附件：

**福州市公共资源交易服务中心**

**电子交易系统漏洞扫描及渗透测试服务项目采购文件**

 我单位拟对福州市公共资源交易服务中心电子交易系统漏洞扫描及渗透测试服务项目进行询价比价方式采购，具体要求如下：

**一、★采购内容（以“★”标示的内容为不允许负偏离的实质性要求，以下采购内容均不允许负偏离）**

| **序号** | **品目编码及品目名称** | **包名称** | **数量** | **允许进口** | **服务需求** | **总品目预算（元）** |
| --- | --- | --- | --- | --- | --- | --- |
| 包1 | [C16990000]其他信息技术服务 | 福州市公共资源交易服务中心电子交易系统漏洞扫描及渗透测试服务 | 1 | 否 | 1.对福州市公共资源电子交易平台（旧政务云26台服务器）、福州市建设工程电子招投标系统（新政务云32台服务器），以上两个信息系统，共计58台服务器，2024年度进行≥3次安全漏洞扫描和渗透测试服务（原则上2024年第2、3、4季度各一次，采购人有特别要求的除外），2025年度进行1次漏洞扫描和渗透测试服务。（原则上2025年第1季度完成，采购人有特别要求的除外）。并分别出具相应报告。2.服务内容见附表。3.按政府部门制定的相关规范和技术要求以及交付完整的材料，并通过政府部门要求的系统安全绩效考核。项目工作成果应符合采购人的保密要求。四、服务时间：合同签订之日起一年内。 | 100000 |

