**项目需求书**

**注:本项目要求的指标中，标注有“★”的条款必须实质性响应（满足或优于），投标人要特别加以注意，若有任何一条负偏离或不满足则导致投标无效。凡标有“▲”的参数不满足将导致严重扣分。**

## 采购项目内容：

|  |  |
| --- | --- |
| **序号** | **采购项目内容** |
| 一 | 网络安全等级保护测评及安全整改加固服务 |

## 网络安全等级保护安全整改加固服务

1. 采购项目背景
2. 项目背景

广东省特种设备检测研究院江门检测院成立于2003年6月30日，是经广东省质量技术监督局授权对锅炉、压力容器、压力管道、电梯、起重机械、厂（场）机动车辆等特种设备的安全性能监督检验的法定机构。是江门市质量技术监督局直属事业单位。

随着信息技术的不断发展，近几年来广东省特种设备检测研究院江门检测院走过了不断发展、完善的信息化历程，经过几次网络升级和改造，构成了一个配置多样的综合性网络平台。广东省特种设备检测研究院江门检测院需要针对主要的门户网站、广东省质量监督造船起重机械检验站（江门）业务管理系统、收费单管理系统等系统做一个全面可靠的安全防护。

为促进信息化建设、应用、管理和服务水平的持续提高，保障江门特检院内部网络、信息系统的安全、稳定运行，需要对目前的网络进行安全加固，并严格参照《信息系统安全基本要求》、《信息系统安全实施指南》、《网络安全法》等标准开展信息系统安全加固，但是安全建设是需要动态防御的，要不断更新防御手段和新增更多的防御措施。

1. 项目目标

本项目的建设目标是结合广东省特种设备检测研究院江门检测院网络的安全现状，确定广东省特种设备检测研究院江门检测院信息管理系统安全建设需求，并且解决“等级保护合规性要求”的网络现状，全面提升江门特检院的网络安全保护及上网办公体验水平，同时通过安全策略加固，使广东省特种设备检测研究院江门检测院网络安全建设处于动态防御的状态，并完成*3个系统（2个业务系统，1个网站系统）*的二级等级保护测评工作，确保《信息系统安全等级测评报告》获得到本地网络安全等级保护主管部门认可，取得公安部门颁发的测评报告回执。

