版本号：V1

信息安全运维

（第 1 标段：局机关安全维护）

采购需求

北京市智慧水务发展研究院

2025 年 12 月

信息安全运维

（第 1 标段：局机关安全维护）

采购需求

说明：采购需求中标注★号指标为实质性要求，实质性要求任一项不满足的将被作为无效投标否决。★号标注在序号前，指本序号所有内容均为实质性要求；★号标注在段落前，指仅本段落内容为实质性要求。一、采购标的

★（一）标的名称

信息安全运维（第 1 标段：局机关安全维护）。

★（二）标的内容

1.notes 网维护：notes 网终端巡检、notes 网终故障诊断与处理、notes 网终端迁移；

2.应用安全：渗透测试服务；

3.安全保障：安全技术咨询服务、信息安全意识培训、安全应急演练、应急响应服务、重要时期现场值守、威胁感知平台现场支持；

4.安全监测：互联网 URL 安全监测服务；

5.安全监督检查：网络安全管理现场检查、敏感信息安全检查服务；

6.网络安全设备维护：楼层弱电间网络线缆维护、骨干网专线维护、网络安全设备巡检、网络故障处置、网络安全策略调整、网络安全设备日志分析、特殊及重要时期网络值守服务、楼层交换机（楼层弱电间利旧交换机）硬件维修、新增网络安全设备硬件维修；

7.网络与安全设备授权：威胁感知平台威胁情报库授权、防火墙特征库授权、防病毒网关特征库授权、IPS 入侵防护特征库授权、上网行为管理特征库授权、漏洞扫描特征库授权；

8.防病毒软件授权服务：PC 端授权服务、服务器端授权服务。

二、商务要求

（一）项目实施期限

项目实施期限：本合同服务期 12 个月（其中，防火墙、防病毒网关、IPS 入侵防护、上网行为管理、漏洞扫描设备的特征库授权服务期为 2026 年 5 月 1 日至 2026 年

12 月 31 日；新增网络安全设备硬件维修服务期为 2026 年 5 月 1 日至 2026 年 12 月 31 日）。

（二）项目实施地点

项目实施地点：北京市。

（三）付款条件

1.付款进度

第一次付款：合同签订生效且财政资金拨付到位后，采购人收到供应商提供合格发票后 10 个工作日内，采购人向供应商支付合同总价款的 50%作为首付款；

第二次付款：汛期运行维护服务结束后，供应商按要求提交标准格式汛期服务总结报告，且采购人在收到供应商合格发票后 10 个工作日内，采购人向供应商支付合同总价款的 35%；

第三次付款：2026 年 12 月 31 日前，采购人在收到供应商合格发票后 10 个工作日内，支付合同总价款的 15%。

2.付款方式：转账支票或汇款方式。

3.付款要求：供应商必须在采购人支付每笔款项前提供符合税法规定并符合采购人财务要求的正规合法有效的税务发票，采购人收到上述发票后 10 个工作日内将款项支付给供应商，否则采购人有权暂不付款，并且不承担违约责任。

4.如采购人未收到财政资金而导致逾期向供应商付款的，则采购人不承担逾期付款的责任。在实际支付时，如遇财政部门国库结账等特殊情况，具体支付将根据财政部门有关要求调整执行，由此造成的支付迟延，采购人不承担任何责任。

5.前期费用

（1）本合同价款中包含 2026 年 1 月 1 日至本合同签订之日期间的维护费用，供应商在收到首付款后 10 日内，应将该费用支付给前期维护单位。逾期支付的，采购人有权在后续合同款项支付中予以扣减。

（2）前期维护费用按照以下标准计取：以本合同确定的各维护项目单价为准。

（3）前期维护费用的确定：前期维护费用由采购人按上述标准和实际发生工作量审定。

（4）供应商因支付前期费用产生的费用包含在本合同价款中，采购人不再另行支付。

三、技术要求

★（一）基本要求

1.采购标的需实现的目标

为保障市水务局网络和信息系统的持续稳定运行，履行《中华人民共和国网络安全法》提出的“网络运营者应当履行安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改”的义务，贯彻落实《党委（党组）网络安全工作责任制实施办法》工作要求，开展网络安全运维工作。

