

一. 项目概况

1.1 概述

总台已部署北京启明星辰信息安全技术有限公司（以下简称“启明星辰”）生产的网络安全统一监测平台系统、天玥网络安全审计系统、运维安全网关、天镜漏洞扫描系统、入侵检测管理系统、超融合检测系统。长春吉大正元信息技术股份有限公司（以下简称“吉大正元”）生产的CA签发系统、RA注册系统、KM密钥管理系统、身份认证网关、LDAP目录服务等数字证书系统。奇安信网神信息技术（北京）股份有限公司（以下简称“奇安信”）生产的天眼分析系统。杭州安恒信息技术股份有限公司（以下简称“安恒信息”）生产的明御APT攻击预警平台。

1.2 服务期限

自签订合同日起12个月，具体开始时间以招标人要求为准。

1.3 服务范围

项目范围内网络安全系统、设备如下表所示，以下简称“安全系统”。

序号	系统名称	型号/描述	厂商	产品形态	数量
1	网络安全统一监测平台系统	TSOC-CSA-TOB	启明星辰	软件	1套
2	网络安全审计系统	天玥DA-6600	启明星辰	硬件	2台
3	运维安全网关	OSM-5600	启明星辰	硬件	4台
4	漏洞扫描系统	天镜漏洞扫描系统608X	启明星辰	软件	1套
5	入侵检测管理系统	天阗NT10000-HD\天阗NT12000-LT-B	启明星辰	硬件	9台
6	超融合检测系统	NT16000-CS	启明星辰	硬件	2台
7	数字证书系统	CA签发系统	吉大正元	软件	1套
		RA注册系统	吉大正元	软件	1套
		KM密钥管理系统	吉大正元	软件	1套
		身份认证网关	吉大正元	硬件	1台
		LDAP目录服务系统	吉大正元	软件	1套
		证书自助注册系统	吉大正元	软件	1套

8	天眼分析系统	天眼分析平台主节点引擎	奇安信	硬件	1台
		天眼流量采集探针产品	奇安信	硬件	1台
9	APT系统	明御APT攻击预警平台	安恒信息	软件	2台

二. 服务内容及指标要求

本项目服务内容包括但不限于：项目范围内网络安全系统的现场技术支持与维护服务、基础服务。

2.1 基本要求

1.安全播出与风险管控要求：投标人在设备维保及安全运维全过程中，能够保障总台节目制作、播出、传输全链路业务系统持续稳定、安全可控运行作为最高核心准则，恪守“先审批、后实施，先预案、后操作”的安全管控流程。严禁开展任何影响总台网络安全、数据安全及安全播出的违规操作、风险测试及高危配置变更；所有系统巡检、设备维保调试、软硬件升级等高风险作业，提前向招标人提交申请，经招标人审核批准后方可落地实施。

2.★因投标人技术操作不规范、防护不到位、应急处置不及时等问题，引发网络安全事件、安全播出事故或舆情问题，投标人须全权承担全部法律责任、经济损失及后续整改责任。

3.服务质量与违约责任要求：投标人严格按照要求完成各项服务内容，提交的所有成果内容真实、数据准确、分析深入、格式规范，满足采购人归档与上报要求。

4.保密要求：投标人为本项目配置的所有人员签订总台专项保密协议。投标人对项目工作过程中获取的总台网络架构、业务资料、账号口令等所有重要和敏感信息实行加密存储、权限管控、操作留痕管理；项目验收后彻底删除所有项目相关文档、数据、资料，并向总台提交删除确认承诺书；严禁以任何形式向第三方泄露、传播、售卖项目相关的任何信息，严禁利用总台相关信息开展任何网络攻击、技术研究等活动。

5.无犯罪记录要求：投标人为本项目配置的所有人员无犯罪记录。

6.资质要求：投标人提供有效的信息安全管理证书。

7.业绩要求：投标人提供自2023年1月1日以来网络安全系统代维类的项目案例（投标人需提供合同复印件，合同复印件至少包括：首页、项目服务内容页、签署/盖章页复印件）。

8.原厂售后服务：为保障总台数字证书、综合审计等系统在产品安全策略、特征库更新及应急响应等方面的延续性与一致性，投标人应具有产品生产厂商——北京启明星辰信息安全技术有限公司、长春吉大正元信息技术股份有限公司、奇安信网神信息技术（北京）

