2025年青浦区电子政务系统安全运维服务项目

补充更正文件

各投标人：

上海青弘工程项目管理有限公司受上海市青浦区行政服务中心委托，以公开招标的方式对2025年青浦区电子政务系统安全运维服务项目进行采购，现就对招标文件对招标文件第三章 项目概况及招标需求进行更正，更正后的项目概况及招标需求如下：

一、服务目标

按照法律、行政法规、国家标准的相关要求，借助专业的安全服务团队，采取技术措施和其他必要措施，保障电子政务网络和系统的安全、稳定运行，有效应对网络安全事件，防范网络违法犯罪活动，维护网络数据的完整性、保密性和可用性，实现覆盖云安全、网安全、应用安全、其他安全的“大安全”运维能力，有效最终提升中心应对网络安全事件、安全隐患的应急保障能力和安全防护水平。

二、服务范围

2025年青浦区电子政务系统安全运维服务项目的范围包括：青浦区政务外网、互联网核心应用系统和青浦区政务外网、互联网骨干网络（各单位内部局域网不在实施范围之内）。设备清单详见附件。

三、服务内容

2025年青浦区电子政务系统安全运维服务项目主要包括“政务云”安全运维、“政务网”安全运维、“政务应用”安全运维和“其他”安全运维服务四个部分。

（一）“云”安全运维服务

1．政务云威胁诱捕与预警分析服务

1）服务要求：为电子政务云提供7*24小时网络威胁攻击诱捕及预警监测分析服务。在政务云部署威胁诱捕分析预警系统，监控网段内存在的蠕虫扩散、病毒传播、端口嗅探、恶意扫描行为进行捕获和分析并提供事件告警。

2）服务范围：政务云网段30个监测节点。

3）服务交付物：

➢提供30个诱捕监测节点（含政务云C类网段10个，子网段节点20个）；

➢服务周期内针对攻击来源、攻击路径、攻击行为等网络数据包分析、威胁预警分析及安全处置，按照处置频次出具处置报告；

➢按周提供《政务云威胁诱捕与预警分析服务报告》；

➢提供 5*8 小时驻场运维，7*24 小时监测、故障应急响应。

2．政务云安全设备监测服务

1）服务要求：针对区政务云的安全设备，协助梳理相关安全设备资产清单、对设备的运行状态、可用性进行实时监控和统计分析，定期对安全设备的配置、管理文档及备份情况进行巡检抽查。

2）服务范围：政务云 27 台安全设备。

3）服务交付物：

➢提供每月一次巡检服务；

➢按周提供《政务云安全设备监测报告》；

➢按服务频次提供《日常检查记录》；

➢提供 5*8 小时驻场运维，7*24 小时故障响应。

（二）“网”安全运维服务

1．政务网威胁诱捕与预警分析服务

1）服务要求：在政务外网、互联网区域部署威胁诱捕分析预警工具，监控政务外网、及互联网网段内存在的蠕虫扩散、病毒传播、端口嗅探、恶意扫描行为进行捕获和分析并提供事件告警，从而提升电子政务网络的威胁感知能力。

2）服务范围：政务网 100 个监测节点。

3）服务交付物：

➢提供 100 个诱捕监测节点（含政务网 C 类网段 30 个 子网段节点 70 个）；

➢服务周期内针对攻击来源、攻击路径、攻击行为等网络数据包分析、威胁预警分析及安全处置，按照处置频次出具处置报告；

- 按周提供《政务外网威胁诱捕与预警分析服务报告》；
- 提供 5*8 小时驻场运维，7*24 小时监测、故障响应。

2．政务网安全设备监测服务

1）服务要求：针对区政务网、互联网区域的安全设备，协助梳理相关安全设备资产清单、对设备的运行状态、可用性进行实时监控和统计分析，定期对安全设备的配置、管理文档及备份情况进行巡检抽查。

2）服务范围：政务网 43 台安全设备。

3）服务交付物：

- 提供每月一次巡检服务；
- 按周提供《政务外网、互联网安全设备监测报告》；
- 按服务频次提供《日常检查记录》；
- 提供 5*8 小时驻场运维，7*24 小时故障响应。

3．违规外联及边界设备监测识别服务

1）服务要求：对网内资产设备进行监测与扫描，对资产的设备类型、品牌型号、系统版本等信息进行识别，对违规外联进行监测，一旦发现，定位其终端地址(内网 IP 和互联网 IP)，关注资产状态、违规行为、弱口令、系统漏洞等威胁信息，实时主动监测、预警威胁信息与风险行为，确保设备运行稳定高效。

2）服务范围：具体覆盖全网范围内的 500+服务器、1550+虚拟机以及 17000+的终端和哑终端。

3）服务交付物：

- 提供实时监测分析服务；
- 《违规外联及边界设备识别监测报告》；
- 《日常检查记录》；
- 提供 5*8 小时驻场运维，7*24 小时应急响应。

（三）“应用”安全运维服务

1．应用系统上线前安全评估服务

1）服务要求：针对区政务外网、互联网、政务云接入发布的业务应用系统及主机，提供上线前的漏洞

扫描和安全配置服务。

2）服务范围：区政务外网、互联网骨干网络、政务云上线接入应用系统及主机。

3）服务交付物：

- 服务期内，提供不少于 30 次的政务外网、互联网、政务云主机及应用上线评估服务；
- 按服务频次提供《应用系统上线安全评估报告》；
- 按服务频次提供《应用主机上线漏洞扫描报告》；
- 按服务频次提供《应用上线发布安全策略评估和审批记录检查》。