2.需执行的国家相关标准、行业标准、地方标准或者其他标准、规范

（1）《中华人民共和国网络安全法》；

（2）《网络安全技术 网络安全运维实施指南》(GB/T 45940-2025)；

（3）《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）；

（4）《信息安全技术 网络安全等级保护实施指南》（GB/T 25058-2019）；

（5）《网络安全技术 信息安全管理体系要求》（GB/T 22080-2025）；

上述标准如有有关机构发布的最新有效版本，以最新版本为准。除非技术规格中另有规定，计量单位均采用中华人民共和国法定计量单位。

（二）具体要求

1.服务内容及要求

（1）notes 网维护

1）notes 网终端巡检

服务内容：供应商应利用检测工具和人工检测相结合的多种方式，定期对 notes 网终端设备进行巡检工作，查找隐患，排除故障。对计算机的运行状态，安全软件的安装更新情况进行检查修复，保证用户的安全使用；做好巡检记录，定期提交运行检查表（每周一次）。

服务范围：notes 网终端设备。

服务频率：每周 1 次。

工作成果：《设备运行检查表》。

2）notes 网故障诊断与处理

服务内容：供应商应协助水务局完成 notes 网终端故障诊断与处理工作，包括对 notes 网网络边界内终端进行维护、对咨询类来电进行解答，对软件操作类问题和故障进行处理、协助 notes 网终端用户安装应用软件及对网络进行维护；同时，协助水务局

对 notes 网终端系统进行管理、配合制定相关 notes 网安全管理制度，并按照北京市保密局、机要局的相关要求，对现有系统进行配置调整等内容，做好诊断工作，提交处理报告。

服务范围：notes 网终端设备。

工作成果：《故障处理报告》。

3）notes 网终端迁移

服务内容：供应商应协助水务局完成 notes 网终端迁移工作，根据水务局工作需求，不定期对 notes 网终端提供迁移服务，防止出现敏感信息泄露情况。

服务范围：notes 网终端设备。

工作成果：《notes 网终端迁移记录》。

（2）应用安全

服务内容：渗透测试服务。供应商应模拟黑客攻击等行为，对水务局指定域名进行非破坏性的渗透测试，分析应用系统所面临的安全威胁和存在的风险，编制渗透测试分析报告。渗透测试为开展安全加固及优化建设提供依据，并指导实施调优及加固工作，渗透测试报告应详细记录测试过程并对测试问题进行总结分析。

服务范围：针对水务在链系统的 URL 全年共开展 25 次渗透测试。

工作成果：《信息系统渗透测试报告》。

（3）安全保障

1）安全技术咨询服务

服务内容：供应商应根据水务局安全需求，提供科学的方案安全技术咨询服务，从风险评估或网络与信息安全等级保护体系建设的角度出发，协助水务局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。安全咨询建议应结合水务局的网络信息安全现状，参照等级保护、ITSS、27000 等系列标准，从国家政策符合性、标准规范符合性、扩展性能、保密性等多方面进行考虑。

服务内容包括但不限于：

①对现有的信息系统、机房及基础网络资产和网络拓扑、数据资产、特权账号资产等提供安全咨询；

②对核心业务系统进行 WEB 安全、数据安全、业务逻辑安全提供安全咨询；

③对使用的云计算基础平台架构及承载的操作系统提供安全咨询。

④对现有运行管理体系进行持续更新，确保管理体系符合等保、27000 系列标准要

求。

⑤对全局网络安全涉及所有互联网资产进行梳理核查，编制资产台帐和风险隐患库，制定安全保障和风险整改方案。

⑥配合开展针对信息化主管的安全检查。

服务频率：本项服务在整个服务期内按采购人需要随时提供。

工作成果：《安全技术咨询服务记录》。

2）信息安全意识培训

服务内容:供应商应根据水务局的业务需要制定切合实际的信息安全意识培训课程和培训计划，通过为水务局提供专业、全面的信息安全理论、信息安全实践等课程，全面提高水务局相关工作人员的安全意识水平和安全技术能力，切实提高水务局信息安全管理能力，保证业务系统安全稳定运行。

现场培训经双方协商，在巡检、现场服务等过程中，对水务局进行的培训，供应商提供教材和教师，水务局提供场地和必要的设施。供应商每次开展的信息安全培训需包括水务局内部及下属各单位，每次开展的规模不少于 300 人。本项目中包含培训所需所有讲师、培训教材、场地租用等费用。

服务频率：每年为北京市水务局提供 2 次的安全相关技术现场培训，以及不少 4 小时的在线视频课程培训。

工作成果：《安全培训记录》。

3）安全应急演练

服务内容：供应商应根据应急预案的要求，协助水务局制定应急演练计划，编制应急演练方案，建立云上和本地网络安全应急机制，并组织云服务商、系统维护商、本地安全服务商等共同开展应急演练工作。通过演练，使水务局熟悉应急演练流程，提高对安全事件的响应能力，同时验证预案的正确性和适用性。在应急演练结束后，总结应急演练的问题，提出整改建议，并配合完成应急预案的修订工作。

