编号：_____

电子政务网络日常运行维护-信息安全服务

甲方：天安门地区综合管理服务中心

乙方：中安网脉（北京）技术股份有限公司

合同书

根据《中华人民共和国民法典》及其他有关法律、法规之规定，甲乙双方遵循公平、自愿、诚实信用的原则，在协商一致的基础上，就电子政务网络日常运行维护-信息安全服务事宜，签订本合同。

1. 合同文件

下列文件构成本合同的组成部分，应当认为是一个整体，彼此相互解释，相互补充。为便于解释，组成合同的多个文件的优先支配地位的次序如下：

a. 本合同书

b. 中标通知书

c. 合同特殊条款

d. 合同一般条款

e. 投标文件（含澄清文件）

f. 招标文件其他内容（含招标文件补充通知）：

2. 服务内容

中安网脉（北京）技术股份有限公司 主要为天安门地区管理委员会信息安全提供运行维护。

主要服务内容包括：基础设施安全信息库修订、安全设备运行维护、漏洞扫描、重要信息系统安全风险检查、协助甲方开展系统等级保护技术合规性检查、专项检查技术协助服务、重要时期信息安全保障、协助甲方开展应急预案编制、协助甲方开展应急演练、应急响应、终端及服务器安全检查服务、安全管理制度修订、渗透测试、安全培训 14 项工作内容。

服务范围为天安门地区管理委员会重要业务系统，包括运行调度中心指挥调度平台（智能全景系统、联网二期系统、指挥调度系统）、财务系统等本地重要系统的漏扫和渗透等安全服务，安全设备和网络设备的安全漏扫服务，协助处理云上部署的管委 OA 系统和城管 OA 系统相关安全工作，安全设备 32 台的运行维护、授权和更新(2026 年 6 台设备停服需更换新设备【更新设备需为官网原设备指定替换型号】，其余设备采购授权 26 台)，所有 PC 终端的安全检查服务以及专用终端软件的安装与更新。（安全设备清单详见附件 2）。

若在本合同服务期间，甲方因具体情况需变更服务项目，乙方应积极配合甲

方。

3. 合同总价

本合同含税总价：人民币（大写 壹佰伍拾捌万 元整）￥ 1580000 元，最终金额以甲方评审结果为准。

4. 付款方式

本合同的付款方式为：电汇。

5. 服务期限

本合同项下委托事项的完成期限为 12 个月，自 2026 年 6 月 1 起至 2027 年 5 月 31 日止。

6. 合同的生效

本合同经双方各自的授权代表签署、加盖单位公章或合同专用章之日起生效。

采购人名称：天安门地区综合管理服务中心（印章）	供应商名称：中安网脉（北京）技术股份有限公司（印章）
授权代表：（签字）	授权代表：（签字）
地址：北京市东城区东交民巷 44 号	地址：北京市丰台区五圈南路 30 号
邮政编码：100000	邮政编码：100070
电话： 010-65118640	电话：010-63705255
开户银行：	开户银行：工商银行北京科技园支行
帐号：	帐号：0200296409200024908
2026 年 5 月 27 日	2026 年 5 月 27 日

第一条 委托事项及内容

信息安全服务外包采购项目主要为天安门地区管理委员会信息安全提供运行维护。

本合同服务内容包括：基础设施安全信息库修订、安全设备运行维护、漏洞扫描、重要信息系统安全风险检查、协助甲方开展系统等级保护技术合规性检查、专项检查技术协助服务、重要时期信息安全保障、协助甲方开展应急预案编制、协助甲方开展应急演练、应急响应、终端及服务器安全检查服务、安全管理制度修订、渗透测试、安全培训 14 项工作内容。

本项服务范围为天安门地区管理委员会重要业务系统，包括运行调度中心指挥调度平台（智能全景系统、联网二期系统、指挥调度系统）、财务系统等本地重要系统的漏扫和渗透等安全服务，安全设备和网络设备的安全漏扫服务，协助处理云上部署的管委 OA 系统和城管 OA 系统相关安全工作，包括服务器 102 台，服务器操作系统 141 套，安全设备 32 台的运行维护、授权和更新(2026 年 6 台设备停服需更换新设备【更新设备性能及吞吐量等参数需不低于原设备】，其余设备采购授权 26 台)，网络设备 61 台，终端 250 余台,所有 PC 终端的安全检查服务以及专用终端软件的安装与更新。（安全设备清单详见附件 2）

若在本合同服务期间，甲方因具体情况需变更服务项目，乙方应积极配合甲方提供。

第二条 委托要求

乙方接受甲方委托所完成的工作成果应当遵循客观、科学、公平、公正原则，符合国家和相关部门、评估专家对该类项目内容和深度规定的要求及甲方的技术、质量要求。

第三条 委托事项完成期限

本合同项下委托事项的完成期限为 12 个月，自 2026 年 6 月 1 日起至 2027 年 5 月 31 日止。

第四条 委托事项履行地点

本合同项下的委托项目咨询服务履行地点为北京市东城区东交民巷 44 号。

第五条 委托报酬及支付方式

1. 本合同项下委托报酬含税总额为（大写 壹佰伍拾捌万 元整）￥ 1580000 元，最终金额以甲方评审结果为准。

2. 甲方将按以下方式向乙方支付委托报酬：

分期支付：在甲方收到足额财政资金的前提下，乙方应在甲方付款前开具等金额发票并确保甲方收到： 2026 年 6 月底前甲方向乙方支付总合同金额的 35%， 2026 年 12 月 15 日前，支付 2026 年预算剩余款项， 2027 年 6 月 30 日前，甲方根据乙方完成合同服务内容情况开展项目验收，验收合格后支付合同尾款。具体支付时间以甲方财政拨款进度为准，甲方付款时间延迟不构成违约。