**附表：**

**招标内容要求**

**本项目招标内容要求全部条款内容均为“以“★”标示的内容”，即均为不允许负偏离的实质性要求。**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **服务项目** | **服务内容** | **交付成果** | **服务频次** | **备注** |
| 1 | 漏洞扫描 | （1）针对内部主机如：服务器、操作系统、网络设备与数据库扫描；（2）针对业务系统开展现场或远程扫描。 | 漏洞扫描报告 | 4次（2024年第2、3、4季度各一次，2025年第1季度一次） |  |
| 2 | 渗透测试 | 利用目标应用系统的安全弱点模拟真正的黑客入侵攻击方法，以人工渗透为主，以漏洞扫描工具为辅。 | 渗透测试报告 | 4次（2024年第2、3、4季度各一次，2025年第1季度一次） |  |
| 3 | 协助安全加固 | 安全加固（包含软件应用基线、数据库基线、中间件基线、操作系统基线等), 安全加固服务采用“人工+工具”加固方式，即通过安全基线检查和安全策略修复，并结合第三方安全加固工具实现对操作系统的全面安全增强, 1)安全加固工具支持内核级的强制访问控制功能，支持基于敏感标记(安全等级)控制文件读写权限（提供对应工具功能截图）2)安全加固工具支持白名单功能，只有属于白名单的进程可以运行，可以有效禁止病毒或木马的执行。（提供对应工具功能截图）3)安全加固工具支持基于MD5的识别技术的文件完整性检查功能，可对文件进行资源完整性监控。（提供对应工具功能截图）4)安全加固工具支持基线检查功能，能对常见的系统脆弱性进行一键扫描和加固修复。（提供对应工具功能截图）5)安全加固工具支持服务器的非法外联管控，避免服务器私自连接外部网络。（提供对应工具功能截图）6)安全加固工具支持外接USB设备的管控，可对接入的第三方USB设备进行控制，防止物理层面的非法接入行为。（提供对应工具功能截图）7）安全加固工具具有中国网络安全审查技术与认证中心颁发的IT产品信息安全认证证书，满足“ISCCC-TR-001-2017《操作系统安全加固产品安全技术要求》（增强级）”相关产品标准及技术要求。（提供对应工具证书复印件证明） | 安全咨询相关内容 | 4次/年 |  |
| 4 | 制度建设辅导 | 协助采购人完善现有安全管理制度，按照等级保护管理部分的标准，从安全管理制度、安全管理机构、人员安全管理、系统建设管理、系统运维管理5个方面协助采购人补充及完善等级保护要求的管理体系建设中涉及到的制度文档，以及相关记录的完善。 | 安全管理制度汇编 | 1次/年 |  |
| 5 | 入侵痕迹排查 | 对中心部署在本地及云平台上的服务器操作系统和应用的运行环境进行入侵痕迹的安全检查，包括可疑的文件、服务、进程、端口、网络连接、网站WebShell后门等，综合评估当前系统运行环境安全情况，生产入侵痕迹检测报告，并提出安全修复建议 | 《入侵清查报告》 | 2次/年 |  |
| 6 | 安全防护设备租赁及演练支撑 | 1. 在网络安全监管部门举办的攻防演练期间租赁包括下一代防火墙（≥3台，要求具备入侵防御、网络防病毒功能）、高级持续性威胁检测设备(APT)（≥1台，要求具备APT攻击预测技术和攻击防御技术）、Web应用防火墙（≥1台，要求具备网页防篡改功能）、态势感知平台（≥1台，具备展示对应安全事件的建议处置方式）及其他的安全厂商认为应增加的设备部署于中心互联网边界，确保基础网络运行安全，在本地和云平台互联网区服务器上部署主机安全防护系统（具有针对服务器入侵检测和防护功能，并配有服务端可实现集中管理与监测，非普通杀毒软件，软件授权一年）。
 | 相关设备 | 每年按需提供（设备租赁时间≥60天） |  |
| 7 | 重要时期安全保障 | 在具有重大政治影响的活动前夕派遣专业安全服务人员提供资产清查、网络及数据安全检查和加固服务，活动期间根据中心需要安排人员提供远程支持，确保各网络及信息系统的安全稳定运行。攻防演练期间安排≥2名安全技术人员远程5\*8小时防守，借助云平台及本地现有和租赁的安全设备及部署的防护软件获取相关数据日志进行分析，根据分析结果进行威胁处置，并提供针对我单位系统的威胁攻击和处置数据的截图或日志（本地和云平台）等，确保单位网络及信息系统不被攻击成功，顺利完成防守任务，并协助中心编写演练相关材料报告。 | 重保相关报告 | 每年按需提供（现场值守时间≥30天） |  |
| 8 | 应急响应服务及疑难网络故障排查 | 在遇到突发事件后，立即开展故障排查，采取紧急措施并恢复业务；调查安全事件发生的原因，避免同类安全事件再次发生；在需要司法机关介入时，提供法律认可的数字证据等，根据中心需要协助开展网络安全应急演练，并对演练过程进行技术指导和支持，在遇到重大疑难网络故障时，安排技术人员协助排查故障原因； | 应急响应报告 | 全年，按需提供 |  |
| 9 | 在线监测服务 | 对中心涉及的web站点提供可用性监控、网页挂马监控、网页敏感信息监控等：（1）网站可用性监控服务全年7\*24小时对网站首页进行轮询探测，网站访问不到则通过邮件或短信等方式进行告警，确保网站的可用性实时掌控；；（2）域名劫持监控服务全年7\*24小时对网站首页进行域名劫持探测，一旦发现域名被劫持则通过邮件或短信等方式进行告警。（3）网页挂马监控服务全年7\*24小时采用远程监控方式对网站页面进行网页挂马分析，一旦识别到网页挂马行为，则进行邮件或短信进行告警。（4）网站暗链监控服务全年7\*24小时采用远程监控方式对网站页面进行暗链分析，一旦识别到网页存在暗链行为，则进行邮件或短信进行告警。（5）敏感内容监控服务全年7\*24小时对关键网页的敏感内容进行监控，识别网站存在政治、低俗等敏感内容情况，并进行邮件或短信进行告警。（6）网站监控警服务针对网站监控平台发现的问题，监控平台自动通过微信或者短信发送告警信息到系统管理员等相关人员。（7）网站安全监控报告安全服务提供商定期汇总安全监控情况，并提交详细的监控报告。 | 安全监测月报（报告每月1份） | 全年 |  |
| 10 | 数据资产梳理服务 | 针对数据库资产以及数据库账户、权限情况进行梳理清查，通过对数据资产的摸底，形成数据资产清单，全局掌握数据资产情况。 | 《数据资产清单》、《数据库账户权限清单》 | 1次/年 |  |
| 11 | 数据安全评估服务 | 针对福州市公共资源电子交易平台、福州市建设工程电子招投标系统以访谈形式提供数据安全评估服务，基于数据资产发现与梳理，识别敏感资产的状况，从数据安全管理、数据生命周期开展评估工作，并根据评估结果提出改善建议。 | 《数据安全评估报告》 | 1次/年 |  |
| 12 | 数据安全管理体系服务 | 协助健全数据安全管理体系，为制定数据安全相关管理制度、规范、流程、策略提供咨询服务。 | 《数据安全组织制度》、《数据安全管理制度》 | 1次/年 |  |
| 13 | 攻防演练防守保障 | 通过网络安全攻防演练，进一步检验网络安全防护能力、监测发现能力、应急处置能力，发现可能在网络安全防护、监测和处置措施中存在的短板，积累有效应对网络安全攻击和威胁的经验，促进网络安全积极防御、协同处置的体系建设，促进网络安全队伍建设，在实战中有效提升网络安全保障能力。针对演练活动提供演练统筹服务、演练前期风险自查服务、演练前期整改加固服务、汇报总结服务等。 | 《检测报告》《总结报告》 | 1次/年 |  |

