**国家癌症中心关键资源（机房和重要系统）安全服务项目**

**技术需求书**

## 1. 项目背景

当前，网络信息技术的持续演进，互联网对整个经济社会发展的融合、渗透、驱动作用日益明显，带来的风险挑战也不断增大。从横扫全球的勒索病毒、坏兔子病毒等各类病毒，到地下黑产规模的不断扩大，以及从未间断的各类黑客攻击事件，要求我们要时刻保持对网络安全事件的警惕和防范。从习总书记在历次网络安全和信息化领导小组工作会议上的重要讲话，到《国家网络空间安全战略》的发布、《网络安全法》的实施，再到《关键信息基础设施安全保护条例》、《网络安全等级保护条例》开始征求意见，无不体现了国家对于网络安全工作的前所未有的重视。

## 2.总体目标

国家癌症中心承担重要信息系统的安全保障责任，履行安全保障义务。随着国家对网络安全要求力度的加大，结合国家关键信息基础设施保护以及“网络安全等级保护2.0”的新要求以及信息系统运行情况，国家癌症中心计划采购关键资源（机房和重要系统）安全能力建设服务，加大保障力度，切实维护相关关键基础资源的安全、稳定和高效运行。

## 3.项目服务原则

**（一）安全保密原则**。投标人在提供安全服务的过程中，要严格遵守合同规定，执行国家《保密法》及有关保密的法律法规，服务过程中凡是涉及到的任何用户信息均属保密信息，不得泄露给第三方单位或个人，不得利用这些信息损害用户利益。

**（二）最小影响原则**。投标人开展的安全服务工作，要尽可能小的影响系统和网络的正常运行，不能对业务的正常运行产生显著影响（包括系统性能明显下降、网络阻塞、服务中断等），如不可抗力无法避免，应对风险进行说明。

**（三）规范性原则**。投标人开展的安全服务工作，要由专业的安全服务人员依照规范的操作流程进行，对操作过程和结果要有相应的记录，提供完整的服务报告。

**（四）可控性原则**。投标人在开展安全服务工作过程中采用的工具、方法和过程要在双方认可的范围之内，保证用户对于服务过程的可控性。

**（五）质量保障原则**。投标人开展的安全服务工作需特别重视项目质量管理，项目的实施需严格按照项目实施方案和流程进行，并由项目协调小组从中监督、控制项目的进度和质量。

## 4.招标内容

安全服务内容包括两部分，一部分是机房安全服务，一部分是重要系统安全服务。机房安全服务内容包括：配电柜、UPS、空调、电池、新风系统、排风系统、消防系统、弱电系统、墙面地板定期安全巡检、定期耗材更换，故障维修。重要信息系统安全服务内容包括：安全巡检、渗透测试、安全加固、应急演练、应急响应、红蓝对抗、安全培训、机房资产梳理、安全通告，保证重要信息系统的安全、稳定运行。

### **4.1 机房安全服务**

|  |  |  |
| --- | --- | --- |
| **序号** | **指标项** | **指标规格** |
|  | **服务内容** | 需指派专业技术服务团队到现场在医院相关负责人现场监督下，对机房内的配电柜、UPS、空调、电池、新风系统、排风系统、消防系统、弱电系统、墙面地板进行定期安全巡检、定期耗材更换，故障维修。减少机房设备安全隐患，确保机房设备安全稳定运行。 |
|  | **服务范围** | 甲方院内悦知楼机房和电池间。 |
|  | **服务期限** | 1年。 |
|  | **服务频次** | 服务期内，夏季（7-9月）保证每周巡检1次，其他时间按季度巡检。 |
|  | **服务成果** | 《机房巡检报告》；  《耗材更换报告》；  《故障维修报告》。 |

### **4.2 系统安全服务**

**1.安全巡检**

|  |  |  |
| --- | --- | --- |
| **序号** | **指标项** | **指标规格** |
| **1** | **服务内容** | 需以“专业工具＋手工检测” 的方式，对服务器、安全设备等IT设施的健康状态进行检测，涉及设备自身硬件资源的使用情况、业务应用服务所占用的网络资源情况、端口服务开放情况的变更等内容，并实施必要的安全维护操作，具体内容包括：设备CPU、内存状态、开放服务检测，日志审计，网站监控，系统故障检查、分析、排除和跟踪，定期更新安全设备登录用户名及口令，定期备份和维护安全设备配置，并做好版本管理，做好巡检记录，维护记录单，提交巡检报告。 |
| **2** | **服务范围** | 国家癌症中心重要信息系统（2个）。 |
| **3** | **服务期限** | 1年。 |
| **4** | **服务频次** | 服务期内，每个季度进行一次巡检。 |
| **5** | **服务成果** | 《重要信息系统安全巡检报告》2份。 |