3. 甲方不应当支付除委托报酬以外的任何其它费用，乙方也不得要求改变报酬总额。

4. 甲方具体支付时间及支付进度视财政拨款到位情况而定，因财政拨款进度导致逾期付款，不视为甲方违约，甲方不承担任何违约责任。若甲方根据实际情况需要调整付款方式及付款进度的，甲方可提前 10 日通知乙方，经双方协商一致变更本协议第五条相关内容，乙方保证对甲方的变更要求无异议。

乙方指定收款账户信息：

账户名称：中安网脉（北京）技术股份有限公司

开 户 行：工商银行北京科技园支行

账 户 号：0200296409200024908

第六条 甲方权利义务

1. 接受乙方提交的符合本合同约定条件的工作成果或者项目执行文档文件；

2. 审定乙方提交的委托项目工作方案和配套工作计划；

3. 检查监督乙方完成委托项目工作的进度，按季度及按日完成的工作，需定期完成巡检报告及相关的文档输出；

4. 对乙方提交的委托项目工作成果（输出项目的巡检报告及相关运维记录文档）进行验收；

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（办公电脑、办公网络等）。

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. 甲方享有信息化系统运维服务过程中生成的相关数据和个人信息数据的管理、访问、利用和支配权利。

8. 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。

第七条 乙方权利义务

1. 有权接受甲方按照合同约定支付的委托报酬；

2. 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 5 个工作日内一次性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；

3. 乙方应于合同签订之日起 10 个工作日内向甲方提交委托项目工作方案和配套工作计划审核。

4. 乙方保证其服务人员具有相应的资质及丰富的从业经验，乙方在其资格证书许可的范围内，依本合同的约定向甲方提供专业的咨询服务，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；

5. 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的真实性、准确性、合法性、有效性全面负责；

6. 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；

7. 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 5 个工作日内给予书面解释或者答复；

8. 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；

9. 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；

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，应当将设备设施完

好的归还给甲方。

11.政务数据与其他数据分开存储处理；未经甲方同意，不得变更用途、用法，不得公开、转让或向第三方提供；合同终止时按照法律法规和相关制度标准执行。

12.发现重大网络安全漏洞、缺陷等网络安全风险，及时向甲方报告，按照相关规定和要求，第一时间采取临时紧急补救措施，防止发生重大网络安全事件。后续措施和计划及时报请甲方网络安全与信息化工作领导小组批准同意，按程序向市网信办报告。未经网信部门或公安部门同意，不得公开或向第三方提供相关信息。

13.处理政务的信息平台应当优先采用安全可信的硬件和软件产品，涉及密码的应符合国家密码管理规定。

14.项目负责人及重要工作人员变更、业务转型、合并重组、投资并购等可能影响政务网络安全的重大事项，应提前向甲方报告。

15.每年向甲方提交网络安全报告。报告至少包括数据安全管理情况、平台关键软件及核心硬件的供应链安全情况、管理技术团队变化等。

16.乙方作为信息化运行维护外包服务提供商，未经甲方事先书面同意，不得访问、修改、披露、利用、转让、销毁数据。

17.乙方作为信息化运行维护外包服务提供商，在为甲方提供信息化运行维护服务过程中，应严格遵守国家关于个人信息保护和数据安全相关法律法规和制度要求，履行责任义务，切实加强个人信息保护。

18.乙方保证安全开展本合同项下的服务内容，定期对乙方相关人员开展安全教育工作，并为其购买人身险、意外险等相关保险，乙方在服务过程中发生的一切安全责任事故及造成的人身、财产损失由乙方自行承担，甲方不承担任何连带责任。

第八条 项目管理小组及技术人员要求

1.双方各指派一名代表作为本项目负责人，甲方负责人为：赵扬，联系电话为：65118201，乙方负责人为：杨瑞斌，联系电话为：18513023797，项目负责人职责范围包括：统筹协调本所涉及的相关服务内容的执行等工作。任何一方更换项目负责人，需提前至少三个工作日通知对方。

2. 项目技术人员资格

乙方须根据项目要求安排专业技术人员，并确保项目实施队伍的稳定。项目实施过程中，乙方如因正当理由需要调整项目技术人员的，应当提前1个月通知甲方，获得甲方书面同意后方可进行。乙方技术人员的具体要求见技术方案。

