提供项目经费；乙方根据甲方要求完成项目委托工作，提交项目工作成果。

（三）项目委托工作成果及质量要求

乙方应向甲方提交以下项目委托工作成果：

1.服务要求

（1）服务规范

乙方须严格按照甲方制定的管理办法、流程及其他汇报制度、应急制度、文档管理、资产管理、人员管理、安全管理等相关制度，开展标准化网络安全服务工作。

（2）考核要求

根据甲方的考核要求，按照制定的绩效考核指标体系及服务承诺要求，乙方接受甲方对服务质量的考核。

（3）安全及保密要求

乙方须严格遵守甲方的相关信息安全规定，不得利用系统维护服务时的便利对甲方数据及其他信息擅自修改或透露给第三方。

（4）响应的及时性

乙方应当提供高效的系统维护服务，有效防范系统风险，服务项目经理7*24小时电话畅通，能够在系统发生网络安全问题时，能够协调专业技术力量在1小时内到达现场提供服务。

2.项目工作成果要求

（1）网络安全咨询及技术保障服务项目工作月报。

（2）网络安全管理制度汇编，安全巡检报告、渗透测试报告、攻防演练总结报告、安全培训记录。

（3）等级保护测评报告。

（4）数据安全风险评估报告。

（5）网络安全咨询及技术保障服务项目工作总结报告。

三、项目进度安排及要求

（一）进度安排

1.乙方应于【2026】年【6】月【15】日前按照甲方要求向甲方报送项目实施方案、项目人员和进度安排等。甲方可就乙方提供的项目实施方案、项目人员和进度安排等提出修改和调整意见。乙方应按照甲方要求及时修改和调整。经甲方审定后，乙方在甲方的指导下组织实施项目工作。

2.乙方应于【2027】年【5】月【31】日项目服务期结束后向甲方提交最终工作成果及全部原始及过程资料。乙方应同时向甲方提供上述材料的电子文件。甲方针对项目最终工作成果组织项目验收。

（二）具体要求

乙方指定的项目负责人及项目组成员能够保证全过程担负实质性项目组织实施工作，并以本合同约定的项目工作成果形式参加甲方组织的项目评审验收。

验收标准主要包括：是否按照本合同约定完成全部项目委

托工作、达到工作质量要求并形成符合本合同约定的相应项目工作成果等。

甲方组织项目评审验收，具体考核内容如下：

（1）与本合同第二条第一款中规定的项目委托工作内容范围相一致；

（2）符合本合同第二条第三款中规定的项目委托工作成果及其质量要求；

（3）项目实施方案、人员及进度安排合理，乙方在项目实施过程中积极接受甲方指导并配合甲方提出调整或修改要求；

（4）乙方项目经费支出符合相关法律法规和政策规定，积极配合甲方提出的与经费支出决算、调整、审计等相关工作；

（5）项目组织实施及项目委托工作成果不得侵犯任何第三方的知识产权以及其他人身和财产权利。

四、费用给付

（一）项目委托经费

本项目合同金额为人民币（大写）玖拾叁万叁仟元整（人民币小写¥933000.00元整），上述金额为含税价格。

除本合同约定的项目经费，甲方无义务向乙方支付其他任何费用。乙方因组织实施本项目而支出的一切费用，包括但不限于劳务费、专家费、食宿费、交通费、税费等，均应由乙方自行承担。

（二）付款方式

本合同项下项目经费共分【2】次支付（适用于中小企业）：

1.甲方于本合同生效之日起【10】个工作日内向乙方支付项目合同金额的【60】%，即人民币（大写） 伍拾伍万玖仟捌佰元整（人民币（小写）：￥559800.00 元整）；

2.项目委托工作全部完成后，乙方将项目经费决算报告以书面形式提供给甲方，甲方进行项目验收和决算评审，项目费用最终结算金额以决算评审结果为准。项目通过验收并决算评审结束后【10】个工作日内，甲方向乙方支付剩余全部费用。

