海淀区政务网络安全监测服务项目
运维服务合同

项目名称：　海淀区政务网络安全监测服务项目

甲　　方：　北京市海淀区大数据中心

乙　　方：　北京启明星辰信息安全技术有限公司

合同编号：

签订地点：　北京市海淀区

合同正文

甲方：北京市海淀区大数据中心

法定代表人：刘大鹏

地址：北京市海淀区中关村南大街 5 号 1 区 689 号海淀科技大厦

乙方：北京启明星辰信息安全技术有限公司

法定代表人：严立

地址：北京市海淀区东北旺西路 8 号 21 号楼启明星辰大厦 102 号

根据《中华人民共和国政府采购法》、《中华人民共和国民法典》等有关法律法规规定，海淀区政务网络安全监测服务项目经甲方公开招标，确定乙方为中标供应商，甲乙双方本着平等、自愿和诚实信用原则，签订本合同。

第一条　　定义

1.下列名词和用语，除上下文另有规定外，应有如下含义：

（1）“项目”指甲方委托乙方的海淀区政务网络安全监测服务项目。

（2）“甲方”是指承担直接投资责任和委托服务业务的一方。

（3）“乙方”是指在工商行政管理部门登记注册，取得企业法人营业执照，为甲方提供本合同约定运维服务的单位。

（4）“日”是指任何一天零时至第二天零时的时间段。

（5）“月”是指根据公历从一个月份中任何一天开始到下个月对应日期的前一天的时间段。

（6）“总投资”是甲方与乙方所签合同的总金额。

（7）“交付”指乙方按本合同约定向甲方提交运维服务过程中产生的技术资料、系统运行报告、故障处理记录、月度/季度服务总结等成果，并经甲方确认接收的过程。

（8）“培训”为确保甲方使用人员能够正常使用系统，乙方向甲方使用人员提供的必要技术培训和技术指导。

（9）“验收”指甲方按照本合同约定的验收要求，对乙方运维服务成果进

行评审，验收通过以双方签署的《海淀区政务网络安全监测服务项目验收单》为标志。

（10）“运维服务”：指乙方根据本合同约定，为甲方海淀区政务网络安全监测服务项目提供的运维相关持续性服务。

（11）“服务期限”：指本合同约定的乙方为甲方提供运维服务的起止时间。

（12）“保密信息”指乙方因履行本合同而取得的甲方未公开的信息，包括但不限于甲方的业务数据、技术文档、用户信息、系统架构、商业计划及本合同内容本身。

2. 本合同适用的法律包括中华人民共和国法律、行政法规、司法解释，以及与运维服务相关的部门规章、项目所在地的地方法规等。

3. 本合同文件（包括主合同、附件、补充协议、双方往来函件等）均使用汉语语言文字书写、解释和说明。若因特殊需要产生其他语言版本，仅作为参考，以汉语版本为准。

第二条　合同文件的组成

本合同由下列文件共同构成，彼此互为解释和补充。若文件内容存在冲突，按以下优先支配地位的次序适用（优先次序高的文件效力优先）

1. 本合同书正文

2. 本合同书的补充协议（含双方就服务变更、标准调整等签订的书面协议）

3. 本合同书、补充协议的附件（附件内容与主文或补充协议冲突的，以正文或补充协议为准）

4. 双方在合同履行过程中形成的书面确认文件

5. 中标通知书。

6. 乙方公开招标的投标文件（包含澄清文件、承诺函等，若与甲方文件冲突，以本合同约定为准）

7. 甲方公开招标的招标文件（含招标文件变更说明、补充通知等）

第三条　服务内容和要求

1. 服务范围及目标

本项目服务目标以《北京市海淀区信息化运行维护项目预算申请报告》为基础设立，服务范围、核心目标应包含以下内容：

（1）根据目前我国信息化建设的现状和要求，中共中央办公厅和国务院办公厅转发了国家信息化领导小组制定的《国家信息化领导小组关于加强信息安全保障工作意见》（中办发[2003]27 号）。中办发[2003]27 号文明确提出了要“积极防御、综合治理”的安全战略方针。根据《智慧教育纳入全域数字化转型统筹管理工作方案》相关要求，从保障海淀区信息化发展的角度出发，统一网络安全运维工作，有必要通过海淀区政务网络安全监测服务项目工作开展，强化海淀区网络安全监测预警的深度，有效提升海淀区网络安全监控与防御水平。提高海淀区政务外网、政务云、视频专网、教育云等的信息化运维水平，进一步保障信息系统基础设施稳定，保障信息系统安全、稳定的运行，满足国家高水平信息化运维要求。

