**广东省英德监狱2024年**

**信息系统安全等级保护测评项目采购需求书**

# 1.项目概况

1.1采购项目名称：广东省英德监狱2024年信息系统安全等级保护测评项目

1.2本项目预算金额：40.7万元

1.3采购内容：确定服务机构，为采购人信息化项目提供信息系统安全等级保护和相关服务。

1.4服务地点：广东省英德监狱

# 2.项目背景

网络安全等级保护是国家信息安全保障的基本制度、基本策略、基本方法。2017年6月1日实施的《中华人民共和国网络安全法》第二十一条中，明确提出了“国家实行网络安全等级保护制度，履行安全保护义务，保障网络免受干扰、破坏或者未经授权访问，防止网络数据泄露或者被窃取、篡改”，为贯彻落实等级保护主管部门关于网络安全等级保护工作的要求，必须规范网络安全等级保护管理，切实提高英德监狱的网络安全防护与管控能力。本次采购主要是对英德监狱的信息系统提供网络安全等级保护测评服务，进一步巩固前期英德监狱在网络安全方面所取得的工作成果和推进等级保护工作落地。

# 3.资格要求

报价供应商资格要求：

3.1应标单位必须是具有独立承担民事责任的能力的在中华人民共和国境内注册的法人或其他组织，具备有效的营业执照（或事业法人登记证等相关证明）复印件。

3.2应标单位必须具备有效期内经公安部认证颁发的《网络安全等级测评与检测评估机构服务认证证书》，并提供复印件加盖公章。

3.3应标单位需提供公司在网络安全等级保护网（https://www.djbh.net/agency?q=agencyIn&tab=2）的在库证明（输入以上网址，查询公司，截图，盖公司章）。

3.4本项目不接受联合体投标。

# 4.等级保护测评依据

《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》([1994]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)

《信息安全等级保护备案实施细则》(公信安[2007]1360号)

GB/T 25058-2019 《信息安全技术网络安全等级保护实施指南》

GB/T 22240-2020 《信息安全技术网络安全等级保护定级指南》

GB/T 22239-2019 《信息安全技术网络安全等级保护基本要求》

GB/T 28448-2019 《信息安全技术网络安全等级保护测评要求》

GB/T 28449-2018 《信息安全技术 网络安全等级保护测评过程指南》

GB/T 20984-2022 《信息安全技术 信息安全风险评估规范》

# 5.服务项目内容

## **5.1信息系统信息安全等级保护测评需求**

根据信息系统安全等级保护定级要求，须对以下2个三级信息系统进行复评，拟对以下2个信息系统进行测评及定级二级，10个信息系统进行一级专家评审，具体情况如下：

|  |
| --- |
| 信息系统信息安全等级保护测评服务 |
| 序号 |
| 1 | 系统名称 | 服务内容 | 数量 | 级别 | 备注 |
| 2 | 监管改造信息管理系统 | 等保测评 | 1 | 三级 | 复评 |
| 3 | 刑罚执行网上协同工作平台 | 等保测评 | 1 | 三级 |
| 4 | 欣档档案管理系统 | 等保测评 | 1 | 二级 | 初评，含定级备案 |
| 5 | 亲情电话管理系统 | 等保测评 | 1 | 二级 |
| 6 | 财务管理系统（用友软件） | 定级备案 | 1 | 一级 | 专家评审意见 |
| 7 | ITC对讲监听 | 定级备案 | 1 | 一级 |
| 8 | 生卫系统 | 定级备案 | 1 | 一级 |
| 9 | 狱务公开查询系统 | 定级备案 | 1 | 一级 |
| 10 | 罪犯减假暂提请资格筛查系统 | 定级备案 | 1 | 一级 |
| 11 | 内网终端管理系统 | 定级备案 | 1 | 一级 |
| 12 | 视频人脸比对 | 定级备案 | 1 | 一级 |
| 13 | 机房动环系统 | 定级备案 | 1 | 一级 |
| 14 | 英德容灾备份系统（爱数） | 定级备案 | 1 | 一级 |
| 15 | 科达监控平台 | 定级备案 | 1 | 一级 |

具体要求：

（1）测评方对采购人的2个三级等保信息系统进行测试评估、分析差距、出具差距测评报告和安全整改建议；

（2）测评方对采购人的2个拟定级二级等保信息系统进行测试评估、分析差距、出具差距测评报告、协助进行系统备案和安全整改建议；

（3）测评方对采购人的10个拟定级一级等保信息系统进行专家评估、出具专家意见、协助采购人出具专家定级评审意见和安全整改建议；

（4）采购人根据差距测评报告与安全整改建议实施安全整改，测评方需协助采购人按照等级保护相关标准完善安全管理制度；

（5）测评方再次对采购人的以上二级、三级信息系统进行测试评估、出具等级保护2.0测评报告，并协助采购人通过等级保护主管部门的备案与检查。

## **5.2网络安全演练需求**

全年开展两次网络安全演练（第三季度、第四季度），具体需求如下：

5.2.1以桌面模拟形式进行网络安全演练，模拟安全事件的发生及处置过程，完成判断、决策、处置等应急响应的流程，检验和提高相关人员的临场组织指挥、应急处置和后勤保障能力。场景：数据泄露、勒索病毒、木马邮件、网页篡改等；