2．漏洞扫描服务

1）服务要求：依据自动化漏洞扫描工具，对现有资产，包括操作系统、中间件、Web 应用、等类型 IT 资产进行漏洞扫描，形成漏洞扫描报告，协助相关单位进行漏洞修复，制定相应的协助处置流程，并对修复结果进行验证，确保安全问题得到解决。

2）服务范围：提供不少于 650 个政务网主机及应用扫描。

3）服务交付物：

- 提供 2 套漏洞扫描服务工具（含政务网、互联网区域）；
- 提供不少于 650 台主机及应用扫描；
- 服务期内每月提供不少于 1 次主机及应用漏洞扫描，并提出安全整改建议；
- 按照服务频率及工作周期提交《漏洞扫描报告》《漏洞修复整改建议》《漏洞整改反馈汇总表》。

3．渗透测试服务

1）服务要求：通过真实模拟黑客使用的工具、分析方法对系统进行准确、全面的测试，发现青浦区信息化系统最脆弱的环节，以便对危害性严重的漏洞及时修补，防止漏洞被利用。在可控的范围内，进行安全渗透测试服务，发现系统脆弱性，并出具相应服务报告，同时提供安全修复指导。

2）服务范围：青浦区 20 个重要业务应用系统。

3）服务交付物：

➢提供安全整改建议，并按时提供复测和人工二次复核；

➢服务期内提供不少于 4 次渗透测试工作；

➢按服务频次提供《渗透测试服务报告》《渗透测试问题整改跟踪表》《渗透测试复测服务报告》。

4．核心业务应用性能监测服务

1）服务要求：提供关键网络节点和重要业务系统全方位实时性能监控服务，主动发现网络和业务异常，及时告警、快速处理，满足网络和业务的运维要求，保证业务连续性。

2）服务范围：大数据资源平台、公文收发系统、信息发布系统、综合窗口系统、即时消息系统、统一用户认证管理、移动办公、信息化基础资源业务管理系统、一体化办公平台等 10 个核心应用。

3）服务交付物：

➢提供业务应用性能监测工具；

➢提供人工驻场处置服务；

➢当性能异常和故障时，触发相关告警，并分析完成提供故障分析报告；

➢提供每周 1 次《业务性能监测服务报告》。

5．网站安全监测预警服务

1）服务要求：围绕网站可用性监控、网站违规内容监控、网站域名劫持监控、网站 HTTP 请求监控、网站内容变更监控、网站木马监控、网站黑链监控、网站 ICP 备案信息监控等多个方面提供 7*24 小时网站安全监测预警服务。

2）服务范围：提供 20 个互联网发布网站，包括但不限于：

序号	应用名称
1	青浦区“一网通办”旗舰店相关应用
2	青浦区“一网通办”主页相关应用
3	青浦区电子证照社会化应用
4	青浦区智能好办

5	青浦区远程政务云服务
6	青浦区在线取号
7	青浦区政务服务一体机
8	青浦区综合窗口信息系统接口服务
9	青浦区自助机事项清单应用
10	青浦区政务服务体系
11	长三角一体化示范区政务服务地图
12	“上海青浦”政府网站
13	视频录制点播系统

3）服务交付物：

➢提供网站安全监测预警工具；

➢提供监测服务频率最小可设置 1 分钟一次，高密度发现网站异常安全事件；

➢发现安全预警后，需在 10 分钟内验证分析告警，及时响应告警事件并通报给相关人员进行处置；

➢按周提供《网站安全监测预警服务报告》。

6．代码审计服务

1）服务要求：结合青浦大数据中心安全需求，进行代码审计服务，包括代码缺陷自动分析、人工审计、加固建议及复测服务。

代码安全审计结合白盒与黑盒的方法，对应用程序程序代码进行病毒代码审计、工具审计、人工审计和业务逻辑安全的审计，审计内容涵盖应用系统的数据安全、业务服务安全、代码编写安全三个层面，从应用系统的整体角度看代码安全。

2）服务范围：提供重要信息系统应用代码审计服务。

3）服务交付物：

➢提供不少于 1 次代码审计服务；

➢提供人工审计服务；

➢提供二次复测服务；

➢出具《代码审计服务报告》《代码审计复测漏洞分析报告》《代码审计漏洞安全加固建议报告》。

7．特权账号监测服务

1）服务要求：提供特权账号自动发现，对资产上的账号进行发现，明晰账号台账，知道资产上有多少账号，有哪些账号。对账号风险进行分析，检测特权账号安全性，确定哪些是正常账号，哪些是幽灵账号、僵尸账号、弱口令账号、长期不改密等账号，给出账号管理建议。根据账号管理的相关规定要求，基于账号台账、账号风险分析报告，对整个资产的账号进行管理规划，建立完善的特权账号安全策略，包括特权账号范围、特权账号清单，第三方账号使用，改密策略等。