（2）总体要求

本项目的总体要求为有效保障海淀网络安全及应用系统业务正常运行，并在发生安全事件时及时响应，及时抑制和消除海淀信息系统安全事件，减少损失和负面影响。

（3）期达到的效果：该项目旨在积极响应国家关于网络安全和信息化的战略部署，特别是在海淀区这一科技创新和信息化建设的前沿阵地，确保政府关键基础设施及业务系统的安全稳定运行。将聚焦于网络安全监测服务的提升，通过采用先进的技术手段和管理策略，构建全方位、多层次的网络安全保障体系。有效保障海淀区政务活动的顺利进行，提升政府服务效率和质量，同时也为海淀区的信息化建设和社会发展提供坚实的网络安全保障。用户对服务满意度不低于 90 分。

2.服务方案及要求

海淀区政务网络安全监测服务工作包括：系统运维管理安全审计服务、系统 Web 应用安全防护服务、系统 Web 应用安全监测服务、系统渗透测试服务、漏洞检测服务、安全加固服务、安全分析服务、应急响应服务、远程运营专家服务、应急演练服务、驻场安全服务、互联网网络空间测绘服务、敏感信息排查服务、安全策略优化服务、日志分析服务、代码审计服务、学校安全检查、内容安全检

测服务、图形验证码服务、风险评估、安全培训、实战化安全防守服务、实战化安全攻击。在重要节假日及特殊时期进行专家级技术人员现场安全保障服务，保障海淀政务云平台、政务外网、教育云及视频专网的业务正常运行。并在发生安全事件时及时响应，执行应急响应流程，通过专家级技术支持进行快速响应与恢复，及时抑制和消除海淀信息系统安全事件，减少损失和负面影响。

（1）政务云、教育云、政务外网及视频专网安全服务需求

政务云、教育云、政务外网及视频专网安全监控围绕政务云、教育云业务系统和政务外网及视频专网进行，通过安全监控的全面监测，了解整体网络的安全态势，实现整体安全防护、防控目标。

政务云、教育云、政务外网及视频专网监测范围：云上虚拟主机千余台，承载各部门业务系统。政务外网由核心区、政务外网接入区、互联网接入区、服务器区、楼层汇聚区、委办局汇聚区、街道汇聚区、站队所汇聚区及其它接入汇聚区组成，其中安全设备 2000 余台，办公终端万余台。视频专网涉及招商办公区核心机房、第一办公区核心机房、上地办公中心核心机房、宝机房、28 个街道及 90 多家接入单位的网络安全设备。

（2）安全监控服务需求

目前，针对政务云、教育云、政务外网及视频专网已初步建立起了安全态势的感知和分析能力，提升了安全监管及运维的效率，但安全监测主要集中在云上业务系统和重要网络出口，网络内各区域的东西向流量和南北向流量监测覆盖范围不足问题凸显，难以应对当前的网络安全形势。

为实现政务云、教育云、政务外网及视频专网的全面监测、了解整体网络的安全态势，需在已有安全建设的基础上进一步增大监测范围，结合网络中已有安全设备、网络设备等各类设备的日志信息，实时监测安全日志的异常，有针对性的对异常日志进行告警，实现对安全事件的精准监测和处置。根据告警内容，可驱动防火墙、流量探针、EDR 等设备实现安全威胁的有效阻断。可将目标网络内网络安全态势、重要信息系统监测统计数据等多种类型安全数据生成报表，根据需求生成日周、周报、月报监测报告。

（3）数据采集需求

为了全面监控全网安全态势和安全威胁，应在政务云、教育云、政务外网部

署必要的设备加强数据采集，主要采集内容包括：

政务外网方面：

需在政务外网互联网出口、网络汇聚环 4 个核心节点和政务外网与政务云边界部署数据采集探针，基于网络流量分析，威胁情报、异常检测规则、深度学习算法等检测方法发现内部失陷主机，精准定位政务外网内已被攻陷的主机；

可采集现网中包括但不限于防火墙、防病毒网关、漏洞扫描、入侵检测、网络审计等设备的安全日志，对于接收到的日志可以存储原始日志，同时能够提供智能分析能力，并对分析后的数据进行展示。

政务云和教育云方面：

需在政务云互联网出口部署数据采集探针，基于网络流量分析，威胁情报、异常检测规则、深度学习算法等检测方法发现内部失陷主机，精准定位云内已被攻陷的主机；

要求能对政务云和教育云的虚拟主机系统脆弱性，应用系统脆弱性进行扫描，准确识别资产属性，清晰定性安全风险，给出修复建议和预防措施；

要求能对政务云和教育云提供互联网访问的应用系统，进行安全监测，包括实时监测应用系统的可用性状态，对访问异常情况进行通报。对应用系统页面敏感信息进行监测，分析验证敏感信息并及时进行告警；针对应用系统存在的安全问题进行通告和协助处置，跟踪处置情况并进行复验，降低应用系统安全风险；