服务频率：本项服务开展不少于 2 次。

工作成果：《应急演练记录》。

4）应急响应服务

服务内容：针对水务局发起的应急需求，对云上、本地数据中心的网络安全事件进行快速响应。工程师到达现场后，需及时抑制和消除水务局信息系统网络安全事件，减少因网络安全事件而引起的损失和负面影响。

①7*24 小时服务

供应商在服务期间，为水务局提供 7*24 小时应急响应服务。

供应商需提供成熟完善的安全监控工具、手段，并在每次到现场服务后提供运维文档。

在维护过程中要保障各系统的安全稳定运行，不得影响日常使用。

②电话响应

供应商设立 7*24 的值班响应电话，并安排有经验的工程师接受申告。当水务局出现上述安全事件时，水务局通过供应商指定的热线响应电话进行报障。供应商应保证服务时间内，95%以上的呼叫接通时间小于 30 秒；当供应商需要查阅相关资料再对水务局的问题进行回复时，应确保在 30 分钟内回复。

③现场服务

对于通过电话支持不能解决的故障，供应商应迅速提供现场支持服务，安排经验丰富的技术支持工程师 2 小时内赴现场分析故障原因，制定故障解决方案，并最终排除故障。水务局可以按照故障紧急程度直接要求供应商进行现场服务。

服务频率：本项服务按需提供。

工作成果：《应急响应报告》。

5）重要时期现场值守（签订合同后提供具体人员，投标阶段不需提供）

服务内容：供应商应在法定节假日、汛期、攻防演练、两会等重要活动及会议期间，派遣至少 1 名信息安全相关专业人员到采购人指定的地点，开展 7*24 小时现场安全值守。实时监控水务局全网安全态势，分析异常流量、安全告警，当发现安全事件时及时上报给采购人，并协助采购人启动应急响应机制，有效提升市水务局在特殊时期的网络安全防护能力。

服务频率：本项服务按需开展。

工作成果：《特殊时期安全值守报告》。

6）威胁感知平台现场技术支持

服务内容：供应商需监测、预警、溯源网络安全攻击行为，协调解决网络安全事件，协助优化网络安全策略与服务配置。现场技术支持人员需具备丰富的网络安全技术以及实践经验，能够对网络信息系统的安全隐患进行排查，对重大网络安全事件做出应急响应。

服务频率：本项服务在整个服务期内持续开展。

工作成果：《威胁感知平台现场技术支持服务报告》。

（4）安全监测

服务内容：**互联网 URL 安全监测服务。**供应商在不影响水务局对外服务系统正常运行的情况下，为水务局指定 web 应用系统提供 7*24 网站安全监测与预警服务。通过专业化的服务，监测其对外服务网站的安全性，防范由于网页挂马、网站篡改等问题而造成用户的数据泄漏、不可用等安全风险。监测内容包括但不限于：可用性监测、脆弱性监测、网页挂马监测、链接监测、安全事件监测、网站内容监测、域名劫持监测、后门监测等。其中网站可用性检测周期为 5 分钟/次，网页篡改和挂马检测周期为 1 小时/次。

服务范围：对不少于 11 个互联网 URL 提供监测服务。

工作成果：《互联网 URL 安全监测报告》。

（5）安全监督检查

1）网络安全管理现场检查

服务内容：结合水务局现有情况，完成现场安全检查工作，包括现场管理检查和现场技术检查。通过现场技术检查、文档查阅、人员访谈等方式开展，检查内容包括单位基本情况、网络安全责任制落实情况、网络安全日常管理情况、网络安全应急工作情况、网络安全教育培训情况、终端安全保密情况等，协助水务局从管理方面了解被查单位的网络安全现状，及时发现管理方面的安全隐患。根据检查中的问题，提出优化整改意见。本项目中包含现场检查所需所有技术工具、检测设备、交通工具等费用。

服务频率：本项服务开展不少于 8 家单位。

工作成果：《网络安全管理现场检查工作报告》。

2）敏感信息安全检查服务

服务内容：供应商针对水务局指定单位，派遣专业技术人员通过安全自查工具、文档查验、人员访谈、现场核查等方式进行敏感信息安全检查，防止敏感信息泄露、失窃事件的发生。

服务频率：本项服务开展不少于 8 家单位。

工作成果：《敏感信息安全检查工作报告》。

（6）网络安全设备维护

1）楼层弱电间网络线缆维护

服务内容：针对通州区留庄路 1 号院 1 号楼和 2 号楼，2-8 层 16 个弱电间内的楼

层接入交换机至墙面信息点配线架的网络线缆定期巡检，包括网线配线架、机柜线路、标签检查等，提供线缆新增、调整、线缆清洁保养等，为网络系统稳定高效运行，提供可靠的信息传输环境。

