北京互联网法院2026年度
网络安全运维服务项目合同书

甲方： 北京互联网法院

乙方： 北京瑞和云图科技有限公司

签约日期：2026年4月17日

北京互联网法院2026年度

网络安全运维服务项目合同

甲方（委托方）： 北京互联网法院

联系人： 赵晶

联系地址： 北京市海淀区西四环中路16号院3号楼

联系电话： 13051622170

乙方（受托方）： 北京瑞和云图科技有限公司

联系人： 文玉如

联系地址： 北京市朝阳区胜古中路2号院5号楼金基业大厦317

联系电话： 18901233782

乙方承揽甲方北京互联网法院2026年度网络安全运维服务项目的运维服务，以确保甲方信息系统网络整体的安全稳定可靠运行。根据甲方有关要求，依据国家相关的法律、法规、综合本项目的具体情况，明确甲乙双方的权利和义务，经甲乙双方协商一致，特签订维护服务合同如下：

第1条 项目概况

1.1 项目名称：北京互联网法院2026年度网络安全运维服务项目。

2.1 服务性质：信息系统网络安全及技术支持。

2.2 服务范围：对甲方整体信息系统的安全防护与管理，包括对法院专网、互联网、政务网、VTEL视频专网、庭审专网等信息系统网络的维护，对信息系

统、安全设备进行有效的运行维护和安全管理。负责为甲方提供信息系统网络的互联网暴露面梳理服务、渗透测试服务、代码审计服务、安全风险评估服务、安全常识培训、安全驻场服务、漏洞扫描服务、安全设备运行维护、重大事件安全值守等，确保法院整体系统功能安全稳定运行。

第 2 条 合同总金额

总金额：人民币（大写）叁拾玖万伍仟元整/年（￥395000.00元）。

第 3 条 付款方式

3.1 本合同分三期支付，其中本合同签订生效后甲方向乙方支付合同总金额的 50%作为首付款，人民币（大写）壹拾玖万柒仟伍佰元整（￥197500.00 元），于 2026 年 11 月，乙方向甲方提交下半年漏扫和渗透测试报告等文档后，甲方向乙方支付本合同总金额的 45%款项，即人民币（大写）壹拾柒万柒仟柒佰伍拾元整（￥177750.00 元），在合同到期前一个月，乙方向甲方提交上半年漏扫和渗透测试报告等文档后，经甲方确认乙方无违约行为的，则甲方在乙方提出尾款支付申请并向甲方交付发票后的 10 个工作日内，向乙方支付本合同总价款的 5%尾款，即人民币（大写）壹万玖仟柒佰伍拾元整（￥19750 元）。

3.2 乙方收款账户信息如下：

账户名	北京瑞和云图科技有限公司
开户银行	中国工商银行北京古城支行
银行账号	0200014409200040886

第 4 条 服务期限

服务期【1 】年，自【2026 】年【5 】月【1 】日至【2027 】年【4 】月【30 】

如运维服务期满后甲方需要乙方继续提供运维服务的，甲方应当按照本合同第2条的费用标准向乙方支付运维服务费。

第5条 服务项目

根据北京互联网法院2026年度网络安全运维服务项目的要求，主要为甲方提供信息系统网络的互联网暴露面梳理服务、渗透测试服务、代码审计服务、安全风险评估服务、安全常识培训、安全驻场服务、漏洞扫描服务、安全设备运行维护、重大事件安全值守等安全运维服务，具体内容如下。

5.1.互联网暴露面梳理

序号	服务名称	服务指标要求	
1	互联网暴露面梳理	服务内容	数字资产暴露面：从外部视角识别组织关联数字资产、网站、应用服务、APP、小程序、邮箱信息、源代码、文档、暗网数据等数字资产暴露面，分析发现相关威胁和潜在的风险。
2			敏感数据泄露监测：系统从攻击者的视角通过在搜索引擎、文库、云盘、第三方共享平台、代码托管（Github/Gitee/Gitlab）等渠道，探测发现用户邮箱、电话、网络资产及指纹、技术方案、员工通讯录、用户名密码甚至系统源码等敏感信息。
3		服务范围	甲方在互联网暴露面
4		服务频次	服务期内提供2次
5		服务成果	《信息系统互联网暴露面梳理报告》

5.2.渗透测试服务

序号	服务名称	服务指标要求	
1	渗透测试服务	服务内容	对甲方指定的信息系统进行受控的、非破坏性的渗透测试，提前发现应用系统的隐患及漏洞，为加固整改提供技术依据，以切实保证信息系统安全。
2			供应商应指派专业安全工程师，对信息系统通过模拟黑客使用的漏洞发现技术和攻击手段，对目标网络、系统、主机应用的安全性进行深入探测，发现系统脆弱环节，帮助深入了解系统面临的威胁和存在的脆弱性，并针对发现漏洞提供漏洞修复建议，指导系统建设方进行安全整改，在安全整改后