5.2.2线下演练时间为2024年第三季度、第四季度各实施一次安全演练，每次选取不同场景作演练，每次演练2名或以上专家。具体时间由采购方决定，演练实施完毕并完成交付符合采购方需求规定的第二次项目成果即视为完成此服务。

## **5.3网络安全培训需求**

根据省局及清远地区年度网络安全检查要求，同时，确实提高监狱警察职工网络安全意识，聘请网络安全专家对全监警察职工开展1天网络安全培训（第三季度前完成），具体需求如下：

5.3.1开展网络安全专题研讨和技术人员专题网络培训，全面提高警察职工的安全意识和技术人员的防护水平，了解前沿网络安全知识，掌握网络安全基础知识及提高应急处理能力；

5.3.2举办网络安全专题讲座培训，由专家进行授课，课时1天（至少两场次）。

## **5.4巡检需求**

安排技术人员对监狱中心机房进行全面巡检（每季度至少1次，一年至少4次），包括运行环境、网络环境、硬件配置的检查，以及对操作系统日志的检查与分析，根据系统的报错信息，发现系统潜在问题，对排查出的故障隐患和安全漏洞，提供解决措施及方案。对以上的巡查过程，形成巡查的记录。

**5.5应急处置需求**

监狱发生突发网络安全事件时，现场协助处理监狱突发网络安

全事件，确保监狱网络安全。具体需求如下：

5.5.1在接到监狱发生二级网络安全事件（网络中断或间断时间在2-3小时，或者系统数据部分损坏、丢失，可以通过备份进行恢复。例如：某服务器被入侵后，数据被删除，被删除数据有备份）寻求技术支撑时，2名或以上的专家8小时内到达现场，并提供可行性解决问题方法或技术；

5.5.2在接到监狱发生一级网络安全事件（网络中断或间断时间在4小时以上，或者系统数据损坏、丢失，并且无法 恢复，或者重要数据泄露，或者系统、网络被破坏，在60分钟内无法恢复）寻求技术支撑时，2名或以上的专家4小时内到达现场，并提供可行性解决问题方法或技术；

5.5.3在网络安全事件处理完毕后形成总结评估报告，包括安全事件发生的原因、事件规模、应急处理手段、处理的效果、事件的调查结果以及对后续风险进行评估并提出改进意见。

# 6.服务实施

## 6.1信息系统信息安全等级保护测评服务目标

通过网络安全等级保护测评服务，对本单位运行的信息系统开展符合性测评，衡量信息系统的安全保护管理措施和技术防护措施是否符合等级保护基本要求，是否具备了相应的安全等级保护能力。找出问题，针对性的制定整改措施，推进信息安全防护体系不断完善。

**6.1.1信息系统信息安全等级保护测评内容**

依据《信息安全技术 网络安全等级保护基本要求》，对采购人各信息系统的安全技术体系和安全管理体系等进行合规性检查，出具《信息系统安全问题清单》。在安全整改工作完成后，投标人组织现场验收测评，符合验收条件后，出具符合公安部门要求的《网络安全等级保护等级测评报告》。等保测评内容分成单项测评和整体测评：

（1）单项测评：

| **安全层面** | **测评内容** |
| --- | --- |
| 安全物理环境测评 | 物理位置选择、物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应、电磁防护等方面的核查、测试 |
| 安全通信网络测评 | 网络架构、通信传输、可信验证等方面的核查、测试 |
| 安全区域边界测评 | 边界防护、访问控制、入侵防范、恶意代码防范、安全审计、可信验证等方面的核查、测试 |
| 安全计算环境测评 | 身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、可信验证、数据完整性、数据备份恢复、剩余信息保护、个人信息保护等方面的核查、测试 |
| 安全管理中心测评 | 系统管理、审计管理等方面的核查、测试 |
| 安全管理机构测评 | 安全策略、管理制度、制定和发布、评审和修订等方面的管理和落实情况 |
| 安全管理制度测评 | 岗位设置、人员配备、授权和审批、沟通和合作、审核和检查等方面的管理和落实情况 |
| 安全管理人员测评 | 人员录用、人员离岗、安全意识教育和培训、外部人员访问管理等方面的管理和落实情况 |
| 安全建设管理测评 | 系统定级和备案、安全方案设计、产品采购和使用、自行软件开发、外包软件开发、工程实施、测试验收、系统交付、等级测评、服务供应商选择等方面的管理和落实情况 |
| 安全运维管理测评 | 环境管理、资产管理、介质管理、设备维护管理、漏洞和风险管理、网络和系统安全管理、恶意代码防范管理、配置管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理、外包运维管理等方面的管理和落实情况 |

