

一. 项目概况

1.1 项目背景

总台已部署防病毒系统、主机安全防护系统、漏洞扫描系统。防病毒系统方面，服务器端使用的是亚信科技（成都）有限公司（以下简称“亚信”）生产的Deep Security产品，为250C主机提供病毒防护。终端使用亚信生产的Office Scan产品和该产品升级版Trust One产品，为13500点终端提供病毒防护。主机安全防护系统使用北京升鑫网络科技有限公司（以下简称“升鑫”）生产的青藤万相主机安全产品，为1000点主机提供安全防护。漏洞扫描系统方面，使用北京神州绿盟科技有限公司（以下简称“绿盟”）生产的2台绿盟漏扫器和北京知道创宇信息技术股份有限公司（以下简称“知道创宇”）生产的2台知道创宇漏扫器，为信息系统提供漏洞扫描服务。

1.2 项目目标

为保障总台防病毒系统、主机安全防护系统和漏洞扫描系统的稳定运行，确保其持续提供网络安全防护能力，本项目通过引入拥有完善服务资质体系的专业网络安全服务商，提供以上安全系统、设备的基础服务、现场技术支持与维护服务。

1.3 项目期限

自签订合同日起12个月，具体开始时间以招标人要求为准。

1.4 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	数量
1	防病毒系统	亚信Deep Security V10.x	250C
		亚信Office Scan V12.x 亚信Trust One V9.0	13500点
2	主机安全防护系统	青藤万相主机安全防护软件 V3.x	1000点
3	漏洞扫描系统	绿盟漏扫器	2台
		知道创宇漏扫器	2台

二. 服务内容与技术指标

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，提前向最终招标人提交申请，经最终招标人审核批准后方可落地实施。若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，投标人承担全部法律责任、经济损失及后续整改责任。

2.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。

3.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。

4.无犯罪要求：投标人为本项目配置的所有人员无犯罪记录。

5.资质要求：投标人提供有效的信息安全管理证书。

6.业绩要求：投标人提供自2023年1月1日以来网络安全系统软件代维类的项目案例，（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）。

7.原厂售后服务：为保障总台防病毒系统、主机安全防护系统及漏洞扫描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——亚信科技（成都）有限公司、北京升鑫网络科技有限公司、北京神州绿盟科技有限公司和北京知道创宇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

2.2.1 授权与更新

1.投标人在服务期内对项目服务范围内的安全系统提供原厂授权和特征库更新服务，第一时间更新安全系统的病毒库、安全事件库、特征库、脆弱性风险库、威胁情报库、告警策略等。安全系统的使用授权与特征库更新要求具体如下：

服务类型	描述	数量	授权周期
基础服务	提供亚信Deep Security V10.x产品的防恶意软件和Web信誉、防火墙和入侵防御模块使用授权许可。	250C	12个月

	提供亚信OfficeScan V12.x和亚信Trustone V9.0产品的防病毒模块使用授权许可。	13,500点	12个月
	提供青藤万相主机安全防护软件V3.x产品的资产清点、风险发现、病毒防护、内存后门、合规基线和入侵检测模块的特征库更新服务。	1,000点	12个月
	提供绿盟、知道创宇漏洞扫描器使用授权许可。	4台	12个月

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安全系统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的配置、策略。依据安全保障需求以及招标人要求，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安全系统是否存在新补丁，并及时更新升级。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：每月对安全系统进行漏洞扫描，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。

2.2.3 原厂技术支持

为确保安全系统的高可用性与安全性，有效应对重大安全事件并满足产品功能完善需求，投标人协调北京升鑫网络科技有限公司、亚信科技（成都）有限公司、北京神州绿盟科技有限公司和北京知道创宇信息技术股份有限公司提供原厂商专家技术支持。具体工作要求包括但不限于以下内容：

- 1.★深度巡检。在项目服务周期内投标人应组织防病毒系统与主机安全防护系统原厂商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。

3.★对于防病毒系统的深度巡检，投标人须提供有能力协调亚信科技（成都）有限公司工程师的承诺函；对于主机安全防护系统的深度巡检，投标人须提供有能力协调北京升鑫网络科技有限公司工程师的承诺函。

4.★专家现场技术支持。投标人承诺有能力协调北京升鑫网络科技有限公司、亚信科技（成都）有限公司、北京神州绿盟科技有限公司和北京知道创宇信息技术股份有限公司的专家提供现场技术支持。

5.★投标人须为本项目提供不少于200小时的专家现场技术支持服务（投标报价中按照200小时计算，具体服务时长以招标人实际需要为准，如服务时长超过200小时，按照200小时结算费用，不足200小时按实际发生数结算费用）。