			进一步复查以验证系统建设方安全整改的效果，有效提高信息系统安全防护能力。
3			每次服务包含初测和若干次复测，并指导系统开发商进行整改，直至无高危漏洞为止。渗透测试工具不得仅使用开源工具，不得使用盗版或破解软件。
4		服务频次	服务期内为至少 7 个系统按用户要求的时间进行 2 次渗透测试。
5		服务范围	至少 7 个系统
6		服务成果	《信息系统渗透测试报告》

5.3.代码审计服务

序号	服务名称	服务指标要求	
1	代码审计服务	服务内容	采用商用源代码分析软件，对应用软件进行分析检测。通过将目标源代码与工具中的软件安全漏洞规则集进行全面地匹配、查找，将源代码中存在的安全漏洞扫描出来，并整理成报告。报告的内容不但包括详细的安全漏洞的信息，还会有相关的安全知识，以及相关的修复建议。
2			审计语言包括：Java、Go、PHP、C、C++、C#、Python、Rust 等。
3			审计范围包括： 1.第三方类库安全审计：对信息系统开发过程中所引入的第三方类库进行漏洞审计，依据 CNVD、CVE 出具第三方类库漏洞审计内容，提供修复建议。 2.前后端开发技术框架安全审计：对搭建信息系统所使用的前后端技术架构进行安全审计，依据 CNVD、CVE 出具前后端开发技术架构洞审计内容，提供修复建议。 3.开源插件、组件安全审计：对搭建信息系统所使用的开源插件、组件进行安全审计，依据 CNVD、CVE 出具开源插件、组件漏洞审计内容，提供修复建议。 4.测试资源投入：服务商自行承担本项目测试所需工具等。
4		服务范围	按需，承诺审计不少于 20 万行代码。
5		服务频次	对同一系统代码进行的复测，不重复计入服务范围。指导系统开发商进行整改，直至无高危漏洞为止。
6		服务成果	测试完成后针对每个系统出具《xxx 系统源代码安全审计报

			告》，报告中需体现针对具体安全漏洞的安全整改建议。

5.4.安全意识和技能培训

序号	服务名称	服务指标要求	
1	安全服务培训	服务内容	为甲方内部人员进行安全意识培训，提升安全认知，培训正确应对技能；通过理论培训、案例分析和实操等方式开展。
2			培训内容包括普通员工的上网安全、邮件安全、通信安全、社会工程学安全、数据安全、防钓鱼、密码和账户安全、数据和隐私保护，物理安全、社交媒体安全、应急响应等。
3			基于本地搭建渗透测试服务平台进行安全技能培训。 提供搭建渗透测试环境平台用于安全服务及技能培训等用途（xss 平台、漏洞扫描器、cms/中间件通用合集工具包、BurpSuite 及其插件、Nmap、SQLmap、ARL 定制款（主要针对字典进行优化，对主动探测功能会更少被 WAF，字典进行优化，并不会影响正常的探测）、Xray（社区版，高级版需要买，现在没有破解的了）、CobaltStrike（红队 shell 工具）、Mimikatz（内网渗透工具 win 服务器）、漏洞文库（收集的漏洞整理为文库性质，包含漏洞编号，漏洞过程，poc 以及修复建议）、CTF 平台（主要用于技能培训或相关考试的平台））
4		服务范围	全员培训、技术人员培训。
5		服务频次	按需提供
6		服务成果	《安全意识培训材料》《安全渗透与攻防技能培训材料》

5.5.安全现场服务

序号	服务名称	服务指标要求	
1	安全现场服务	服务内容	提供专业安全工程师常驻用户现场提供安全值守服务，全面监控信息系统安全运行状态，及时监控、发现、报告，提出安全解决措施，协助甲方组织处置。
2			承担所有安全设备的策略配置和策略维护工作；协同进行网络设备策略制订。
3			根据甲方安全设备授权情况，负责组织安全设备提供方进行软件更新和补丁管理，备份和恢复管理，负责进行安全审计和日志管理，软硬件健康检查，性能优化等，负责安全巡检、风险评估，配合网络安全检查，审核各类访问权限，协助甲

			方制订安全策略
4		服务频次	工作时间每日 9:00-18:00
5		服务范围	所有系统
6		服务人员	工作日现场至少 1 名专业技术人员服务
7		服务成果	《信息系统安全事件处置报告》 《信息系统安全值守服务报告》