1. 采购项目技术规格、参数及要求
2. 整体说明
3. 完成所采购安全策略加固服务内容，满足等级保护合规性要求。
4. 采购清单

网络安全等级保护安全整改加固服务

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| 身份鉴别 | 修改应用程序、数据库、网络设备、安全设备，增加密码复杂度检查功能，建议密码的最小强度为至少8位长度，及3类字符或3类字符以上；  修改应用程序、数据库、网络设备、安全设备，增加用户登录失败处理功能，推荐设置为3~5次以及锁定时间推荐设置为30分钟。 |
| 访问控制 | 由授权主体配置访问控制策略，并严格限制默认帐户admin的访问权限；建议安装三全分立原则授予不同帐户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系（如设置系统管理员、安全管理员、审计管理员等）。 |
| 安全审计 | 隐藏或删除审计模块的“删除”菜单，保证无法删除、修改或覆盖审计记录。 |
| 入侵防范 | 遵循最小安装原则，修改关闭不需要的组件、端口和应用程序；  限制终端接入方式。 |
| 恶意代码防范 | 对应用系统服务器进行安装杀毒软件，并定期升级和更新。 |
| 数据完整性、通信保密性 | 1、采用校验码技术保证通信过程中数据的完整性，建议使用https、ssh；  2、在通信双方建立连接之前，应用系统利用校验码技术进行会话初始化验证，建议使用https、ssh；  对通信过程中的敏感信息字段进行加密。 |
| 资源控制 | 1、对系统的最大并发会话连接数进行限制；  2、对单个帐户的多重并发会话进行限制。 |
| 漏洞扫描 | 按照等级保护2.0要求提供漏洞扫描服务，需对系统漏洞、WEB漏洞、基线配置、弱口令进行扫描和分析并且出具全面漏扫报告，对扫描结果进行人工验证，保证扫描结果的真实性。针对存在的漏洞提供修复建议，并提供精准可落地的漏洞修复方案。 |
| 信息安全意识培训 | 按照等级保护2.0要求提供信息安全意识现场培训服务，针对招标人的信息管理安全运维开展现场培训。包含但不限于网站安全、电子邮件安全、通信安全、设备安全、人员信息安全、密码安全等场景，并提供专业性安全培训教材。总共提供不少于2人天的现场安全意识培训服务。 |
| 安全检查服务 | 针对服务所涉及资产提供专业性安全检查服务，验证识别相关资产的脆弱性，并支持指定资产的小范围脆弱性修复，及时验证脆弱性修复的真实情况。 |
| 漏洞修复 | 根据初评结果对漏洞扫描及渗透测试漏洞进行修复 |
| 数据备份恢复 | 对测评所包含应用程序、数据库、网络设备、安全设备进行数据备份，并且进行数据恢复演练。 |
| 安全管理制度 | 根据实际情况定制可落地安全管理制度，并满足等级保护测评的要求。 |
| 定级备案 | 协助编写备案材料进行定级备案。 |
| 基线核查 | 对重要服务器、操作系统、网络设备、安全设备、中间件、数据库等基于信息安全风险的角度进行配置核查，检测网络设备的安全策略弱点和部分主机的安全配置错误等安全隐患。提出整改建议，指导运维人员优化配置策略，从而达到相应的安全防护要求。 |
| 安全风险评估 | 从技术性角度，参考国家及行业的标准规范，运用科学的方法与手段，识别评估资产存在的风险性，评估安全事件发生所可能造成的影响以及危害，提出有针对性的抵御威胁的防护对策和整改措施，将风险控制在可接受的水平。 |

1. **安全工具要求**

1、★投标人必须为保证所使用的所有工具和软件不会产生所有权和知识产权纠纷，并保证工具和软件的可用性和可靠性，投标人不是服务工具制造商的必须提供服务工具原厂商针对本项目的不存在知识产权纠纷及产品合格的书面证明函。由此产生的一切责任由投标人负完全责任。

2、★本项目使用的所有工具和软件（包括但不限于以下网络边界完整性检查工具、网络安全事件调查处置系统、内网安全管理系统工具）无需本项目采购方购买，均由中标人自行提供。

3、工具要求

|  |  |  |
| --- | --- | --- |
| 序号 | 指标项 | 详细参数 |
| 1 | 风险分布 | 支持从“高危”、“中危”、“低危”、“信息”四个维度的安全级别展示漏洞风险等级的分布情况（提供截图并盖章） |
| 2 | 风险统计 | ▲支持全局风险统计功能，可通过扇形图、条状图、标签、表格等形式展示，具备查看资产风险分布、漏洞风险等级分布、紧急漏洞、风险资产清单等信息详情功能。（提供截图并盖章） |
| 3 | 任务类型 | ▲支持全面扫描、资产发现、系统漏洞扫描、弱口令扫描、WEB漏洞扫描、基线配置核查六种任务类型，其中全面扫描支持系统漏洞扫描、WEB漏洞扫描、弱口令扫描等多种任务类型同时执行。（提供截图并盖章） |
| 4 | 基线配置检查 | 支持对Windows、Linux等操作系统按照等保二级、等保三级要求实施基线配置核查。（提供截图并盖章） |
| 5 | 等保合规自检 | ▲支持业务系统登记功能，保护等级支持第二级和第三级，可根据不同域类别添加资产到业务系统中。（提供截图并盖章） |
| 6 | 合规检测统计 | ▲提供检测结果综述分析，按照等保2.0的检测项要求，统计客户业务系统存在的不符合、部分符合、符合、待确认、不适用检测项，直观了解自身业务系统等保合规情况。（提供截图并盖章） |
| 7 | 报告管理 | ▲产品支持对系统漏洞、WEB漏洞、基线配置、弱口令进行扫描和分析，可同时输出包含系统漏洞扫描、WEB漏洞扫描、基线配置核查、弱口令扫描结果的报表。（提供截图并盖章） |
| 8 | 报告导出 | ▲支持统一管理所有业务系统的合规情况，合规报告可导出。（提供截图并盖章） |
| 9 | 工具资质要求 | ▲服务提供商须具备所使用漏扫工具制造厂商的合法授权（提供授权证明材料并盖章） |

