附件：

北京市卫生健康委会计核算服务中心

关于信息系统安全检测和应急服务项目的

遴选文件

为保障北京市卫生健康委会计核算服务中心信息系统安全检测和应急服务项目工作顺利开展，根据工作安排与需要，现面向社会公开遴选项目的第三方服务机构，有关事项公告如下：

一、委托单位

北京市卫生健康委会计核算服务中心（以下简称核算中心）。

二、项目背景

按照2015年公安部、中央网信办、中央机构编制委员会办公室、工业和信息化部联合发布了《关于印发党政机关、事业单位和国有企业互联网网站安全专项整治行动方案的通知》（公信安〔2015〕2562号），并根据《国家有关机构关于Treck公司开发的用于物联网设备的TCP/IP协议存在远程代码执行、敏感信息泄露等系统高危漏洞的情况通报》，要求“全面加强党政机关、事业单位和国有企业网站安全监测、应急处置和责任追究”，“督促网站开办单位加强网站安全监测,制定网站安全应急处置预案，健全完善网站应急保障措施，定期开展应急演练，及时处置网站安全事件（事故）”。

根据中央领导关于网络安全工作的重要指示精神和《网络安全法》的相关规定，为全面提升核算中心网络安全保障能力和防护水平，按照公安部《关于开展2019年网络安全执法检查工作有关情况的函》（公信安〔2019〕1137号）要求，依据国家相关政策规定及国家网络安全技术标准规范，推动和加强网络安全检测和安全应急工作实施。

为了检查、督促落实各项安全保障措施来防范和控制系统所面临的安全隐患、确保核算中心信息系统安全稳定运行，拟委托专业服务机构针对核算中心各业务信息系统开展渗透测试、源代码安全监测、网站安全监控、应急响应等工作，以检测信息系统与相应安全防护等级标准要求的符合程度，识别系统本身具有的脆弱性和安全保障措施的不足，基于安全服务阶段成果并结合业务需求，提高信息系统的安全性、稳定性、可靠性，减少安全隐患，加强对系统服务和业务数据的有效保护，实现信息安全长久机制，保证业务的平稳运行。

三、项目需求

根据对本项目需求及建设目标的分析，落实本次项目的总体建设任务如下：

（一）渗透测试

在不影响业务正常开展的前提下，通过模拟黑客攻击的方式，充分考虑国家有关机构关于Treck公司开发的用于物联网设备的TCP/IP协议存在远程代码执行、敏感信息泄露等系统高危漏洞的通报情况，设立全面的渗透测试技术方案，验证核算中心网站等信息系统抵御黑客攻击的能力，从而发现信息系统的安全隐患和脆弱点，并提出安全整改建议，以指导相关人员对系统进行安全优化和加固。

（二）源代码安全检测

通过工具扫描和人工检测相结合的方式对代码进行检测，以识别代码中的安全漏洞、逻辑错误、安全缺陷等问题，使核算中心更加真实的了解信息系统安全状况，避免安全问题蔓延，并指导应用系统开发人员对代码进行优化。

（三）网站安全监控

通过工具化监测和远程专家值守对网站系统提供全年365天不间断的远程网站监测服务，为网站系统实现远程安全监测、安全检查、实时响应和人工分析服务。一旦网站遇到风险状况后，安全监测团队会在第一时间进行确认，并提供专业的解决方案建议，为构建完善网站安全体系的奠定基础。

（四）应急响应

在核算中心信息系统发生安全事件时第三方服务专家须及时响应，执行应急响应流程，通过专家级技术支持和快速响应，及时抑制和消除信息系统安全事件，减少损失和负面影响，提高核算中心信息系统业务连续性。

# 四、项目技术规范要求

（一）渗透测试

渗透测试是在实际网络环境下，由安全测试人员发起的，经过客户授权的高级安全检测行为。渗透测试过程借鉴了黑客攻击的手法和技巧，在可控的范围内为证明网络防御能够按照预订计划正常运行而提供的一种检测方法，它可以高度精确的反映客户系统面临的风险。在渗透测试的过程中，通过充分暴露和发掘潜在的漏洞，能直观的让管理人员知道自己维护的系统中仍然存在的安全缺陷。

