网络信息安全运维服务项目服务需求文件

为切实加强中心网络信息安全，提高信息系统安全管理水平及应急处置能力，健全网络信息安全体系，拟采购网络信息安全运维服务。服务期限1年。

一、服务内容

1、信息安全风险评估：依据GB/T20984风险评估规范，对中心信息系统的资产、威胁、脆弱性、已有安全措施进行综合风险识别与分析，掌控系统安全风险现状，并提供专业的安全解决方案和建议。

2、安全策略制定：根据风险评估结果，制定针对性的安全策略，提升中心整体信息安全防护水平。

3、安全制度梳理：保护网络信息资产的安全和完整性，确保网络信息系统的可用性，保障中心业务的连续性和合规性

4、安全设备管理：依据成熟性、实用性、可靠性等原则选择网络设备，并考虑设备的先进性、开放性和可管理性，根据业务需求和安全策略，合理配置网络设备的参数和功能，确保设备能够满足安全性能的要求。（我中心现有安全设备近50台，涉及深信服、奇安信等市场主流品牌）

5、等级保护咨询：提供信息系统定级、差距分析评估、安全规划与方案设计、系统整改、等保合规设计、以及辅助测评等全等级保护周期咨询服务，并可根据中心实际需求，提供定制化服务模块。

6、分级保护咨询：按照分级保护要求，对信息系统进行系统加固、风险评估、管理体系建设等安全服务。

7、密码安全评估：依据《信息系统密码应用测评要求》等文件要求，对网络和信息系统密码应用的合规性进行评估，生成密码应用安全性评估报告。

8、漏洞检测：通过“工具”+“人工”的方式对中心信息系统的资产进行全面、深入的漏洞检测。利用漏洞检测工具进行漏洞检测，检测完成后进行高风险漏洞验证，并提出专业的漏洞安全解决方案和建议。

9、弱口令检查：通过“工具”+“人工”的模式通过在线检查和离线破解的手段对中心内外网系统和应用进行弱口令检查。

10、系统风险评估：通过对系统进行分析，识别潜在的风险和威胁，并按照严重程度对其进行分类。

\*11、安全巡检：针对中心已有的业务系统及资产提供周期性上门巡检服务，包含漏洞识别、基线核查、安全设备日志分析，并提供安全巡检报告。

12、安全加固：针对在安全评估、检查、测试过程中发现的安全风险、不符合项、漏洞提供修复建议并协助中心进行加固整改的服务，包括但不限于安全策略类加固、漏洞补丁类加固和后门木马清除等。

13、安全事件应急响应：建立快速响应机制，对发生的安全事件进行及时处置，减少损失。安全事件及告警信息分析处置：对安全事件和告警信息进行深入分析，找出原因并提出改进措施。

14、安全事件趋势汇总与分析：定期汇总安全事件趋势，为中心信息安全防护提供数据支持。

15、网络安全脆弱性分析：分析中心网络架构的脆弱性，根据分析结果，制定针对性的信息安全加固方案。

\*16、安全迎检：根据中心要求随行迎检，明确检查目的和内容，针对性准备，提前自查自纠，整改隐患，准备好相关网络安全管理制度和技术防护材料。

\*17、重要时期安全保障：在中心重要安全保障时期，提供驻场人员处理在信息系统安全工作中出现的故障、安全事件以及安全管理方面的问题，保障中心业务系统完整性、保密性，使业务系统高效持续运行。

18、安全培训：提高参训人员的网络安全意识，掌握基本的网络安全防护措施，应对常见网络安全威胁。

二、服务要求

1、投标人成立独立项目组，确定项目经理，负责项目整体管理，且项目实施服务过程中不得更换项目经理。

2、在服务期间，要求提供7\*24小时技术支持服务，重大活动时，提供人员驻场服务。驻场次数要求：每3个月不低于30人·次，每次不低于3小时。

3、应急响应要求：工作期间应急响应1分钟，到场60分钟内；非工作日应急响应时间1分钟，到场时间120分钟以内。

4、现场服务的工程师应服从中心统一的工作安排，严格遵守作息时间，工作期间不得从事其它活动；严格遵守中心的规章制度和保密制度，并与中心签订《信息安全承诺书》。一经发现违规，必将追究法律责任。