（2）整体测评：

等级保护对象整体测评从安全控制点、安全控制间和区域间等方面进行测评和综合安全分析，从而给出等级测评结论。整体测评包括安全控制点测评、安全控制间测评和区域间测评。安全控制点测评是指对单个控制点中所有要求项的符合程度进行分析和判定。安全控制点间安全测评是指对同一区域同一类内的两个或两个以上不同安全控制点间的关联进行测评分析，其目的是确定这些关联对等级保护对象整体安全保护能力的影响。区域间安全测评是指对互联互通的不同区域之间的关联进行测评分析，其目的是确定这些关联对等级保护对象整体安全保护能力的影响。层面间安全测评是指通过对同一区域内的两个或两个以上不同层面的关联进行测评分析，这些关联对信息系统整体安全保护能力无影响。

## 6.1.2等保测评服务要求

（1）定级备案

响应机构需要协助XX单位完成本次项目信息系统的定级工作，组织相关专家和工作人员商讨系统定级情况，并将所需的定级备案资料提交至当地公安机关，最终取得《信息系统安全等级保护备案证明》。

（2）网络安全等级保护差距测评

差距测评委托具备网络安全等级保护测评资质的第三方测评机构根据《信息安全技术 网络安全等级保护基本要求》、《信息安全技术 网络安全等级保护测评要求》等标准实施并评估信息系统合规情况，并在完成实施后出具《信息系统安全问题清单》。

（3）协助整改咨询服务

响应机构需根据测评结果，在整改实施过程中，提供协助整改咨询服务。

（4）网络安全等级保护验收测评

在安全整改工作完成后，响应机构组织现场验收测评，根据被测评对象实际测评结论（优、良、中、差）出具2021版《网络安全等级保护【被测评对象】等级测评报告》，报告中必须明确相应信息系统是否满足等级保护要求。

（5）成果交付物

系统测评完成后需提供以下内容：

1. 《信息系统安全等级保护备案证明》；
2. 《信息系统安全问题清单》；
3. 《网络安全等级保护等级测评报告》；
4. 其它相关的项目过程文档。

（6）服务周期

合同签订之日后4个月内完成此项服务。

（7）服务验收标准

服务通过验收须满足以下所有条件：

（1）完成差距测评工作，并出具《信息系统安全问题清单》；

（2）完成验收测评工作，并出具《网络安全等级保护等级测评报告》；

（3）提交调研表、现场测评记录表、会议纪要等服务过程材料；

（4）符合公安部门提出的信息安全等级保护测评相关要求。

（8）售后服务要求

响应机构必须在服务期内提供7×24小时线上技术支持和服务，8小时内作出实质性响应。如通过电话，远程等非现场的方式无法解决问题，需要及时安排技术人员前往客户现场解决问题在问题解决后24小时内，提交问题处理报告，说明问题种类、问题原因及造成的损失等情况。

# **6.1.3**测评工具要求

（1）本项目在实施过程中所使用到的专业安全服务工具由投标人提供，响应供应商必须保证所使用的所有工具和软件不具有所有权和知识产权纠纷，并保证工具和软件可用性和可靠性。由此产生的一切责任由响应供应商负完全责任。（此费用已包含在本项目报价中，采购人不在另付费用。）