服务频率：本项服务按需开展。

服务成果：《楼层弱电间网络线缆维护报告》。

2）骨干网专线维护

服务内容：通过工具+人工的方式对骨干网专线运行状态进行安全巡检，确保传输数据网络的可用性。一旦发现网络故障问题，专业技术工程师启动应急响应机制，通过技术排查确认局中心的网络通断情况，并通过电话联系局属单位确认故障详情；若仍无法解决，则电话向运营商报修，同时协助局中心和局属单位进行现场处置，最大限度减少业务中断时间，保障骨干网络线路的持续稳定运行。

服务频率：每月 1 次。

服务成果：《骨干网专线维护报告》。

3）网络安全设备巡检

服务内容：针对网络安全设备运行状态进行监控、检测、管理和维护，网络巡检主要内容包括网络设备外观、接电情况、指示灯、CPU 利用率、内存负载、接口状态、模块状态。

服务频率：每月 1 次。

服务成果：《网络安全设备巡检报告》。

4）网络故障处置

服务内容：接到网络故障报告，立即启动故障响应机制，远程或现场接入进行故障排查，通过专业的故障排查工具和技术手段，对故障进行精确诊断和定位，包括检查物理连接、设备状态、网络配置、安全策略等多个方面，以确定故障的具体原因和位置，根据故障诊断结果，采取相应的修复措施。在故障修复后，对网络设备和系统进行全面的检查和优化，以预防类似故障的再次发生。

服务频率：本项服务按需开展。

服务成果：《网络故障处置报告》。

5）网络安全策略调整

服务内容：针对网络环境的持续变化和新出现的威胁，对网络安全策略进行全面审查、评估与优化。包括：配置策略比对、配置策略增添、配置策略删减、配置策略修订、

配置策略备份、配置策略分析等。

服务频率：本项服务按需开展。

服务成果：《网络安全策略调整报告》。

6）网络安全设备日志分析

服务内容：通过收集、整理来自防火墙、防病毒网关、IPS、上网行为管理、漏洞扫描等各类网络安全设备的日志数据，并进行必要的格式化和标准化处理，以便于后续的分析和挖掘。根据设备日志分析网络运行状态，提取出关键的安全事件、异常行为模式以及潜在的安全威胁。

服务频率：每月 1 次。

服务成果：《网络安全设备日志分析报告》。

7）特殊及重要时期值守

服务内容：供应商应在法定节假日、汛期、攻防演练、两会等重要活动及会议期间，派遣至少 1 名网络相关专业人员提供 7*24 小时网络安全设备现场保障。针对网络安全设备进行监控，通过检查设备运行参数（例如 CPU、内存等）、设备运行日志或病毒库等信息，及时发现网络安全设备存在的潜在安全隐患，当网络安全设备发生故障后，协助采购人完成设备隐患排查、设备故障处置等工作，必要时协调设备原厂进行技术支持，从而保障网络安全设备的稳定运行。

服务频率：本项服务按需开展。

工作成果：《特殊及重要时期值守报告》。

8）楼层交换机（楼层弱电间利旧交换机）硬件维修

服务内容：快速响应并解决各类设备硬件故障，包括故障检测、损坏部件更换、性能恢复验证及预防性维护建议等，确保楼层网络畅通无阻，提升整体网络环境的稳定性和可靠性。

设备清单如下：

序号	名称	型号	单位	数量	服务期
1	48 口交换机	华为 5735S-S48T4X-A1	台	9	2026 年 1 月 1 日 -2026 年 12 月 31 日

工作成果：《硬件设备维修记录》。

9）新增网络安全设备硬件维修

服务内容：快速响应并解决各类设备硬件故障，包括故障检测、损坏部件更换、性

能恢复验证及预防性维护建议等，确保楼层网络畅通无阻，提升整体网络环境的稳定性和可靠性。

设备清单如下：

序号	名称	型号	单位	数量	服务期
1	核心交换机	H3C S10508X-G	台	2	2026 年 5 月 1 日-2026 年 12 月 31 日
2	汇聚交换机	H3C S7506X	台	2	
3	24 口交换机	H3C S5560X-30C-PWR-EI	台	7	
4	防火墙	NSG3300-7680-F	台	3	
5	防病毒网关	NSG3300-5680-F	台	2	
6	IPS 入侵防护	P3300-5680-H	台	1	
7	上网行为管理	NSA-GCH-H/V7.0	台	1	
8	日志审计	DAS-LOG-A1500-HU	台	1	
9	堡垒机	DAS-USM/V2.0	台	1	
10	漏洞扫描	DAS-RAS-A2000-KU/V3.0	台	1	
11	光电转换器	netlink HTB-GS-03/SFP	台	40	