**二、供应商资格要求**

1.符合《中华人民共和国政府采购法》第二十二条规定条件；

2.落实政府采购政策需满足的资格要求：

(1)本合同包专门面向中小微企业采购，非中小微企业的投标将被视为无效投标。①根据《政府采购促进中小企业发展管理办法》（财库〔2020〕46号），投标人应为符合该办法规定的小微企业，应当按要求提供符合规定的《中小企业声明函》，无须提供其他证明材料。②根据《关于政府采购支持监狱企业发展有关问题的通知》（财库〔2014〕68号）文件规定，符合规定的监狱和戒毒企业(以下简称监狱企业)参加政府采购活动视同小型、微型企业，应当提供由省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件。③根据《关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141号）文件规定，符合规定的残疾人福利性单位参加政府采购活动视同小型、微型企业，应当提供通知规定的《残疾人福利性单位声明函》并对声明的真实性负责。④本项目为服务类，采购标的对应的中小企业划分标准所属行业详见采购标的一览表。（如属于专门面向中小企业采购的项目,供应商应为中小微企业、监狱企业、残疾人福利性单位)

3.本项目的特定资格要求：

(1)资格承诺函（若有）：根据《福州市财政局关于进一步推进政府采购领域优化营商环境工作的通知》（榕财采〔2021〕52号），2022年1月1日起，预算金额在500万元以内的政府采购项目推行供应商资格证明材料承诺制。供应商在投标（响应）时，可自行选择是否按该通知规定提供资格承诺函，若按规定提供资格承诺函的，无需再提交财务状况、缴纳税收和社保资金缴纳等证明材料。注：采购人有权在签订合同前要求中标人提供相关证明材料以核实中标人承诺事项的真实性。投标人应当遵循诚实守信的原则，不得作出虚假承诺，承诺不实的，属于提供虚假材料谋取中标、成交，依法追究相关的法律责任。

4.境内具有独立法人资格且具备合格有效的营业执照，具有独立承担民事责任和履行合同能力，在近三年内的经营活动中没有重大违法记录（须提供公告发布之日后通过“信用中国”网站(www.creditchina.gov.cn)及中国政府采购网(www.ccgp.gov.cn)查询其上述信用记录的信用信息查询结果网页打印件或者截图（均注明网址））。

5.供应商代表法人授权书原件（须提供法定代表人及供应商代表身份证正反面复印件），法人代表亲自参加的，可不提供授权书，只需提供法定代表人身份证即可。

**三、比价方法和标准**

1.供应商须按报价文件格式提供1份报价文件。所有资料加盖公章、装订成册后，加盖骑缝章，用信封密封并在封口处加盖公章。

2.截止时间前有效的报价供应商数量不少于3家，且比价期间符合所有比价条件的报价人不少于3家，否则本次采购程序终止，除采购任务取消情形外，将重新组织采购。

3.合同包采用最低价比价方法和标准：经比价小组评审，在提交的报价文件全部满足采购文件实质性要求的供应商不少于三家的前提下，依据统一的价格要素评定最低报价（报价不具合理性作无效报价处理），以提出最低报价的报价人作为成交候选供应商。

4.比价小组由3人组成。

附件：报价文件格式

**1.中小企业声明函（服务）**

 本公司郑重声明，根据《政府采购促进中小企业发展管理办法》（财库﹝2020﹞46 号）的规定，本公司参加福州市公共资源交易服务中心电子交易系统漏洞扫描及渗透测试服务全部由符合政策要求的中小企业承接。相关企业的具体情况如下：

 （标的名称），属于（采购文件中明确的所属行业），对应的中小企业划分标准所属行业为其他未列明行业；承接企业为（企业名称），从业人员 人，营业收入为 万元，资产总额为 万元，属于（中型企业、小型企业、微型企业）；

……

 以上企业，不属于大企业的分支机构，不存在控股股东为大企业的情形，也不存在与大企业的负责人为同一人的情形。

 本企业对上述声明内容的真实性负责。如有虚假，将依法承担相应责任。

 企业名称（盖章）：

 日期：

※注意：

1、从业人员、营业收入、资产总额填报上一年度数据，无上一年度数据的新成立企业可不填报。

2、供应商须按采购文件中明确的所属行业填列，否则，其提供的中小企业声明将被判定为无效声明函，由此造成的后果由供应商自行承担（涉及资格的按无效投标处理；涉及价格评审优惠的，不予认定）。

3、供应商应当对其出具的《中小企业声明函》真实性负责，供应商出具的《中小企业声明函》内容不实的，属于提供虚假材料谋取成交。

**残疾人福利性单位声明函（若有）**

（以资格条件落实中小企业扶持政策时适用，若有）

 本供应商郑重声明，根据《财政部 民政部 中国残疾人联合会关于促进残疾人就业政府采购政策的通知》（财库[2017]141号）、《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）的规定，本供应商为符合条件的残疾人福利性单位，且本供应商参加贵单位的（“福州市公共资源交易服务中心电子交易系统漏洞扫描及渗透测试服务”）项目采购活动：

由本供应商承接（ ）服务；

本供应商对上述声明的真实性负责。如有虚假，将依法承担相应责任。

备注：

1、请供应商按照实际情况编制填写本声明函。

2、若《残疾人福利性单位声明函》内容不真实，视为提供虚假材料。

供应商：（全称并加盖单位公章）

日期： 年 月 日

**监狱企业证明材料（若有）**

供应商为监狱企业，提供本单位承接的服务，并在报价文件中提供省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件。