（2）响应供应商需提供承诺使用符合国家标准的漏洞扫描设备辅助完成测评工作工具的函（格式自拟）。

（3）为确保响应供应商开展信息系统安全测评的服务质量，响应供应商必须采用符合国家标准的漏洞扫描设备辅助完成测评工作，参数要求如下：

| **指标项** | **指标要求** |
| --- | --- |
|  | 任务管理 | 支持手动创建重要信息系统检查、行业主管部门检查、备案单位检查、网站检查、自定义检查任务。 |
| 支持检查任务并行检查及并行检查结果合并。 |
| 支持任务的打开、另存为、修改、删除、关闭。 |
| 支持与等级保护监察平台数据的上报和下发。 |
| 检查任务 | 检查范围：支持行业主管部门、备案单位、重要信息系统、网站四类检查对象的检查范围。支持基本情况、定级备案检查范围。 |
| 检查内容：支持系统定级情况、岗位设置情况、安全审计情况检查内容。 |
| 检查要点：支持检查对象检查内容具体检查指标项进行检查。 |
| 检查结果录入类型：单项判定：支持判定未检、不适用、0分、1分、2分、3分、4分、5分。检查结果录入：支持录入检查结果记录。 |
| 针对每个检查要点应提供相应的检查方法，检查结果判定依据相关检查知识，以便引导进行现场检查。 |
| 支持对检查过程中具体检查对象（例如：主机、网络设备）进行调整功能，要求可以选择已有的检查对象或录入新的检查对象。 |
| 支持将任务导出成检查模板，检查人员能够根据被检查单位情况，灵活分配各自的检查任务，支持导出检查表单提前让被检查单位人员对应进行自查，检查人员经现场检查核对无误之后，可以直接将检查表单数据导入到工具箱中。 |
| 检查层面、检查内容、检查指标项支持保存为模板，模板可导入、导出。 |
| 支持检查工具检查结果信息的展现功能。 |
| 支持导出、导入检查项。 |
| 支持手动填写测评概述，概述内容包括测评目的、测评依据、测评方法、测评结论、整体测评结果汇总。 |
| 数据汇总 | 支持一键导入功能，将检查工具集、检测结果自动导入到工具箱。 |
| 支持手动导入工具检查结果到工具箱及关联任务检查对象。 |
| 支持工具检查结果自动关联知识库。 |
| 检查结果导出 | 导出的检查结果应按照指定的接口规范导出。 |
| 支持自动生成不同类型检查任务的检查报告，检查报告应包含不符合项的风险描述信息和安全评分。 |
| 兼容性 | 支持与工具箱监察管理系统数据的上报和下发。 |
| **监察指标库升级维护** | 指标库要求 | 监察指标库包含：控制点和要求项。 |
| 指标库升级维护 | 提供监察知识库升级功能，可以对监察知识库进行手动更新。 |
| 应提供升级检测和提醒功能。 |
| 监察知识库升级应有日志记录。 |
| **监****察****知****识****库****升****级****维****护** | 知识库要求 | 知识库内容必须覆盖所有检查指标。 |
| 知识库内容应包含检查指标的检查方法、检查结果判定依据和不符合项的风险提示。 |
| 知识库可以依据网络安全的标准和分析模型，对检查工具的检查结果进行自动分析，给出相应的检查结果记录。 |
| 知识库可以针对不同类型的检查任务，对检查结果进行自动分析和安全评分，自动生成相应的检查结果记录。 |
| 知识库内容应描述正确，并具有明确的引导作用。 |
| 知识库升级维护 | 知识库内容必须覆盖所有检查指标。 |
| 知识库内容应包含检查指标的检查方法、检查结果判定依据和不符合项的风险提示。 |
| 知识库可以依据网络安全的标准和分析模型，对检查工具的检查结果进行自动分析，给出相应的检查结果记录。 |
| **工****具****管****理** | 升级管理 | 技术支持网站应提供检查工具升级提示功能，当检查工具有更新时，采购人可以进行检查工具的升级操作。 |
| 检查工具升级操作应在工具箱留有日志记录。 |
| 结果管理 | 应提供结果分析，依据内置知识库自动对工具检查结果进行分析，自动判别相应检查指标的检查结果。 |
| 结果导入操作应留有日志记录。 |
| 风险提示 | 所有检查工具启动时，默认都会进行风险提示，支持通过配置是否下次启用风险提示。 |
| **系****统****管****理** | 配置管理 | 配置管理应对工具箱监察管理系统参数进行配置:支持系统最大登录次数设置；支持锁定用户时间设置；支持软件自动锁定功能；支持口令强度策略设置。 |
| 用户管理 | 支持对采购人账户进行管理，支持管理员、操作员、审计员角色账户增加、口令修改；支持对账户新增、修改、删除；内置角色默认权限；支持用户密码找回功能。 |
| 日志管理 | 可查看操作日期、操作用户、操作对象日志记录。 |
| 提供日志筛选功能。 |
| 提供日志导出备份功能。 |
| 系统升级 | 应提供升级功能，升级操作应简单。 |
| 技术支持网站应提供升级提示功能。 |
| 设备厂商应定期发布离线升级包，支持手动导入升级。 |
| 升级操作应留存日志记录。 |
| 工具箱监察管理系统具有登录尝试失败锁定功能。 |
| 访问控制 | 应依据安全策略严格控制用户文件，数据表重要信息资源的操作。 |
| 应确保不提供已注销用户的任何信息，包括鉴别信息。 |
| 安全审计 | 指标库、知识库、监察工具升级操作。 |
| 用户登录和注销事件。 |
| 数据导入、导出事件。 |
| 通信安全 | 应采取措施确保导入和导出数据的完整性。 |
| U盘安全检查工具向工具箱提交的检查结果数据的完整性。 |
| **等级保护工具箱配备U盘安全检查工具集** |
| Windows主机安全配置检查工具 | 支持检查主机系统配置信息，包括：计算机名、用户名、操作系统、版本、内存大小、磁盘大小、系统路径、共享目录；支持检查USB接入设备信息；支持检查Internet Explorer、Chrome、Firefox等浏览器上网记录、Cookie记录；支持检查主机硬件信息，包括：CPU信息、主板信息、内存信息、显卡信息、硬盘信息、网卡信息；支持检查主机开机自启动项程序；查看主机上已经启动的可能有风险的服务程序，包括：如Task Scheduler、Print Spooler、Remote Registry等服务；支持检查账户安全策略信息，包含口令长度、复杂度、定期更换、登录失败、锁定次数等；对系统账户进行检查，可智能识别系统影子账户（隐藏账户）；查看系统是否开启系统审核、系统登录事件、审核账户登录事件等安全审计策略；运行环境支持Windows XP、Windows7、Windows Server 2003、Windows Server 2008等操作系统类型；支持在线更新、离线升级。 |
| 主机病毒检查工具 | 支持对操作系统的关键机制，如系统服务、内存、注册表、启动进程；检测操作系统的安全模型，包括访问控制、特权和审计；反馈系统安全配置、文件访问，驱动、引导系统深度进行检查； 检查流氓软件、蠕虫病毒、其它恶意程序等；支持快速扫描、全盘扫描、自定义目录扫描；运行环境支持Windows XP、Windows7、Windows Server 2003、Windows Server 2008等操作系统类型；支持在线更新、离线升级。 |