5.6.漏洞扫描服务

序号	服务名称	服务指标要求	
1	漏洞扫描服务	服务内容	漏洞扫描服务流程： 1.供应商应对漏洞扫描的目标对象进行全面梳理和识别，识别内容包含但不限于资产类型、IP 地址、责任人、用途、操作系统、数据库等； 2.供应商应提交漏洞扫描工具的情况（包括但不限于：设备厂商、设备型号、网络关键设备和网络安全专用产品安全认证等）、漏洞扫描工作方案（包括但不限于：目标对象、扫描时间、风险规避措施等）及漏洞扫描申请，用户授权后，方可进行； 3.供应商应对漏洞扫描结果进行人工验证，保证漏洞扫描结果的真实性； 4.供应商应提交针对性的解决方案，保证漏洞修复可落地。
2			供应商所使用的漏洞扫描设备具备公安部颁发的《检验检测报告》（提供证书复印件，加盖原厂公章）
3			支持 windows、linux、linux 数据库、linux 网络设备、中间件、IIS 离线检查
4			工具支持对主流虚拟化软件平台进行扫描，包括：OpenStack、KVM、Vmware、Xen、Docker、Huawei FusionSphere 等
5			工具支持对主流操作系统的识别与扫描，包括：Windows、Redhat、Ubuntu、深度、红旗、中标麒麟等
6			扫描针对 windows 系统可采集操作系统基本信息、硬件基本信息、应用软件、进程、活动端口开放情况、开机自启动项、用户列表、主机日志信息、补丁信息、安全审计信息和安全策略配置情况，能够采集浏览器上网记录、USB 使用记录（提供证明截图，加盖原厂公章）

7			支持 NAT 基础功能截图证明，包括 NAT 地址池配置、端口归属地址池、查看 NAT session 功能。（提供证明截图，加盖原厂公章）
8			支持能力组件 VRF 基础功能截图证明，包括创建/删除 VR、加入/退出 VRF、VRF 的动静态路由功能。（提供证明截图，加盖原厂公章）
9			支持地址池、虚拟化网络、路由表管理功能。（提供证明截图，加盖原厂公章）
10			支持安全态势展示功能，包括但不限于资产攻防、资产脆弱性、暴露面等态势统计。（提供证明截图，加盖原厂公章）
11			扫描支持对网站中存在的违规图片进行检测（提供证明截图，加盖原厂公章）
12			扫描支持定位到篡改的页面源码位置并高亮显示。（提供证明截图，加盖原厂公章）
13			扫描支持与微软 WSUS 补丁系统联动。（提供证明截图，加盖原厂公章）
14		服务频次	按需提供
15		服务范围	按需提供
16		服务成果	《信息系统漏扫扫描报告》《信息系统加固整改报告》

5.7.重大保障安全值守

序号	服务名称	服务指标要求	
1	重大保障安全值守	服务内容	每年攻防演练、重大活动会议保障期间，提供 24 小时安全监测服务、安全分析服务、安全加固服务、攻击溯源分析服务等，指派专业技术人员到指定地点开展值守。
2		服务范围	按需提供
3		服务频次	按需提供
4		服务成果	《重大活动网络安全保障报告》

5.8.安全设备、网络设备运行维护

序号	服务名称	服务指标要求	
1	安全设备网络设备运行维护	服务内容	驻场运维提供对安全设备和网络设备的日常运行维护、巡检、监测，保障安全和网络设备稳定运行。出现设备工作异常或者故障，及时报告并提供解决方案意见。每年对安全设备和

			网络设备运行情况进行全面排查检查，提供完善和优化意见建议。
2		服务范围	按需提供
3		服务频次	按需提供
4		服务成果	《安全设备、网络设备运行情况排查报告》

5.9.应急响应服务

序号	服务名称	服务指标要求	
1	应急响应服务	服务内容	提供服务期内应急响应服务。7×24 小时响应甲方突发网络安全事件处置，安全专家工作时间 2 小时内、非工作时间 4 小时内到达现场实质响应，应急内容包括事件确认分析、威胁风险评估、威胁清除、协助系统恢复等。
2		服务范围	按需提供
3		服务频次	按需提供
4		服务成果	《应急响应及巡检服务报告》

