**贵阳一中“五育融合”大数据平台三级等级保护测评服务项目**

**资格要求及技术参数**

1. **项目名称：**

贵阳一中网络安全等级保护测评项目

1. **投标人资格要求**
   1. 在中华人民共和国境内注册的合法经营企业，提供投标人营业执照、组织机构代码证、税务登记证（或三证合一的营业执照）；
   2. 未被列入“信用中国”网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）违法、失信记录的投标企业，对列入失信被执行人、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的，将会被拒绝参加此项目投标；（提供投标截止时间10日内查询页面截图；）
   3. 投标人须在全国网络安全等级测评与检测评估机构目录中，并具备公安部第三研究所认证发放的《网络安全等级测评与检测评估机构服务认证证书》（复印件加盖公章）；
2. **服务内容概述及要求**

**1.贵阳一中网络安全等级保护系统情况详见下表：**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 网络系统名称 | 级别 | 备注 |
| 1 | “五育融合”大数据平台 | 三级 |  |
|  |  |  |  |
| 具体系统名称以备案回执或备案证上的系统名称为准 | | | |

**2.服务期限要求：**

被测评系统满足测评条件后60工作日内完成等级保护测评工作。

**3.服务地点：**

贵阳一中校内 。

**4.服务人员要求：**

1. 派遣有经验的人员完成本项目服务工作，进入现场实施人员从事本行业工作不少于2年，具有等级保护测评中级及以上经验。
2. 投标人拟派专业的服务团队，服务团队成员不少于4人，其中项目负责人1人。
3. 为了保障测评过程中被测系统网络正常运行，项目组需要具备一定的安全保障能力，并具有网络安全应急处置机制及安全应急人员，同时根据《网络安全等级保护测评过程指南》要求，现场测评工作需要进行渗透测试，该项目需要具备专业渗透测试人员。

**5.服务技术要求：**

当前，随着大数据、物联网、云计算的快速发展，信息化建设的不断推进，国内外安全风险威胁急剧上升，愈演愈烈的网络攻击已经成为国家安全的新挑战，国家关键信息基础设施可能时刻受到来自网络攻击的威胁。网络安全的态势之严峻，迫切需要我们在网络安全领域具备更强的防护能力，我国充分认识到信息系统在各行业各层面的重要性，把信息安全上升到事关国家安全的地位。为了充分保护我国基础信息网络和重要信息系统，推出信息安全等级保护制度，并作为国家信息安全保障工作的基本制度，“等保测评”应运而生。

通过本次等级测评，可以掌握“五育融合”大数据平台的安全保护能力，排查系统安全隐患和薄弱环节、明确“五育融合”大数据平台安全建设整改的需求。并衡量“五育融合”大数据平台的安全保护管理措施和技术措施是否符合信息系统安全等级保护基本要求，是否具备了相应的安全保护能力。同时等级测评结果作为公安机关等安全监管部门进行监督、检查、指导的参照，可以更加有效的督促、检查、指导“五育融合”大数据平台的安全建设整改工作。

### 5.1.法律及相关规定：

根据《中华人民共和国计算机信息系统安全保护条例》（国务院[1994]147 号令）要求，信息系统实行等级保护制度。随后有多部法规、国家标准对信息安全进行了规定。

* 《中华人民共和国网络安全法》
* 中华人民共和国公安部，公网安〔2020〕1960号《贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见》
* 《信息安全等级保护管理办法》（公通字[2007]43号）
* 《中华人民共和国计算机信息系统安全保护条例》
* GB∕T 22239-2019 信息安全技术 网络安全等级保护基本要求
* GB∕T 22240-2020 信息安全技术 网络安全等级保护定级指南
* GB∕T 25058-2019 信息安全技术 网络安全等级保护实施指南
* 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 36627-2018 信息安全技术 网络安全等级保护测试评估技术指南
* GB∕T25070-2019 信息安全技术 网络安全等级保护安全设计技术要求
* GB17859-1999 计算机信息系统 安全保护等级划分准则
* 网络安全等级保护测评高风险判定指引（2020定稿）