第九条 委托项目工作成果的评价、验收

1. 乙方向甲方提交完整的委托项目工作成果（输出项目的巡检报告及相关运维记录文档等文件）后，应当在甲方指定的地点接受甲方对其工作成果进行验收。

2. 乙方项目负责人应当对工作情况做出必要说明，并可以对验收结果申述意见。

3. 如乙方提交的工作成果未通过验收的，乙方应当在甲方规定的期限内进行修改并承担修改费用，并重新申请进行验收；如乙方未在甲方规定的期限内完成修改工作或者经修改后仍未能通过验收的，乙方应当承担违约责任并赔偿由此给甲方造成的全部损失（包括但不限于诉讼仲裁费、律师费、法院或者仲裁机构最终裁定的侵权赔偿费用及甲方承担其他侵权责任所造成的经济损失等）。

4. 乙方提交的委托项目工作成果通过验收的，经双方法定代表或委托代理人签字确认后，作为委托项目工作成果验收合格的依据。

第十条 保密义务

1. 乙方对其在履行合同过程中所知悉的甲方项目技术秘密、商业秘密、国家秘密和工作秘密事项（以下统称保密信息）承担保密责任。

2. 乙方应加强对本方运行维护人员的教育和管理，严格控制甲方提供文件资料的知悉范围。

3. 乙方保证对甲方所提供的保密信息予以妥善保存，仅使用于与完成委托项目工作有关的用途或者目的，并采取行之有效的措施，保证保密法规和要求的落实，确保不发生任何失泄密行为；在缺少相关保密条款约定时，应当至少采取适用于对自己的保密信息同样的保护措施和审慎程度进行保密。一经甲方提出要求，乙方应当按照甲方的指示在收到甲方的书面通知后5个工作日内将收到的含有保密信息的所有文件或者其他资料归还甲方，并不得留档。未经甲方书面同意，乙方一律不得将涉及运维事项的任何资料（包括书面资料和电子文档）转交任何

机构和个人，不得公开甲方的商业秘密。

4. 甲乙双方应签订保密协议作为本合同的附件。乙方技术人员应签订保密承诺书。

5. 本合同项下约定的保密期限为长期。

第十一条 知识产权

1. 在本合同有效期内，乙方利用甲方提供的技术资料和工作条件所完成的新的技术成果，归　甲方排他所有；合同有效期内，甲方利用乙方提交的技术咨询工作成果所完成的新的技术成果，归甲方排他所有。

2. 乙方保证委托项目成果是其独立实施完成，不会受到任何第三方基于侵犯其专利权、商标权、著作权、商业秘密等的诉讼。如果甲方收到上述诉讼，乙方应当配合甲方积极应诉，并承担违约责任以及因此给甲方造成的全部损失，包括但不限于诉讼仲裁费、律师费、法院或者仲裁机构最终裁定的侵权赔偿费用及甲方承担其他侵权责任所造成的经济损失等。

第十二条 违约责任

1. 甲方有下列情形之一的，应当承担违约责任：

（1）因甲方责任造成委托项目工作需要进行重大修改或者返工重作的，应当另行增加费用，其数额由双方商定。

（2）甲方向支付乙方委托报酬以财政资金批复时间为准，若批复资金到位日后，延期支付委托报酬的，每延期一日，按照应付而未付部分的 0.05%向乙方支付违约金。

2. 乙方有下列情形之一的，应当承担违约责任：

（1）乙方未按合同规定的日期提交委托项目工作成果的，每延期一日，应当支付委托报酬 0.1%的违约金；如超过约定期限 30 个工作日仍未能提交的，甲方可以单方解除合同，要求乙方退还全部已支付款项并要求乙方另行支付违约金人民币 30,000.00 元。

（2）如因乙方原因造成合同规定（见附件 1）中的事故等级并且不能按照约定时间处理完成的，一级事故等级，乙方支付违约金人民币 30,000.00 元；二级事故等级，乙方支付违约金人民币 20,000.00 元；三级事故等级，乙方支付违

约金人民币 10,000.00 元；四级事故等级，乙方支付违约金人民币 5,000.00 元。累计因乙方原因造成事故超过 5 次的，甲方有权解除本合同。

（3）如因乙方原因造成乙方提供的工作成果中出现错误，则乙方应当按甲方应当支付的委托报酬的 1%向甲方支付违约金，并赔偿因此给甲方造成的全部直接损失、间接损失以及因理赔或者诉讼所发生的一切费用。

（4）如乙方违反合同第十一条约定，应当采取有效措施防止该保密信息的泄密范围进一步扩大，同时乙方应当向甲方支付违约金人民币 20,000.00 元并赔偿由此给甲方造成的全部直接损失、间接损失以及因理赔或者诉讼所发生的一切费用。

（5）由于地震、台风、战争、政府行为、火灾、疫情、基础电信网络故障、黑客攻击、尚无有效防御措施的计算机病毒的发作及其它各方不能预见并且对其发生和后果不能防止并避免的不可抗力原因，致使任何一方不能履行其在本合同项下的义务，该方不承担由此给他方造成的损失。