3. 双方一致同意本项目最终结算金额以甲方决算评审结果为准，最高不超过本项目预算金额。如决算评审结果低于甲方已经向乙方支付的经费数额，乙方应在评审结束后【10】个工作日内向甲方退还多支付的经费。

（三）发票

乙方应根据约定的付款方式在每次付款时向甲方提供等额有效的发票或国家和本市有关部门规定的有效凭证，如因乙方原因怠于提供发票、凭证或发票、凭证不符合甲方要求的，甲方有权延迟付款，直至乙方提供符合甲方要求的发票或凭证，且甲方不承担任何违约责任。

（四）经费使用要求

乙方应加强对项目经费的财务管理，实行专款专用，保证项目经费用于本项目委托工作。乙方及项目人员不得擅自截留、挪用。

项目经费列表（可根据实际修改）：

1.人工成本费：¥933000.00 元

合计：人民币 ¥933000.00 元。

序号	分项名称	单价（元）	数量	合价（元）	备注/说明
1	基础信息安全运维服务	358000	1项	358000	含税
2	安全保障服务	361500	1项	361500	含税
3	等级保护测评服务	95500	1项	95500	含税
4	信息系统数据安全风险评估服务	118000	1项	118000	含税
总价（元）				933000	含税

五、双方权利和义务

双方均应共同遵守《中华人民共和国民法典》等法律法规和相关政策规定，严格遵守并认真履行本合同各项条款。

（一）甲方的权利义务

1.甲方有权要求乙方按照本合同约定的内容并在本合同约定的期间内提交本项目的项目实施方案、项目人员和进度安排以及项目委托工作成果。

2.若乙方提交的项目实施方案、项目人员和进度安排以及项目委托工作成果不符合甲方及本合同要求，甲方有权要求乙方进行修改或调整，直至符合甲方要求。

3.甲方有权监督、检查本合同履行情况。合同履行期间，甲

方根据需要对乙方履行本合同情况进行检查、监督，监督检查的方式和频率由甲方决定，但应尽量减少对于乙方正常工作的影响。乙方完成全部项目委托工作后，甲方组织项目验收。

4.甲方应按照本合同约定向乙方支付费用。

5.甲方享有对项目配套资金检查的权利。

（二）乙方的权利义务

1.乙方应为项目实施提供条件支撑和管理服务。乙方应按照项目申报书中的承诺和项目实施方案中确定的人员安排指定专人负责本项目组织实施工作，并编制项目经费预算、决算，严格执行批准的预算。如因故需要变更项目主要负责人或实施人员，乙方必须向甲方提交书面申请，并经甲方书面同意后方可变更。否则，乙方应按照本合同经费预算金额的【5】%支付违约金。

2.本合同执行过程中，甲方有权对项目委托工作内容和要求作出合理调整，乙方有义务予以积极配合。同时，乙方应严格履行合同义务，保证按时完成项目委托工作任务。

3.乙方应严格按照项目经费预算及本合同约定的支出范围执行项目经费支出，保证专款专用，杜绝弄虚作假、截留、挪用、挤占项目经费等行为。乙方应积极配合甲方对于本合同约定的经费支出的监督和检查。必要时，应积极配合甲方延伸审计。

4.乙方开展的一切与项目有关的活动应确保全部项目工作人员遵守有关法律法规。乙方如因执行本项目而导致人员生命、

健康、财产等受到侵害或使环境受到损害，乙方应负全部责任。

5.未经甲方书面同意，乙方不得擅自将本项目委托工作任务转委托给其他第三方，不得将本合同项下主要义务全部或部分转让给他人履行。

6.乙方应积极完成本项目委托工作，确保完成质量，且不得无故拖延。

六、知识产权条款

（一）乙方向甲方提交的项目报告、项目成果（包括项目原始材料、中间过程性材料及成果和项目最终成果等）的知识产权归甲方单独所有。甲方有权行使本项目所产生知识产权的完整权利，任何其他方无权干预。未经甲方书面同意，任何其他方不得使用本项目产生的知识产权。