第 6 条 甲乙双方的责任和义务

6.1 甲方的责任和义务：

（1）甲方发现系统有异常情况出现后，应及时通知乙方并详细说明故障现象，以便于乙方根据故障现象进行相应准备。

（2）乙方在对系统进行维护或升级过程中，甲方为乙方提供必要的协调帮助和便利设施。维护完毕后，甲方及时派人进行检查和验收并签字确认。

（3）在运维过程中，甲方应给予乙方必要的协助工作，负责协调处理与其它部门以及其它工种的配合事宜。

（4）甲方应根据合同条款及时支付乙方相应的维护费用。

6.2 乙方责任和义务

（1）为信息系统安全防护提供技术支持和保障，确保系统的安全稳定运转。

（2）乙方运维期间，必须遵守甲方的规章制度及安全环保等各项规定。乙方保证严守甲方监控系统设备布局秘密,严防外界人员恶意侵犯。

（3）系统在平时使用过程中出现故障，乙方应在接到甲方正式通知后及时响应。

第 7 条 违约责任

7.1 乙方未按约定提供服务

乙方未按合同规定的服务条款提供技术服务时，应按年度技术服务费的 10%向甲方支付违约金，因乙方未按约定提供服务，影响甲方系统网络正常运营时，应按照受影响期间的天数与合同期间的比例，扣除相应的服务费。给甲方造成损失的，还须承担赔偿责任。除非甲方解除合同，违约金和赔偿金的支付并不免除乙方继续履行合同义务的责任。

7.2 甲方未按约定提供服务

如果甲方不能按期支付乙方服务费，则应从逾期支付七个工作日起，每日按迟延支付金额的 1‰向乙方支付违约金。此项违约金总额不超过迟延支付价款的 10‰。

7.3 由于特殊情况（非乙方原因所致），造成运维服务拖延或不能正常进行，甲方应按实际情况调整维护保养服务时间和内容，不计入违约之内。

第 8 条 合同争议解决

8.1 争议的解决

因履行本合同所发生的和与本合同有关的一切争议，甲、乙双方应首先通过协商方式解决。若协商不成，任何一方均可甲方所在地人民法院提起诉讼。

8.2 争议期间服务的连续性

如果用户和乙方之间发生争议，乙方有义务继续按照服务内容条款中的要求提供服务，不得中断。如果争议的内容是有关甲方应支付的费用，乙方能且只能在做出并向甲方发出书面通知 6 个月之后，终止合同并停止服务。

第 9 条 保密条款

9.1 乙方因承接本合同约定所知悉的该合同信息或甲方信息，以及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，乙方应按照甲方关于保密工作的相关要求，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。

9.2 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协议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。

9.3 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。

9.4 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》。

9.5 乙方承担上述保密义务的期限为长期有效，不因本合同终止或解除而失效。

9.6 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，应按本协议约定承担违约责任。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。

第 10 条 知识产权条款

10.1 乙方保证甲方在使用乙方提供的任何产品、服务时，不受第三方提出的侵犯知识产权指控。如果任何第三方提出与乙方提供的任何产品、服务有关的

侵权指控，乙方须与第三方交涉并承担因此发生的一切法律责任和费用。甲方因上述指控或诉讼赔偿第三方损失的，有权向乙方追偿。

10.2 对在运维过程中获知的甲方或为甲方提供服务的第三方的知识产权，都受本条款保护。

第 11 条 廉政承诺

11.1 乙方承诺：乙方在与甲方缔约、履约及履约结束后，乙方及乙方的工作人员(或通过第三人)不得以任何形式向甲方的工作人员行贿，包括但不限于提供金钱、回扣或其他利益，或就相关利益作出允诺，以获得缔约机会、抬高合同价款、降低合同履行标准。如存在上述情形，一经查实，甲方有权解除本合同，乙方还应向甲方支付相当于本合同已履行金额 30%的违约金，如给甲方造成其他损失，乙方还应赔偿甲方的其他损失。乙方违反本条款，在本合同履约结束后 10 年内，甲方均有权向乙方行使本条款相关权利。乙方承担上述违约责任，不影响乙方和相关人员承担刑事责任。

11.2 甲方承诺：甲方工作人员如有向乙方索要贿赂情形，乙方应及时向甲方或纪检监察机关举报。

第 12 条 其它

12.1 本合同一式肆份，甲乙双方各执贰份，自双方盖章之日起生效。所属附件（如有）与本合同具有同等法律效力。

12.2 本合同执行过程中，所有补充协议经甲乙双方协商签订，盖章签字之日起生效，属于本合同的组成部分，与本合同具有同等法律效力。

12.3 由于非正常原因（地震、洪灾、雷击、台风等自然灾害，火灾等）或人为损坏及操作不当造成的损坏，恢复正常工作所需经费由甲方支付。

12.4 其它未尽事宜，双方协商解决。

（以下无正文，为本合同签署盖章内容）

甲方（盖章）：北京互联网法院　　**乙方（盖章）：北京瑞和云图科技有限公司**

授权代表（签字）：　　授权代表（签字）：

签署时间：【2018】年【4】月【17】日