| 主机木马检查工具 | 支持检查系统中的木马程序、Rootkit、间谍程序等；提取操作系统的关键机制，如系统服务、内存、注册表、启动进程；检测操作系统的安全模型，包括访问控制、特权和审计；反馈系统安全配置、文件访问，驱动、引导等系统深度信息；支持快速扫描、全盘扫描、自定义目录扫描；运行环境支持Windows XP、Windows7、Windows Server 2003、Windows Server 2008等操作系统类型；支持在线更新、离线升级。 |
| 网站恶意代码检查工具 | 支持asp、asa、cer、jsp、jspx、php等文件格式检查；支持自定义文件后缀格式；支持异性、变异WEBSHELL后门代码检查；支持关键恶意特征码定位；支持快速扫描、全盘扫描、自定义路径扫描；支持自定义扫描策略、可扩充恶意特征码；支持自定义文件大小扫描；运行环境支持Windows XP、Windows7、Windows Server 2003、Windows Server 2008等操作系统类型；支持在线更新、离线升级。 |
| **等级保护工具箱配备在线检查工具集** |
| Linux主机安全配置检查工具 | 支持检查主机系统配置信息，包括：计算机名、用户名、操作系统、版本、内存等；支持检查系统安全补丁升级情况；支持检查不必要的服务和端口（如TELNET、SSH、SNMP、HTTP等）；支持检查账户安全策略信息，包含口令长度、复杂度、定期更换、登录失败、锁定次数等；支持SNMP、SSH服务、版本信息检查；支持检查安全审计配置情况、包含事件类型；支持检查屏幕保护恢复时间；支持RedHat、Ubuntu、Debian、Fedora、Suse、Centos操作系统类型；支持在线更新、离线升级。 |
| 网络及安全设备配置检查工具 | 支持对华三、思科、华为路由器、交换机通用系列网络设备安全分析检查；支持对天融信、网神、启明星辰、网御星云、Juniper防火墙通用系列设置安全分析检查；支持检查账户安全策略信息，包含口令长度、复杂度、定期更换、登录失败、锁定次数等；支持检查安全审计策略，包含事件类型、SYSLOG服务器；支持检查不必要的服务和端口（如TELNET、FTP、SNMP、HTTP、Sendmail）；支持SNMP、SSH服务、版本信息检查；运行环境支持Windows XP、 Windows7、 Windows Server 2003、Windows Server 2008等操作系统类型；支持在线更新、离线升级。 |
| 弱口令检查工具 | 应用服务支持类型：SSH、SMB、TELNET、FTP、RDP、SQL Server、Oracle、MySQL、POP3等协议应用程序弱口令检查；支持自定义账户、口令字典；支持自定义应用协议TCP端口；内置常见弱口令字典（如口令为：123456、88888888、12345等）；支持本地、远程主机及多协议同时检查；运行环境支持Windows XP、Windows7、Windows Server 2003、Windows Server 2008等操作系统类型；支持在线更新、离线更新。 |
| 数据库安全检查工具 | 支持IPV6地址检查；支持对数据库弱点、不安全配置、安全策略、补丁升级、弱口令安全检查；支持主流Oracle、SQL Server、DB2、Informix、MySQL、Sybase数据库类型；支持授权扫描，使用具有DBA权限的数据库用户，执行选定的安全策略实现对目标数据库检查；非授权扫描,采购人在没有授权的情况下（即：不需要数据库用户名、密码），根据选定的安全策略对目标数据库进行的检测；策略自定义,提供扫描策略可自定义模式，操作者可以灵活选择默认策略的同时也可以自定义添加策略；支持在线更新、离线升级。 |
| 网站安全检查工具 | 支持WEB 2.0，支持各类JavaScript脚本解析；支持WAP站点扫描；支持FLASH解析；支持基于HTTPS应用系统的扫描；支持实时存储扫描项目文件、断点续扫；支持ERP等复杂的Web应用系统扫描；支持易通、织梦、、Discuz、Ecshop、易思、方欣、大汉、科讯、通达OA、PHPCMS、PHP168、PHPCMS2008、phpcms v9、SHOPEX、SiteServer CMS、TRS、 Nginx代码执行、Spring代码执行、亿邮邮件系统命令执行等国内、国外知名WEB应用程序漏洞扫描；支持JSP、CGI、ASP、.NET等类型动态页面；支持IP地址、域名地址、批量网站扫描；支持无人值守模式下的全自动扫描；支持HTTP 1.0和1.1标准的Web应用系统；支持Oracle、SQL Server、DB2、Informix、Sybase、MySQL、PostgreSQL、Access、Ingres等后台数据库类型；支持对SQL注入、XSS跨站脚本、伪造跨站点请求、网页木马、隐藏字段、表单绕过、AJAX注入、弱配置、敏感信息泄漏、HI－JACK攻击、弱口令、Xpath注入、LDAP注入、框架注入、操作系统命令注入、Flash源代码泄漏、Flash跨域攻击、Cookies注入、敏感文件、第三方软件、其他各类CGI等漏洞进行扫描；支持在线更新、离线升级。 |
| 系统漏洞检查工具 | 支持对Microsoft Windows XP/2003/Vista/2008/7、Sun Solaris、HP Unix、IBM AIX、IRIX、Linux、BSD等操作系统进行漏洞扫描；支持对Web、FTP、电子邮件等应用系统以及Office、Apache等常用软件进行漏洞扫描；支持对网络设备进行漏洞扫描；支持多种扫描策略，包括常规完全扫描、高强度完全扫描、高强度扫描、中强度扫描、低强度扫描、Windows主机扫描、类Unix主机扫描等扫描策略，方便采购人快速选择；支持自动统计总体漏洞数量、统计不同操作系统类型的主机数量、统计所有开发端口、可用帐户、列出每一个漏洞所存在的主机、详细描述与修补建议。漏洞详细描述包括：漏洞名称、详述、修补方案、CVE/Bugtraq/CNCVE/CNNVD编号、CVSS评分等；支持在线、离线更新；支持导出Word、PDF常见格式报表。 |
| 运行安全 | 不得改变检查对象当前配置； |
| 不影响检查对象正常运行； |
| 不影响检查对象所属网络正常运行； |
| 不在检查对象中遗留痕迹。 |
| 数据安全 | 存储安全 | U盘检查工具应对所有检查数据采用国产加密算法进行加密，防止监察数据被非法读取。 |
| 痕迹安全 | U盘检查工具应对所有检查数据采取痕迹消除措施，以防止信息泄露。 |
| **安全性** | 支持等级保护检查过程的采购人信息的安全保护，所有数据以加密方式存储传输。 |
| U盘自身具有病毒、木马程序免疫功能，防止病毒、木马程序感染U盘内文件。 |
| **报表中心** | 支持生成信息系统检查任务报告、行业主管部门检查任务报告、备案单位任务报告、网站安全检查任务报告、自建检查任务报告；支持检查任务汇总、预览；支持对信息系统检查任务检查结果进行得分汇总，并以饼形图的方式进行展示；支持生成等保测评报告、工具检测类型报表，等保测评报告采用最新的测评报告2015模板；支持WORD、HTML格式报表导出；支持下载自查表。 |
| **辅助****功能** | 工具箱监察管理系统和U盘安全检查工具应提供软件截图工具，便于实时保存系统关键界面信息。 |