1. 渗透测试的范围：核算中心指定的信息系统和门户网站。其中信息系统包括北京市卫生财务管理信息系统、北京市卫生经济标准指标信息平台、北京市医疗服务项目价格信息管理平台、北京市卫生局财务人员队伍建设培训管理信息系统等8个业务系统。
2. 渗透测试的方式：外部的渗透测试，黑盒渗透测试，非破坏性测试。
3. 服务频次：1次
4. 渗透测试方案
5. 方案制定部分：应涵盖信息收集、操作方案、风险规避措施。
6. 分析报告输出：渗透测试人员根据测试的过程结果编写直观的渗透测试服务报告。内容包括具体的操作步骤描述；响应分析以及最后的安全修复建议。
7. 修复后复测：待系统按安全修复建议进行修复加固后，测试人员须按核算中心要求对部分高中危安全问题进行复测，以确保安全问题得到正确关闭。
8. 主要交付物：提交渗透测试报告（包括渗透测试Treck公司开发的用于物联网设备的TCP/IP协议是否存在远程代码执行、敏感信息泄露等系统高危漏洞的情况）和安全整改方案。渗透测试报告中，应综合利用难度、危害、影响，对发现的风险进行在线实际环境下进行威胁度排序。安全整改建议中，应综合威胁程度、加固难度给出加固建议。

（二）源代码安全检测

通过工具扫描和人工检测相结合的方式对代码进行检测，以识别代码中的安全漏洞、逻辑错误、安全缺陷等问题，使核算中心更加真实的了解信息系统安全状况，避免安全问题蔓延，并指导应用系统开发人员对代码进行优化。

1. 检测范围：核算中心指定的信息系统和门户网站。其中信息系统包括北京市卫生财务管理信息系统、北京市卫生经济标准指标信息平台、北京市医疗服务项目价格信息管理平台、北京市卫生局财务人员队伍建设培训管理信息系统等8个业务系统。
2. 服务方式：采用工具审计和人工审计相结合的方式开展代码审计工作，通过对应用系统开发框架、应用程序、客户端程序、接口及第三方组件和应用配置等方面进行深入的安全检测、审查和分析，从而发现应用系统源代码存在的安全缺陷和漏洞。
3. 服务频次：1次
4. 人工审计要求：在工具审计的代码分析基础上，需要进一步对检测结果进行筛选、分析和验证，确保检测结果的有效性，人工审核的内容包括但不限于：代码注入；跨站脚本；密码管理。
5. 服务方案：根据实际情况得到的相关信息，例如应用系统的数量、源代码行数等制定源码安全分析实施方案，方案内容包括源码安全分析的范围、流程、方法、内容以及人员分配和时间安排，同时提出源码安全分析所需的前置条件。
6. 主要交付物：《源代码安全检测报告》等。
7. 网站安全监控
8. 服务范围：核算中心指定的信息系统和门户网站。其中信息系统包括北京市卫生财务管理信息系统、北京市卫生经济标准指标信息平台、北京市医疗服务项目价格信息管理平台、北京市卫生局财务人员队伍建设培训管理信息系统等8个业务系统。
9. 服务频次：365天\*24小时
10. 服务需求：通过工具化监测和远程专家值守对网站系统提供全年365天不间断的远程网站监测服务，为用户网站系统实现远程安全监测、安全检查、实时响应和人工分析服务。监测内容必须涵盖：系统可用性监测、DNS解析监测、首页篡改监测、网页挂马监测、敏感关键字监测、暗链监测、钓鱼监测等服务。一旦网站遇到风险状况后，安全监测团队应在第一时间进行确认，并提供专业的解决方案建议，为构建完善网站安全体系的奠定基础。
11. 主要交付物：《网站安全监控月报》《网站安全监控季报》《网站安全监控年报》等。

（四）应急响应

1. 应急响应服务：突发安全事件，包含不限于网站攻击、网络入侵事件、大规模病毒爆发、遭受拒绝服务攻击等情况下的应急保障。驻场人员无法解决的问题，支撑团队要求2小时内到现场，4小时内处理解决安全事件。
2. 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。
3. 服务频次：按实际情况开展应急响应服务
4. 主要交付物：根据事件紧急程度，安排工程师现场、电话等解决问题，同时提供《应急响应报告》等 。