2）服务范围：核心业务平台、核心业务数据库

3）服务交付物：

➢提供核心业务平台、核心业务数据库不少于 100 个资产；

➢服务期内，实现对资产账号的有效管控；

➢按月提供《资产账号风险报告》，账号发现、巡检（审计）后提供，对资产的账号情况进行综合分析；

➢按服务频次《资产账号管理规划建议》，基于相关的要求，提供账号管理的合理化建议；

➢提供 5*8 小时驻场运维，7*24 小时监测、故障响应。

8．API 安全监测服务

1）服务要求：提供 API 生命周期管理、安全防护。解决 API 的海量请求、恶意访问、非法攻击等问题，以保障业务安全性与稳定性。重点解决协议覆盖、资产梳理和攻击检测，整合安全资源，达到攻击预防、阻断及敏感数据泄露防护为目的，实时保障 API 安全。

2）服务范围：政务外网区域 API 接口。

3）服务交付物：

➢提供 API 安全监测服务；

- 提供不少于 100 个 API 接口监测管理；
- 提供每月不少于 1 次的《API 安全监测服务报告》；
- 提供 5*8 驻场运维、7*24 小时安全监测、故障响应。

9．风险暴露面检测与溯源分析服务

1）服务要求：利用专业的高级威胁防范及溯源检测工具，加强政务网信息系统遭到网络攻击时的检测发现能力，网络安全防范能力。通过安全服务能够在第一时间发现攻击行为，并对受害目标及攻击源头进行精准定位，对入侵途径及攻击者背景进行研判与溯源，从源头上解决网络中的安全问题，尽可能地减少安全威胁对带来的损失。

2）服务范围：政务外网

3）服务交付物：

- 威胁检测与溯源分析服务；
- 提供每月不少于 1 次的《分析服务报告》；
- 提供 5*8 小时驻场，7*24 小时安全监测、故障响应。

10．应用效能评估服务

1）服务要求：围绕云、网、数、链、端，以已建成的政务信息系统运行为靶向，建立针对各靶向目标的效能评估指标体系，并结合效能评估要求进行效能指标模型权重的设置。通过实时数据采集技术采集各指标所需系统运行产生的数据，结合评估类指标的评估资料填报，综合进行效能评估打分，形成评估结果。

2）服务范围：青浦区数据局核心应用系统。

3）服务交付物：

- 提供实时的应用对接和评估服务；
- 每月《评估报告》；
- 提供 5*8 小时驻场运维，7*24 小时故障响应。

（四）“其他”安全运维服务

1．重保、护网安全保障专项准备布防服务

1）服务要求：在国家、市等各项重要活动期间，提供重保、护网安全保障专项准备布防服务，协助用户提升安全防护能力和应急处置能力。

2）服务范围：青浦区大数据中心

3）服务交付物：

- 提供不少于 8 次的重保、护网安全保障专项准备布防服务；
- 按服务频次提供《重保、护网保障方案》；
- 按服务频次提供《安全防护产品部署实施方案》；
- 按服务频次提供《漏洞扫描报告》《渗透测试报告》《重保防护资产清单》。

2．重保、护网安全保障专项值守服务

1）服务要求：在国家、市等各项重要活动期间，根据方案现场和远程的值守服务，负责监控安全监控设备、及时发现和处置重保期间的信息安全事件，协助用户提升安全防护能力和应急处置能力。

2）服务范围：青浦区大数据中心

3）服务交付物：

- 服务期内提供不少于 8 次的 7*24 小时重保值守服务；
- 按服务频次提供《重保值守排班表》；
- 按服务频次提供《重保安全值守监控日报》；
- 按服务频次提供《信息安全事件上报跟踪表》；
- 按服务频次提供《信息安全事件应急处置报告》。

3．应急预案和应急演练服务

1）服务要求：针对青浦大数据中心的相关业务应用系统，优化和制定应急响应保障体系，从组织架构、岗位角色、应急响应流程、应急演练计划、应急响应场景进行编制。并完善应急演练预案、编写应急演练脚本、搭建应急演练环境，开展应急演练服务。

2）服务范围：青浦区大数据中心

3）服务交付物：

- 服务期内提供不少于 1 次应急预案的修订工作和应急演练服务；
- 按服务频次提供《网络安全事件应急响应保障方案》；
- 按服务频次提供《网络安全事件应急演练预案》；
- 按服务频次提供《网络安全事件应急演练记录表》；
- 按服务频次提供《网络安全事件总结报告》。

四、其他要求

（一）服务周期

自合同签订之日起 1 年。

（二）服务团队要求

1．服务团队人员数量要求

1）项目服务团队人员数量不少于 12 人，一线驻场工程师不少于 6 人。

- 项目经理:1 人
- 一线驻场工程师：6 人(5*8 小时安全值守)
- 二线工具实施与部署工程师：2 人
- 二线应急响应团队：2 人
- 二线网络安全专家巡检支撑团队：1 人

2）服务提供方应详细说明实施团队每一成员所任角色、相关资质。

3)实施团队成员必须是服务提供方的专职全职人员(不得为该单位兼职人员，也不得在其他单位兼职)，项目主管以上必须具备 10 年以上项目管理经验，驻场工程师必须具备 2 年以上安全运维工作经历。