## 6.2**网络安全演练需求**

全年开展两次网络安全演练（第三季度、第四季度），具体需求如下：

 （1）从以下网络安全事件场景中选取两种不同类型中的两个场景，以桌面模拟形式进行网络安全演练，模拟安全事件的发生及处置过程，完成判断、决策、处置等应急响应的流程，检验和提高相关人员的临场组织指挥、应急处置和后勤保障能力。具体网络安全事件场景如下：





（2）线下演练时间为2024年第三季度、第四季度各实施一次安全演练，每次演练2名或以上专家。

（3）演练内容应当贴合采购方环境实际，供应商应及时与采购方沟通，并在接到采购方演练需求时，准确无误制作演练方案，并在10天内提交演练方案给采购方，采购方有权要求供应商对演练内容进行修改直至符合演练需求。

（4）供应方应在演练前提供以上21种常见故障类型的应急处置预案，演练结束后，形成完整的演练报告并提交给采购方。

## 6.3网络安全培训要求

**6.3.1网络安全培训内容**

培训内容包括网络安全意识，网络安全基础知识，前沿网络安全知识，网络安全隐患，安全上网建议等切实贴合监狱警察职工工作实际的网络安全内容。

**6.3.2 网络安全培训时间与服务周期**

网络安全培训服务周期为签订合同后3个月内实施完毕，提供培训课件给采购方，提前与采购方沟通授课内容及授课事宜，两场次网络安全培训具体培训时间以采购方要求为准，两场次培训不在同一工作日且每场次时长不少于3.5小时，培训完成即视为完成网络安全培训服务。