1. 采购项目商务要求

**1.加固**

（1）★中标人应依照采购文件的要求和投标文件的承诺，将服务范围内所包含的系统安全策略加固至符合等级保护合规性要求。

**2.人员及企业资质要求**

（1）★具有信息系统安全及风险评估、管理体系等相关资质；

（2）★具有信息安全保障人员认证证书；

（3）★具有主流安全厂商认证安全服务工程师认证证书；

（4）★需要提供2年内所做安全加固的合同证明。

**3.其他重要事项说明或要求**

（1）在执行合同的过程中，所有经双方签署确认的文件（包括会议纪要、补充协议、往来信函）即成为合同的有效组成部分。

（2）如一方地址、电话、传真号码有变更，应在变更当日内书面通知对方，否则，应承担相应责任。

（3）★除采购人事先书面同意外，中标人不得部分或全部转让其应履行的合同项下的义务。

## 网络安全等级保护测评服务

1. 基本情况

为贯彻落实《中华人民共和国网络安全法》、《信息安全等级保护管理办法》等的文件要求，规范项目实施及管理工作，保证各项指标符合设计标准和建设规范，广东省特种设备检测研究院江门检测院采购具有网络安全等级保护测评服务，满足公安机关对广东省特种设备检测研究院江门检测院信息系统的安全等级保护备案要求及监督检查要求，通过测评，实现以下目标：

一是掌握系统的安全状况，排查系统安全隐患和薄弱环节，明确系统安全建设整改需求；

二是衡量系统的安全保护技术措施和管理措施是否符合等级保护的基本要求，是否具备了相应的安全保护能力；

三是增强网络安全等级保护的整体性、针对性和实效性，系统平台安全管理更加突出重点、统一规范、科学合理，提高安全保障能力，维护国家安全、社会稳定和公共利益，保障和促进信息化建设。

在此基础上，广东省特种设备检测研究院江门检测院按照国家有关规定和标准规范要求对信息系统进行安全建设，并达到国家信息安全等级保护相关要求，通过公安等级保护主管部门的备案审核。切实提高采购人的信息安全防护水平，增强信息安全防护能力。

1. 系统清单

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 信息系统名称 | 数量 | 拟定级别 |
| 1 | 广东省特种设备检测研究院江门检测院门户网站 | 1 | 二级 |
| 2 | *广东省质量监督造船起重机械检验站（江门）业务管理系统* | 1 | 二级 |
| 3 | *收费单管理系统* | 1 | 二级 |

1. 项目服务要求

### 1. 测评目标

对广东省特种设备检测研究院江门检测院的信息系统开展，包括协助定级备案、差距测评、指导整改实施、完成验收测评并出具等级保护测评报告等。按照工作需求出具测评报告，在报告中明确各信息系统是否达到相应的等级保护要求，并加盖公章。

### 2. 测评原则

#### 2.1 最小影响原则

所有测评方法、测评工具对被测系统的影响最小，最大程度保证被测系统的安全、稳定、连续运行。首先，在进行配置核查、工具测评和渗透测评前，需要对关键数据做好备份工作，并对可能出现的影响制定相应的处理方案；进行配置核查、工具测评时，安排好测试时间，尽量避开业务高峰期，在系统资源处于空闲状态时进行，并需要委托方工作人员对整个测试过程进行监督；测评完成时，与委托方工作人员一起，确认被测系统恢复至被测前状态；必要时，所有测评工作可邀请被测系统厂商一起参与，由测评单位、被测系统厂商、委托方共同评估测评方法，保证测评工具对系统影响最小。其次，各测评方法遵守的具体测评原则如下：