**2.报价书**

致： 福州市公共资源交易服务中心

根据贵方为 项目的报价邀请，本签字代表（全名、职务）正式授权并代表报价人提交纸质报价文件一份。

据此函，签字代表宣布同意如下：

1. 所附报价表中提交的应提供和交付的货物及服务报价：福州市公共资源交易服务中心电子交易系统漏洞扫描和渗透测试服务项目人民币（小写） ，即 （大写） （中文表述）；

2.报价人已详细审查全部采购文件，包括修改文件（如有的话）和有关附件，将自行承担因对全部采购文件理解不正确或误解而产生的相应后果。

3.报价人保证遵守采购文件的全部规定，报价人所提交的材料中所含的信息均为真实、准确、完整，且不具有任何误导性。

4.报价人将按采购文件的规定履行合同责任和义务。

5.本报价文件自报价日起报价有效期为：90个日历日的期限内保持有效。

6.报价人同意提供按照贵方可能要求的与其报价有关的一切数据或资料，完全理解贵方不一定要接受最低的报价或收到的任何报价。

8. 与本报价有关的一切正式往来通讯请寄：

地址： 邮编：

电话： 传真：

报价人代表签章：

报价人（全称并加盖公章）：

日 期： 年 月

（报价文中个人签章应真实、有效。**请各潜在报价人特别注意**。）

**3.法定代表人授权书**

 致 福州市公共资源交易服务中心 ：

（报价人全称）法定代表人 授权 （报价人代表姓名）为报价人代表，代表本公司参加贵中心组织的 项目比价活动，全权代表本公司处理报价过程的一切事宜，包括但不限于：报价、比价、签约等。报价人代表在报价过程中所签署的一切文件和处理与之有关的一切事务，本公司均予以认可并对此承担责任。报价人代表无转委权。特此授权。

本授权书自出具之日起生效。

报价人代表： 性别： 身份证号：

单位： 部门： 职务：

详细通讯地址： 邮政编码: 电话：

（报价人代表应为报价公司的正式工作人员，否则视为无效报价。）

**[身份证件复印件]**

法定代表人、报价人代表身份证件复印件正反面：

授权方

报价人（全称并加盖公章）：

法定代表人签章：

日 期：

接受授权方

报价人代表签章：

日 期：

（报价文中个人签章应真实、有效。**请各潜在报价人特别注意**。）

**4.法人营业执照**等资格证明文件

致 福州市公共资源交易服务中心：

现附上由 （签发机关名称）签发的我方法人具有统一社会信用代码的营业执照副本复印件，该执照业合格真实有效。

（注：需复印包括能说明合格有效的内容，由企业加盖公章并注明复印件与原件一致。）

 报 价 人（全称并加盖公章）：

 报价人代表签章：

 日 期：

（报价文中个人签章应真实、有效。**请各潜在报价人特别注意**。）

**5.报价人的资格声明**

致 福州市公共资源交易服务中心：

我方在此声明：我方具备并满足下列各项条款的规定，本声明如有虚假或不实之处，我方将失去合格报价人资格且我方承担由此引起的一切法律责任。

（1）具有独立承担民事责任的能力；

（2）具有良好的商业信誉和健全的财务会计制度；

（3）具有履行合同所必需的设备和专业技术能力；

（4）有依法缴纳税收和社会保障资金的良好记录；

（5）参加政府采购活动前三年内，在经营活动中没有重大违法记录；

（6）报价人代表为我公司的正式工作人员；

（7）参加政府采购活动近三年无行贿犯罪记录；

（8）信用记录无任何应被拒绝参与政府采购活动的相关信息 (如列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单或其他不符合《中华人民共和国政府采购法》第二十二条规定条件的问题等情况)；