工作成果：《硬件设备维修记录》。

（7）网络与安全设备授权

为采购人提供以下网络与安全设备威胁情报库/特征库授权，具体如下：

序号	设备名称	品牌型号	单位	数量	授权期限
1	威胁感知平台	微步在线（TB-TDP-A-2500-FP）	套	1	2026 年 1 月 1 日-2026 年 12 月 31 日
2	威胁感知平台	微步在线（TB-TDP-A-1100-FP）	套	19	
3	防火墙	网神 SecGate 3600 防火墙 NSG3300-7680-F(万兆)/V3.6.6.0	套	3	2026 年 5 月 1 日-2026 年 12 月 31 日
4	防病毒网关	网神 SecGate 3600 防火墙 NSG3300-5680-F(万兆)/V3.6.6.0	套	2	
5	IPS 入侵防护	网神 SecIPS3600 入侵防御系统 P3300-5680-H(万兆)/V1.1	套	1	
6	上网行为管理	奇安信网神网络安全审计系统 NSA-GCH-H/V7.0	套	1	
7	漏洞扫描	DAS-RAS-A2000-KU/V3.0	套	1	

（8）防病毒软件授权服务

服务内容：提供国产化终端及服务器病毒库升级服务，为水务局的业务运行提供可靠的安全保障。

提供现有奇安信网神国产终端防病毒产品升级服务授权，确保水务局内的国产化服务器及办公终端的病毒查杀功能持续有效，定期更新病毒库，提供病毒查杀服务。

具体软件授权清单如下：

序号	设备名称	品牌型号	单位	数量
1	PC 端授权服务	奇安信网神终端安全管理系统（国产终端安全管理系统）V8.0-PC 端一年升级服务	套	4379
2	服务器端授权服务	奇安信网神终端安全管理系统（国产终端安全管理系统）V8.0-服务器端一年升级服务	套	2

2.服务标准

确保 notes 网终端正常运行率到达 95%及以上，当终端出现故障时，供应商 10 分钟内做出响应；

确保安全设备巡检率达到 99%及以上；

突发安全事件应急响应程度达到 99%及以上；

重要时期确保 7*24 小时不间断安全保障。

3.为落实政府采购政策需满足的要求

（1）本项目不专门面向中小企业预留采购份额。

（2）根据《政府采购促进中小企业发展管理办法》（财库[2020]46 号），供应商为小型或微型企业，价格给予 10%的扣除。

（3）根据《财政部民政部中国残疾人联合会关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141 号），残疾人福利性单位视同小微企业。

（4）根据《关于政府采购支持监狱企业发展有关问题的通知》（财库〔2014〕68 号），监狱企业视同小微企业。

★（5）本项目采购产品必须为国产，不接受进口产品。

4.其他要求

汛期及全年运行维护服务结束后，供应商按要求提交服务总结报告，对汛期及全年工作进行总结，服务总结报告内容包括但不限于采购需求服务内容中要求的服务成果文件以及期间开展工作的过程记录等，以便采购人全面准确的了解维护服务实施情况。

5.技术支持

要求供应商拥有一只稳定的保障队伍，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；服务团队有明确分工和侧重点，基本人员均掌握安全服务方法并能解决常见设备的故障问题；技术支持服务形式包括电话、E-Mail 和 Internet 网站等多种技术支持方式。

★服务团队至少配备 3 名现场驻场人员，包括态势感知平台现场技术支持驻场 1 名，安全工程师 1 名，网络工程师 1 名。

项目团队具备 7*24 小时技术支持及应急响应服务能力，接到采购人技术支持请求后，必须立即做出实质性响应，对于驻场人员不能现场解决或其他人员不能通过远程方式解决的问题，项目团队在 30 分钟内给予响应，协调能力更强的资深专业人员 2 小时到达现场，4 小时内予以解决。

6.解决方案或者组织方案

（1）工作组织方案

①notes 网终端巡检

第一等次：制定了工作组织方案，包括工作方法及流程、时间安排、人员安排等主要内容；工作方法及流程清晰，关键点、重点明确，有利于项目实施保障；时间安排计划明确到具体时间；人员安排明确到具体人员，并明确了人员分工职责。