定期针对海淀区重点应用系统进行渗透测试，包括对 SQL 注入渗透测试、XSS 跨站脚本渗透测试、网页挂马渗透测试、缓冲区溢出渗透测试、上传漏洞渗透测试、源代码泄露渗透测试、隐藏目录泄露渗透测试、弱口令渗透测试、管理地址泄露渗透测试等，定期形成渗透测试报告进行通报并跟踪处置情况。

（4）安全管控需求

面向海淀区政务云的运维管理及云上业务系统虚拟机系统管理操作进行安全审计，包括对所有运维管理操作进行审计，对运维账号进行集中管理。根据审计内容提供审计数据分析、统计和取证，定期生成运维审计报告。对发现的安全威胁进行预警通告，协助处置并跟踪处置情况。

要求能对上能够提供互联网访问的重要业务系统，提供安全防护服务，重点针对 Web 攻击行为进行检测和拦截，对 Web 攻击行为追踪分析，提供 Web 攻击

告警分析。

（5）全网威胁发现与分析展示需求

要求分别在政务云、教育云、政务外网及视频专网部署态势感知平台，通过收集目标网络的流量、日志、资产、漏洞数据信息，经过安全分析、智能分析和建模分析后将海淀区云中心及政务外网的安全数据按各种场景分析之后提供多维度态势统计分析，并支持根据预设定的规则进行安全告警，支持安全态势的大屏展示。可以展示实时网络攻击事件态势，直观的展示攻击事件轨迹情况，快速感知最新攻击信息。并对态势进行分析，包括全网风险态势、资产态势、攻击态势、漏洞态势等态势。

（6）安全分析及检索需求

通过多种智能模型实现安全分析。支持安全日志全方位检索，支持检索日志的导出，可进行日志溯源。

（7）安全告警和处置需求

通过分析海量的安全数据，通过特征分析、状态分析、情报匹配等方式发现威胁，并基于自动化和规则化的方式产生告警，告警能够通过邮件、短信等多种方式通知到安全运营人员，便于安全运营人员进一步的研判分析。安全运营人员可以根据告警研判情况进行处置。可根据告警信息进行自动处置，平台根据威胁情况、风险情况来判断是否需要处置，如果符合规定的条件，可以自动联动相关安全设备进行威胁阻断。

（8）安全服务技术需求

安全服务周期一年。服务地点为北京市海淀区，可能涉及区辖境内相关网络和机房，以及政务云和教育云等。

（9）驻场安全服务

服务内容，提供不少于 6 人 5*8 小时的现场安全值守服务，负责监控政务云、教育云、政务外网及视频专网的运行状态，及时反馈和处理各类故障问题，对于信息安全事件有效预警、上报、反馈，对各项值守服务工作形成记录报告，保障海淀政务云、教育云、政务外网及视频专网的日常办公的正常运转。在重保期内，提供 7*24 小时现场安全值守服务。提供视频专网的日常巡检和设备维护工作。

服务频次，提供不少于 6 人 5*8 小时的现场安全值守服务，在重保期内，提

供 7*24 小时的现场安全值守服务和 7*24 小时响应。每周输出一次日常现场安全值守服务报告，重保期间每天进行报告，每个阶段输出阶段报告。提交成果，《现场安全值守周报》、《现场安全值守月报》

（10）实战化演练服务

服务内容，通过模拟真实的 APT 攻击在可控的范围内对视频专网开展攻击测试，深度查找安全隐患。提供演习方案设计、沟通、演习组织协调、编写攻防双方演习手册、编制攻防评分标准。组织安全团队协同配合参与攻防演练工作，按照监测分析、事件研判、应急处置、联络协调进行分工分组。各小组对攻击事件实时监测、分析、处置、并按照攻防演练流程进行事件的应急处置及上报。服务频次，每年提供两次实战化演练服务。提交成果：《实战化演练预案》、《演练总结报告》

（11）重要时期安全保障服务

服务内容，在重要节假日及特殊时期进行专家级技术人员现场安全保障服务，保障海淀区的业务正常运行。并在发生安全事件时及时响应，执行应急响应流程，通过专家级技术支持进行快速响应与恢复，及时抑制和消除海淀区信息系统安全事件，减少损失和负面影响。服务频率，在重要节假日及特殊时期，包括国家或北京市组织重大活动期间。提交成果：《重要时期安全保障报告》