（9）法律、行政法规规定的其他条件。

就我方全部所知，兹证明上述声明是真实、准确的，并已提供了全部现有资料和数据，我方同意根据贵方要求出示文件予以证实。

报价人（全称并加盖公章）：

报价人代表签章：

日 期：

**6.响应部分**

技术和服务要求响应表

项目名称：福州市公共资源交易服务中心电子交易系统漏洞扫描及渗透测试服务项目

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 品目号 | 品目编码及品目名称 | 商品名称 | 技术规格、服务及验收要求 | **响应情况** | 是否偏离及说明 |
| 1 | [C16990000]其他信息技术服 | 福州市公共资源交易服务中心电子交易系统漏洞扫描及渗透测试服务 | 1.福州市公共资源电子交易平台（旧政务云26台服务器）：在2024年度进行≥3次安全漏洞扫描服务（原则上2024年第2、3、4季度各一次，采购人有特别要求的除外），2025年度进行1次安全漏洞扫描服务（原则上2025年第1季度完成，采购人有特别要求的除外）。 |  |  |
| 2.福州市公共资源电子交易平台（旧政务云26台服务器）：在2024年度进行≥3次渗透测试服务（原则上2024年第2、3、4季度各一次，采购人有特别要求的除外），2025年度进行1次渗透测试服务（原则上2025年第1季度完成，采购人有特别要求的除外）。 |  |  |
| 3.福州市建设工程电子招投标系统（新政务云32台服务器）：在2024年度进行≥3次安全漏洞扫描服务（原则上2024年第2、3、4季度各一次，采购人有特别要求的除外），2025年度进行1次安全漏洞扫描服务（原则上2025年第1季度完成，采购人有特别要求的除外）。 |  |  |
| 4、福州市建设工程电子招投标系统（新政务云32台服务器）：在2024年度进行≥3次渗透测试服务（原则上2024年第2、3、4季度各一次，采购人有特别要求的除外），2025年度进行1次渗透测试服务（原则上2025年第1季度完成，采购人有特别要求的除外）。 |  |  |
| 5.服务要求内容见附表。 |  |  |
| 6.按政府部门制定的相关规范、技术要求交付符合采购人要求的完整材料，并通过政府部门要求的系统安全绩效考核。项目工作成果应符合采购人的保密要求。 |  |  |
| 7.交付时间： 合同签订之日起一年内。 |  |  |

注：1、响应情况项下应填写具体的响应内容并与“技术规格、服务及验收要求”项下的内容逐项对应；2、对“技术规格、服务及验收要求”项下涉及“≥或>“、”≤或<”及某个区间值范围内的内容，应填写具体的数值。3、投标人需要说明的内容若需特殊表达，应先在本表中进行相应说明，再另页应答，否则报价无效。