4）项目开始实施后，服务提供方有责任保持实施团队成员的长期稳定，当人员变动确实无法避免时，服务提供方必须保证实施团队成员的数量及技术水平，并立即告知青浦区行政服务中心（青浦区大数据中心）。

5）本服务项目不允许转包第三方。

2．服务团队人员资质要求

1）项目经理资质要求：

从事信息安全工作 10 年以上，本科及以上学历，具有省市及以上工信部门、人社部门颁发的信息安全相关的高级职称或者具有国家认可的权威部门颁发的信息安全师认证证书，具有信息化项目经验，须提供有效证书扫描件和近六个月投标人为其缴纳的社保证明、劳动合同。

2）一线驻场工程师资质要求：

2 年以上安全运维或应急响应经验，需具有省市及以上工信部门、人社部门颁发的信息安全相关的中级及以上职称证书、注册信息安全专业人员证书。需提供有效证书扫描件和近六个月投标人为其缴纳的社保证明、劳动合同。

3）项目团队其他人员要求：

具备有效的注册信息安全专业人员证书；需提供有效证书扫描件和近六个月投标人为其缴纳的社保证明、劳动合同。

（三）服务工具要求

项目开始实施后，服务提供方必须满足但不限于提供以下服务工具，同时必须承诺所有工具在项目合同签订后 15 日内完成安装和调试工作，自主软件需要提供相关证明文件，第三方厂商软件平台需要提供原厂商授权或购买凭证。

工具名称	用途	要求	数量
蜜罐工具	威胁攻击诱捕、仿真蜜罐	提供蜜罐能力，支持仿真系统服务类，数据库类，web 应用类，漏洞类蜜罐。支持 TCP、http、https 类型代理蜜罐。（提供截图证明）	2
		提供基于 Web 攻击识别、行为捕获、流量捕获的安全能力。支持发现 SQL 注入、XSS 攻击、远程代码执行、爬虫探测、Webshell 攻击等恶意行为；支持捕获和保存流经蜜罐的流量包，并提供下载功能；支持对攻击阶段，事件类别，事件行为，属性标签，User-agent，Referer，Cookie，url，请求体，响应体等字段攻击行为捕获。	
		提供威胁展示能力，支持按照不同维度添加自定义仪表盘，如事件分析、威胁源分析	

		仪、被攻击资产分析、系统运维等维度仪表盘，支持将自定义的仪表盘设置为默认加载仪表盘。	
		提供威胁高级分析能力，包含汇总信息和详情。支持展示威胁事件汇总信息，包括攻击等级概览、攻击阶段概览、数据量图、区域分布等 10+个威胁事件概览视图，并支持通过概览视图进行事件检索，简化搜索流程。支持展示威胁事件详情，事件详情既支持通过点击汇总信息中的统计项进行筛选、搜索条件进行筛选。（提供界面截图）	
		提供 web 业务蜜罐溯源能力，可获取攻击者信息包含但不限于：IP 地址，指纹，显卡，操作系统，真实 IP，主流社交账号信息方便溯源。（提供界面截图）	
核心业务性能监测工具	自动发现	自动识别和添加网络中的多种类型新设备和服务。	1
	性能监控	持续监测系统资源（如 CPU、内存、磁盘 I/O 和网络流量）。	
	可用性监控	检查服务和应用程序是否正常运行，并提供响应时间度量。	
	自定义监控项	允许通过脚本、命令行工具等创建特定于业务需求的监控项。	
	灵活的通知机制	在发生故障或其他重要事件时通过邮件、短信等多种方式进行告警，可以创建和自定义消息模板。	
	可视化仪表板	提供多种图形类型、环境和基础设施拓扑、自定义仪表盘等直观的数据展示方式，帮助快速理解系统状态。	
	Web 监控	模拟用户操作步骤来监控 Web 应用程序的功能和性能。	
	日志监控	实时跟踪日志文件的变化，及时捕获潜在问题。	
	模板化管理	使用预定义模板简化监控项目的配置。	
	宏支持	在配置中使用变量进行动态替换。	
	API 接口	提供编程接口用于远程管理和集成。	
	安全特性	保护系统的通信安全和个人信息。	

网站安全监测预警工具	SSL 安全	支持 SSL 协议漏洞监测，包括常见心脏出血漏洞、BEAST 漏洞和 POODLE 漏洞等（需提供截图证明，加盖原厂公章）	1
		支持 SSL 证书配置监测，包括证书到期、证书吊销、证书域名不符等监测（需提供截图证明，加盖原厂公章）	
		支持检测证书相关信息，包括证书绑定域名信息、证书颁发者、证书开始时间以及证书到期时间等（需提供截图证明，加盖原厂公章）	
	暗链	利用静态分析技术对网页源代码进行分析，查找不可见的外链接，并对这些链接进行云特征匹配	
	挖矿	支持网页门罗币挖矿劫持检测，可基于敏感域名检测、基于敏感文件检测及可基于 JavaScript 方法检测	
	挂马	支持页面源代码分析，可深入检查该页面所有自动加载资源，包括脚本、框架、CSS 等	
	坏链	支持检测业务系统中无法正常访问的链接地址，如报错 404、500 响应码等	
	风险外链	支持检测外链中是否存在挖矿、挂马、暗链、违规内容等信息及外链域名是否未备案，支持源码取证（需提供截图证明，加盖原厂公章）	
	可用性	支持全国范围内至少具备 10 个监测点，电信、联通和移动都具备监测点	
		检测网站首页响应速度，判断网站是否掉线，支持 Ping、HTTP 请求等多种方式探测网站连通速度，网站是否可用	
特权账号管理工具	系统配置	支持通过专用客户端进行管理（提供产品功能截图，并加盖原厂红章）	1
	用户管理	支持 IP 源防护、支持 MAC 防护（提供产品功能截图，并加盖原厂红章）	
	用户管理	支持父子层级的部门权限管理，如总部做为父级可查看各子公司，各子公司可查看管辖范围内的三级公司（提供产品功能截图，并加盖原厂红章）	
	资产管理	支持对物联网设备的管理，比如摄像头、ETC 门架等（提供产品功能截图，并加盖原	

