第五部分 招标项目需求

说明：

1、投标人须对同一采购项目为单位的服务进行整体响应，任何只对其中一部分内容进行的响应都被视为无效投标。

2、招标项目需求中打“★”号条款为实质性条款，投标人如有任何一条负偏离则导致投标无效。

3、招标项目需求中打“▲”号条款为重要技术条款，负偏离不作为无效投标条款。

一、项目概况

日常信息安全服务项目负责对高训大厦终端设备、服务器、网络信息安全等进行日常扫描及漏洞修复，对网络安全设备开展日常巡检、策略配置优化等服务，在重大活动期间或重大网络安全事件期间，提供信息安全保障服务。

二、具体技术要求

服务内容

序号	服务项目	服务内容	服务要求	服务频率
1	★信息安全服务人员	1、项目负责人一名， 安全技术总监（至少一名）。 2、提供一名工程师进行驻场服务，每周驻场时间不少于五天。	驻场工程师负责和采购人对接、协调双方资源配合开展信息安全工作。工作时间一周不低于40小时； 驻场工程师职责如下： 1、对采购人的电脑、打印机、服务器等相关办公设备进行软件和硬件维护、病毒查杀、补丁修复等（采购人现有终端电脑500余台、打印机40余台。） 2、对采购人网络进行日常维护。 3、对采购人在用信息安全设备（包括防火墙、上网行为管理、日志审计、入侵防御系统、交换机等）进行日常巡查和安全策略配置服务；每天检查运行日志，发现问题及时处理，设备出现故障及时通知采购人安排维修。（项目验收时提供巡检服务报告） 4、安全预警及修复 根据国家、省、市信息安全要求，对安全事件	全年

			进行提前预警和防护，杜绝安全事件发生；如有安全事件发生，第一时间对事件进行分析和修复。（项目验收时提供《安全事件处理报告》） 5、上级单位检查迎检服务 完成上级单位信息安全相关考核工作，提前开展自查、准备迎检材料，确保各项指标要求达标； 6、信息安全制度修订服务 根据采购人信息安全工作方案要求，完成信息安全制度的修订工作。 7、文档资料整理 服务合同到期后，将服务期内所有服务记录、工作文档移交采购人，做好交接工作。	
2	漏洞扫描服务	根据采购人信息安全工作要求，完成所有从采购人网络出口的终端电脑、服务器、网络设备等的漏洞安全扫描及修复工作。	1、对所有从采购人网络出口的终端设备、服务器、网络及网络设备定期开展漏洞安全扫描工作，并对其高、中风险的安全漏洞进行修复及复核（项目验收时提供扫描和修复报告）。 2、中标商自带漏洞扫描工具，漏扫工具要求如下： ▲（1）系统应支持针对指定 IP 段，同时一键下发系统扫描、Web 扫描、口令猜解扫描任务，其中 Web 扫描支持暗链检测、网站木马检测、检测深度、爬虫策略、HTTP 请求头、表单填充内容、最大页面数、页面最大 KB 数、例外 URL、例外操作按钮、例外文件类型、例外特定参数设置；支持对单个服务进行口令猜解的最大线程并发数限制在 50 个范围内。（提供产品功能截图） ▲（2）系统应支持检测的系统漏洞数不少于 45 万个，漏洞信息包含编号、风险级别、年份、CVE、CVSS、CNVD、CNNVD、CNCVE、Bugtraq ID、	全年