**附表：**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **服务项目** | **服务内容** | **交付成果** | **服务频次** | **备注** |
| 1 | 漏洞扫描 | （1）针对内部主机如：服务器、操作系统、网络设备与数据库扫描；（2）针对业务系统开展现场或远程扫描。 | 漏洞扫描报告 | 4次（2024年第2、3、4季度各一次，2025年第1季度一次） |  |
| 2 | 渗透测试 | 利用目标应用系统的安全弱点模拟真正的黑客入侵攻击方法，以人工渗透为主，以漏洞扫描工具为辅。 | 渗透测试报告 | 4次（2024年第2、3、4季度各一次，2025年第1季度一次） |  |
| 3 | 协助安全加固 | 安全加固（包含软件应用基线、数据库基线、中间件基线、操作系统基线等), 安全加固服务采用“人工+工具”加固方式，即通过安全基线检查和安全策略修复，并结合第三方安全加固工具实现对操作系统的全面安全增强, 1)安全加固工具支持内核级的强制访问控制功能，支持基于敏感标记(安全等级)控制文件读写权限（提供对应工具功能截图）2)安全加固工具支持白名单功能，只有属于白名单的进程可以运行，可以有效禁止病毒或木马的执行。（提供对应工具功能截图）3)安全加固工具支持基于MD5的识别技术的文件完整性检查功能，可对文件进行资源完整性监控。（提供对应工具功能截图）4)安全加固工具支持基线检查功能，能对常见的系统脆弱性进行一键扫描和加固修复。（提供对应工具功能截图）5)安全加固工具支持服务器的非法外联管控，避免服务器私自连接外部网络。（提供对应工具功能截图）6)安全加固工具支持外接USB设备的管控，可对接入的第三方USB设备进行控制，防止物理层面的非法接入行为。（提供对应工具功能截图）7）安全加固工具具有中国网络安全审查技术与认证中心颁发的IT产品信息安全认证证书，满足“ISCCC-TR-001-2017《操作系统安全加固产品安全技术要求》（增强级）”相关产品标准及技术要求。（提供对应工具证书复印件证明） | 安全咨询相关内容 | 4次/年 |  |
| 4 | 制度建设辅导 | 协助采购人完善现有安全管理制度，按照等级保护管理部分的标准，从安全管理制度、安全管理机构、人员安全管理、系统建设管理、系统运维管理5个方面协助采购人补充及完善等级保护要求的管理体系建设中涉及到的制度文档，以及相关记录的完善。 | 安全管理制度汇编 | 1次/年 |  |
| 5 | 入侵痕迹排查 | 对中心部署在本地及云平台上的服务器操作系统和应用的运行环境进行入侵痕迹的安全检查，包括可疑的文件、服务、进程、端口、网络连接、网站WebShell后门等，综合评估当前系统运行环境安全情况，生产入侵痕迹检测报告，并提出安全修复建议 | 《入侵清查报告》 | 2次/年 |  |
| 6 | 安全防护设备租赁及演练支撑 | 1. 在网络安全监管部门举办的攻防演练期间租赁包括下一代防火墙（≥3台，要求具备入侵防御、网络防病毒功能）、高级持续性威胁检测设备(APT)（≥1台，要求具备APT攻击预测技术和攻击防御技术）、Web应用防火墙（≥1台，要求具备网页防篡改功能）、态势感知平台（≥1台，具备展示对应安全事件的建议处置方式）及其他的安全厂商认为应增加的设备部署于中心互联网边界，确保基础网络运行安全，在本地和云平台互联网区服务器上部署主机安全防护系统（具有针对服务器入侵检测和防护功能，并配有服务端可实现集中管理与监测，非普通杀毒软件，软件授权一年）。
 | 相关设备 | 每年按需提供（设备租赁时间≥60天） |  |
| 7 | 重要时期安全保障 | 在具有重大政治影响的活动前夕派遣专业安全服务人员提供资产清查、网络及数据安全检查和加固服务，活动期间根据中心需要安排人员提供远程支持，确保各网络及信息系统的安全稳定运行。攻防演练期间安排≥2名安全技术人员远程5\*8小时防守，借助云平台及本地现有和租赁的安全设备及部署的防护软件获取相关数据日志进行分析，根据分析结果进行威胁处置，并提供针对我单位系统的威胁攻击和处置数据的截图或日志（本地和云平台）等，确保单位网络及信息系统不被攻击成功，顺利完成防守任务，并协助中心编写演练相关材料报告。 | 重保相关报告 | 每年按需提供（现场值守时间≥30天） |  |
| 8 | 应急响应服务及疑难网络故障排查 | 在遇到突发事件后，立即开展故障排查，采取紧急措施并恢复业务；调查安全事件发生的原因，避免同类安全事件再次发生；在需要司法机关介入时，提供法律认可的数字证据等，根据中心需要协助开展网络安全应急演练，并对演练过程进行技术指导和支持，在遇到重大疑难网络故障时，安排技术人员协助排查故障原因； | 应急响应报告 | 全年，按需提供 |  |
| 9 | 在线监测服务 | 对中心涉及的web站点提供可用性监控、网页挂马监控、网页敏感信息监控等：（1）网站可用性监控服务全年7\*24小时对网站首页进行轮询探测，网站访问不到则通过邮件或短信等方式进行告警，确保网站的可用性实时掌控； （2）域名劫持监控服务全年7\*24小时对网站首页进行域名劫持探测，一旦发现域名被劫持则通过邮件或短信等方式进行告警。（3）网页挂马监控服务全年7\*24小时采用远程监控方式对网站页面进行网页挂马分析，一旦识别到网页挂马行为，则进行邮件或短信进行告警。（4）网站暗链监控服务全年7\*24小时采用远程监控方式对网站页面进行暗链分析，一旦识别到网页存在暗链行为，则进行邮件或短信进行告警。（5）敏感内容监控服务全年7\*24小时对关键网页的敏感内容进行监控，识别网站存在政治、低俗等敏感内容情况，并进行邮件或短信进行告警。（6）网站监控警服务针对网站监控平台发现的问题，监控平台自动通过微信或者短信发送告警信息到系统管理员等相关人员。（7）网站安全监控报告安全服务提供商定期汇总安全监控情况，并提交详细的监控报告。 | 安全监测月报（报告每月1份） | 全年 |  |
| 10 | 数据资产梳理服务 | 针对数据库资产以及数据库账户、权限情况进行梳理清查，通过对数据资产的摸底，形成数据资产清单，全局掌握数据资产情况。 | 《数据资产清单》、《数据库账户权限清单》 | 1次/年 |  |
| 11 | 数据安全评估服务 | 针对福州市公共资源电子交易平台、福州市建设工程电子招投标系统以访谈形式提供数据安全评估服务，基于数据资产发现与梳理，识别敏感资产的状况，从数据安全管理、数据生命周期开展评估工作，并根据评估结果提出改善建议。 | 《数据安全评估报告》 | 1次/年 |  |
| 12 | 数据安全管理体系服务 | 协助健全数据安全管理体系，为制定数据安全相关管理制度、规范、流程、策略提供咨询服务。 | 《数据安全组织制度》、《数据安全管理制度》 | 1次/年 |  |
| 13 | 攻防演练防守保障 | 通过网络安全攻防演练，进一步检验网络安全防护能力、监测发现能力、应急处置能力，发现可能在网络安全防护、监测和处置措施中存在的短板，积累有效应对网络安全攻击和威胁的经验，促进网络安全积极防御、协同处置的体系建设，促进网络安全队伍建设，在实战中有效提升网络安全保障能力。针对演练活动提供演练统筹服务、演练前期风险自查服务、演练前期整改加固服务、汇报总结服务等。 | 《检测报告》《总结报告》 | 1次/年 |  |