（6）除非本合同另有约定，乙方违约的，应向甲方支付委托报酬的 3%作为违约金。

（7）本合同项下约定的乙方违约金的金额，不足以弥补甲方全部损失的（包括直接损失、可得利益损失及主张权利的费用等，例如：诉讼仲裁费、保全费、律师费、公证费、法院或仲裁机构最终裁定的侵权赔偿费用及甲方承担其他侵权责任所造成的经济损失等），甲方有权追偿。

第十三条 争议的解决

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

1. 提交 北京市 仲裁委员会仲裁，仲裁裁决为终局裁决；

2. 依法向甲方所在地有管辖权的人民法院起诉。

第十四条 廉政承诺

合同双方承诺共同加强廉洁自律、反对商业贿赂。

第十五条 其他

1. 本合同自双方签字并盖章之日起生效。

2. 未尽事宜或合同修改，经双方协商一致，签订补充协议，方为有效。补充协议与本合同具有同等法律效力。

3. 本合同一式肆份，甲、乙双方各执贰份，具有同等法律效力。

附件：1. 技术方案

2. 安全设备清单

3. 保密协议

（以下无正文）

（本页无正文，为合同签署页）

采购人名称：天安门地区综合管理服务中心（印章）

授权代表：（签字）

地址：北京市东城区东交民巷 44 号

邮政编码：100000

电话： 010-65118640

开户银行：

帐号：

2026 年 5 月 27 日

供应商名称：中安网脉（北京）技术股份有限公司（印章）

授权代表：（签字）

地址：北京市丰台区五圈南路 30 号

邮政编码：100070

电话：010-63705255

开户银行：工商银行北京科技园支行

帐号：0200296409200024908

2026 年 5 月 27 日

附件 1：技术方案

本项服务范围为天安门地区管理委员会重要业务系统，包括运行调度中心指挥调度平台（智能全景系统、联网二期系统、指挥调度系统）、财务系统等本地重要系统的漏扫和渗透等安全服务，安全设备和网络设备的安全漏扫服务，协助处理云上部署的管委 OA 系统和城管 OA 系统相关安全工作，包括服务器 102 台，服务器操作系统 141 套，安全设备 32 台的运行维护、授权和更新**(2026 年 6 台设备停服需更换新设备【更新设备需为官网原设备指定替换型号】，其余设备采购授权 26 台，投标人须在分项报价表中列明各设备采购授权的金额)**，网络设备 61 台，终端 250 余台，所有 PC 终端的安全检查服务以及专用终端软件的安装与更新。

天安门地区管理委员会经过多年信息化建设，已建立了完备的信息安全责任体系及标准操作规程，实现了信息系统的规范化管理。

技术要求

1.整体服务内容

为天安门地区管理委员会重要业务系统，包括运行调度中心指挥调度平台（智能全景系统、联网二期系统、指挥调度系统）、财务系统等本地重要系统的漏扫和渗透等安全服务，安全设备和网络设备的安全漏扫服务，协助处理云上部署的管委 OA 系统和城管 OA 系统相关安全工作，包括服务器 102 台，服务器操作系统 141 套，安全设备 32 台的运行维护、授权和更新(2026 年 6 台设备停服需更换新设备【更新设备需为官网原设备指定替换型号】，其余设备采购授权 26 台)，网络设备 61 台，终端 250 余台，所有 PC 终端的安全检查服务以及专用终端软件的安装与更新。

1.1 基础设施安全信息库修订

服务内容

本项工作主要为协助甲方完善天安门地区管理委员会基础设施安全信息库，对天安门地区管理委员会内现有信息资产安全档案开展安全漏洞分析，涵盖网络设备、服务器主机、数据库、业务应用软件、中间件、安全防

护设备等各类资产。通过资产底数梳理，实现基础设施发生安全隐患时，可快速匹配对应信息资产、精准定位故障点位、明确问题风险属性。

供应商将调配专业技术人员全程协助甲方实施该项工作，逐台登录各类基础设施设备，详实采集记录各设备安全配置信息，并依据设备在网络架构中的功能用途完成分类归档。

服务频率

本项服务按需提供，服务期 1 年。

服务成果

本项服务应提交服务成果包含但不限于以下文档：

《基础设施资产分类梳理报告》

《安全设备配置采集报告》

《基础设施设备安全配置采集表》

1.2安全设备运行维护

本项服务是指对天安门地区管理委员会安全设备进行配置维护，包括设备巡检、设备升级、策略梳理、策略配置及备份、安全事件分析等。

1.2.1 设备巡检

服务内容

每天，安全工程师将通过巡检等手段，对天安门地区管理委员会安全设备的运行状态进行巡检。包括防火墙、VPN、入侵检测系统、云主机免疫系统等监视信息系统运行环境信息，包括设备网络数据流量、关键设备内存和 CPU 使用情况、硬盘容量情况、访问日志情况、配置日志情况、IDS/IPS 告警情况等数据，云服务器运行情况，逐渐形成常态情况下的环境数据。

服务频率

本项服务的服务频率为每天 1 次，服务期 1 年。

服务成果

本项服务应提交服务成果包含但不限于以下文档：

《XX 年 XX 月 XX 日安全设备巡检记录表》

1.2.2 设备升级

服务内容

运维人员每周对项目范围内 32 台安全产品开展巡检，核查厂商软件版本、规则库及特征库更新通告，并及时向用户方反馈；依据用户反馈结果，对具备采购授权条件的设备统一完成授权采购及版本升级。