5、信息安全设备维护要求：

对于安全故障问题进行现场检查，如当场判定为软件故障，需在当天排除故障，保障中心可正常使用。如确定为硬件故障，在保修期内需协调供货商进行配件维修或更换，保证三日内排除故障；在保修期外需制定维修方案，经中心确认后执行，保证五日内排除故障。对于无法维修的设备，提供详细说明，协助中心人员进行设备的报废处理和固定资产管理。

服务期内，需按照中心要求，提供对信息安全设备的上架安装、标签整理、线缆整理等工作，中心人员进行资产变更管理。协助中心人员对机房内的线缆进行相关的巡线，理线等工作，并整理相应的端口对照表。

服务期内设备出现软硬件漏洞或BUG，需免费提供实施方案设计和现场系统稳定版本升级服务。

6、培训次数要求：服务期内，满足中心人员要求提供的相关技能培圳，对主流版本及新兴技术进行案例讲解，每月不低于两次。

7、服务中台：按照科室要求定期参与运维驻场，驻场时负责接听科内所有来电，对来电内容进行记录及故障初步筛查（含医院业务系统问题），属于网络信息安全范畴的须立即处理解决并第一时间上报科内信息安全专员。

三、比选评分标准

采用综合评分法对各个提交报价的供应商进行评审，评分因素及权值如下：

|  |  |  |  |
| --- | --- | --- | --- |
|  | 项目 | 分数 | 标准 |
| 一、商务部分 | 企业履约能力 | 9 | 1、具备信息技术服务管理体系认证证书（ISO20000）得2分，没有不得分；  2、具备质量管理体系认证证书（ISO9001）得1分，没有不得分；  3、具备ITSS信息技术服务标准符合性证书（三级）及以上得3分，没有或级别不满足要求不得分；  4、具备隐私信息管理体系认证证书（ISO27701）得3分，没有不得分。 |
| 类似业绩 | 6 | 近三年信息安全项目业绩提供（运维服务或设备供应），每提供1个有效合同案例（须提供合同首页、合同金额页、合同内容页、盖章页的复印件，并加盖本单位公章，不符合要求的不得分）得2分，最多6分。 |
| 二、价格部分 | 价格部分 | 30 | 在规定范围内：按最低价格最高分原则。  价格得分=评选基准价/实际报价\*价格权重\*100 (满足比选要求且价格最低的报价为评选基准价)。 |
| 三、技术部分 | 服务要求 | 20 | 按采购服务需求中要求评审。服务指标全部满足招标要求的为20分，其中有1项“\*”号条款不满足的，扣3分；有1项其他条款不满足的，扣1分；扣完为止，最低得分0分。 |
| 技术方案 | 20 | 根据供应商提供技术方案水平的完整性、科学性、合理性进行综合评审依据综合得分：  1、完全满足采购需求得20分；  2、技术方案相对完整、相对科学合理基本满足采购需求，得15分；  3、技术方案一般、科学性合理性一般，不能满足采购需求，得10分；  4、未提供技术方案的得0分。 |
| 售后服务 | 9 | 根据供应商的售后服务承诺、维护响应计划、维修服务能⼒进⾏评分,包括售后服务安排的合理性、具体的售  后服务内容、故障响应时间、响应⽅式等⽅⾯进行综合评价：  1、提供的售后服务方案较为合理，符合用户实际需求，服务内容较为详实、响应及时、售后服务人员资质较为齐全，得9分；  2、提供的售后服务方案较为一般，基本满足用户采购需求，得6分；  3、方案内容不符合项目实际情况且未提供具体实施细节及措施，得2分；  4、未提供售后服务方案的得0分。 |
|  | 项目人员 | 6 | 项目服务人员要求（至少为4人，需同时具备以下两条件，人员不能重复，同时满足两条件的得6分，只满足一项不得分）  （1）具备市场主流网络设备认证资质，3人（如华为、华三、浪潮等）；  （2）具备市场主流安全设备认证资质，1人（如华三、深信服、天融信等）  以上人员均需提供资质复印件及在本公司的社保证明，并加盖公司公章。 |