### 5.2.测评内容简述：

依据《中华人民共和国网络安全法》等国家相关法律、标准要求，对以上1个三级，并出具《等级测评报告》。若首次测评后被测信息系统需要进行整改，在约定的整改期限内提供复测服务。

服务方式：现场和远程

交付成果：测评报告。

### 5.3.测评内容和方法：

1. 定级备案

协助采购人对测评范围内未定级、未备案的系统形成定级、备案相关材料，组织开展专家评审会，完成定级备案等相关服务工作。

服务时间：7\*24小时

服务方式：现场

交付成果：备案证明。

1. 测评服务范围

等级测评的现场实施过程由单元测评和整体测评两部分组成。

对应《信息安全技术网络安全等级保护基本要求》各安全控制点的测评称为单元测评，具体可分为安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理和安全运维管理10个测评任务。同时由于业务目标的不同、使用技术的不同、应用场景的不同等因素，不同的等级保护对象会以不同的形态出现，表现形式可能称之为基础信息网络、信息系统(包含采用移动互联等技术的系统)、云计算平台/系统、大数据平台/系统、物联网、工业控制系统等。为了便于实现对不同级别的和不同形态的等级保护对象的共性化和个性化保护，等级保护要求需要增加安全扩展要求：云计算安全扩展要求、移动互联安全扩展要求、物联网安全扩展要求、工业控制系统安全扩展要求。

整体测评是在单元测评的基础上，通过进一步分析信息系统安全保护功能的整体相关性，对信息系统实施的综合安全测评。

依据《信息安全技术 网络安全等级保护基本要求》，测评内容包括但不限于：安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全人员管理、安全建设管理、安全运维管理等十个层面开展测评工作。

（1）安全物理环境测评内容：

物理位置的选择、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。

（2）安全通信网络测评内容：

网络架构、通信传输、可信验证。

（3）安全区域边界测评内容：

边界防护、访问控制、入侵防范、恶意代码和垃圾邮件防范、安全审计、可信验证。

（4）安全计算环境测评内容：

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、数据保密性、数据备份恢复、剩余信息保护、个人信息保护。

（5）安全管理中心测评内容：

系统管理、审计管理、安全管理、集中管控。

（6）安全管理制度测评内容：

安全策略、管理制度、制定和发布、评审和修订。

（7）安全管理机构测评内容：

岗位设置、人员配备、授权和审批、沟通和合作、审核和检查。

（8）安全管理人员测评内容：

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。

（9）安全建设管理测评内容：

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。

1. 安全运维管理测评内容：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。

### 5.4.测评工作过程：

1. 测评准备服务

* 信息收集、工具准备、工具接入作业指导书编制、编制测评计划书、调查问卷收集等；
* 资产调研：对信息系统运营使用单位所有网络设备、安全设备、服务器、存储阵列、机房设施等进行资产调研。
* 管理现状调研：对信息系统运营使用单位的管理制度进行系统调研。
* 技术现状调研：对信息系统运营使用单位的网络拓扑、业务数据流拓扑、安全防护现状等进行系统调研。
* 应用系统调研：对信息系统运营使用单位的业务细信息系统进行系统调研。本预算以单个信息系统为参考进行估算。

1. 测评方案编制

* 测评方案编制、测评对象确认、测评指标确认、测评内容确认、整体测评方法确认、风险分析方法确认、开发指导书、编制结果记录表等；

1. 现场测评

* 现场根据测评指导书对运营使用单位的信息系统进行现场测评并进行结果证据收集确认；通过访谈、检查、测试、分析等方法。
* 漏洞扫描及验证：通过漏扫工具接入测试验证，检查网络层面漏洞、主机层面漏洞等，针对漏扫结果进行验证威胁性，验证其安全防御体系的有效性。
* 等保渗透测试：依据等保标准，对应用安全的各项指标进行渗透测试及验证漏洞扫描工具发现的漏洞威胁情况，包括信息收集、渗透测试、报告编制。

1. 报告编制与评审

* 依据单元测评结果汇总进行整体测评分析、风险分析、结果汇总、结论形成、结果判定、整改建议等