供应商全称：（盖章）

授权代表：（签字）

日期： 年 月 日

7.**报价部分**

报 价 表

项目名称：福州市公共资源交易服务中心电子交易系统漏洞扫描及渗透测试服务项目

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 品目号 | 品目编码及品目名称 | 商品名称 | 技术规格、服务及验收要求 | **报价（元）** | 是否进口 |
| 1 | [C16990000]其他信息技术服务 | 福州市公共资源交易服务中心电子交易系统漏洞扫描及渗透测试服务 | 1.福州市公共资源电子交易平台（旧政务云26台服务器）：在2024年度进行≥3次安全漏洞扫描服务（原则上2024年第2、3、4季度各一次，采购人有特别要求的除外），2025年度进行1次安全漏洞扫描服务（原则上2025年第1季度完成，采购人有特别要求的除外）。 |  | 否 |
| 2.福州市公共资源电子交易平台（旧政务云26台服务器）：在2024年度进行≥3次渗透测试服务（原则上2024年第2、3、4季度各一次，采购人有特别要求的除外），2025年度进行1次渗透测试服务（原则上2025年第1季度完成，采购人有特别要求的除外）。 |
| 3.福州市建设工程电子招投标系统（新政务云32台服务器）：在2024年度进行≥3次安全漏洞扫描服务（原则上2024年第2、3、4季度各一次，采购人有特别要求的除外），2025年度进行1次安全漏洞扫描服务（原则上2025年第1季度完成，采购人有特别要求的除外）。 |
| 4.福州市建设工程电子招投标系统（新政务云32台服务器）：在2024年度进行≥3次渗透测试服务（原则上2024年第2、3、4季度各一次，采购人有特别要求的除外），2025年度进行1次渗透测试服务（原则上2025年第1季度完成，采购人有特别要求的除外）。 |
| 5.服务内容见附表。 |
| 6.按政府部门制定的相关规范、技术要求交付符合采购人要求的完整材料，并通过政府部门要求的系统安全绩效考核。项目工作成果应符合采购人的保密要求。 |
| 7.交付时间：合同签订之日起一年内。 |