			描述、解决办法等信息。（提供产品功能截图） ▲（3）系统应支持按任务、按资产的报表导出模式，导出格式支持 HTML、WORD、PDF、EXCEL、XML，导出方式可选择详细报表或统计报表，可以设置压缩包密码、是否展示弱口令密码，报表列表支持展示报表名称、报表类型、报表格式、所属用户、导出进度、生成日期、操作。（提供产品功能截图）	
3	应急响应	发生上级部门预警或确切的安全事件时，提供应急响应。	在发生上级部门预警或确切的安全事件时，应急响应实施人员第一时间赶到现场，及时采取行动限制事件扩散和影响的范围，限制潜在的损失与破坏服务基础上，实施人员协助检查所有受影响的系统，在准确判断安全事件原因的基础上，提出整体安全解决方案，排除系统安全风险并协助追查事件来源、提出解决方案、协助后续处置。（项目验收时提供《网络与信息安全突发事件应急预案》）	全年
4	信息安全知识培训服务	根据采购人信息安全工作方案要求，为全体工作人员提供信息安全知识培训。	1、为全体工作人员提供信息安全知识培训，制订培训计划，并提交培训记录； 2、针对不同岗位和职责的人员提供不同培训内容，包括信息安全意识教育、网络攻防、应用安全开发和国家等级保护相关标准的培训。（项目验收时提供培训课件）	至少 1 次/年
5	重要活动保障服务	在重大活动期间（两会、七一、国庆等）或重大网络安全事件期间，提供信息安全保障	1、在重大活动期间（两会、七一、国庆等）或重大网络安全事件期间，提供信息安全保障服务 。 2、免费提供多种业界标准工具对采购人网络设备、终端等进行监测。 3、提供至少 1 次重要活动期间现场值守保障服务，根据具体重保任务要求，对安全告警日志	至少 1 次/年

		服务 。	查看、安全告警信息排查等现场安全值守服务，提供具有丰富的应急处理能力和安全服务技术经验的工程师。（项目验收时提供《重保总结报告》） 4、重保工具功能要求如下： ▲（1）支持辅助快速创建钓鱼邮件、钓鱼文件、钓鱼网站，支持统计钓鱼邮件点击数、钓鱼网站访问数、客户端上线数；可以展示网站名称、网站链接、网站类型、创建日期、点击次数、上线次数、部署状态、操作信息。钓鱼文件支持 Word/Excel/可执行程序三种文件类型，支持 Windows、Linux 操作系统，x86、x64cpu 架构；钓鱼网站支持配置网站名称、网站路径、端口，部署位置可选本机、VPS，网站类型支持克隆站、模板站。（提供产品功能截图） ▲（2）支持多种格式客户端生成，包括可执行文件格式如 exe、elf、powershell、dll 等，以及原始 Shellcode 的生成；提供权限清除接口，可一键清除获取到的权限；新增 Webshell 支持自定义代理设置，包含 http、https、socks4、socks5 协议，支持用户名+密码的方式进行认证。（提供产品功能截图） ▲（3）支持利用 http、DNS 等协议远程获取外带数据；支持通过内置方法反弹交互 shell 到平台，执行 vim、交互执行操作等功能。（提供产品功能截图）	
6	安全咨询服务	结合现有 IT 基础架构系统，为不断完善信息安全防护方案提	以现有 IT 基础架构系统和安全防护框架为基础，为客户完善信息安全防护技术方案，提高信息安全防护水平提供技术咨询方案。	全年

		供技术咨询。		

三、商务要求

★（一）服务期限

本项目服务期限为2026年3月24日至2027年3月23日。本项目为长期服务项目，服务期满两个月前，由采购人根据中标供应商履约情况确定是否延长合同期限，合同每年一签，但最长不超过三年。

（二）服务地点：

采购人指定地点。

（三）报价要求：

1、投标人报价应以人民币报价，包括但不限于管理费用、人员费用、税费、生产材料费用、设施硬件配置费用等与完成本项目服务工作有关的全部费用。

2、投标人报价不得超过预算金额，否则投标无效。

（四）付款方式：

合同签订生效且采购人收到中标人出具的发票后10个工作日内支付合同金额的50%，合同执行6个月经采购人中期验收合格且采购人收到中标人出具的发票后10个工作日内支付合同金额的40%，合同到期验收合格且采购人收到中标人出具的发票后10个工作日内支付合同金额的10%。

服务要求中打**“★”号**的部分为核心要求即实质性服务条款，不允许负偏离，投标人的投标不符合要求会导致投标无效。