未经甲方事先书面同意，乙方不得擅自转让、处分本项目委托工作成果。

（二）乙方在本项目评审结束前，不得发表本项目工作成果。乙方公开发表本项目工作成果，事先须经甲方书面同意，并且必须注明该成果为甲方所有。

如乙方未经甲方同意公开发表或使用本项目工作成果，甲方将依法追究乙方的责任，要求乙方承担项目预算经费金额【5】%的违约金。

（三）乙方保证所提交的研究成果没有侵害任何第三方的知识产权等相关权利。如发生侵犯第三方知识产权等相关权利的相关情形，乙方承担因侵犯第三方知识产权等权利而产生的

法律责任。

七、保密条款

本合同双方应对本项目相关信息及履行本合同过程中接收或知悉的其他方的所有保密信息（包括但不限于内部资料、数据、商业秘密等）予以严格保密；非经法律法规授权的部门依据相关法律法规的权限及程序调取或要求或征得信息披露方事先书面同意，不得向任何无关第三方宣传、透露或扩散，亦不得促使或允许他人披露上述保密信息，不得将保密信息用于本合同业务之外的其他用途；并应就保密责任对其工作人员或代理人、分支机构、关联方等的行为负责。

本保密期限为长期，直至保密信息经正当程序而成为公开信息为止；本保密条款为独立条款，不因本合同的变更、解除、终止而失效。

八、违约责任

（一）甲方应承担的违约责任

在乙方按规定履约且项目经甲方审核通过的前提下，甲方未按约定向乙方支付项目经费时，甲方应承担逾期付款违约金。每逾期一日，违约金按到期未付金额的千分之一计算。逾期30日的，乙方可终止本合同。

（二）乙方应承担的违约责任

1. 乙方未按本合同规定的期限提交工作成果或所提交的工作成果不符合合同或甲方要求，最终导致本项目未在规定的期限内完成的，乙方除有义务继续履行服务直至经甲方确认合格

外，还应向甲方支付违约金，每逾期一日，违约金按已收取项目经费总额的千分之一计算。乙方逾期30日仍未提交工作成果的，甲方有权无条件解除合同，自乙方收到甲方向其发出的书面解除通知时，该合同即告解除。合同终止后，甲方无需支付合同余款，甲方已付费用超过乙方实际工作量所对应的应付费用时，超过部分乙方应予全部返还，造成甲方其他经济损失的，乙方应予赔偿。

2. 乙方无正当原因未履行本合同时，甲方有权解除本合同，并停拨、追缴部分或者全部经费，由此造成的经济损失由乙方承担。

3. 乙方未经甲方批准，擅自实施或者转让项目委托工作成果或转让本合同项下权利义务，应当向甲方支付相当于本合同约定项目预算经费金额【5】%的违约金，并将实施或转让项目所得收益全部上缴甲方。

4. 乙方违反经费使用规定或经甲方检查确认计划进度不符合本合同约定的，甲方有权减拨或停拨后续项目经费，由此产生的损失由违约方承担；情节严重的，甲方有权终止本合同，同时要求乙方向甲方支付相当于本合同约定的项目经费预算金额【5】%的违约金并返还已拨付的经费。

5.乙方提供的项目工作成果如存在违反相关法律法规、规范性文件或侵犯任何第三方的知识产权、人身权、财产权等权利的，则甲方有权解除本合同，乙方应向甲方支付本合同约定的项目经费预算金额【5】%的违约金并返还已拨付的经费。因此

发生的一切纠纷由乙方自行解决和处理，甲方不承担任何责任，如甲方因此遭受经济损失的，则乙方还应赔偿甲方因此遭受的全部损失。

6. 由于甲方原因造成乙方完成项目时间延误，并经甲方确认的，乙方不承担违约责任；甲方付款延期，本合同按延期时间顺延，甲乙双方不承担违约责任。

（三）除本合同另有约定外，任何一方违反本合同约定的，守约方可就违约事项书面通知违约方要求违约方纠正。如违约方在收到守约方发出的纠正违约通知后【10】日内仍不纠正，或虽已纠正但仍未获得守约方满意的，则构成根本违约，守约方据此可以向违约方发出书面通知单方面终止本合同。