股份有限公司、杭州安恒信息技术股份有限公司出具的关于售后服务或技术支持服务或应急服务等方面授权。

2.2 基础服务

投标人为总台网络安全统一监测平台、综合审计系统与数字证书等系统、设备提供运维保障，通过标准化、流程化管理，确保各类安全系统与设备持续稳定运行、防护能力实时更新，及时排查并消除问题隐患。

2.2.1 授权与更新

投标人在服务期内对项目服务范围内的网络安全系统提供授权与特征库更新服务，保障网络系统、设备持续发挥防护作用。

2.2.2 升级与维护

投标人在服务期内对项目服务范围内的网络安全系统、设备提供升级与维护服务，包括但不限于以下内容：

1.软件版本管理。在原厂商发布相应产品的软件更新版本时，第一时间开展现有产品的升级方案论证工作。分析现有版本与更新版本的功能差异，制订升级策略，并以文档形式提交《安全产品版本升级方案》。方案至少包含：功能差异分析、升级实施步骤、功能验证测试、失败回退方案等内容。

2.配置管理。周期性备份安全系统、设备的配置、策略。依据安全保障需求以及最终用户部门要求，及时判断是否需要重大配置变更。开展重大配置变更时，第一时间开展配置变更方案论证工作，以文档形式提交《安全产品配置变更方案》。方案至少包含：变更差异分析、变更实施步骤、配置验证测试、失败回退方案等内容。

3.补丁管理。服务期内每月至少一次查看网络安全系统、设备是否存在新补丁，并及时更新。针对重要补丁启动紧急更新流程，确保最短时间内得到更新。

4.漏洞修复：每月对所有网络安全系统、设备进行漏洞扫描，全面排查安全隐患。对发现的漏洞制定修复计划，跟踪整改进度，直至通过复测验证。

5.为保障项目范围内安全产品的常态化检查工作快速有效开展，弥补传统固定检测方式灵活性不足、应急排查效率低等问题，配合安全系统版本升级、配置变更、补丁更新、漏洞修复等运维工作，及时发现各类安全风险，投标人需为本项目提供便携式安全检测工具。该工具通常为移动存储介质形态。

6.投标人能够提供便携式安全检测工具，并提供相关材料（产品说明、功能介绍等）证明该工具具备系统漏洞扫描、Web漏洞扫描、安全配置核查、口令核查功能。

2.2.3 备品备件服务要求

投标人建立专门的备品备件库，提供服务范围内所有设备的备品备件服务，确保设备故障时能够及时更换。

1.★当设备出现故障时，在4小时之内提供备品备件替换服务，在造成系统重大影响的紧急情况下，在1小时内提供备品备件支持。

2.若产品系统软、硬件出现无法修复的故障，且产品原厂商已无法正常保证产品软件修复升级的情况下，投标人服务团队需提供产品升级替换服务，确保系统能够正常运行。

3.投标人定期进行风险预警评估，分析设备运行状况和故障概率，并根据评估结果提前储备相应备品，以提前发现并告知最终用户可能造成系统重大故障的隐患，在问题出现前及时进行产品维护工作。

4.投标人如需进行备件更换时，提前征得最终用户同意并进行备案，更换过程在最终用户的监督下进行，更换下来的故障备件交由最终用户处理。

2.2.4 培训服务

1.投标人服务期内为招标人提供系统技术（技术原理、日志分析、故障定位、故障恢复、维修维护技术等）培训和现场系统操作培训。提供现场技术交流和 technical 问题讲解服务。

2.提供面向招标人运维人员的培训，使得运维人员具备设备日常配置、维护、管理的能力，能自主地分析和处理设备的各类告警信息，可以进行快速的故障定位和故障处理。

2.2.5 深度巡检

1.★投标人承诺在项目服务周期内协调网络安全统一监测平台系统、天玥网络安全审计系统、运维安全网关、天镜漏洞扫描系统、入侵检测管理系统、超融合检测系统的原厂商人员（须是现场技术支持工程师以外人员）提供不少于四次的深度巡检。

2.巡检内容至少包括：检查产品版本与产品授权、核查安全策略与配置基线、评估性能容量与系统高可用以及历史事件复盘与优化建议。

2.2.6 分析服务

1.基于天眼分析系统，投标人在项目周期内提供不少于20次的分析服务，并提供分析报告。分析服务由原厂安全专家现场分析完成，针对Web攻击、APT攻击、恶意邮件行为分析、数据库行为分析、口令爆破等各类高级威胁事件，结合最新威胁情报和业务应用情况，得出威胁分析结果并给出解决建议。