--------------------------------------------

（1） 人员访谈、文档审查等测评工作对被测系统无影响。

（2） 实地察看等保测评工作在委托方工作人员的陪同和监控下进行，测评人员严格遵守现场管理规定和设备管理规定，在未得到委托方工作人员的授权下，不擅自触碰任何设备。

（3） 配置检查等测评工作在委托方工作人员的陪同和监控下进行，该测评工作仅查看设备安全配置情况，不对配置进行修改，且不接入测评工具，测评时，测评人员提出需要查看的内容，由委托方工作人员进行操作，调出相关配置信息以供测评人员分析、取证，避免由于测评人员对某些专用设备不熟悉造成误操作。

（4） 工具测评在委托方工作人员的陪同和监控下进行，该测评工作需要在被测系统中接入测评工具，会对被测系统产生一定影响。为了保证测评工作影响最小，测评前对测评风险进行充分分析，在保证测评风险可控和可接受的前提下，在委托方工作人员监控下开展测评；如果测评对象不能接受测评风险，将抽样被测设备从被测系统中分离，对分离的设备进行测评；如果抽样被测设备不能从被测系统中分离，在被测单位的协助下，建立被测设备的仿真实验环境，在仿真实验环境环境中开展测评。

#### 2.2 标准规范原则

测评过程严格依据《中华人民共和国网络安全法》等政策法规、信息系统安全等级保护系统标准等相关规定，使测评工作有据可依，标准规范。

#### 2.3 保密性原则

与委托单位签署保密协议和非侵害性协议，保守在测评过程中知悉的关于委托单位和被测系统的国家秘密、商业秘密、敏感信息和个人隐私，并严格控制知悉范围。

#### 2.4 安全可控原则

保证测评工作安全可控，包括人员可控、工具可控、测评过程可控。开展测评工作前，测评方事先向委托方介绍测评工作流程，明确需要得到委托方协作的工作内容，并充分分析测评工作可能带来的测评风险，并制定相应的风险规避措施，确保测评工作的顺利进行。在测评过程中，对整个过程进行详细记录，保证有据可寻。

#### 2.5 高效有序原则

成立专项项目组，制定详细的测评工作实施方案、工作计划，保证测评工作高效、有序进行。

#### 2.6 充分有序原则

测评工作充分覆盖被测系统中的各种安全关键设备或系统，保证测评范围的完整性，并使用多种测试方法和工具，有效发现被测对象中的信息安全隐患。

--------------------------------------------

#### 2.7 客观公正原则

保证测评工作客观真实反应被测对象的信息安全现状和安全防护水平，减少人为因素对测试工作的影响，最大程度保证测评结果的客观公正。

#### 2.8 质量保障原则

测评过程中，对发现的问题与委托单位进行确认，对发现的重要安全问题进行截图，并形成正式文字资料，避免双方对测评结果产生争议。

### 3. 测评过程

信息系统等级保护测评过程需按照《信息系统安全等级保护测评过程指南》开展工作，等级测评过程分为四个基本测评活动：测评准备活动、方案编制活动、现场测评活动、分析及报告编制活动。测评双方之间的沟通与洽谈贯穿整个等级测评过程。

### 4. 测评准备

测评准备工作包括信息收集和分析、工具和表单准备等

### 5. 方案编制

方案编制活动包括测评对象确定、测评指标确定、测试工具接入点确定、测评内容确定、测评指导书测评指导书开发及测评方案编制六项主要任务：一、测评对象确认、二、测评指标确定、三、工具测试点确定、四、测试内容确定、五、测评指导书开、六、测评方案编制。

### 6. 现场测评

现场测评活动通过与测评委托单位进行沟通和协调，为现场测评的顺利开展打下良好基础，依据测评方案实施现场测评工作，将测评方案和测评工具等具体落实到现场测评活动中。现场测评工作应取得分析与报告编制活动所需的、足够的证据和资料。