（12）风险评估服务

服务内容，针对全网进行风险评估，通过分析资产、脆弱性、威胁的属性，明确其可能的组合，通过威胁和脆弱性确定安全事件发生可能性，由资产和脆弱性确定安全事件的损失，以及由安全事件发生的可能性和安全事件的损失确定风险值。服务频次，每季度一次；提交成果：《风险评估报告》

（13）系统渗透测试服务

服务内容，通过部署必要的安全服务工具提供安全服务，定期针对海淀区 50 个重点应用系统进行渗透测试，包括对 SQL 注入渗透测试、 XSS 跨站脚本渗透测试、网页挂马渗透测试、缓冲区溢出渗透测试、上传漏洞渗透测试、源代码泄露渗透测试、隐藏目录泄露渗透测试、弱口令渗透测试、管理地址泄露渗透测试等，定期形成渗透测试报告进行通报并跟踪处置情况。服务频率，每季度进行一次渗透测试，提供渗透测试报告。提交成果：《渗透测试报告》

（14）漏洞检测服务

服务内容，通过部署必要的安全服务工具提供安全服务。

面向海淀区政务云、教育云，对云上的虚拟主机系统脆弱性，应用系统脆弱性进行扫描，准确识别资产属性，清晰定性安全风险，给出修复建议和预防措施。系统脆弱性评估能够定期监测系统整体安全风险，从全局把控全局的安全风险等级，为安全管理人员提供有针对性的整改处置意见，从而能够持续性的降低系统整体安全风险。

至少使用三种漏洞扫描工具，对海淀区政务外网网络设备、安全设备、服务器操作系统、数据库系统、应用软件系统等进行扫描检查，发现其存在的漏洞，并分析漏洞和配置缺失情况，准确评估漏洞风险程度。并提交扫描报告。

服务频率，每个月进行一次漏洞扫描，提供漏洞扫描报告。提交成果：《漏洞扫描报告》。

（15）代码审计服务

服务内容，对 2 个应用系统的代码审计服务，软件自身的安全性是确保应用系统安全稳定运行的关键。通过人工方式对应用系统源代码开展安全审计工作，可以减少应用系统的安全漏洞和缺陷隐患，审查软件中可能存在的后门和隐蔽信道，有效降低应用系统安全风险，保障应用系统安全稳定运行。服务频次，全年提供不少于 2 个系统的代码审计服务。提交成果：《代码审计报告》。

（16）安全加固服务

服务内容，通过部署必要的安全服务工具提供安全服务。面向政务外网主机系统，基于网络流量分析，应用威胁情报、异常检测规则、深度学习算法等检测方法发现内部失陷主机，精准定位政务外网内已被攻陷的主机。定期形成失陷主机定位及分析服务报告。对发现的安全威胁进行预警通告，协助处置并跟踪处置情况。根据漏扫报告，对海淀区政务云、教育云、政务外网及视频专网中安全设备、网络设备、操作系统、应用中间件、数据库发现的问题进行安全加固，通过策略调整、版本升级、增打补丁等，使系统环境能够正常运作，通过打补丁、强化帐号安全、加固服务、修改安全配置、优化访问控制策略、增加安全机制等方法，堵塞漏洞及“后门”，合理进行安全性加强，提高健壮性和安全性，提升整体网络安全防范水平。服务频率，每个月根据漏洞扫描结果，协助安全加固工作，

提供安全加固报告。提交成果：《安全加固报告》

（17）Web 应用安全防护与监测服务

服务内容，通过部署必要的安全服务工具提供安全服务，面向海淀区政务云、教育云上能够提供互联网访问的重要业务系统（其中防护站点 200 个，监测站点 400 个），提供安全防护与监测服务，重点针对 Web 攻击行为进行检测和拦截，对 Web 攻击行为追踪分析，提供 Web 攻击告警分析。提供实时监测应用系统的可用性状态，对访问异常情况进行通报；对应用系统页面敏感信息进行监测，分析验证敏感信息并及时进行告警；针对应用系统存在的安全问题进行通告和协助处置，跟踪处置情况并进行复验，降低应用系统安全风险；定期形成应用安全防护与监测报告。服务频率，提供 7*24 小时的设备实时监测分析和 5*8 小时的人工监测分析服务，每周输出一次报告。提交成果：《Web 应用安全防护报告》、《Web 应用安全监测分析报告》。

（18）安全审计与检测服务

服务内容，通过部署必要的安全服务工具提供安全服务，面向海淀区政务云运维管理及云上业务系统虚拟机系统管理操作进行安全审计，包括对所有运维管理操作进行审计，对运维账号进行集中管理，管理账号数量不少于 300 个。根据审计内容提供审计数据分析、统计和取证，定期生成运维审计报告。对发现的安全威胁进行预警通告，协助处置并跟踪处置情况。