针对厂商已停止服务、无法在线升级的设备，供应商负责提供设备更换方案，完成设备替换部署，全程保障现有业务与系统功能稳定运行不受影响。

对于非原厂供货类设备，由供应商运维人员协同设备原厂商开展升级作业；所有升级操作前均完成系统配置文件备份、升级包完整性校验测试，确保升级后设备正常运行，全程操作记录完整归档备案。

服务频率

本项服务的服务频率为每周 1 次，服务期 1 年。

服务成果

本项服务应提交服务成果包含但不限于以下文档：

《安全设备升级更新记录》

1.2.3 策略梳理

对天安门地区管理委员会安全设备进行 1 次策略配置行优化，对冗余的策略和废弃的策略进行梳理，在和业务系统相关人员进行确认后进行删除，提高安全产品运行效率。

服务频率

本项服务的服务频率为每年 1 次，服务期 1 年。

服务成果

本项服务应提交服务成果包含但不限于以下文档：

《XX 安全设备安全策略运维记录》

1.2.4 策略配置及备份

业务系统的每一次上线、变更都会涉及到网络安全防护策略的调整，在此过程中，供应商应按照天安门地区管理委员会总体安全策略，分析业务系统实际安全需求和安全产品功能，对安全产品的安全策略进行配置，配置过程遵循策略配置流程，对策略需求进行严格审核。

为了保证安全产品出现故障时能够及时恢复，每次安全产品策略变更后均需对产品的配置和策略进行备份，备份内容存放在专用的服务器，并对备份操作记录备案。

服务频率

本项服务按需提供，服务期 1 年。

服务成果

本项服务应提交服务成果包含但不限于以下文档：

《XX 安全设备安全策略运维记录》

1.2.5 安全告警及事件分析

安全产品会产生大量的网络访问日志、管理行为记录、操作行为记录、产品运行记录和网络流量等数据，以及安全监测产生的大量告警信息，这些信息数量庞大并且无明显关系，但其中可能隐含着潜在的网络攻击行为或已经发生但未发现的攻击行为、产品故障等。供应商应利用安全管理平台等工具，结合资产信息等实际情况，找出这些海量数据中的关联关系，设置各种关联分析规则和过滤条件，挖掘出有价值的网络攻击、运行故障等信息。

通过以上服务可以在保证及时发现安全产品运行状态异常的情况的同时，在某局部出现异常时能够做到提前预警，安全事件发生时能够及时有效处理。

服务频率

本项服务按需提供，服务期 1 年。

服务成果

本项服务应提交服务成果包含但不限于以下文档：

《XX 年 XX 月 XX 日安全告警事件处置记录》

1.3 漏洞扫描

服务内容

使用漏洞扫描系统对天安门地区管理委员会天安门地区管理委员会所有信息系统进行一次全面的工具扫描评估。网络扫描主要依靠带有安全漏洞知识库的网络安全扫描工具对信息资产进行基于网络层面安全扫描，其特点是能对被评估目标进行覆盖面广泛的安全漏洞查找，并且评估环境与被评估对象在线运行的环境完全一致，能较真实地反映主机系统、网络设备、应用系统所存在的网络安全问题和面临的网络安全威胁。

服务频率

本项服务的服务频率为每三个月 1 次，每年 4 次。

服务成果

本项服务应提交服务成果包含但不限于以下文档：

《天安门地区管理委员会信息系统 X 年 X 月安全扫描报告》

《天安门地区管理委员会信息中心信息系统 X 年 X 月安全扫描加固建议》

1.4 重要信息系统安全风险检查

服务内容

对天安门地区管理委员会在用的重要信息系统进行安全检查，检查内容包括：

系统风险评估，对信息系统进行网络设备、操作系统、安全设备及应用中间件进行脆弱性评估，涉密检查，评估将采用人工登录操作及检查工具的方式进行。

检查范围涵盖 61 台网络设备、32 台安全设备等。

服务频率

本项服务按需提供，服务期 1 年。

服务成果

本项服务应提交服务成果包含但不限于以下文档：

《XX 系统安全风险检查报告》

1.5 系统等级保护技术合规性检查

服务内容

按照信息系统等级保护基本要求对天安门地区综合业务管理平台、天安门地区运行调度中心指挥调度平台（包括三个子系统：视频监控联网二期系统、天安门地区管理委员会运行调度中心指挥调度系统、智能全景系统）、财务系统、及其他甲方要求的信息系统的应用层面、数据等层面进行符合等级保护测评及密码应用安全性评估的合规性检查。

服务频率

本项服务按需提供，服务期 1 年。

服务成果

本项服务应提交服务成果包含但不限于以下文档：

《XX 系统技术合规性检查报告》

1.6 专项检查技术协助服务

服务内容

需按照中央网信办相关要求在指定时间段内，在行业范围内开展专项安全检查工作，检查对象为 2-3 个天安门地区管理委员会直属单位。在此过程中，供应商应提供专项技术协助服务，包括：