**6.4 中心机房安全巡检要求**

**6.4.1中心机房安全巡检内容**

供应方对监狱中心机房进行全面巡检，包括机房运行环境、网络环境、硬件配置的检查，以及对操作系统日志的检查与分析，根据系统的报错信息，发现系统潜在的问题，对排查出的故障隐患和安全漏洞，提供解决措施及方案。巡检人员对以上的巡查过程，形成机房巡检记录表，形成机房巡检报告、整改建议并提供给采购方。

**6.4.2中心机房安全巡检过程**

对监狱中心机房核心设备如交换机、路由器、服务器、存储阵列、网络及安全、综合布线、各应用系统等，包括硬件设备的检查，运行环境、硬件配置的检查，以及对系统日志的检查与分析、性能调优、故障隐患排除等，并填写设备巡检记录表。

**6.4.3中心机房安全巡检服务周期**

中心机房安全巡检周期以签订合同后12个月内实施完毕，采取每季度至少全面巡检监狱中心机房1次（含1次），共4次以上（包含4次）的全面巡检服务。

**6.5网络安全事件应急处置。**

为保障监狱网络安全，提高监狱发生突发网络安全事件时处理突发事件的能力，增强处置突发事件的力量。供应方需按照要求，提供专家现场协助监狱信息技术部门处理监狱突发网络安全事件。

**6.5.1网络安全事件应急处置过程**

1. 供应方在接到监狱发生二级网络安全事件（网络中断或间断时间在2-3小时，或者系统数据部分损坏、丢失，可以通过备份进行恢复。例如：某服务器被入侵后，数据被删除，被删除数据有备份）寻求技术支撑时，2名或以上具有网络中级职称或以上的专家8小时内到达现场，并提供可行性解决问题方案或技术提交给采购方；

b）供应方在接到监狱发生一级网络安全事件（网络中断或间断时间在4小时以上，或者系统数据损坏、丢失，并且无法 恢复，或者重要数据泄露，或者系统、网络被破坏，在60分钟内无法恢复）寻求技术支撑时，2名或以上专家（其中1名必须为高级职称专家，1名或以上为中级职称或以上专家）4小时内到达现场，并提供可行性解决问题方案或技术提交给采购方；

c）在网络安全事件处理完毕后形成总结评估报告，包括安全事件发生的原因、事件规模、应急处理手段、处理的效果、事件的调查结果以及对后续风险进行评估并提出改进意见。

**6.5.2网络安全事件应急处置周期**

网络安全事件应急处置周期以合同签订之日为服务起始时间，服务期为12个月。

# 服务团队要求

本项目服务团队人员资质证明材料（盖章版），均在确定中标方后，中标方于中标后10个工作日内提供给采购方核验。

**7.1等保测评人员要求**

供应商需要成立不少于5人的项目服务团队，供应商为本项目配备的至少1名（包含1名）项目经理需同时具备信息安全等级保护高级测评师、公安部信息安全等级保护评估中心颁发的重要信息系统保护人员（CIIPT）证书、中国信息安全测评中心颁发的注册信息安全专业人员（CISP）证书、ISACA认证中心颁发的国际信息系统审计师（CISA）证书。

本项目配备的至少4名（包含4名）技术人员具有公安部信息安全等级保护评估中心的信息安全等级测评师证书、具备中国信息安全测评中心颁发的注册信息安全专业人员（CISP）证书、中国网络安全审查技术与认证中心颁发的信息安全保障人员认证（CISAW）证书。均为中标单位正式工作人员，均需提供资格证书证明材料及近半年内人员在本单位购买社保证明。

**7.2网络安全演练人员要求**

网络安全演练实施过程要求专家为具有工业和信息化部颁发的计算机类人员中级或以上（含中级）资质，均为中标单位正式工作人员，提供近半年内人员在本单位购买社保资料证明。

**7.3网络安全培训人员要求**

网络安全培训实施过程所要求专家为具有工业和信息化部颁发的计算机类人员中级或以上（含中级）资质，均为中标单位正式工作人员，提供近半年内人员在本单位购买社保资料证明。

**7.4中心机房巡检人员要求**

中心机房巡检过程要求供应方安排机房巡检技术人员为该单位在册员工（以社保缴纳证明为认定依据）。必须要具有一定的专业素养，熟悉机房管理规范流程，具备丰富的机房管理运维能力，对主流数据库及存储有丰富维护经验，熟悉国产主流厂家网络及安全设备的管理维护，具备数据包分析和网络安全防护能力，具备管理和维护服务器和磁盘阵列等硬件和软件系统，解决应用系统故障和问题，对服务器系统进行必要的配置和变更，部署、管理虚拟化平台，对业务系统数据进行完整性、安全性保护，熟悉PC技术原理和整体架构、常用操作系统及软件，有视频监控、对讲报警、门禁、广播等安防系统的维护经验和能力。