现场测评涉及协助自查和验收测评两个阶段，在协助自查结束后，中标人编制整改建议，待招标方完成整改后开展验收测评。

现场测评活动包括现场测评准备、现场测评和结果记录、结果确认和资料归还三项主要任务。

### 7. 测评报告编制

在现场测评工作结束后，测评机构应对现场测评获得的测评结果或称测评证据进行汇总分析，形成等级测评结论，并编制测评报告。测评人员在初步判定单元测评结果后，还需进行整体测评，经过整体测评后，有的单元测评结果可能会有所变化，需进一步修订单元测评结果，而后进行风险分析和评价，形成等级测评结论。分析与报告编制活动包括单项测评结果判定、单元测评结果判定、整体测评、风险分析、等级测评结论形成及测评报告编制六项主要任务。

--------------------------------------------

### 8. 服务成果要求

整理和汇总测评系统的拓扑、建设文档等资料，形成备案单位表、备案系统表和定级报告，为提供等定级备案资料。项目成果交付表要求如下：

1. 《网络安全等级保护测评方案》
2. 《信息系统安全等级保护管理制度模板》
3. 《网络安全等级保护差距评估报告》或《问题清单及整改建议》
4. 《问题清单整改加固报告》
5. 《网络安全等级保护测评报告》
6. 《信息系统安全等级保护备案证明》
7. 《网络安全等级保护测评服务保密承诺书》
8. 其它相关的项目过程文档。
9. **项目标准**
10. 政策与法律法规：

|  |
| --- |
| 《中华人民共和国网络安全法》 |
| 《中华人民共和国计算机信息系统安全保护条例》（国务院147号令） |
| 《关于加强信息安全保障工作的意见》（中办发[2003]27号） |
| 《关于信息安全等级保护工作的实施意见》（公通字[2004]66号） |
| 《信息安全等级保护管理办法》（公通字〔2007〕43号） |
| 《关于开展全国重要信息系统安全等级保护定级工作的通知》（公信安[2007]861号） |
| 《公安机关信息安全等级保护检查工作规范》（公信安[2008]736号） |
| 《关于开展信息安全等级保护安全建设整改工作的指导意见》（公信安[2009]1429号 |
| 网络安全等级保护条例（总要求/上位文件） |
| 《广东省计算机信息系统安全保护条例》 |

2. 技术标准：

|  |
| --- |
| 计算机信息系统安全保护等级划分准则（GB 17859-1999）（上位标准） |
| 《信息安全技术 网络安全等级保护实施指南》（GB/T 25058-2019） |
| 《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019） |
| 《信息安全技术 网络安全等级保护测评要求》（GB/T 28448-2019） |
| 《信息安全技术 网络安全等级保护定级指南》（GB/T 22240-2020） |
| 《信息安全技术 网络安全等级保护测评过程指南》（GB/T 28449-2018） |
| 《信息安全技术 网络安全等级保护测试评估技术指南》（GB/T 36627-2018） |
| 《信息安全技术 信息安全风险评估规范》（GB/T 20984-2007） |
| 《信息技术 安全技术 信息安全管理体系要求》(GB/T 22080-2016) |
| 《信息安全技术 信息系统安全管理要求》（GB/T 20269-2006） |
| 《信息安全技术 信息系统安全通用技术要求》（GB/T 20271-2006） |
| 《信息安全技术 操作系统安全技术要求》（GB/T 20272-2019） |
| ，信息安全技术 服务器技术要求》（GB/T 21028-2007） |
| 《信息安全技术 数据库管理系统安全技术要求》（GB/T 20273-2019） |

1. **采用的技术与规范**
2. **服务期**

自合同签订之日起*60*个工作日内完成测评服务所有工作，其余服务工作在一年内完成。

1. **保密要求**

★中标人及中标人安排的人员须和采购人签订保密协议，中标人对项目下的保密资料应尽到管理人的义务，保密义务最低不得低于其对自己保密信息应尽的审慎态度。如保密资料涉及国家机密，中标人应当遵守国家有关国家机密的保密规定。采购人应与中标人签订保密协议，以厘清中标人保密职责与义务。保密条款包括但不限于以下：