通过部署必要的安全服务工具（云互联网出口和政务外网边界、视频专网、核心汇聚环 4 个骨干节点）提供安全检测服务，对海淀区政府政务云、教育云、政务外网及视频专网进行 7*24 小时不间断监控，并将产品的日志和告警信息集中收集、分析，通过监测及采集网络中的系统安全事件、用户访问行为、运行日志、运行状态等各类信息，经过规范化过滤、归并和告警分析等处理，以检测出诸如网络入侵、病毒攻击、反常行为、异常流量等安全威胁与安全风险，快速识别病毒攻击、异常流量以及用户非法行为等重要的安全信息，从而有针对性地配置和调整网络整体安全策略，实现对信息系统整体安全状况的全面管理，保证网络的安全。服务频率，提供 7*24 小时的设备实时监测分析和 5*8 小时的人工监测分析服务，每周输出一次报告。提交成果：《安全审计报告》、《安全检测分析报告》。

（19）安全检查分析与响应服务

服务内容，对安全设备的安全基线优化和业务访问控制策略进行统计和分类筛选，结合系统资产进行比对，及时发现网络设备、安全设备防护策略配置不当、防护策略失效等安全策略配置弱点并提出整改建议。并对防火墙、日志审计等安全设备的日志进行全量日志解析预处理，并基于日志进行安全事件查询分析使用。协助客户梳理并对防火墙、日志审计等安全设备的日志进行全量日志解析预处理，并基于日志进行安全事件查询分析使用。

通过网络空间测绘技术，发现教育云互联网资产暴露面、未知资产类型等关键安全信息，实现互联网资产的可查、可定位、操作可识别。全面排查海淀区教育网络环境互联网侧暴露风险点，排查范围覆盖互联网的各种信息泄露渠道，以攻促防，做到防微杜渐。提高日常安全运营中或红蓝对抗场景下的互联网侧信息管理工作。

安全应急响应是对区政务云、教育云、政务外网及视频专网发生的安全故障、安全事件立即做出实时性响应，派出专家级技术团队，核实情况，收集事件信息，通过研判分析，快速应急处置，排除问题并恢复网络正常运行。在网络出现恶意入侵、恶意资源消耗、病毒爆发以及其他各类安全事件时，在规定的安全应急响应时间内，派出安全工程师对安全事件进行分析和处理。在出现各类型安全事件后，对安全事件进行分析，开展安全事件入侵追踪和取证、犯罪取证、事后安全分析和加固的服务。实时发现网络中故障设备，协调厂商技术人员现场排查，并联系相关厂商对设备进行检修、提供备机，以最快的速度恢复网络的正常运行。

服务方式，通过安全检查分析、监测、通报等途径发现系统安全事件，须在3分钟内响应并通知使用单位，10分钟内判断安全事件的级别，30分钟内处置完成。针对严重的安全事件，按要求启动安全应急响应流程，二线、三线技术支持人员须在安全事件出现后的30分钟内进行响应，2小时内到达现场进行应急处理，3小时内解决问题。若3小时后仍不能解决安全事件，须联系或组织第三方进行安全应急响应。信息安全事件处理完毕后，需对整个事故进行分析研究，并提交报告，报告中应详细记录应急响应事件的起因、处理过程、建议改进的安全方案等。提交成果：《安全事件应急响应报告》

（20）内容安全检测及图形验证码服务

服务内容，提供内容检测工具与服务人员，按照海淀区教育科学研究院网络安全服务要求，面向资源平台、网站及其他业务系统，定期提供内容安全检测，在信息系统重要保障时期如两会、国庆等期间，对各平台的历史存量数据进行检测，并针对平台安全整改提供指导建议。

图形验证码服务属于业内成熟的用于区分人机行为的服务，传统验证码采用的是字符型验证码，通过字符识别、数字计算等方式区分人机，考虑到随着计算机 AI 自动识别技术的发展，简单的验证码数字图形不再安全，很容易被黑客攻破，安全性得不到保障并且用户体验极差，此项目需要提供基于用户行为信息、用户设备信息综合判断是否为恶意行为的检测服务。服务频次，提供 7*24 小时的实时监测服务，每月输出一次报告。提交成果：《内容检测服务报告》。