**7.5应急处置实施人员要求**

应急处置过程要求监狱发生二级网络安全事件时，2名或以上具有网络中级职称或以上的专家为具有工业和信息化部颁发的计算机类人员中级或以上（含中级）资质，均为中标单位正式工作人员，提供本公司社保资料证明（提供证明材料）；发生一级网络安全事件时，2名或以上专家中1名为具有工业和信息化部颁发的计算机类人员高级职称资质，1名为具有中级或以上（含中级）资质，均为中标单位正式工作人员，提供近半年内人员在本单位购买社保资料证明。

**7.6其他要求**

供应商必须保证从事本项目工作的相关人员具备完成合同规定的工作所需的资历和技能，并向采购人如实提供相关人员专业经验和水平的证明材料。

投标人须承诺，如在项目实际执行过程中发生项目经理不能按采购文件要求胜任相关工作的，采购人有权要求更换项目经理，投标人须在两周内调整为符合采购文件要求且能胜任相关工作的项目经理并到位开展工作，否则采购人有权终止合同并报相关管理部门进行处理。投标人承诺的项目经理和开发实施的主要人员未经用户同意不得调整；投标人如中途更换项目经理和主要开发技术人员，应征得用户同意，否则采购人有权终止合同。

服务商应指派固定的团队为本项目提供专业服务。如须调整服务团队成员，须书面向采购人提出申请，说明申请理由，经采购人书面同意方可调整团队人员，调入人员的资历和从业经验不低于调出人员，否则视为违约行为，采购人有权终止服务合同。

# 8.报价要求

8.1本次预算价为40.7万元，控制价为40.7万元，报价金额需以预算价为基数报具体金额，并不得超过控制价，报价须包含完成本项工作的全部费用。

8.2定标原则为最低价中标。

注:所有文件需盖公章。

**9.保密要求**

9.1投标人应签订保密协议，对其因身份、职务、职业或技术关系而知悉的采购人商业秘密和党政机关保密信息应严格保守，保证不被披露或使用，包括意外或过失。

9.2投标人不得以竞争为目的、或出于私利、或为第三人谋利而擅自保存、披露、使用采购人商业秘密和党政机关保密信息；不得直接或间接地向无关人员泄露采购人的商业秘密和党政机关保密信息；不得向不承担保密义务的任何第三人披露采购人的商业秘密和党政机关保密信息。投标人在从事政府项目时，不得擅自记录、复制、拍摄、摘抄、收藏在工作中涉及的保密信息，严禁将涉及政府项目的任何资料、数据透露或以其他方式提供给项目以外的其他方或投标人内部与该项目无关的任何人员。

9.3投标人对于工作期间知悉采购人的商业秘密和党政机关保密信息（包括业务信息在内）或工作过程中接触到的政府机关文件（包括内部发文、各类通知及会议记录等）的内容，同样承担保密责任，严禁将政府机关内部会议、谈话内容泄露给无关人员；不得翻阅与工作无关的文件和资料。

9.4严禁泄露在工作中接触到的政府机关科技研究、发明、装备器材及其技术资料和政府工作信息。

9.5如涉及涉密信息设备运维，则提供服务的人员必须具备国家许可的相应资质。

**10.验收支付**

**10.1验收要求**

10.1.1完成对广东省英德监狱监管改造信息管理系统（三级）以及广东省英德监狱刑罚执行网上协同工作平台（三级）的等级保护测评，并提供符合等保2.0测评标准的最终等级保护安全测评报告。

10.1.2完成对广东省英德监狱欣档档案管理系统（二级）以及广东省英德监狱亲情电话管理系统（二级）的等级保护测评，并提供符合等保2.0测评标准的等级保护安全测评报告，协助采购方完成主管部门对系统的备案与检查后的回执证明。

10.1.3完成对财务管理系统（用友软件）、ITC对讲监听、生卫系统、狱务公开查询系统、罪犯减假暂提请资格筛查系统、内网终端管理系统、视频人脸比对、机房动环系统、英德容灾备份系统（爱数）以及科达监控平台等10个拟定一级等保信息系统进行专家评估、出具专家意见，协助采购人出具专家定级评审意见和安全整改建议。

**10.2支付条款**

10.2.1合同价按中标价签订；

10.2.2履约保证金：合同签订后五个工作日内中标人需向采购人缴纳中标金额5%的履约保证金，验收合格后1个月内无质量问题的履约保证金给予无息全额退还；中标方未完成项目，采购方不予退回履约保证金。

10.2.3本项目预算所有费用总价为40.7万元。采购方结合项目的实施进度，2024年11月30日前须完成等级保护测评，应急演练，网络安全培训以及完成至少两次中心机房巡检服务，支付项目金额的70%；完成项目验收后1个月内，中标方进行项目支付申请，采购方支付项目剩余金额30%并返还履约保证金。