九、不可抗力

因不可抗力（包括但不限于自然灾害、战争或任何其它类似事件等在合同签订、履行期间内发生的不能合理控制、不可预见、无法避免的事件）以及政策调整的原因妨碍、影响或延误任何一方履行合同全部或部分义务，均依法享有违约责任豁免。

出现不可抗力事件时，发生不可抗力的一方应于【】日内及时、充分地向其他方以书面形式发出通知，并告知该类事件对本合同可能产生的影响，并积极采取措施，尽力避免损失的扩大，还应当在合理期限内提供相关证明。

由于不可抗力事件致使合同不能履行或延迟履行，则本合同各方彼此间不承担任何违约责任。因迟延履行后发生不可抗

力的，不能免除责任。

十、其他约定

（一）本合同受中华人民共和国法律管辖并按其进行解释。如双方就本合同内容或其履行过程中发生的任何争议，双方应通过友好协商进行解决；协商不成的，双方均有权向甲方所在地有管辖权的人民法院提起诉讼。在协商或诉讼期间，甲乙双方对于本合同无争议的条款仍应继续履行。

（二）各方的详细通信地址均记载在合同中，各方任何对于本合同的履行、终止、解除或其他出于合同履行的需要而必须发送的通知均以该地址为准，如因地址欠详、不实或收件方拒收，由此导致的责任由收件方全部承担，且被退回的信件可以作为信件内含的通知已经送达给对方的证据。

一方变更通讯地址，应自变更之日起【10】日内，以书面形式通知其他方；否则，由地址变更方承担由此而引起的相关责任。

（三）本合同的任何一方未能及时行使本合同项下的权利不应被视为放弃该权利，也不影响该方在将来行使该权利。任何一方一次行使或部分行使本合同项下任何权利或其他补救不应影响其再次行使该项权利或补救或任何其他权利和补救。

如果本合同中的任何条款无论因何种原因完全或部分无效或不具有执行力，或违反任何适用的法律，则该条款被视为删除。但本合同的其余条款仍应有效并且有约束力。

（四）本合同经甲乙双方负责人、法定代表人或授权代表

签字并加盖单位公章（含骑缝章）后生效。

（五）本合同一式【伍】份，甲方执【叁】份，乙方执【贰】份，每份均具有同等法律效力。

（六）本合同包括以下文件作为附件，包括但不限于：招投标相关文件（如有）、项目工作初步计划或方案以及其他甲方或乙方认为应当作为附件的文件。附件与本合同具有相同法律效力。

（以下无正文）

附件

政务云租用及网络安全运维项目安全运维服务采购项目（网络安全咨询及技术保障服务）实施方案

一、项目工作内容及要求

（一）工作目标

通过专业的咨询和保障服务，帮助北京市知识产权局识别和评估网络和数据安全风险，提高应急响应效率，提供有效的防护策略和措施，在满足法规和政策要求基础上进一步提高网络和数据安全防护的整体水平。

（二）服务内容及要求

政务云租用及网络安全运维项目安全运维服务采购项目(网络安全咨询及技术保障服务)包括基础信息安全运维服务、安全保障服务、等级保护测评服务、信息系统数据安全风险评估服务，具体服务内容如下：

（一）基础信息安全运维服务	
安全咨询服务	安全咨询服务，安全咨询建议应结合用户网络信息安全现状，参照等级保护、商用密码应用安全等系列标准，从国家政策符合性、监管要求、标准规范符合性、扩展性等多方面进行考虑，协助用户做好与信息化同步的网络安全建设工作，健全网络与信息安全保障体系。 （1）对现有的信息系统的主机操作系统、数据库、管理账号等安全策略配置提供安全咨询，对配置存在的