# 五、服务方式及服务期限

（一）现场服务：根据工作要求，提供现场服务，完成系统安全检测和应急服务的各种工作。

（二）远程服务：根据工作要求，提供远程服务，如电话、email等各种远程服务。

（三）服务期限：12个月

# 六、项目团队要求

（一）投标人要建立项目实施团队，包括项目经理，渗透测试组，代码审计组，远程监控组、应急处置组等。项目团队人员均需提供近半年的社会保险缴纳证明，相关证书复印件，并加盖投标人单位公章。

（二）项目经理在项目实施全过程中未经招标人许可不得变更，提交承诺函，并加盖投标人单位公章。

（三）中标方应在中标结果公示期满后7天内，严格按照投标文件的承诺组建项目团队，备齐相关资质证明材料备查。如未能在规定时间内或未能严格按照投标文件组建项目团队，将被认定为虚假应标，承担相应法律责任。投标人须提交承诺函，并加盖投标人单位公章。

 七、申报和评审事宜

（一）申报期限：2020年7月10日—2020年7月19日。

（二）下载材料：投标人可登录北京市卫生健康委会计核算服务中心网站（http://www.wsjhszx.org.cn/）下载《项目承办申请书》。

（三）填写材料：申请材料填写内容应简明扼要，突出重点。

（四）提交材料：投标人应在2020年7月19日18:00前将盖章的《项目承办申请书》、营业执照复印件等相关材料纸质版邮寄至北京市卫生健康委会计核算服务中心（地址：北京市西城区红莲南里30号红莲大厦B座502室），电子版提交至：bgs@wjw.beijing.gov.cn，并在邮件主题处注明“信息系统安全检测和应急服务项目遴选文件”字样。

（五）组织评审：核算中心将组织评审小组，对投标人的申请书等进行评审，择优遴选1家作为项目承担单位。

（六）结果公示：核算中心将对评审结果在核算中心网站予以公示。

八、项目经费

项目经费预算40万元。

九、评分标准和评分方法

评标方法：综合评分法。总分100分。其中投标报价10分、投标人资质业绩25分、投标技术方案及人员配置50分、服务能力支撑15分。最低报价不作为中标的保证。

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **评分指标** | **评分标准** | **分值** |
| **一级指标** | **二级指标** |
| 1 | 投标报价（10分） | 价格分计算方法:1.基准价=满足招标文件要求且投标价格最低的投标报价，其价格分为满分。2.合格投标人的报价得分=[评标基准价/投标报价]\*10\*100%中小企业参加政府采购活动如提供《中小企业声明函》，价格扣除标准按《政府采购促进中小企业发展暂行办法》执行。本次招标对小型和微型企业产品的价格给予6%的扣除。 | 10分 |
| 2 |  投标人资质业绩（25分） | 投标人 资质（20分） | 具有国家互联网应急中心cncert《网络安全应急服务支撑单位》国家级证书的得 7分，省级得5分，没有不得分。 | 0-7分 |
| 具有信息安全等级保护安全建设服务机构能力评估合格证书资质得3分，没有不得分 | 0-3分 |
| 具有国家信息安全测评中心安全开发类资质：具备得5分，不具备不得分 | 0-5分 |
| 具有国家信息安全测评中心安全工程类资质（能力范围应涵盖安全风险评估、安全监控和维护）：三级得5分，二级得2分，一级得1分，不具备不得分 | 0-5分 |
| 投标人 业绩（5分） | 投标人自2017年1月1日起所承担的同类安全服务项目有效业绩证明（须提供合同首页、关键条款页、合同金额页、双方签字盖章页的复印件，并加盖投标人公章），其金额在50万以上每提供一个得1分，最高得5分。 | 0-5分 |
| 3 | 投标技术方案及人员配置（50分） | 人员 配置（10分） | 项目经理具有5年以上的安全服务项目经验，需要同时具备CISP、PMP资格证书，提供项目经理简历、近半年社保证明、资质证书清晰扫描件。满足得2分，没有不得分。 | 2分 |
| 代码审计人员需具备大学本科以上学历，具备工信部电子通信行业数据分析师（高级）并提供相应简历及近半年社保证明，得4分，不满足不得分。 | 5分 |
| 项目组织结构设置合理、岗位明确、职责清楚，人员专业符合项目实施需要和管理要求。优：3分；良好：2分；其余得0-1分 | 0-3分 |
| 技术 方案（40分） | 技术方案设计全面、完善、具体、合理，符合招标要求和招标人实际情况，优：8-10分；良好：4-7分；一般：2-3分，差：0-1分 | 0-10分 |
| 对招标人现状描述清晰，内容具体、符合招标人实际需求。优：4-5分；良好：2-3分；一般：1分；差0分。 | 0-5分 |
| 提供的安全服务内容全面、具体，可行，符合招标人实际需求，服务方案包括但不限于服务内容、服务流程、服务成果等。优：8-12分；良好：4-7分；一般：2-3分，差：0-1分 | 0-12分 |
| 实施组织计划时间安排合理，项目特点突出、切实可行。优：4-5分；良好：2-3分；一般：1分；差 0分 | 0-5分 |
| 质量保障措施内容全面、措施有力，服务质量方面能够得到有效的保证。优：3分；良好：2分；一般：1分；差0分 | 0-3分 |
| 项目管理方案完善、合理、各阶段流程完备。优：4-5分；良好：2-3分；一般：1分；差 0分 | 0-5分 |
| 服务能力支撑（15分） | 漏洞发现能力（10分） | 提供2017年-2019年内，报送国家信息安全漏洞共享平台原创漏洞证明，提供100个以上原创漏洞得2分、提供200个以上原创漏洞得5分、提供300个以上原创漏洞得10分、不满100个不得分。 | 0-10分 |
| 技术支撑能力（5分） | 具备国家重大活动网络安全保卫技术支撑能力 | 0-5分 |
| 合计 |  | 100分 |