**2.渗透测试**

|  |  |  |
| --- | --- | --- |
| **序号** | **指标项** | **指标规格** |
| **1** | **服务内容** | 在国家癌症中心的授权和监督下，对指定的重要信息系统进行受控的、非破坏性的渗透测试，提前发现应用系统的隐患及漏洞，为加固整改提供技术依据，以切实保证信息系统安全。  服务商指派专业安全工程师，在模拟环境中对信息系统通过模拟黑客使用的漏洞发现技术和攻击手段，对目标网络、系统、主机应用的安全性进行深入探测，发现系统脆弱环节，帮助深入了解系统面临的威胁和存在的脆弱性，并针对发现漏洞提供漏洞修复建议，指导系统建设方进行安全整改，在安全整改后进一步复查以验证系统建设方安全整改的效果，有效提高信息系统安全防护能力。  每次服务包含初测和若干次复测，并指导系统开发商进行整改，直至无高危漏洞为止。  渗透测试需包括工具和人工两种方式。服务商须使用等级测评机构（与完成当年度等级测评工作为同一机构）的工具及专业人员完成本项工作。  提供的渗透测试服务方案须包括但不限于  1、渗透方法和流程；  2、渗透测试风险评估和控制方案；  3、渗透测试须采用国内外商业检测工具或自有检测工具。 |
| **2** | **服务范围** | 国家癌症中心重要信息系统（2个）。 |
| **3** | **服务期限** | 1年。 |
| **4** | **服务频次** | 服务期内、针对指定信息系统提供2次服务。 |
| **5** | **服务成果** | 《渗透测试服务报告》。 |

**3.安全加固**

|  |  |  |
| --- | --- | --- |
| **序号** | **指标项** | **指标规格** |
| **1** | **服务内容** | 在安全巡检和渗透测试的基础上提出安全加固方案，在经过癌症中心相关负责人批准后，由相应的信息系统承建单位实施安全加固操作，系统安全加固实施后由安全工程师审查加固实施情况，进行安全加固补遗工作，保障信息系统的安全运行，排除安全隐患。 |
| **2** | **服务范围** | 国家癌症中心重要信息系统（2个）。 |
| **3** | **服务期限** | 1年。 |
| **4** | **服务频次** | 服务期内、针对指定信息系统提供2次服务。 |
| **5** | **服务成果** | 《信息系统网络安全加固报告》。 |

**4.应急演练**

|  |  |  |
| --- | --- | --- |
| **序号** | **指标项** | **指标规格** |
| **1** | **服务内容** | 需根据前期制定的应急预案，结合信息系统存在的脆弱性和面临的威胁，协助制定应急预案演练工作计划，并模拟在信息系统及重要设备出现故障等紧急情况下，依据前期制定的应急预案进行处理，其中包括事件的发现、上报、处理等环节。通过演练，使相关方熟悉应急响应流程，提高对安全事件的响应能力；同时验证预案正确性和适用性，进行总结分析，并根据需要对应急预案进行修订。 |
| **2** | **服务范围** | 以某一重要信息系统为应急演练对象。 |
| **3** | **服务期限** | 1年。 |
| **4** | **服务频次** | 服务期间提供1次。 |
| **5** | **服务成果** | 《重要信息系统应急演练报告》。 |

**5.应急响应**

|  |  |  |
| --- | --- | --- |
| **序号** | **指标项** | **指标规格** |
| **1** | **服务内容** | 在信息系统发生安全事件时及时响应，执行应急响应流程，通过专家级技术支持和快速响应，及时抑制和消除用户信息系统安全事件，减少损失和负面影响，提高用户信息系统业务连续性。 |
| **2** | **服务范围** | 重要信息系统 |
| **3** | **服务期限** | 1年。 |
| **4** | **服务频次** | 服务期间提供不少于2次。 |
| **5** | **服务成果** | 《信息系统应急响应报告》 |