3.服务质量标准

乙方应按照合同要求完成如下质量指标、数量指标和时效指标，并提供绩效完成情况报告，包括前期绩效自行评估，绩效监控，绩效分析等内容。

（1）质量指标：

突发事件处置率＝100%；

（2）数量指标：

系统运维安全审计账号数量≥300 个；

Web 应用安全防护和安全监测服务网站数量≥400 个；

每季度针对海淀区政务云平台和政务外网重点应用系统进行渗透测≥50 个；

（3）时效指标：

每次网络安全突发事件的应急响应时间≤2 小时。

项目各项工作应交付的报告、服务、知识产权或成果符合项目预期；

项目文档齐全，项目管理过程合规，项目人员管理到位；

在规定时间内顺利通过专家验收评审。

4.服务期限

本合同自 2025 年 11 月 1 日起至 2026 年 10 月 31 日止。

在不改变合同其它条款的情况下，可视服务情况与中标（成交）供应商续签合同，续签次数不得超过两次，总服务期限不得超过三年。

5.服务人员和要求

乙方提供5*8运维服务，服务人员19人，其中驻场6人，非驻场13人。

其中技术总监1人，高级工程师7人、中级工程师7人、技术专家4人。

乙方更换驻场服务人员的，需提前（填写具体天数，如7个工作日）书面通知甲方并说明理由，经甲方书面同意后方可更换，新人员资质不得低于原人员。若乙方擅自更换服务人员，未符合合同约定的人员要求，乙方应及时改正。甲方可按照乙方未符合约定人员要求的情况，扣减相应人员资质差额。

6.运维资产管理

（1）合同签订后，甲乙双方按照附件1《运维资产清单》共同对运维资产进行盘点。甲乙双方共同盘点确认运维资产范围后，乙方对运维范围内的硬件设备（含服务器、网络设备、存储设备等）、软件系统（含操作系统、应用软件、授权证书等）及附属配件等运维资产具有保管义务。

（2）因乙方保管不善、盘点失误、操作不当等原因，导致运维资产缺失、损坏或数据丢失的，甲方有权按照实际损失向乙方追偿。

（3）服务期限内新增、报废、调拨、盘点运维资产时，乙方需按甲方要求完成相关手续。

第四条　　验收

1.验收流程

乙方应在服务期限结束后5个工作日内，向甲方提交验收申请及验收材料；对验收材料不完整的，甲方应告知乙方需补充的内容，乙方需在5个工作日内补正。

甲方组织验收评审，验收合格的，双方签署《海淀区政务网络安全监测服务项目验收单》；不合格的，乙方应在5个工作日内完成整改，并重新申请验收。

2.验收材料

《运维服务方案》*（包括但不限于工作内容、人员配置、响应措施等）*

《运维服务年度总结报告》*（例如包含运维服务内容完成情况、信息系统运行指标、故障处理统计等）*；

《运维项目自评报告》。

3.结算审核

乙方应按照甲方要求，配合结算审核单位开展项目结算审核工作。乙方应按照结算审核要求在规定时限内提供或补充项目材料、参加结算沟通会、配合现场核查等。

若因乙方提供虚假材料，导致结算金额调整或甲方损失，甲方有权按照实际损失向乙方追偿。

第五条　　价款及支付

1.本合同以人民币为货币单位，均为含税价格。

2.总价款

本合同总价款为：人民币 7,785,000.00 元（大写：人民币柒佰柒拾捌万伍仟元整）。

本价款为包含全部服务成本、税费、利润及合同约定的其他所有费用的最终固定价款，除本合同另有约定外，甲方无需向乙方支付其他任何费用。

3.付款方式

本合同分为两次付款。

首付款：合同签订之日起六个月内，甲方向乙方支付合同总价的 50%服务费人民币 3,892,500.00 元（小写）（大写：人民币叁佰捌拾玖万贰仟伍佰元整）。

尾款：乙方完成本合同全部服务内容、经甲方验收合格后，甲方在合同总价中扣除首付款和以下款项后，向乙方支付不超过合同总价的 50%服务费人民币 3,892,500.00 元（小写）（大写：人民币叁佰捌拾玖万贰仟伍佰元整）。