	安全缺陷指导相应的业务支撑单位完成修复工作； （2）对现有网络安全管理体系进行持续更新，对局安全管理制度，进行修订完善，确保管理体系符合等保及监管要求。 （3）对北京市知识产权局网络安全涉及所有信息系统资产进行梳理，编制风险隐患台账，跟踪安全整改进度，提供技术咨询。 （4）针对网络安全态势、重要系统漏洞等安全预警通告或安全整改通知，及时向北京市知识产权局告知相关危害、影响范围及应对方案。 （5）在各系统信创改造建设整改过程中提供安全咨询，结合网络安全法律法规、监管通知、网络安全等级保护、数据安全风险管理等方面相关要求提出安全建议。
安全巡检	根据采购人要求，采用人工检查和工具扫描相结合的方式，登录信息系统相关主机，对操作系统的账户、端口及进程异常情况进行人工分析，对信息系统文件进行后门排查分析，协助清理后门。
办公终端安全运维	（1）提供非涉密终端涉密检查技术支持，主要包括检查软件准备及人工现场检查配合等；如检查发现安全风险，配合进行整改后结果复查，对两次检查结果进行数据汇总与分析。每年按甲方要求的时间段提供相关服务 （2）终端防病毒控制中心巡检，协助运维管理终端

	防病毒控制中心，包括策略配置、规则库更新等；定期对终端防病毒控制中心病毒查杀情况等安全告警进行巡检及分析，发现安全风险提供安全整改建议及整改后复查。
渗透测试	在采购人的授权和监督下，利用已掌握的漏洞信息，针对采购人指定的业务信息系统（不少于3个）开展非破坏性的模拟黑客攻击测试，发现漏洞反馈整改建议简报，修复后配合进行复测，以确认漏洞是否被完全修复（包括初测及复测），最终出具完整渗透测试报告，报告中需详细记录测试过程。
（二）安全保障服务	
应急响应及重点保障	（1）根据监管要求，在春节、两会、五一、国庆等重要时期，提供7×24远程值守保障服务，对互联网开放信息系统运行情况进行实时监控，及时发现潜在的安全隐患或突发安全事件。 （2）及时响应信息系统的突发安全事件，将事件的损失降到最低，协助清除安全事件对业务系统产生的影响，恢复业务系统的运行，并开展相应的事后分析。
特殊时期护网攻防演练	在监管机构护网攻击前，组织攻击队伍（至少4人）对北京市知识产权局面向互联网的业务系统，通过远程的网络攻击技术，以拿到预定核心目标主机权限或数据库权限为目标，模拟黑客入侵和攻击方法对真实环境系统进行非破坏性攻击测试，全面高效地发现信息系统不

	同层面的薄弱环节，将发现的安全风险进行分析提供安全整改建议，并组织复测，最终结果形成攻防演练总结报告。
安全自查整改服务	根据监管单位要求，制定网络安全检查方案及检查表单，对局机关、促进中心、保护中心及公共服务中心安全管理制度制定及落实情况，安全技术防护措施落实情况进行全面的安全检查（包括对办公终端的漏洞扫描),总结反馈发现的安全风险,提交安全整改建议报告。
源代码审计服务	使用专业工具和人工对指定信息系统源代码依据最佳安全实践，挖掘存在的安全漏洞及系统严重 BUG，有效提升代码质量以及信息系统的网络安全防护能力。满足合规性 GB/T 28448-2019《信息安全技术 网络安全等级保护测评要求》中“应核查是否具有软件安全测试报告和代码审计报告，明确软件存在的安全问题及可能存在的恶意代码”要求。
网络安全培训	依据落实网络安全责任制要求，协助组织开展安全培训工作。根据网络安全、数据安全与等级保护测评等相关法律法规，结合日常工作开展中存在的安全风险及隐患，协助开展有关日常安全意识或网络安全技术技能等维度的安全培训（不少于 4 次)。
（三）等级保护测评服务	
等级保护测评服务	依照国家《GB/T 22239-2019 信息安全技术 网络等级保护基本要求》中三级的要求，提供网络安全等级保