（1）中标人对于保密资料仅可为本项目服务使用，不得挪作它用。

（2）未经采购人及建设单位书面同意，中标人不得利用连接互联网的电脑设备存储及处理保密资料。

（3）双方均须把保密资料的接触范围严格限制在因本项目规定目的而需接触保密资料的各自负责任的代表的范围内。

（4）在对外技术交流中，不得泄露和发表涉及本项目合作中保密资料。

（5）在未经采购人书面同意，中标人不得擅自对外(包括中标人的上下级单位)复制、转让采购人及建设单位提供的数据。

（6）中标人应当约束接触本次合作保密信息的员工遵守保密义务并签订保密协议。

（7）合作完成后，中标人须彻底删除与本次合作中有关的所有资料数据，不得私自作任何资料数据保留和备份，不得将资料数据泄漏给第三方。

--------------------------------------------

（8）违约责任

中标人违反本协议的约定，造成数据泄露，给国家的安全和利益造成损害的，中标人须负全部责任，且采购人可依据有关规定追究中标人的责任，并视情况作出处理，给采购人造成的损失由中标人承担。

1. **项目人员要求**
2. ★供应商必须承诺签订合同后为本项目成立不少于7人的本地化等级保护测评小组。由测评组长统一负责，测评项目组原则上不少于 1 名高级测评师、不少于 3 名中级测评师、不少于 3 名初级测评师组成，并提供项目组成员资质证明材料以及社保缴费证明材料（注：项目组成员可以是供应商或测评机构人员组成）。
3. ★中标人需具有公安部第三研究所颁发的网络安全等级测评与检测评估机构服务认证证书，如是供应商为测评机构代理商或者服务商，承诺签订合同时出具具有公安部第三研究所颁发的网络安全等级测评与检测评估机构服务认证证书的测评机构出具针对本项目服务承诺函。

**附件2： 报 价 表**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **采购内容** | **数量** | **报价**  **（人民币元）** | **备注** |
| 1 | 网络安全等级保护测评及安全整改加固服务 | 1 |  |  |

联系人： 联系电话：

**注：**

1. **供应商必须按报价表的格式填写，不得增加或删除表格内容。除单价、金额或项目要求填写的内容外，不得擅自改动报价表内容，否则将有可能影响成交结果，不推荐为成交候选人；**
2. **所有价格均系用人民币表示，单位为元，均为含税价；**
3. **平台上报价与报价表合计不一致的，以报价表合计（经价格核准后的价格）为准**
4. **报价表必须加盖单位公章，否则视为无效报价。**

供应商名称（单位盖公章）：

日期：

**附件3： 用户需求书响应声明函**

**致：广东省特种设备检测研究院江门检测院：**

关于贵单位、贵司发布网络安全等级保护测评及安全整改加固服务的招标公告，本公司（企业）愿意参加采购活动，并作出如下声明：

本公司（企业）承诺在报名时已对于用户需求书中的各项条款、内容及要求给予充分考虑，明确承诺对于本项目的用户需求中的各项条款、内容及要求均为完全响应，不存在任意一条负偏离或不响应的情况。本公司（企业）清楚，若对于用户需求书各项条款存在任意一条负偏离或不响应的情况，不被推荐为成交候选人的要求。

本公司（企业）承诺在本次采购活动中，如有违法、违规、弄虚作假行为，所造成的损失、不良后果及法律责任，一律由我公司（企业）承担。

供应商名称（单位盖公章）：

日期：

## 附件4：承诺函

**致：广东省特种设备检测研究院江门检测院：**

关于贵单位、贵司发布网络安全等级保护测评及安全整改加固服务项目的招标公告，本公司（企业）愿意参加竞价，并承诺：

本公司（企业）在本项目中会随时进行技术支持。同时向用户提供免费安装服务，使其达到完全掌握系统的使用方法为止。

否则，由此所造成的损失、不良后果及法律责任，一律由我公司（企业）承担。

单位名称：

日期：