1）协助编制现场检查方案和现场抽查技术方案；

2）协助下发及收集调查问卷、汇总调查结果数据、编制调查报告等；

3）协助对检查对象进行远程渗透；

4）协助对检查对象进行现场漏洞扫描及关键系统安全配置检查等技术操作类检查，形成现场检查报告；

5）协助对天安门地区管理委员会以外的检查对象进行现场安全意识、安全责任、安全管理制度等方面的检查。

服务频率

本项服务按需提供，服务期 1 年。

1.7 重要时期信息安全保障

服务内容

在重大节假日，安排专业技术人员双人 7*24 小时驻场值守服务，对该期间网络及重要信息系统安全运行情况进行实时监控，并提供 7*24 小时安全事件应急响应服务：包括事件起因分析、后门检查、漏洞分析，安全事件抑制、消除和恢复系统正常，安全事件总结与分析等。在接到应急响应服务请求后，安全专家依据安全事件的分类和应急响应的目标，及时提供远程或现场应急响应，协助用户和现场工程师进行有效的应急处理。

在“两会、五一、国庆”等重要时期，加强驻场和二线人力保障，对该期间网络及重要信息系统安全运行情况进行实时监控，确保各类安全事件在第一时间处理解决，保障天安门地区管理委员会网络与信息系统的安全运行。

服务频率

本项服务服务期内按需提供，服务期 1 年。

服务成果

本项服务应提交服务成果包含但不限于以下文档：

《重要时期安全服务应急保障方案》

1.8 应急预案

服务内容

甲方结合地区信息系统重要程度、业务运行特点，严格落实国家及北京市信息安全保障相关政策要求，自主开展信息系统专项应急预案编制，健全应急响应组织体系，完善风险预防、安全预警工作机制，并依据系统运行特性及各类突发安全事件场景，规范梳理应急处置流程。针对已完成等保定级备案的业务系统，按照网络安全等级保护相关规范要求，完成对应应急预案完善修订工作。供应商依托专业技术支撑能力，结合安全风险分析成果，为甲方预案编制工作提供专业咨询、优化完善建议。

服务频率

本项服务的服务频率为每年 1 次，服务期 1 年。

服务成果

本项服务应提交服务成果包含但不限于以下文档：

《天安门地区管理委员会 XX 系统专项应急预案》

1.9 应急演练

服务内容

甲方依据自身应急预案及既定应急处置流程，编制应急演练方案并组织开展应急模拟演练，使各相关方熟练掌握应急响应流程，提升安全事件应急处置能力；同时通过演练验证应急预案的科学性与适用性，做好总结复盘，结合实际需求完成应急预案修订完善工作，明晰各岗位人员应急职责与处置流程，确保安全事件发生时能够规范有序开展应急处置，最大限度降低事件造成的危害与损失。供应商安排专业技术人员开展安全分析，为甲方演练方案编制、演练实施及预案优化完善工作提供专业参考与合理化改进建议。

服务频率

本项服务的服务频率为每年 2 次，服务期 1 年。

服务成果

本项服务应提交服务成果包含但不限于以下文档：

《天安门地区管理委员会信息安全应急演练方案》

《天安门地区管理委员会信息安全应急演练报告》

1.10 应急响应

服务内容

本项服务采用本地和远程两种方式并行，供应商在安排现场保障人员之外，还应具有专业、强大的应急专家资源保证，能在天安门地区管理委员会出现紧急情况、发生安全事件时，派出技术专家在 2 小时内到达现场进行及时有效的应急处理，最大限度减少安全事件的损失和影响。

服务频率

本项服务按需提供，服务期 1 年。

服务成果

本项服务应提交服务成果包含但不限于以下文档：

《天安门地区管理委员会应急响应支持报告》

1.11 终端及服务器安全检查服务

服务内容

供应商应派出专业化服务人员，针对天安门地区管理委员会及 2-3 个直属单位涉及的 250 余台终端进行安全抽查检查，针对关键计算机进行重点检查；对管委系统部署的云上及本地服务器进行安全检查。检查人员在获得用户授权许可的前提下，采用登录相关的终端和使用检查工具扫描，以发现存在的安全隐患，并提出改进建议。

服务频率

本项服务的服务频率为每季度开展 1 次，每年共开展 4 次，服务期 1 年。

服务成果

本项服务应提交服务成果包含但不限于以下文档：

《天安门地区管理委员会第 X 季度终端安全检查报告》

1.12 安全管理制度修订

服务内容

本项服务主要围绕天安门地区管理委员会信息安全管理组织架构优化完善、信息安全管理体系健全提升开展相关工作。由甲方结合实际管理需求，完成信息安全管理制度、规范及相关要求的修订完善工作，最终相关制度成果按要求通过地区组织专家评审。