	护技术方面的测评和管理方面的测评，根据差距分析的结果给出整改建议，提供整改咨询。由专业的测评机构，依照国家《信息安全技术 网络安全等级保护基本要求》中三级的要求，进行回归测评，出具符合公安要求的测评报告。
（四）信息系统数据安全风险评估服务	
信息系统数据安全风险评估服务	信息系统数据安全风险评估服务，对指定信息系统依照数据安全合规性评估规范流程开展评估，评估团队开展合规性评估，包括正当必要性评估、基础性安全评估和数据全生命周期安全评估，研判合规性评估结果，对数据处理活动的安全风险进行分析研判，并及时开展风险处置，确保安全风险可控。

（三）服务时间

本项目服务时间为 2026 年 6 月 1 日之日起 1 年。

（四）项目成果文档

1.网络安全咨询及技术保障服务项目工作月报；

2.网络安全管理制度汇编，安全巡检报告、渗透测试报告、攻防演练总结报告、安全培训记录、安全季报；

3.等级保护测评报告；

4.数据安全风险评估报告；

5.网络安全咨询及技术保障服务项目工作总结报告。

二、项目人员配置

为保质保量完成项目任务，乙方为该项目服务团队配备 1

名项目经理及若干名项目团队专职人员，为本项目提供实施服务工作。人员配置表如下：

序号	姓名	性别	年龄	拟在本项目的任职	在本项目承担的工作内容
1	雷雪	女	38	项目经理	实施基础信息安全运维服务、安全保障服务、等级保护测评服务及数据安全风险评估服务，推进项目实施进度，整体负责项目质量管理，整理项目月报、季报等。
2	石磊	男	45	安全专家（项目总监）	实施安全咨询服务，网络安全培训及数据安全风险评估服务。
3	李新宇	男	33	技术负责人	实施基础信息安全运维服务、安全保障服务、等级保护测评服务。
4	刘遥	男	33	技术专家	实施安全保障服务、数据安全风险评估服务。
5	赵清海	男	34	安全服务工程师	实施安全保障服务、等级保护测评服务。
6	李锐	男	29	安全服务工程师	实施基础信息安全运维服务、安全保障服务、数据安全风险评估服务。

7	赵城	男	32	安全服务工程师	实施基础信息安全运维服务、等级保护测评服务、数据安全风险评估服务。
8	阴建军	男	30	安全服务工程师	实施基础信息安全运维服务、安全保障服务、数据安全风险评估服务。
9	刘泓然	男	28	安全服务工程师	实施基础信息安全运维服务、安全保障服务、等级保护测评服务、数据安全风险评估服务

三、项目服务方案

在项目执行期间，乙方严格遵守甲方项目管理要求，每月总结月度工作完成情况，在次月5日前提交网络安全工作月报，按照甲方要求汇报工作情况。具体项目实施方式及计划如下：

（一）基础信息安全运维服务

1.安全咨询服务

（1）策略配置咨询，整个项目执行期间对现有的信息系统的主机操作系统、数据库、管理账号等安全策略配置提供安全咨询，对配置存在的安全缺陷指导相应的业务支撑单位完成修复工作。

（2）管理制度体系更新，在2026年9月至11月期间对现有网络安全管理体系进行持续更新，对局安全管理制度，进行

修订完善，确保管理体系符合等保及监管要求。

（3）风险台账更新，每月对北京市知识产权局网络安全涉及所有信息系统资产进行梳理，编制风险隐患台账，跟踪安全整改进度，提供技术咨询。

（4）日常针对网络安全态势、重要系统漏洞等安全预警通告或安全整改通知，及时向北京市知识产权局告知相关危害、影响范围及应对方案。

（5）在各系统信创改造建设整改过程中提供安全咨询，结合网络安全法律法规、监管通知、网络安全等级保护、数据安全风险管理等方面相关要求提出安全建议。

（6）安全季报，乙方在2026年7月、10月及2027年1月、4月协助甲方总结上一季度网络安全工作情况，编制网络安全工作季报。

2.安全巡检

乙方在2026年8月至10月期间采用人工检查和工具扫描相结合的方式，登录4个信息系统所有相关主机，对操作系统的账户、端口及进程异常情况进行人工分析，反馈检查发现的安全风险，提出安全整改建议，协助复测验证整改情况。