		厂红章）	
	资产管理	支持资产规则库流程自动化，实现资产的快速对接（提供产品功能截图，并加盖原厂红章）	
	特权账号管理	账号巡检，支持巡检账号数、风险账号数和风险资产数、风险类型的展示（提供产品功能截图，并加盖原厂红章）	
		支持特权账号的增、删、改、查；支持设置特权账号的类型及改密权限；支持关联改密策略；支持特权账号的校验；支持特权账号的连接；支持特权账号的授权	
		支持通过软件开发工具包（SDK）或者应用程序接口（API）的方式实现对数据库内嵌账号密码的同步（需涉及应用改造）	
	密码策略管理	支持配置改密策略的时间策略，如单次执行或者周期执行、时间回避等（提供产品功能截图，并加盖原厂红章）	
	密码策略管理	支持配置改密策略的密码规则，如密码长度、密码字符集、密码安全、密码兼容性等（提供产品功能截图，并加盖原厂红章）	
	国密密码保险箱系统	支持国密 SM 系列密码算法（提供产品功能截图，并加盖原厂红章）	
	前置代理服务端	可以随管理桌面客户端、特权账号管理服务器端同时部署到环境中（提供产品功能截图，并加盖原厂红章）	
API 安全监测工具	API 接口梳理	支持内置接口类型识别规则和自定义接口类型识别规则，对接口进行自动分类，支持接口标签标识。	1
		支持接口重要性等级管理，支持根据接口业务、接口调用量以及接口涉及敏感数据情况进行规则设置，对接口进行重要等级划分。（需提供截图证明，加盖原厂公章）	
	资产展示	支持客户端 IP 列表，展示所有调用接口的客户端 IP 基本信息，关联信息、风险标签等信息；（需提供截图证明，加盖原厂公章）	

	资产分析	基于大数据分析、行为分析以及 AI 技术，对应用、接口、账号、客户端 IP、数据维度建立全面的资产画像分析，包含资产基本信息、统计数据和周期时间内的访问趋势和敏感数据访问分析、访问基线、访问时间偏好分布、关联风险（脆弱性）等。（需提供截图证明，加盖原厂公章）	
	风险识别策略	支持从接口权限、接口异常调用行为、接口数据传输行为、以及 web 攻击等维度进行接口风险监测；	
		支持灵活的自定义风险识别规则，可基于访问主体、访问对象、请求、响应等元素进行规则设置，并支持基线选择；	
	脆弱性识别策略	支持根据接口参数、接口样例等进行接口安全脆弱性识别；	
	脱敏合规策略	支持内置脱敏合规检测策略，包含在相同接口中存在部分未脱敏数据、在相同应用中存在应脱未脱、以及存在相关应用未按照行业规范脱敏等情况；	
	细粒度审计	支持审计记录完整的语句详情信息。包括：客户端 IP、应用账号、应用名称、服务端 IP、接口、域名、敏感数据标签、请求时间、响应码、响应体大小、响应时长、状态码、消息头和响应等至少 18 个审计信息。	
	会话关联	支持根据会话关联接口请求日志，帮助会话还原。会话信息包括：会话开始时间、持续时长、客户端 IP、目标服务端 IP、应用账户、请求总数以及各风险级别请求数等。（需提供截图证明，加盖原厂公章）	
	告警管理	支持根据风险审计规则进行告警。可对告警进行处置，如忽略、确认等；支持告警详情查看，包括告警基本信息、告警描述和处置建议、分析图表以及关联日志抽样查看、以及风险关联查看等。	
风险暴露	流量采集	支持常见应用协议的解析和还原，如 IP、TCP、UDP、ICMP、HTTP、SMTP、IMAP、POP3、SMB、FTP、TELNET、DNS、SSL、MYSQL、ORACLE、RDP、SSH、TLS 等	1