供应商依托专业技术能力开展现状梳理与风险研判，为甲方相关工作提供专业支撑及合理化优化建议，主要工作配合内容包括：

协助梳理审视安全风险现状及风险处置计划；

配合明确信息安全管理体系文件整体框架；

为甲方体系文件编制工作提供专业参考建议；

配合开展信息安全管理体系文件相关审核优化工作。

服务频率

本项服务的服务频率为每年 1 次，服务期 1 年。

服务成果

本项服务应提交服务成果包含但不限于以下文档：

《天安门地区管理委员会信息安全制度汇编》

1.13 渗透测试

服务内容

供应商需对天安门地区管理委员会在用的业务系统包括但不限于综合业务管理平台、天安门地区运行调度中心指挥调度平台、财务系统等重要业务系统进行受控的、非破坏性的渗透测试和分析，查找存在的安全隐患，并针对安全隐患提出解决办法，切实保证对外服务的信息系统的安全。在对信息系统进行渗透测试之后，应通过报告形式说明渗透测试结果，还应向信息系统服务商或开发商讲解安全渗透测试结果并指导开发人员完成网站系统应用漏洞的加固操作，需要根据客户要求和实际业务要求对检查问题的整改情况提供复测服务配合开发商完成漏洞修复。

服务频率

本项服务的服务频率为每半年 1 次，服务期 1 年。

服务成果

本项服务应提交服务成果包含但不限于以下文档：

《XX 渗透报告》

1.14 安全培训

服务内容

供应商应组织协调中级、高级信息安全工程师，针对天安门地区管理委员会及 2-3 个直属单位工作人员进行安全知识培训。

服务频率

本项服务的服务频率为每年开展 1 次，服务期 1 年。

服务成果

本项服务应提交服务成果包含但不限于以下文档：

《信息安全培训 PPT》

一、其他要求

1. 服务团队要求

为了保证本项目顺利实施，确保项目质量并达到预期目标，加强项目管理和协调合作，使工作和责任更加清晰明确，本项目应建立分工明确，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。供应商须为本项目组建稳定的、专业的、独立的服务团队，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。

本项目的项目经理应至少具有 5 年以上相关项目实施经验。主要技术人员应至少具有 3 年以上信息安全技术服务经验，人员要求全职参与该项目。服务团队有明确分工和侧重点，基本人员均掌握一般的服务方法并能解决普遍性安全问题。

服务团队人员要严格遵守采购人的各项规章制度和管理规定，爱岗敬业，不得擅离职守或做与工作无关的事情，能够与客户进行很好的沟通，具有很强的工作责任心和客户服务意识。

2. 服务质量保证

由于信息技术的专业性、复杂性和长期性，在服务保障方面，提出了以下服务要求：提供项目实施的工作计划，工作内容以及服务进度安排，制订并遵循服务规程。具有高端的网络维护与网络安全专业技术团队、具有专业的服务方案制作和故障分析人员、具有专业的维护人员和团队支持。能够提供规范的全方位的技术培训，具有良好的职业道德，不损害用户利益。中标方在服务过程中应严格按照相关安全标准，针对服务的各个环节，有专门的项目质量管理保障，包括完善的项目实施流程、实施文档模版和质量记录文档。

3. 保密要求

供应商应严格遵守合同中保密相关规定，遵守国家《保密法》及保密相关法律法规，严格遵守采购人的保密规定和工作制度，并承担相应的保密责任；供应商所有参与本项目的服务人员，都必须签订《保密承诺书》。中标方负责对《保密承诺书》归档保管，接受采购人检查。供应商要对承诺履行情况负有监督责任，一经发现违反承诺情况，要及时向采购人报告。供应商应自觉接受采购人的安全

保密监督和管理，供应商如违反安全保密条款，采购人将追究其责任，对重大的泄密事件将移交司法部门追究其法律责任；对供应商泄露系统资料，对采购人造成负面影响和损失的，除依据有关规定追究有关责任人员法律责任外，还将依法承担相应的民事责任。

4. 安全服务基本要求

（1）驻场服务人员不少于 2 人，提供 5×8 小时现场工作，工作时间与采购人的人员工作时间保持一致；

（2）驻场服务人员要求具备丰富的安全运维服务经验以及资质证书；

（3）开展信息安全服务过程中不得影响天安门地区管理委员会信息系统正常运行。

附件 2：安全设备清单

类型	设备名称用途	品牌型号	设备启用时间	序列号	备注说明
政务外网	平台网防火墙-公安分局防火墙	绿盟-CK7300	2019	18-52-P-1132	
	平台网防火墙-公安分局防火墙	绿盟-CK7300	2019	18-52-P-1131	
	SAS 安全审计系统	绿盟	2019	18-52-P-0546	停服需更新
	SAS 安全审计系统	绿盟	2019	18-52-P-0545	停服需更新
	TAC 威胁分析系统	绿盟	2019	18-52-P-0547	
	DAS 数据路审计系统	绿盟	2019	18-52-J-1059	
	LAS 日志审计系统	绿盟	2019	18-52-P-1139	停服需更新
	OSMS 运维安全管理系统	绿盟	2019	18-52-J-0460	
	RSAS 远程安全评估系统	绿盟	2019	18-52-J-0421	
	平台网防火墙	绿盟_CK6200	2019	18-52-J-1133	停服需更新
	平台网防火墙	绿盟_CK6200	2019	18-52-J-1134	停服需更新
	四库网防火墙	华为_USG6310S	2019	21500500642SG8900175	永久有效
	外联单位防火墙	绿盟_CK7300	2019	18-52-P-1130	
	外联单位防火墙	绿盟_CK7300	2019	18-52-P-0539	
	外联单位入侵检测	绿盟	2019	18-52-J-1137	
	外联区 NAT 防火墙_短信平台 FW	绿盟_CK7300	2019	18-52-L-0469	停服需更新
	平台入侵防护系统	绿盟	2019	18-52-J-1135	