（1）未实际发生的备品备件零件维修及设备更换费用；

（2）根据合同规定应扣减的款项；

尾款 = 合同总价款 – 首付款 – 上述扣减款项。

4.支付方式

甲方通过银行转账方式支付款项，乙方指定收款账户信息如下：

开户名：北京启明星辰信息安全技术有限公司

开户行：招商银行双榆树支行

账号：861583890110001

乙方账户信息变更的，应提前（5 个工作日）日书面通知甲方，否则因此产

生的付款延误由乙方承担。

5.发票

甲方付款前，乙方应向甲方提供等额、合法、有效的增值税普通发票。因乙方发票问题导致甲方付款延迟的，责任由乙方承担，甲方不承担违约责任。

6.财政拨款延迟处理

乙方知晓甲方支付款项来源于财政拨款，若因财政拨款未及时到账导致甲方付款延迟的，付款时间自动顺延。顺延期间，甲方不承担违约责任，乙方不得因此暂停服务。

7.按照第四条验收的相关约定，如因乙方未能按时提供材料导致甲方未能按期付款，产生的付款延误后果由乙方承担。

第六条　　合同变更

1.合同变更的前提与变更形式

在本项目服务核心目标不变的前提下，因以下情形需变更合同内容的，双方应协商一致并签署书面补充协议：

（1）甲方因业务需求调整导致服务范围发生细微变化的；

（2）系统运行环境发生非预期变动，需调整运维方案的；

（3）双方约定的其他合理情形。

补充协议经甲乙双方法定代表人或授权人签字并加盖公章后生效，与本合同具有同等法律效力。

2.变更后的价款限制

除本合同另有约定或因不可抗力导致的必要变更外，合同变更后的总价款（含原合同价款及变更新增费用）不得超过本合同总价款。超出部分甲方不予支付，相关费用由乙方自行承担。

若变更导致服务内容减少的，总价款应按实际减少的服务量相应扣减。

第七条　　权利和义务

1.本合同服务期间产生的所有数据（包括但不限于系统运行日志、故障处理记录、用户反馈数据等）及成果（包括但不限于技术方案、运维手册、服务总结

报告等）的所有权归甲方所有。

乙方应在服务期满或合同终止后（5 个工作日）日内，将上述数据及成果按甲方要求的格式及方式，完整交付给甲方，不得留存副本（经甲方书面同意的除外）。

2.甲方应在本合同生效后（5 个工作日）日内，向乙方提供服务所需的基础信息、数据及相关资料，并确保所提供资料的真实性、完整性。因资料缺失或错误导致乙方服务延误的，责任由甲方承担，服务期限相应顺延。乙方仅可将甲方提供的基础信息、数据及相关资料，用于本合同约定的服务，不得用于其他用途，服务结束后应及时返还或销毁。

3.乙方履行合同需与第三方配合的，甲方应在收到乙方书面协调请求后（5 个工作日）日内牵头组织协调。若因甲方未及时协调或协调无果导致乙方服务无法正常进行的，乙方可书面申请本合同延长服务期限。

4.甲方应按本合同第五条价款与支付的约定，按时足额向乙方支付款项。

5.乙方应于每周一通过 OA 系统运维管理模块向甲方提交上周周报（电子版）。周报内容包括但不限于服务完成情况、故障处理明细、系统运行指标记录、存在问题及下周计划。

6.乙方应于每月 5 日前通过 OA 系统运维管理模块向甲方提交上月月报。月报内容包括但不限于月度服务总结、运维质量达标情况、备品备件实际发生费用明细及下月计划。

7.乙方应配合甲方对合同服务完成内容、进度、质量做验证。验证方式包含书面核查、现场核查、第三方验证。

8.乙方应在验收通过后 5 个工作日内，配合甲方梳理项目资料并按甲方要求归档（电子版存入指定服务器，纸质版装订成册）。

9.若乙方未履行资产管理义务，导致资产损失，甲方有权依据合同约定追究其违约责任，包括但不限于扣除服务质量保证金、要求赔偿损失、解除合同等。

第八条　　知识产权及保密义务

1.乙方保证依据本合同向甲方提供的备品备件等货物、服务（以下简称“知识产权标的”）均符合法律法规规定，不侵犯任何第三方的知识产权（包括但不

限于专利权、商标权、著作权等）、所有权、担保物权等合法权益，也不违反社会公共利益。若第三方因甲方使用知识产权标的向甲方主张权利（包括但不限于提起诉讼、仲裁、索赔等），乙方应在收到甲方书面通知后 2 个工作日内主动出面处理，并承担由此导致甲方的全部损失（包括但不限于诉讼费、律师费、保全费、差旅费、公证费、赔偿金等）。