3.办公终端安全运维

（1）乙方根据监管单位检查时间提供非涉密终端涉密检查技术支持，主要包括检查软件准备及人工现场检查配合等；如

检查发现安全风险，配合进行整改后结果复查，对两次检查结果进行数据汇总与分析。每年按甲方要求的时间段提供相关服务。

（2）终端防病毒控制中心巡检，乙方协助运维管理终端防病毒控制中心，包括策略配置、规则库更新等；每月对终端防病毒控制中心病毒查杀情况等安全告警进行巡检及分析，发现安全风险提供安全整改建议及整改后复查。

4.渗透测试

乙方于2027年1月至4月期间在甲方的授权和监督下，利用已掌握的漏洞信息，针对甲方指定的业务信息系统（不少于3个）开展1次非破坏性的模拟黑客攻击测试，发现漏洞反馈整改建议简报，修复后配合进行复测，以确认漏洞是否被完全修复，最终出具完整渗透测试报告。

（二）安全保障服务

1.应急响应及重点保障

（1）乙方根据监管要求，在春节、两会、五一、国庆等重要时期，提供7×24远程值守保障服务，对互联网开放信息系统运行情况进行实时监控，及时发现潜在的安全隐患或突发安全事件。

（2）乙方及时响应信息系统的突发安全事件，将事件的损失降到最低，协助清除安全事件对业务系统产生的影响，恢复

业务系统的运行，并开展相应的事后分析。

2.特殊时期护网攻防演练

乙方在2027年4月至5月期间，组织攻击队伍（至少4人）对北京市知识产权局面向互联网的业务系统，开展1次攻防演练工作，通过远程的网络攻击技术，以拿到预定核心目标主机权限或数据库权限为目标，模拟黑客入侵和攻击方法对真实环境系统进行非破坏性攻击测试，全面高效地发现信息系统不同层面的薄弱环节，将发现的安全风险进行分析提供安全整改建议，并组织复测，最终结果形成应急演练总结报告。

3.安全自查整改服务

乙方在2027年7月至11月期间，制定网络安全检查方案及检查表单，对局机关及三个中心安全管理制度制定及落实情况，安全技术防护措施落实情况进行全面的安全检查（包括对办公终端的漏洞扫描），总结反馈发现的安全风险，提交安全整改建议报告。

4 源代码审计服务

乙方在2026年11月-12月期间使用专业工具和人工对指定信息系统源代码依据最佳安全实践，挖掘存在的安全漏洞及系统严重BUG,有效提升代码质量以及信息系统的网络安全防护能力。满足合规性 GB/T 28448-2019《信息安全技术 网络安全等级保护测评要求》中“应核查是否具有软件安全测试报告和代

码审计报告，明确软件存在的安全问题及可能存在的恶意代码”要求。

5.网络安全培训

依据落实网络安全责任制要求，乙方在2026年9月、2027年4月分别协助甲方开展1次安全意识培训和训1次安全技术培训（合计4次网络安全培训）。

（三）等级保护测评服务

乙方在2027年3月至6月期间协助对1个等级保护三级系统完成如下等级保护相关工作：

依照国家《GB/T 22239-2019 信息安全技术 网络等级保护基本要求》中三级的要求，提供网络安全等级保护技术方面的测评和管理方面的测评，根据差距分析的结果给出整改建议，提供整改咨询。由专业的测评机构，依照国家《信息安全技术 网络安全等级保护基本要求》中三级的要求，进行回归测评，出具符合公安要求的测评报告。

（四）信息系统数据安全风险评估服务

乙方在2027年2月至4月期间，对甲方指定的1个信息系统依照数据安全合规性评估规范流程开展评估，包括正当必要性评估、基础性安全评估和数据全生命周期安全评估，研判合规性评估结果，对数据处理活动的安全风险进行分析研判，反馈数据安全风险评估报告。

四、验收标准

乙方为甲方提供的服务质量应按照本合同约定完成全部项目委托工作、达到工作质量要求并形成和向甲方提交符合本合同约定的相应项目工作成果等。