6.产品漏洞支持。当安全系统所用产品自身出现漏洞或兼容性问题时，结合招标人实际状况，提供修复评估建议和修复参考方案，必要时提供现场技术支持服务。

7.定制化研发支持。当招标人提出产品的新功能需求或定制化开发要求时，基于安全系统现状，提供可行性定制化开发参考方案及原厂级产品研发支持服务。

8.安全事件风险应对。基于对国际、国内网络安全态势的实时监控，提供及时、精准的安全风险预警信息。同时，提供风险文件、病毒样本的深度风险分析和专业处理建议，并在紧急情况下提供应急响应技术支持。

2.3 代维服务

2.3.1 服务团队要求

投标人建立健全项目管理体系，组建专项项目管理团队，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、2名现场技术工程师，各岗位职责如下：

1.项目经理：为投标人公司在职人员，全面负责项目整体统筹管理，对接最终招标人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。

项目经理具备北京升鑫网络科技有限公司颁发的关于产品售后的“认证万相高级工程师”证书，具备亚信科技（成都）有限公司颁发的关于产品售后的“认证信息安全（售后）专家”证书，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）。

2.现场技术工程师：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。

现场技术工程师均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.项目管理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，如需更换核心管理人员，需提前30天以书面形式通知最终招标人，经同意并完成工作交接后方可变更。

2.3.2 现场技术支持要求

为保障安全系统持续稳定运行，投标人提供的2名现场技术工程师完成常态化巡检，在安全系统出现产品版本升级或主要功能变更时通过线上或线下的方式为安全系统使用人员提供培训，协助完成安全系统相关工单和告警的处置以及最终招标人布置的其他相关网络安全工作。具体工作要求包括但不限于以下内容：

1.★投标人为本项目配置的现场技术工程师，均须提供5×8小时现场技术支持以及7×24小时电话紧急响应支持服务。项目周期内现场技术支持时间不少于2080小时/人，其中工作日每人提供不少于2000小时服务，节假日或重大活动等网络安全重要保障期每人提供不少于80小时服务。

2.由于总台隔离网络中的机架服务器和终端采用独立组网方式运行，无法通过总台已部署的防病毒系统、主机安全系统进行防护。为满足上述服务器、终端的杀毒需求，投标人需提供即插即用式的扫描工具。该工具通常为移动存储介质形态。

3.扫描工具。投标人提供即插即用式的扫描工具。该工具至少：

1）支持适配Windows Embedded 7 Standard SP1 32/64位、Windows Embedded 8 Standard 32/64位、Windows Server 2008 for Embedded Systems 32/64位、Windows Server 2012 for Embedded Systems 64位等操作系统；

2）支持查找和移除计算机或设备中的安全威胁，而无需安装防病毒程序；支持使用具有Internet连接的任意计算机更新组件、更改扫描设置或检查日志。

4.培训方案。现场技术工程师结合安全系统招标人实际情况制定培训手册，该手册内容包括但不限于：安全系统的登录方法、客户端安装与卸载、告警与处置、安全策略配置和日常注意事项等；根据培训手册对安全系统招标人提供培训服务，使其能够熟悉安全系统的各项功能，并掌握安全系统的运维操作；对培训服务进行记录，记录内容包括但不限于受培训人员联系方式、培训地点、培训时间和培训使用材料等。

5.日常巡检。每个工作日对安全系统所属服务器的磁盘空间、CPU和内存等资源使用

情况进行巡检，如资源使用率超过90%，需及时排查并解决；对安全系统所属管理控制台的登录状态、页面展示内容、核心服务与进程的运行情况进行巡检，如发现异常，需及时排查并解决；对安全系统所属数据库的业务连通状态、备份执行情况进行巡检，如发现异常，及时排查并解决；对安全系统所属升级代理服务器的更新源连接状态、下载特征库情况进行巡检，如发现异常，需及时排查并解决；日常巡检执行后，出具安全系统日常巡检报告，报告内容包括但不限于：资源使用情况、管理控制台健康状态、数据库运行状态和升级代理服务器下载情况等。

6.设备巡检。每月对安全系统所属机架服务器的外观与指示灯、电源与风扇、线缆与环境以及标签与位置进行巡检，确保硬件设备运行稳定，规避因硬件问题导致的系统中断风险。设备巡检后，出具安全系统设备巡检报告，报告内容包括但不限于以上巡检内容的确认结果。

7.现场技术工程师负责安全系统相关网络安全工单的接收、处置与归档；协助最终招标人安全运营团队开展态势感知平台告警事件的初步核实与处置工作。

8.现场技术工程师离职或更换时，投标人提前30天书面通知项目最终招标人。现场技术工程师日常考勤严格遵守项目最终招标人制定的考勤管理制度。

9.按照项目最终招标人要求提供其他相关巡检服务，完成最终招标人交办的其他网络安全相关工作。

2.3.3 应急演练

投标人针对安全系统内的网络安全系统、设备，结合最新网络安全态势变化，从设备故障处置、安全事件处置的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。