**6.红蓝攻防演练**

|  |  |  |
| --- | --- | --- |
| **序号** | **指标项** | **指标规格** |
| **1** | **服务内容** | 基于真实业务的网络环境，开展攻防对抗；不限制攻击方的攻击手 段，攻击入口，以获取到目标系统的系统层权限、业务数据、业务控制权限为目的，开展攻 击；防守方检测攻击事件，拦截攻击行为，溯源攻击者，以防护信息资产为目的。 |
| **2** | **服务范围** | 重要信息系统 |
| **3** | **服务期限** | 1年。 |
| **4** | **服务频次** | 1次。含技能培训在内，演练一周。 |
| **5** | **服务成果** | 《红蓝对抗演练总结报告》 |

**6.机房资产梳理**

|  |  |  |
| --- | --- | --- |
| **序号** | **指标项** | **指标规格** |
| **1** | **服务内容** | 需对院区悦知楼机房和顺义数据中心的资产进行全面资产梳理，包括资产情况、业务流转、网络拓扑等，并对路由策略、交换机ACL策略和防护墙策略等进行梳理、配置和文档化，通过安全策略的梳理和配置能够使管理人员清晰的了解网络内的流量传输和控制情况，优化网络安全配置。 |
| **2** | **服务范围** | 院区悦知楼机房和顺义数据中心。 |
| **3** | **服务期限** | 1年。 |
| **4** | **服务频次** | 服务期间提供1次。 |
| **5** | **服务成果** | 《机房资产梳理报告》。 |

**7.安全通告**

|  |  |  |
| --- | --- | --- |
| **序号** | **指标项** | **指标规格** |
| **1** | **服务内容** | 需搜集整理的漏洞信息、系统补丁信息、病毒信息等安全状态信息及时或定期有针对性地指定部门或人员发布，确保癌症中心在第一时间内得到相关的信息安全信息，并给出相应的解决方案，使癌症中心能够及时预防和防御安全风险，降低损失和负面影响 |
| **2** | **服务范围** | 不限系统。 |
| **3** | **服务期限** | 1年。 |
| **4** | **服务频次** | 服务期内，每周通告1次。 |
| **5** | **服务成果** | 《网络安全信息通告》。 |

**8.安全培训**

|  |  |  |
| --- | --- | --- |
| **序号** | **指标项** | **指标规格** |
| **1** | **服务内容** | 需通过专业、全面的信息安全理论、信息安全实践等课程，全面提高相关人员的安全意识水平和安全技术能力，切实提高用户信息安全管理能力，保证业务系统安全稳定运行。  1. 帮助癌症中心相关工作人员了解安全策略、掌握信息安全基础知识；  2. 帮助癌症中心相关工作人员熟悉各类安全产品的使用和管理；  3. 帮助癌症中心相关工作人员理解相应安全管理机制和应急保障工作流程等。 |
| **2** | **服务范围** | 癌症中心相关技术人员。 |
| **3** | **服务期限** | 1年。 |
| **4** | **服务频次** | 服务期内提供1次。 |
| **5** | **服务成果** | 《网络安全培训过程文档》。 |

## 5.项目实施服务需求

投标人需根据项目的采购、技术规格要求，采用满足要求的服务进行投标，服务必须满足项目采购主要技术规格要求，并保证能对选用服务进行很好的实施，如遇所选服务不能满足项目建设要求或项目中存在缺漏项情况，投标人应承担相应损失，投标总报价不做调整。

投标人需要具有丰富的安全实施团队保证整体项目实施的完整性、安全性、可靠性，保质保量的按时完成。需针对本次项目提供完整的实施进度计划，项目管理计划，要从项目组织架构管理、项目进度管理、质量保证管理等多方面确保项目成功实施。

投标人须服从国家癌症中心的统一协调，与本工程的相关单位进行积极主动的合作，在系统规划、方案设计、实施方案设计、系统集成、技术支持、运行维护等方面相互配合。

**（一）项目工期要求。**

本项目服务期限为一年。

投标人的项目进度管理应该遵循以下原则：

1.依据项目合同约定的工期目标，组织项目进度管理；

2.在确保项目质量和安全的原则下，控制项目进度。

**（二）项目实施团队成员要求。**

投标人应有专门的技术部门并指定固定技术力量用于本项目的实施，主要实施人员要保持稳定，除离职外一般不得随意更换，确需要更换要甲方同意。

投标人应按照项目的需求建立完善的组织结构和职责分工，进行相关的项目管控和随时调整项目实施方向。针对本项目成立专门的项目组，整体成员不少10人，包括1名项目经理，1名技术专家团队组长，确保人力、物力的投入，项目组成员必须稳定，项目实施的主要技术成员在项目终验前如果退出或更换，需要报甲方同意。