第二等次：制定了工作组织方案，包括工作方法及流程、时间安排、人员安排等主要内容；但工作方法及流程阐述简单，关键点、重点不明确，不利于项目实施保障；或时间安排计划未明确到具体时间；或人员安排未明确到具体人员，或未明确人员分工职责。

第三等次：制定了工作组织方案，但方案整体简单，工作方法及流程或时间安排或人员安排等主要内容有缺失。

第四等次：未制定工作组织方案，或存在不合理。

②notes 网终端故障诊断与处理

第一等次：制定了工作组织方案，包括工作方法及流程、时间安排、人员安排等主要内容；工作方法及流程清晰，关键点、重点明确，有利于项目实施保障；时间安排计划明确到具体时间；人员安排明确到具体人员，并明确了人员分工职责。

第二等次：制定了工作组织方案，包括工作方法及流程、时间安排、人员安排等主要内容；但工作方法及流程阐述简单，关键点、重点不明确，不利于项目实施保障；或时间安排计划未明确到具体时间；或人员安排未明确到具体人员，或未明确人员分工职

责。

第三等次：制定了工作组织方案，但方案整体简单，工作方法及流程或时间安排或人员安排等主要内容有缺失。

第四等次：未制定工作组织方案，或存在不合理。

③notes 网终端迁移

第一等次：制定了工作组织方案，包括工作方法及流程、时间安排、人员安排等主要内容；工作方法及流程清晰，关键点、重点明确，有利于项目实施保障；时间安排计划明确到具体时间；人员安排明确到具体人员，并明确了人员分工职责。

第二等次：制定了工作组织方案，包括工作方法及流程、时间安排、人员安排等主要内容；但工作方法及流程阐述简单，关键点、重点不明确，不利于项目实施保障；或时间安排计划未明确到具体时间；或人员安排未明确到具体人员，或未明确人员分工职责。

第三等次：制定了工作组织方案，但方案整体简单，工作方法及流程或时间安排或人员安排等主要内容有缺失。

第四等次：未制定工作组织方案，或存在不合理。

④渗透测试服务

第一等次：制定了工作组织方案，包括工作方法及流程、时间安排、人员安排等主要内容；工作方法及流程清晰，关键点、重点明确，有利于项目实施保障；时间安排计划明确到具体时间；人员安排明确到具体人员，并明确了人员分工职责。

第二等次：制定了工作组织方案，包括工作方法及流程、时间安排、人员安排等主要内容；但工作方法及流程阐述简单，关键点、重点不明确，不利于项目实施保障；或时间安排计划未明确到具体时间；或人员安排未明确到具体人员，或未明确人员分工职责。

第三等次：制定了工作组织方案，但方案整体简单，工作方法及流程或时间安排或人员安排等主要内容有缺失。

第四等次：未制定工作组织方案，或存在不合理。

⑤安全技术咨询服务

第一等次：制定了工作组织方案，包括工作方法及流程、时间安排、人员安排等主要内容；工作方法及流程清晰，关键点、重点明确，有利于项目实施保障；时间安排计划明确到具体时间；人员安排明确到具体人员，并明确了人员分工职责。

第二等次：制定了工作组织方案，包括工作方法及流程、时间安排、人员安排等主要内容；但工作方法及流程阐述简单，关键点、重点不明确，不利于项目实施保障；或时间安排计划未明确到具体时间；或人员安排未明确到具体人员，或未明确人员分工职责。

第三等次：制定了工作组织方案，但方案整体简单，工作方法及流程或时间安排或人员安排等主要内容有缺失。

第四等次：未制定工作组织方案，或存在不合理。

⑥信息安全意识培训

第一等次：制定了工作组织方案，包括培训内容、授课人员、日程安排等主要内容。培训内容具体细化，授课人员明确清晰，日程安排科学合理。

第二等次：制定了工作组织方案，包括培训内容、授课人员、日程安排等主要内容，但培训内容或授课人员或日程安排描述笼统，缺少关键细节。

第三等次：制定了工作组织方案，但方案整体简单，培训内容或授课人员或日程安排等主要内容有缺失。

第四等次：未制定工作组织方案，或存在不合理。

⑦安全应急演练

第一等次：制定了工作组织方案，包括演练内容、演练人员、日程安排等主要内容。演练内容具体细化，演练人员明确清晰，日程安排科学合理。

第二等次：制定了工作组织方案，包括演练内容、演练人员、日程安排等主要内容，但演练内容或演练人员或日程安排描述笼统，缺少关键细节。

第三等次：制定了工作组织方案，但方案整体简单，演练内容或演练人员或日程安排等主要内容有缺失。

第四等次：未制定工作组织方案，或存在不合理。

⑧应急响应服务

第一等次：制定了工作组织方案，包括应急响应人员安排、应急响应程序、故障预判与解决方案、故障响应及处置措施等主要内容。应急响应人员安排明确清晰；应急响应程序规范具体；故障预判与解决方案全面可行；故障响应及处置措施到位。