面检测与溯源分析服务		支持导入多个 HTTPS 证书，支持 RSA、AES、DES 等多种加密算法，可对加密流量进行解密和还原 支持导入 HTTPS 证书，对加密流量进行解密及还原：支持 SSL3.0，TLS1.0/1.1/1.2；支持 RSA、AES、DES 等多种加密算法；密码套件支持但不限于 TLS_RSA_WITH_NULL_MD5、TLS_RSA_WITH_NULL_SHA、TLS_RSA_WITH_RC4_128_MD5、TLS_RSA_WITH_RC4_128_SHA、TLS_RSA_WITH_3DES_EDE_CBC_SHA 、TLS_RSA_WITH_AES_128_CBC_SHA 、TLS_RSA_WITH_AES_256_CBC_SHA 、TLS_RSA_WITH_NULL_SHA256 、TLS_RSA_WITH_AES_128_CBC_SHA256 、TLS_RSA_WITH_AES_256_CBC_SHA256 、TLS_RSA_WITH_AES_128_GCM_SHA256、TLS_RSA_WITH_AES_256_GCM_SHA384	
	资产管理	具备基于流量发现内部资产与互联网设备互联的能力，并能准确显示互联的方向，支持拓扑图的形式展示资产和互联网以及内网各资产之间互联情况	
	威胁检测	支持邮件深度安全检测，包括对邮件的链接、附件、发件人员 IP、发件人邮箱、邮件正文等的异常检测；支持邮件附件按照发件人、主题、附件名称、附件 MD5、发件 IP 等进行数据聚合展示，支持按照文件分析状态、威胁等级、附件文件类型等进行快捷筛选	
		支持网络流量中漏洞攻击检测，包含系统漏洞、协议漏洞、软件服务漏洞等	
		支持网络设备攻击检测,包含 D-Link 注入攻击、Huawei 远程漏洞执行、Cisco 内存溢出、Cisco 漏洞攻击等	
	溯源分析	支持数据库操作行为提取，包括数据库类型、数据库版本、数据库操作语句、操作结果信息	
		提供 C/S 架构专用数据包分析客户端，对告警事件关联的网络原始数据包进行会话级别的深度分析，实时查看原始数据包内容，并进行会话跟踪、上下文关联等溯源分析	
		支持对 TB 级原始流量数据进行多层级的迭代分析，并记录用户分析策略，形成分析行为记忆链，支持记忆链中各节点条件显示，用户可即时回归迭代分析的任意节点，	

		并以该节点为起始点进行后续分析	
		支持基于多窗口的情景交互分析功能，主窗口保留主线的分析现场和分析思路，其他窗口进行可疑线索的全局关联分析、聚合统计分析、流量日志分析等多模式扩展分析，并可与主窗口进行互动，极大的保障了分析思路的延续性	
		支持对百万级别会话流量进行二次可视化统计分析，包括 IP 对的上下行流量信息、资产、协议、地区、端口等作统计和多角度展示	
	安全事件告警	支持将多个检测模型产生的海量分散的威胁告警信息自动关联形成威胁事件进行分类告警，标记威胁类型标签；支持内置至少 200 种威胁标签，并支持用户添加自定义标签	
违规外联及边界设备监测识别服务工具	违规外联监测	支持违规外联监测，可监测范围内终端的两网互通（同时连接内网和互联网）的行为，并可在两网互通监测平台子模块中定位其终端地址（内网 IP 和互联网 IP）。（需提供第三方检测报告复印件，并加盖厂商公章）	1
	网中网监测	支持网中网监测，提供网中网分析，可监测视频网中存在的包括 NAT 设备等的私有局域网情况。（需提供第三方检测报告复印件，并加盖厂商公章）	
	边界安全监测	支持边界安全监测，可显示网闸设备、小型路由器、代理服务器等边界安全设备的监测信息。（需提供第三方检测报告复印件，并加盖厂商公章）	
	违规桌面终端监测	支持违规桌面终端，监测网络违规设备（移动设备/Windows 8 系统）接入，提供设备接入地址、设备类型、所在地市位置等信息。	
	DNS 服务器监测	支持 DNS 服务器，监测网络中的未报备的 DNS 服务器，提供服务器地址、所在位置、解析域名详细信息等信息。	
	FTP 服务监测	支持 FTP 服务监测，可监测网络中存在的 FTP 服务器，并提供服务器地址、FTP 软件类型、匿名登录状态、服务器位置等信息。可监测用户访问 FTP 服务器的行为，并提供用户终端地址、FTP 服务器地址、上传下载文件名、文件大小、用户名、密码等信息。（需提供第三方检测报告复印件，并加盖厂商公章）	

应用效能评估工具	应用系统资产管理	在系统内录入信息并生成资产编号，作为指标数据对接时的唯一识别码。	1
	效能指标管理	做到数据拟合，进行模拟评分等工作来验证指标数据按照要求正常接入了效能评估系统。（需提供截图证明，加盖原厂公章）	
	效能评估模型管理	根据应用业务形态，结合考核要求，选取或新增效能指标形成一个评估模型，根据考核的侧重点进行权重的配置。（需提供截图证明，加盖原厂公章）	
	效能评估打分管理	针对填报材料对填报类指标进行评分，针对形成的效能评估任务，结合分数情况进行总结和提出相应的改进建议并最终形成效能报告。	
	效能评估报告	通过环比，反应效能过往评分的变化情况。	

（四）服务验收要求

投标人应按国家、行业、地方等相关标准对所交付安全服务开展验收，并向招标人提供国家标准所要求的各类文档，作为项目验收依据。

安全服务验收合格的条件必须至少满足以下四个要求：

1．安全服务交付过程及方式方法，需满足国家《网络安全法》《数据安全法》《个人信息保护法》《关键信息基础设施安全保护条例》、《信息安全技术 网络安全等级保护基本要求 2.0》等相关政策法规要求以及项目服务合同和实施方案的要求；