2.3 代维服务

投标人组建专职驻场服务团队，为总台网络安全统一监测平台、综合审计系统与数字证书等系统、设备提供常态化现场技术支持服务，保障安全问题的快速响应与闭环处置，

持续提升平台整体网络安全运营水平。驻场人员实行5×8小时现场值守，提供7×24小时远程技术支持，节假日及重要活动保障期根据招标人要求进行现场值守。

2.3.1 服务团队要求

投标人建立健全项目管理体系，组建专项项目服务团队，统筹协调本项目全流程服务交付，确保各项服务内容按时、按质、按量完成。项目服务团队至少配备1名项目经理、1名现场技术支持工程师，各岗位职责如下：

1.项目经理：全面负责项目整体统筹管理，对接最终用户部门的日常沟通与需求响应，制定项目整体服务计划与资源调配方案，组织召开定期服务回顾会议，跟踪落实服务质量改进措施，协调解决项目执行过程中的各类问题。

2.现场技术支持工程师：负责统筹管理现场安全运维与应急处置工作，在发生重大网络安全事件、严重设备故障或重大保障任务时，第一时间启动应急响应机制，协调内外部技术资源开展处置工作，确保业务快速恢复。

3.项目服务团队建立完善的内部沟通与协作机制，确保信息传递及时准确；关键岗位人员保持稳定，如需更换核心人员，需提前30天以书面形式通知最终用户部门，经同意并完成工作交接后方可变更。

4.项目服务团队签订《保密承诺书》，严格遵守最终用户部门的各项管理制度；如需更换驻场人员，需提前30天书面通知最终用户部门，经同意并完成工作交接、签订《离职保密承诺书》后方可离场。

2.3.2 现场技术支持人员及服务内容及要求

1.★投标人应配备1名现场技术支持工程师提供驻场服务，服务期内累计现场服务时长不少于2048小时，其中工作日现场服务不少于2000小时，节假日及网络安全重要保障期现场服务不少于48小时。

2.投标人配备的现场技术支持工程师具备由中国信息安全测评中心颁发的注册信息安全专业人员（CISP）证书或由中国网络安全审查认证和市场监管大数据中心（原中国网络安全审查技术与认证中心）颁发的信息安全保障人员认证证书（CISAW）。

3.现场技术支持工程师负责项目范围内安全系统的日常运维管理与安全保障工作，具体职责包括：

1) 协助最终用户对系统知识库内容进行维护，记录和更新系统维修、维护和变更信息，确保知识库内容的准确性和完整性；

2) 负责服务范围内的设备/系统日常运行维护，每日检查系统运行状态，记录系统运行日志，确保系统的可靠性和可用性；

3) 负责安全系统的策略修改、规则优化及相关文档的维护，根据网络环境变化和业务需求调整安全策略和检测规则，提高系统的防护效果；

4) 负责安全系统告警事件的实时监控、分析、信息丰富与级别定义，及时处置各类安全告警，过滤误报信息，上报真实安全事件；

5) 负责安全系统的升级更新、缺陷修补、功能改进等优化工作，确保系统功能不断完善；

6) 协助业务系统完成重大安全事件总结报告，分析事件原因，提出改进建议。总结、归纳各类安全事件，更新事件记录和解决方案，完善知识库，提高安全事件处置效率，协助进行故障处理和应急处置；

7) 定期发布安全公告，通报最新安全事件或动态，增强用户的安全意识；

8) 定期对业务系统进行漏洞扫描和安全检查工作，发现安全漏洞并提出整改建议；

9) 提供安全预警服务，及时向用户通报最新的安全漏洞、安全威胁和安全事件，并提供相应的防护建议。

2.3.3 应急演练

投标人针对项目范围内安全系统，结合最新网络安全态势变化，从设备故障处置、安全事件处置两个维度进行应急演练，并对现有安全系统整体应急处置预案以及各设备应急处置预案进行优化。

1.投标人在服务期内对安全系统提供不少于一次的应急演练和应急处置预案完善服务。

2.投标人以文档形式提供优化后的《网络安全系统应急处置预案》。

三. 付款方式

服务费每年结算两次，合同首款在合同签署后支付，采购人向供应商支付合同金额的30%。当年服务期结束时采购人根据《服务价款与结费依据》中约定的结算原则进行考核，考核后确认实际尾款数额。