项目经理至少具有5年以上安全集成或安全服务项目实施经验，具有类似运维服务的项目经历，提供个人简历和相关资质证明文件复印件。

技术专家团队组长至少具有5年以上相关工作经验，具备网络安全规划分析能力，并具有类似运维服务的项目经历，提供个人简历和相关资质证明文件复印件。

技术团队成员应至少具有3年以上相关工作经验，具有相应的资质和良好的技能，能够分析和处理常见网络安全事件日志，编写分析报告等，以便于项目顺利进行，具有类似运维服务的项目经历并提供人员名单和相关资质证明文件复印件。

**（三）项目质量保障要求。**

投标人需要求给出切实可行的项目实施方案，方案中要包含项目管理控制措施、风险管理、进度管理、变更管理、沟通管理、文档管理、质量管理等内容；

在项目实施的全过程中，甲方有对项目进度、质量进行监督控制的职责和权利，投标人应全面配合，定期向甲方提交项目进展情况报告。

**（四）项目安全保密要求。**

投标人要严格遵守《中华人民共和国保守国家秘密法》及有关保密的法律法规，选派具有良好职业道德的人员参与和从事本项目工作，教育相关人员恪守职业道德，服从甲方的管理，严格遵守甲方的保密规定和工作制度，并承担相应的保密责任。

投标人须签订《保密协议》，所有参与本项目的服务人员须签订《保密承诺书》。

投标人所有参与本项目的服务人员自觉接受甲方的安全保密监督和管理，如违反安全保密条款，甲方将追究其责任，对重大的泄密事件将移交司法部门追究其法律责任；对泄露系统资料，造成伤害的，除依据有关规定追究有关责任人员法律责任外，还应依法承担相应的民事责任。

**（五）项目售后服务要求。**

投标人应针对本项目提供详细的技术支持及服务方案，包括服务方式、响应时间、服务热线、服务保障措施等内容，投标人需具备完善的服务体系。

在服务实施过程中，投标人需成立专门二线技术服务队伍，提供7×24小时电话服务响应；如电话不能解决用户发起的问题请求，需提供现场排除及解决软硬件故障的服务，在接到用户故障报告后响应时间不超过30分钟，如电话不能解决问题，需2个小时内赶到用户现场进行问题分析和处理。

**（六）项目验收要求。**

需提交的验收文件资料主要包括:

1.项目验收申请表；

2.项目设计方案及工程过程文档；

3.项目建设合同和有关修改、调整情况的纪要文件；

4.项目的技术报告和工作总结报告；

5.项目建设的主要成果技术资料及过程文档。

## 6.项目服务成果

服务成果交付：投标人应在项目实施期间或项目实施完毕后，提交包括但不限于如下服务成果：

《国家癌症中心悦知楼机房巡检报告》；

《国家癌症中心悦知楼机房耗材更换报告》；

《国家癌症中心悦知楼机房故障维修报告》；

《国家癌症中心重要信息系统安全巡检报告》，分系统；

《国家癌症中心重要信息系统渗透测试服务报告》，分系统；

《国家癌症中心重要信息系统网络安全加固报告》，分系统；

《国家癌症中心信息系统应急演练报告》；

《国家癌症中心信息系统应急响应报告》；

《国家癌症中心红蓝攻防演练报告》；

《国家癌症中心机房资产梳理报告》；

《国家癌症中心网络安全信息通告》；

《网络安全培训过程文档》。

## 7.资质要求

1)中国网络安全审查技术与认证中心颁发的信息系统安全运维服务资质一级。

2)中国网络安全审查技术与认证中心颁发的信息安全应急处理服务资质一级。

3)国家信息安全测评信息安全服务资质证书（安全工程类）二级及以上资质。

4)近三年（2018年1月1日起）合同额100万以上的安全服务类项目案例5份。