**附表：**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **服务项目** | **服务内容** | **交付成果** | **服务频次** | **备注** |
| 1 | 漏洞扫描 | （1）针对内部主机如：服务器、操作系统、网络设备与数据库扫描；（2）针对业务系统开展现场或远程扫描。 | 漏洞扫描报告 | 4次（2024年第2、3、4季度各一次，2025年第1季度一次） |  |
| 2 | 渗透测试 | 利用目标应用系统的安全弱点模拟真正的黑客入侵攻击方法，以人工渗透为主，以漏洞扫描工具为辅。 | 渗透测试报告 | 4次（2024年第2、3、4季度各一次，2025年第1季度一次） |  |
| 3 | 协助安全加固 | 安全加固（包含软件应用基线、数据库基线、中间件基线、操作系统基线等), 安全加固服务采用“人工+工具”加固方式，即通过安全基线检查和安全策略修复，并结合第三方安全加固工具实现对操作系统的全面安全增强, 1)安全加固工具支持内核级的强制访问控制功能，支持基于敏感标记(安全等级)控制文件读写权限（提供对应工具功能截图）2)安全加固工具支持白名单功能，只有属于白名单的进程可以运行，可以有效禁止病毒或木马的执行。（提供对应工具功能截图）3)安全加固工具支持基于MD5的识别技术的文件完整性检查功能，可对文件进行资源完整性监控。（提供对应工具功能截图）4)安全加固工具支持基线检查功能，能对常见的系统脆弱性进行一键扫描和加固修复。（提供对应工具功能截图）5)安全加固工具支持服务器的非法外联管控，避免服务器私自连接外部网络。（提供对应工具功能截图）6)安全加固工具支持外接USB设备的管控，可对接入的第三方USB设备进行控制，防止物理层面的非法接入行为。（提供对应工具功能截图）7）安全加固工具具有中国网络安全审查技术与认证中心颁发的IT产品信息安全认证证书，满足“ISCCC-TR-001-2017《操作系统安全加固产品安全技术要求》（增强级）”相关产品标准及技术要求。（提供对应工具证书复印件证明） | 安全咨询相关内容 | 4次/年 |  |
| 4 | 制度建设辅导 | 协助采购人完善现有安全管理制度，按照等级保护管理部分的标准，从安全管理制度、安全管理机构、人员安全管理、系统建设管理、系统运维管理5个方面协助采购人补充及完善等级保护要求的管理体系建设中涉及到的制度文档，以及相关记录的完善。 | 安全管理制度汇编 | 1次/年 |  |
| 5 | 入侵痕迹排查 | 对中心部署在本地及云平台上的服务器操作系统和应用的运行环境进行入侵痕迹的安全检查，包括可疑的文件、服务、进程、端口、网络连接、网站WebShell后门等，综合评估当前系统运行环境安全情况，生产入侵痕迹检测报告，并提出安全修复建议 | 《入侵清查报告》 | 2次/年 |  |
| 6 | 安全防护设备租赁及演练支撑 | 1. 在网络安全监管部门举办的攻防演练期间租赁包括下一代防火墙（≥3台，要求具备入侵防御、网络防病毒功能）、高级持续性威胁检测设备(APT)（≥1台，要求具备APT攻击预测技术和攻击防御技术）、Web应用防火墙（≥1台，要求具备网页防篡改功能）、态势感知平台（≥1台，具备展示对应安全事件的建议处置方式）及其他的安全厂商认为应增加的设备部署于中心互联网边界，确保基础网络运行安全，在本地和云平台互联网区服务器上部署主机安全防护系统（具有针对服务器入侵检测和防护功能，并配有服务端可实现集中管理与监测，非普通杀毒软件，软件授权一年）。
 | 相关设备 | 每年按需提供（设备租赁时间≥60天） |  |
| 7 | 重要时期安全保障 | 在具有重大政治影响的活动前夕派遣专业安全服务人员提供资产清查、网络及数据安全检查和加固服务，活动期间根据中心需要安排人员提供远程支持，确保各网络及信息系统的安全稳定运行。攻防演练期间安排≥2名安全技术人员远程5\*8小时防守，借助云平台及本地现有和租赁的安全设备及部署的防护软件获取相关数据日志进行分析，根据分析结果进行威胁处置，并提供针对我单位系统的威胁攻击和处置数据的截图或日志（本地和云平台）等，确保单位网络及信息系统不被攻击成功，顺利完成防守任务，并协助中心编写演练相关材料报告。 | 重保相关报告 | 每年按需提供（现场值守时间≥30天） |  |
| 8 | 应急响应服务及疑难网络故障排查 | 在遇到突发事件后，立即开展故障排查，采取紧急措施并恢复业务；调查安全事件发生的原因，避免同类安全事件再次发生；在需要司法机关介入时，提供法律认可的数字证据等，根据中心需要协助开展网络安全应急演练，并对演练过程进行技术指导和支持，在遇到重大疑难网络故障时，安排技术人员协助排查故障原因； | 应急响应报告 | 全年，按需提供 |  |
| 9 | 在线监测服务 | 对中心涉及的web站点提供可用性监控、网页挂马监控、网页敏感信息监控等：（1）网站可用性监控服务全年7\*24小时对网站首页进行轮询探测，网站访问不到则通过邮件或短信等方式进行告警，确保网站的可用性实时掌控； （2）域名劫持监控服务全年7\*24小时对网站首页进行域名劫持探测，一旦发现域名被劫持则通过邮件或短信等方式进行告警。（3）网页挂马监控服务全年7\*24小时采用远程监控方式对网站页面进行网页挂马分析，一旦识别到网页挂马行为，则进行邮件或短信进行告警。（4）网站暗链监控服务全年7\*24小时采用远程监控方式对网站页面进行暗链分析，一旦识别到网页存在暗链行为，则进行邮件或短信进行告警。（5）敏感内容监控服务全年7\*24小时对关键网页的敏感内容进行监控，识别网站存在政治、低俗等敏感内容情况，并进行邮件或短信进行告警。（6）网站监控警服务针对网站监控平台发现的问题，监控平台自动通过微信或者短信发送告警信息到系统管理员等相关人员。（7）网站安全监控报告安全服务提供商定期汇总安全监控情况，并提交详细的监控报告。 | 安全监测月报（报告每月1份） | 全年 |  |
| 10 | 数据资产梳理服务 | 针对数据库资产以及数据库账户、权限情况进行梳理清查，通过对数据资产的摸底，形成数据资产清单，全局掌握数据资产情况。 | 《数据资产清单》、《数据库账户权限清单》 | 1次/年 |  |
| 11 | 数据安全评估服务 | 针对福州市公共资源电子交易平台、福州市建设工程电子招投标系统以访谈形式提供数据安全评估服务，基于数据资产发现与梳理，识别敏感资产的状况，从数据安全管理、数据生命周期开展评估工作，并根据评估结果提出改善建议。 | 《数据安全评估报告》 | 1次/年 |  |
| 12 | 数据安全管理体系服务 | 协助健全数据安全管理体系，为制定数据安全相关管理制度、规范、流程、策略提供咨询服务。 | 《数据安全组织制度》、《数据安全管理制度》 | 1次/年 |  |
| 13 | 攻防演练防守保障 | 通过网络安全攻防演练，进一步检验网络安全防护能力、监测发现能力、应急处置能力，发现可能在网络安全防护、监测和处置措施中存在的短板，积累有效应对网络安全攻击和威胁的经验，促进网络安全积极防御、协同处置的体系建设，促进网络安全队伍建设，在实战中有效提升网络安全保障能力。针对演练活动提供演练统筹服务、演练前期风险自查服务、演练前期整改加固服务、汇报总结服务等。 | 《检测报告》《总结报告》 | 1次/年 |  |

供应商全称：（盖章）

授权代表：（签字）

日期： 年 月 日

**8.其他采购文件要求的文件**

致 福州市公共资源交易服务中心：

现附上

 报 价 人（全称并加盖公章）：

 日 期：

（报价文中个人签章应真实、有效。**请各潜在报价人特别注意**。）