	平台入侵防护系统	绿盟	2019	18-52-J-1136	
	安天智甲杀毒（终端）-政务云	安天智甲	2020	a178a193f7eb7e70a52ccf77db0254ef	政务云 OA
	安天智甲杀毒（服务器）-政务云	安天智甲	2020	f838ed4de4f1d79d10df75888e8r6e38	政务云 OA
	北信源数据内容保密检查系统	北信源	2024	c9cc837d1870-465d-bdb8-6c673995be81	每年按需求采购授权
	安信天行主机免疫系统	安信天行	2018	softwaresign	长期有效
平台互联网	平台互联网防火墙	绿盟	2023	23-23-Q-0128	
	平台互联网入侵检测	绿盟	2023	23-23-Q-0129	
委互联网	360 天擎-虚拟机	奇安信	2020	V6BJ-03QH-VWL2-FQB4-9JG9	
	互联网潜伏威胁探针	深信服_STA100	2019	240A4DE6	
	互联网防火墙	深信服_AF2000	2019	B3F0C6CA	
	互联网上网行为管理系统	深信服_ADBJ1050	2023	2704852F	
	互联网防火墙	深信服_AF2000	2019	24B587E3	
	互联网上网行为管理系统	深信服_ADBJ1050	2023	D75276EA	
	安全感知平台	深信服_SIP1000	2019	A87EA9F5	
政务外网杀毒软件	360 天擎-虚拟机	奇安信	2020	V6BJ-03QH-CJFG-LQJC-Y9WZ	

附件 3：保密协议

保密协议

甲方：天安门地区综合管理服务中心

乙方：　中安网脉（北京）技术股份有限公司

为了确保电子政务网络日常运行维护—信息安全运行维护服务外包项目的国家秘密、工作秘密安全，根据《中华人民共和国保守国家秘密法》及有关保密法律法规的规定，经甲乙双方友好协商，签订如下协议：

一、乙方应严格遵守《中华人民共和国保守国家秘密法》及有关保密法律法规的规定，履行保密义务。

二、甲方提供给乙方的所有与电子政务网络日常运行维护安全运维相关的文件、资料、载体（包括光、电、磁、纸介质）、信息等，乙方均需严格保密，未经甲方授权或许可（书面形式），乙方不得以任何形式将所知悉的内容公开宣传、报道，不得以任何形式将相关信息向第三方泄露。

三、乙方应加强保密管理，对工作参与人员定期进行保密教育，签订保密承诺书，禁止工作参与人员泄露所知悉的电子政务网络日常运行维护安全运维相关信息。

四、乙方应保证提供符合保密要求的场所、设备、设施处理电子政务网络日常运行维护安全运维相关文件、资料、载体（包括光、电、磁、纸介质）、信息。设备、设施应与互联网及其它公共信息网络物理隔离，计算机设备应安装“三合一”防护系统和打印刻录审计系统。

五、乙方应采取有效措施，妥善保管与电子政务网络日常运行维护安全运维相关的各种文件、资料、载体（包括光、电、磁、纸介质）、信息等，防止丢失、被盗和扩散。

六、乙方不能独立完成工作任务，需将电子政务网络日常运行维护安全运维相关文件、资料、载体、信息等提供给第三方协助完成的，应征求甲方同意。乙方选择的第三方单位须具备相应保密资格，不得将电子政务网络日常运行维护安全运维相关文件、资料、载体、信息等提供给无保密资格的第三方单位，乙方应对其选择的第三方单位的保密义务承担连带责任。

七、工作完成后，乙方应将所持有的电子政务网络日常运行维护安全运维相

关文件、资料、载体、信息等全部移交甲方，并将计算机硬盘、移动存储介质等存储的过项目（服务）相关信息的存储介质交给甲方进行销毁。确因工作需要留存的文件、资料，应征得甲方同意，并按保密规定进行管理，不得私自复制留存。

八、甲方有权对乙方执行本协议情况、处理电子政务网络日常运行维护安全运维相关信息的场所、设备、设施等进行检查，乙方应配合甲方检查工作。

九、如发生泄密事件，乙方应积极配合甲方的查处工作。因乙方责任造成泄密的，依据具体情节乙方应承担相应的法律责任。

十、本保密协议一式肆份，甲乙双方各执贰份。自签订之日起生效，并长期有效。

（以下无正文，为协议签署页）

甲方（盖章）：天安门地区综合管理服务中心（印章）

法人或授权代表：

签约日期：2026.5.27

乙方（盖章）：中安网脉（北京）技术股份有限公司（印章）

法人或授权代表：

签约日期：2026.5.27