第二等次：制定了工作组织方案，包括应急响应人员安排、应急响应程序、故障预判与解决方案、故障响应及处置措施等主要内容，但应急响应人员安排或应急响应程序或故障预判与解决方案或故障响应及处置措施描述笼统，缺少关键细节。

第三等次：制定了工作组织方案，但方案整体简单，应急响应人员安排或应急响应程序或故障预判与解决方案或故障响应及处置措施等主要内容有缺失。

第四等次：未制定工作组织方案，或存在不合理。

⑨重要时期现场值守

第一等次：制定了工作组织方案，包括值守时间安排、值守人员安排、应急处置流程等主要内容。值守时间规划合理详细，明确值守具体时间；人员安排明确到具体人员，并明确了人员分工职责；应急处置流程规范清晰，有利于项目实施保障。

第二等次：制定了工作组织方案，包括值守时间安排、值守人员安排、应急处置流程等主要内容。但值守时间安排未明确到具体时间；或值守人员安排未明确到具体人员，或未明确人员分工职责；或应急处置流程阐述简单，不利于项目实施保障。

第三等次：制定了工作组织方案，但方案整体简单，值守时间安排或值守人员安排或应急处置流程等主要内容有缺失。

第四等次：未制定工作组织方案，或存在不合理。

⑩威胁感知平台现场技术支持

第一等次：制定了工作组织方案，包括工作方法及流程、时间安排、人员安排等主要内容；工作方法及流程清晰，关键点、重点明确，有利于项目实施保障；时间安排计划明确到具体时间；人员安排明确到具体人员，并明确了人员分工职责。

第二等次：制定了工作组织方案，包括工作方法及流程、时间安排、人员安排等主要内容；但工作方法及流程阐述简单，关键点、重点不明确，不利于项目实施保障；或时间安排计划未明确到具体时间；或人员安排未明确到具体人员，或未明确人员分工职责。

第三等次：制定了工作组织方案，但方案整体简单，工作方法及流程或时间安排或人员安排等主要内容有缺失。

第四等次：未制定工作组织方案，或存在不合理。

⑪互联网 URL 安全监测服务

第一等次：制定了工作组织方案，包括工作方法及流程、时间安排、人员安排等主要内容；工作方法及流程清晰，关键点、重点明确，有利于项目实施保障；时间安排计划明确到具体时间；人员安排明确到具体人员，并明确了人员分工职责。

第二等次：制定了工作组织方案，包括工作方法及流程、时间安排、人员安排等主要内容；但工作方法及流程阐述简单，关键点、重点不明确，不利于项目实施保障；或

时间安排计划未明确到具体时间；或人员安排未明确到具体人员，或未明确人员分工职责。

第三等次：制定了工作组织方案，但方案整体简单，工作方法及流程或时间安排或人员安排等主要内容有缺失。

第四等次：未制定工作组织方案，或存在不合理。

⑫网络安全管理现场检查

第一等次：制定了工作组织方案，包括工作方法及流程、时间安排、人员安排等主要内容；工作方法及流程清晰，关键点、重点明确，有利于项目实施保障；时间安排计划明确到具体时间；人员安排明确到具体人员，并明确了人员分工职责。

第二等次：制定了工作组织方案，包括工作方法及流程、时间安排、人员安排等主要内容；但工作方法及流程阐述简单，关键点、重点不明确，不利于项目实施保障；或时间安排计划未明确到具体时间；或人员安排未明确到具体人员，或未明确人员分工职责。

第三等次：制定了工作组织方案，但方案整体简单，工作方法及流程或时间安排或人员安排等主要内容有缺失。

第四等次：未制定工作组织方案，或存在不合理。

⑬敏感信息安全检查服务

第一等次：制定了工作组织方案，包括工作方法及流程、时间安排、人员安排等主要内容；工作方法及流程清晰，关键点、重点明确，有利于项目实施保障；时间安排计划明确到具体时间；人员安排明确到具体人员，并明确了人员分工职责。

第二等次：制定了工作组织方案，包括工作方法及流程、时间安排、人员安排等主要内容；但工作方法及流程阐述简单，关键点、重点不明确，不利于项目实施保障；或时间安排计划未明确到具体时间；或人员安排未明确到具体人员，或未明确人员分工职责。