2．安全服务交付问题得以解决和改进；

3．安全服务指标中的交付物已按合同要求全部提供。

4. 项目验收过程中，如果发现存在不符合项，中标人必须在小于 3 个工作日的时间内无条件修正，由此产生的费用由中标人承担。如本项目连续 3 次验收未获通过，招标人有权解除项目合同并要求中标人承担违约责任。

（五）服务绩效考核指标

招标人将对中标人的运维服务进行服务质量评估，评估结果作为服务费结算的重要依据。

1．服务质量考核指标

服务质量考核评估主要针对完成交付的每个服务项进行评估，以交付质量评估结果确定服务项的质量系数。服务质量考核评估内容主要包括服务质量、服务交付、服务过程管理和服务满意度等方面，服务质量考核评估分值满分为100分。根据服务项交付质量评估分值按下表确定对应的服务项质量系数：

服务质量评估分值	等级	质量系数
≥90分	A	1
≥80分，<90分	B	0.95
≥70分，<80分	C	0.9
≥60分，<70分	D	0.85
<60分	E	应先进行整改，整改后评估分值≥60分时质量系数为0.8；整改后评估仍不合格的，质量系数为0。

服务质量评估的评分标准如下：

一级考核指标	二级考核指标	指标权重	评分标准
服务响应	响应时效性	5	及时响应服务项需求，以及方案提交、团队组建、临时任务等其他要求的得5分；每延期一周响应扣2分，扣完为止
	方案规范性和完整性	5	提交的服务实施方案应格式规范、内容完整，经评审一次性通过的，得满分；每发生1次评审未通过的，扣2分，扣完为止
	需求满足情况	5	方案完全响应并满足服务需求的，得满分； 未满足服务需求的，每项扣1分，扣完为止（需求如发生变更，以客户认可的最终版本为准）
	实施计划合理性	5	提交的团队组成和进度计划合理可行、满足服务需求的得5分；团队组成不合理扣2分、进度计划不合理扣3分
服务项交付	考核指标达标率	10	根据服务项考核指标项的完成比率评分，即得分=10*完成的指标项数量/全部指标项数量
	绩效目标完成度	10	①绩效目标完成度＜60%的为0分； ②绩效目标完成度≥60%的，得分=10*绩效目标完成度

	交付质量	15	根据服务项交付成果的质量情况进行评价，满分 15 分；并按以下方式扣分，扣完为止： ①由招标方或内部质量核查人员发现的运维质量问题，每发现 1 项扣 1 分； ②被使用单位发现并查证的有责运维质量问题,每次扣 2 分； ③被使用单位发现并查证的有责其他交付物使用问题，每次扣 2 分； ④由招标方或内部安全核查人员发现的安全隐患，每 1 个隐患扣 1 分； ⑤被上级单位或主管单位发现存在安全隐患，每 1 个隐患扣 5 分； ⑥服务项交付验收未通过的，每次扣 5 分； ⑦要求整改的问题未按时完成整改的，每项每延迟一周扣 1 分。
	交付时效	5	服务项按时完成交付得 5 分；每延期 1 周扣 2 分，扣完为止；
服务过程管理	人力资源投入	10	满足服务项人员要求且保持团队稳定的，得 10 分；并按以下方式扣分，扣完为止： ①未经批准，实际投入人员与报送人员名单不符的，每发现 1 人扣 2 分； ②未经批准,团队重要成员擅自脱岗或未达到考勤率要求的，每发现 1 人次扣 2 分； ③未按照要求及时更替技术能力与岗位不相符的人员，并投入技术能力与岗位相符的人员，每出现一次扣 2 分； ④团队成员流失率或更替率每超 10%扣 2 分,超过 60%及以上该项不得分。
	人员行为规范	5	团队人员完全遵守各类制度规范的，得 5 分；并按以下方式扣分，扣完为止： ①招标方检查发现团队成员违反外包服务管理要求的，每发现 1 次扣 1 分，扣完为止； ②其他各类内部、外部检查中发现并通报团队成员违反相关规定的，每发现 1 次扣 2 分，扣完为止。
	服务沟通	5	服务沟通及时顺畅、各类报告材料满足要求，得 5 分； ① 关键责任人在重要项目会议缺席，每发现一次扣 1 分，扣完为止； ② 服务周报、月报或其他必要材料缺失、拖延或内容不完整，每被投诉 1 次扣 1 分，扣完为止； ③ 团队人员沟通态度问题,每被投诉 1 次扣 1 分，扣完为止。