十、联系方式

联系单位：核算中心

地　　址：北京市西城区红莲南里30号红莲大厦B座502室

联 系 人：邱老师、李老师

联系电话：010-63291296

北京市卫生计生委会计核算服务中心

项目承办申请书

一、基本情况

|  |  |
| --- | --- |
| 项目名称 |  |
| 项目申报单位 |  |
| 通讯地址 |  | 邮政编码 |  |
| 电子信箱 |  | 传真电话 |  |
| 法定代表人 |  | 统一社会信用代码 |  |
| ———— | 姓名 | 职务 | 办公电话 | 手机 |
| 负责人 |  |  |  |  |
| 联系人 |  |  |  |  |
| 投标金额（单位：万元） |  |

二、申报单位简介

|  |
| --- |
|  |

三、项目方案

|  |
| --- |
|   |

四、经费预算

单位：元

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 服务内容 | 预算报价 | 备注 |
| 1 |  |  |  |
| 2 |  |  |  |
| 3 |  |  |  |
| 4 |  |  |  |
| 合计合计（单位：万元） |  |

五、申报单位承诺

|  |
| --- |
| 我们确认项目申报内容的真实性，并愿意承担相应的责任。负责人签字： 申报单位公章 年 月 日 |

资料清单及要求

（所有资料均须加盖公章）

一、资料清单

（一）封面（标明参选项目名称、参选人全称，由参选人加盖公章，并由法定代表人（或委托人）签字或盖章）

（二）目录

（三）承诺书

承诺愿意承担核算中心信息系统安全检测和应急服务项目，遵守遴选工作要求，认同遴选条件、程序和结果；近三年未有任何违法行为，本单位及其工作人员未受到任何因工作原因而导致的法律制裁；履行保密义务；所提供资料完全属实，如有弄虚作假，本公司赔偿一切由此引起的损失。

（四）法定代表人身份证明书

（五）法定代表人授权委托书

（六）项目承办申请书（附件1）

（七）相关证明材料

1.有效营业执照、安全服务资质以及其他资质证明材料复印件；

2. 缴纳社会保障资金的证明材料，应提供遴选前三个月内任意一个月的缴纳社会保险的凭据（专用收据或社会保险缴纳清单）复印件；

3.近三年工作业绩及合同（关键页）复印件等。

（八）服务团队人员保障、职责分工情况

（九）参选人认为需要提供的其他资料

二、资料份数和签署

1.参选人应准备1套正本、4套副本纸质版及相应的PDF电子版遴选文件。

2.纸质版与电子版遴选文件，字迹应清晰，便于辨认，内容一致。

3.全套参选资料应无涂改。

三、资料装订

1.参选资料须胶装，不能使用活页装订，并在封面标明“正本”或“副本”。

2.纸质版资料及存储电子版本的介质（光盘）应封装在密封袋中，并在密封袋封口处加贴密封条加盖公章。

3.密封袋外层应标（注）明参选人名称，并加盖公章。

4.如未在规定时间和地点递交遴选资料，则视为放弃。