2.乙方应对保密信息严格保密，未经甲方书面事先同意，不得向任何第三方披露，也不得用于履行本合同以外的任何目的。

3.乙方仅可为本合同目的，向其确有必要知悉保密信息的雇员披露，且应提前与该等雇员签订保密协议，明确其保密义务，并对雇员的违约行为承担连带责任。

4.下列情形不受保密义务限制：

（1）保密信息已通过合法渠道为公众所知悉；

（2）依据法律法规、司法机关或行政主管部门的强制性要求必须披露的；

（3）乙方在未违反保密义务的情况下，从第三方合法获得或独立开发的与保密信息相同或相似的信息。

5.本保密义务在本合同期满、解除或终止后持续有效。

第九条　　违约责任

1. 甲乙双方如有一方违约，由违约方承担因此给对方造成的经济损失。

2. 乙方未按时提交周报、月报的，累计达到 5 次，构成“违约”。

3. 甲方验证乙方服务质量未达到服务质量标准的，累计达到 3 次，构成“违约”。因服务质量不达标引发的后果应由乙方承担，甲方有权向乙方追偿损失。

4. 乙方对甲方造成严重损失的构成“违约”。

5. 其他构成“违约”的情形：无

6. 乙方构成“违约”的，应按照合同总金额 0.06%的标准向甲方支付违约金。甲方优先从应付未付款项中扣减；应付未付款项不足的，乙方应在收到甲方书面通知后（5 个工作日）日内补足差额。逾期未补足的，甲方有权按日加收差额 0.6‰的滞纳金，且有权单方解除合同。

7. 因乙方未按约定开始服务的，每逾期一日，乙方应按相应阶段应付款项的

1%支付违约金；逾期达到5个工作日的，甲方有权解除合同，乙方除退还甲方已支付但尚未产生的费用外，还应按照合同总金额0.01%的标准向甲方支付违约金。违约金的支付并不能解除乙方继续履行合同的责任和义务。

8.本合同约定的违约金不足以赔偿甲方实际全部损失（包括不限于律师费、诉讼费、保全费、检验费、公证费、差旅费等）的，乙方应当补足。甲方有权从后续应付的合同款中直接扣除上述违约金和赔偿款。

9.乙方保证其具备在相关采购文件中已承诺的相关资质。若乙方不具备资质，甲方有权解除合同，乙方应返还全部款项。

第十条　不可抗力

1.本合同中不可抗力指地震、台风、火灾、水灾、战争、罢工、政府命令以及其他不能预见、不能避免并不能克服的客观情况。

2.由于不可抗力致使合同无法履行的，受不可抗力影响一方应立即将不能履行本合同的事实书面通知对方，并在不可抗力发生之日起30日内提供相关政府部门或公证机关出具的证明文件。

3.由于不可抗力致使合同无法履行的，本合同在不可抗力影响范围及其持续期间内将中止履行，本合同执行时间可根据中止的时间相应顺延，甲乙双方无须承担违约责任。不可抗力事件消除后，甲乙双方应就合同的履行及后续问题进行协商，按照该事件对合同履行的影响程度，决定继续履行合同或终止合同。

第十一条　法律适用及争议解决

1.本合同按中华人民共和国法律解释，受中华人民共和国法律管辖。

2.因执行本合同所发生的或与本合同有关的一切争议，双方应首先通过友好协商解决。协商不成时，任一方均有权向北京市海淀区人民法院提起诉讼。

第十二条　其他

1.本合同一式陆份，甲方执叁份，乙方执叁份，具有同等效力。

2.本合同自双方法定代表人或授权代表签字并加盖公章/合同专用章之日起

生效，至双方权利义务履行完毕之日终止。

3.本合同附件应由双方签署，为本合同不可分割的组成部分，与本合同具有同等法律效力。

第十三条　附件

附件 1. 海淀区政务网络安全监测服务项目预算明细

签署页

甲方	单位名称	北京市海淀区大数据中心（盖章）
	法定代表人（或授权代表）	签字：
	项目负责人	张蕊
	电　　话	87130829
	通讯地址	北京市海淀区中关村南大街 5 号 1 区 689 号海淀科技大厦
	签署日期	2025年 10月 31日
乙方	单位名称	北京启明星辰信息安全技术有限公司（盖章）
	法定代表人（或授权代表）	签字：
	项目负责人	卫海燕
	电　　话	010-82779088
	通讯地址	北京市海淀区东北旺西路 8 号 21 号楼启明星辰大厦 102 号
	签署日期	2025年 10月 31日

附件 1　海淀区政务网络安全监测服务项目预算明细

序号	分项名称	单价（元）	数量	合价（元）	备注/说明
1	驻场安全服务	1,005,000	1	1,005,000	/
2	实战化演练服务	260,000	1	260,000	/
3	重要时期安全保障服务	420,000	1	420,000	/
4	风险评估服务	320,000	1	320,000	/
5	系统渗透测试服务	720,000	1	720,000	/
6	漏洞检测服务	960,000	1	960,000	/
7	代码审计服务	810,000	1	810,000	/
8	安全加固服务	160,000	1	160,000	/
9	Web 应用安全防护与安全监测服务	810,000	1	810,000	/
10	安全审计与检测服务	960,000	1	960,000	/
11	安全检查分析与响应服务	960,000	1	960,000	/
12	内容安全检测及图形验证码服务	400,000	1	400,000	/
总价（元）柒佰柒拾捌万伍仟元整					¥7,785,000