第三等次：制定了工作组织方案，但方案整体简单，工作方法及流程或时间安排或人员安排等主要内容有缺失。

第四等次：未制定工作组织方案，或存在不合理。

⑭网络安全设备维护

第一等次：制定了工作组织方案，包括工作方法及流程、时间安排、人员安排等主要内容；工作方法及流程清晰，关键点、重点明确，有利于项目实施保障；时间安排计

划明确到具体时间；人员安排明确到具体人员，并明确了人员分工职责。

第二等次：制定了工作组织方案，包括工作方法及流程、时间安排、人员安排等主要内容；但工作方法及流程阐述简单，关键点、重点不明确，不利于项目实施保障；或时间安排计划未明确到具体时间；或人员安排未明确到具体人员，或未明确人员分工职责。

第三等次：制定了工作组织方案，但方案整体简单，工作方法及流程或时间安排或人员安排等主要内容有缺失。

第四等次：未制定工作组织方案，或存在不合理。

（2）项目管理人员组织安排

1）供应商拟派项目负责人的能力

第一等次：拟派项目负责人具有信息安全相关专业高级及以上技术职称或者信息系统项目管理师职业资格。

第二等次：拟派项目负责人具有信息安全相关专业中级技术职称或者信息安全工程师职业资格。

第三等次：其他。

注：需提供有效职称证书或信息系统项目管理师职业资格证书或信息安全工程师职业资格证书复印件或扫描件作为证明材料，信息安全相关专业以职称证书上写明的专业为准，未提供有效证明不予计分。

2）供应商拟投入本项目其他专业技术人员的能力（除项目负责人外）

第一等次：拟投入本项目其他专业技术人员中有网络规划设计师、信息安全工程师、系统规划与管理师。

第二等次：拟投入本项目其他专业技术人员中有上述任意 2 类人员。

第三等次：拟投入本项目其他专业技术人员中有上述任意 1 类人员。

第四等次：其他。

注：需提供有效网络规划设计师职业资格证书或信息安全工程师职业资格证书或系统规划与管理师职业资格证书复印件或扫描件作为证明材料，未提供有效证明不予计分。

（3）质量控制措施

第一等次：制定了质量控制措施，方案包括针对各项工作内容制定相应的质量控制方法和流程、时间安排、人员安排等主要内容；质量控制方法和流程阐述系统详尽，关键点、重点突出，有利于项目实施保障；时间安排计划明确到具体时间；人员安排明确

到具体人员，并明确了人员分工职责。

第二等次：制定了质量控制措施，方案包括针对各项工作内容制定相应的质量控制方法和流程、时间安排、人员安排等主要内容；但质量控制方法和流程阐述简单，关键点、重点不明确，不利于项目实施保障；或时间安排计划未明确到具体时间；或人员安排未明确到具体人员，或未明确人员分工职责。

第三等次：制定了质量控制措施，但方案整体简单，各项工作内容制定相应的质量控制方法和流程或时间安排或人员安排等主要内容有缺失。

第四等次：未制定质量控制措施，或存在不合理。

（4）资源配置计划

第一等次：项目实施所需工器具及设备配置充足，且工器具及设备具有智能、先进等特点，能提高工作质量和效率。

第二等次：项目实施所需工器具及设备配置满足需求，但工器具及设备智能、先进性不足。

第三等次：项目实施所需工器具及设备配置满足需求，但比较落后。

第四等次：未提供项目实施所需工器具及设备，或不满足项目需求。

（5）保密方案及保障措施

第一等次：结合项目组织实施，制定了有效的保密制度，明确重点、难点，并提出保障措施。

第二等次：结合项目组织实施，制定了有效的保密制度，但没有明确重点、难点及保障措施。

第三等次：制定了保密制度，但未与本项目实施结合，针对性差。

第四等次：未制定保密制度，或存在不合理。

（三）验收标准

供应商应于合同服务期结束后的 15 个工作日内向采购人提交验收申请及项目验收材料，经采购人审核后组织召开双方参与的会议，汇报年度服务情况和合同执行情况。项目验收材料包括但不限于以下内容：项目合同、周期报告、日常维护记录、工作总结报告、验收申请报告等。采购人检查验收材料，对运维情况进行评价，并出具正式的验收意见。项目验收通过后，供应商应按照档案归档要求整理验收资料，并将资料移交给采购人。验收不合格的，由供应商按要求弥补缺陷后再次组织验收，直至验收合格。

具体验收方案见合同履约验收方案。