	问题解决	10	对各类事件、故障和问题及时响应并处置解决，得 10 分： ① 紧急事件、故障和问题应 30 分钟内响应，8 小时内解决；未按时响应的每延时 10 分钟扣 2 分，扣完为止；未按时解决的每延时 1 小时扣 2 分，扣完为止； ② 一般事件、故障和问题应 24 小时内解决；未按时解决的每次扣 2 分，扣完为止； ③ 包括新需求相关问题在内的其他问题应当当天响应、一周内解决；未按时解决的每延迟 1 周扣 1 分，扣完为止。
	文档及备案管理	5	服务项按相关服务要素单以及服务规范要求完成响应文档，同时相关材料在中心备案，得满分： ① 所提交文档在内容、格式等方面不符合要求的，每发生 1 次扣 2 分，扣完为止；每份文档每延期提交 1 周扣 2 分，扣完为止； ② 相关要求材料未向中心备案的，每发生 1 次扣 2 分，扣完为止。
服务满意度	服务满意度	5	按照服务满意度评价结果对此项评分，满分得 5 分；并按以下方式扣分，扣完为止： ① 满意度＜60 分的得 0 分； ② 满意度≥60、＜80 分的，得 4 分； ③ 满意度≥80 分的，得 5 分。
	有责投诉	5	在服务周期内未受到投诉或通报的，得 5 分；并按以下方式扣分，扣完为止： ① 中心各部门、各委办单位或第三方监管机构的有责投诉，受到投诉 1 次扣 2 分，受到投诉 2 次及以上该项不得分； ② 上级单位或第三方单位通报存在安全问题或其他严重问题的，该项不得分。

其他加分扣分项	重大责任事故	N/A	① 产生严重不良社会影响或者被业务、行业主管单位及领导通报的重大责任事故，扣 50 分； ② 发生严重数据泄露事件，扣 50 分；发生较大数据泄露事件，扣 20 分； ③ 受到安全攻击致使业务受到严重影响的扣 50 分，受到安全攻击致使业务受到较大影响的扣 20 分。
	重点保障服务	N/A	能提供重要事件或重点时刻及时保障服务的，每发生 1 次，加 1 分,最多加 5 分
	专业培训服务	N/A	应招标方要求提供专业培训服务，每次加 1 分，最多加 5 分；
	高水平规划方案	N/A	应招标方要求提供高水平规划方案，如：三区安全管理。经评审通过每个方案加 1-2 分，最多加 5 分。
合计		100	含加分、扣分的总分最高为 100 分

2．重大事故违约金

中标人在履行运维服务过程中出现重大事故时，由第三方监管机构界定责任边界和严重程度，招标人将依据事故严重程度计算重大事故违约金，并有权根据合同约定视中标人责任情况采取终止合同、将该中标人报财政部门备案、列入黑名单等措施。

重大事故违约金按以下方式确定：

序号	问题描述	罚款金额
1	因运维服务的人为失误导致服务中断	10 万元
2	依据本招标要求未能履行具体条款	20 万元
3	因运维服务的责任事故导致服务中断	20 万元
4	因运维服务的责任事故导致数据丢失	50 万元
5	因运维服务的责任事故导致数据泄露	50 万元
6	因运维服务重大责任事故导致数据无法使用	100 万元

（六）保密要求

1、中标人因履行本项目而知悉的所有数据、信息和资料（包括但不限于账号信息、图表、文字、计算过程、任何形式的文件、访谈记录、现场实测数据、招标人相关工作程序等）以及因履行本项目而形成的

数据、信息和任何形式的工作成果，均是招标人要求保密的信息。未经招标人书面同意，中标人不得对外泄露招标人要求保密的信息，不得用于其他用途，否则中标人需承担由此引起的法律责任和经济责任，包括但不限于直接损失、间接损失、律师费、诉讼费/仲裁费、调查费、公证费等。

2、中标人对招标人提拱的临时使用账号要保密，不得公开，对组件开发的账号密码需进行加密，避免信息泄露，确保信息安全。未经招标人的同意不得利用招标人的网络及平台进行短信、彩信发送，否则产生的一切后果由中标人负责。

3、中标人应采取必要的有效措施保证其参与本项目的人员（包括中标人的聘用人员、借调人员、实习人员等）无论是在职或离职后，以及中标人的合作方无论是合作中或合作终止后，都能够履行本项目约定的保密义务。若中标人人员或合作方违反本条规定，中标人应承担连带责任。

4、中标人（含中标人参与本项目的人员及合作方）未经招标人书面许可，不得以任何形式自行使用或以任何方式向第三方披露、转让、授权、出售与本项目有关的技术成果、计算机软件、源代码、策划文档、技术诀窍、秘密信息、技术资料和其他文件。中标人不以实施项目为名，侵害本项目各参与单位的技术、商业秘密或者知识产权。

5、本招标需求书仅作为投标人投标依据，未经招标人书面许可，不可转发第三方或随意传播。

6、以上内容的保密期限自投标人知悉保密信息起至保密信息被合法公开之日止。

五、其他说明

1、为保证招标的合法性、公平性，投标人认为上述项目技术需求存在排他性或歧视 性条款，可在收到或下载招标文件之日起七个工作日内提出并附相关证据，招标人将及时进 行调查或组织论证，如情况属实，招标人将对上述相关技术需求做相应修改。

2、招标人在附件中指出的工艺、材料和设备标准以及参照的规格、型号仅起说明作用，并没有任何限制性，投标人在投标中可以选用其他替代标准、规格或型号，但这些修改和替代要实质上优于招标人在附件中要求及指出的工艺、材料和设备的标准以及参照的规格、型号的要求。

以上补充更正内容为采购文件的组成部分，并对各投标人具有约束力。除上述内容补充更正外，采购文件的其他内容和要求不变。

上海青弘工程项目管理有限公司
2024 年 12 月 13 日