用户需求书

1、项目名称

项目名称：电教馆系统等级测评

2、项目背景

海南省电化教育馆承担省教育厅的信息化和网络安全工作，随着系统运行时间逐渐增多，系统安全存在威胁，需加强安全管理，互联网安全监管等; 且随着新技术新应用的发展，网络攻击手段越来越多样，海南省电化教育馆相关安全配套保障设施处于较为薄弱现状。

依据《信息安全等级保护管理办法》(公通字[2007]43 号)规定，公安部和海南省公安厅网络职能部门建议和要求，第二级信息系统应当每两年至少进行一次等级测评，第三级信息系统应当每年至少进行一次等级测评。我单位将委托符合国家规定的测评机构依据国家《网络安全法》的法规要求和网络安全等级保护 2.0 的相关要求，对我单位重要信息系统进行等级测评，出具海南省公安厅认可的《网络安全等级保护测评报告》; 并在完成网络安全等级保护测评工作后，依照网络安全等级保护测评工作中所发现的安全问题，通过采用安全巡检、安全培训等服务作为网络安全等级保护测评工作的后续配套服务，进一步贯彻落实国家网络安全等级保护制度，深入推进我单位的网络安全等级保护工作，提高我单位信息系统的安全保障能力和防护水平，更好地提升本单位网络安全管理的整体水平。

通过本项目的建设：

- 掌握等级保护对象的安全状况、等级保护对象的安全隐患和薄弱环节;
- 衡量等级保护对象的安全保护管理措施和技术防护措施是否符合相应等级保护基本要求，是否具备了相应等级的安全保护能力;

- 明确等级保护对象的安全建设整改需求，避免重复投资、重复建设，避免信息安全事件发生造成的经济损失；
- 落实国家网络安全等级保护 2.0 相关政策与标准要求。
- 通过持续化的检查，及时发现等级保护对象存在的安全漏洞、安全隐患以及可能发生的安全事件，可以快速地进行修补改进，防患于未然；
- 提前消除安全事件带来的影响，降低安全事件带来的损失和风险；

3、项目（交付期）和地点

项目（交付期）：签订合同后 60 个工作日内交付测评报告。

地点：用户指定。

4、项目需求

4.1 项目建设内容

序号	信息系统名称	安全保护等级	备案编号
1	海南省教育厅网站	第三级（S3A3G3）	4600043009-18015
2	海南中等职业教育网	第三级（S3A3G3）	46000043009-16004
3	海南省高考综合改革信息化平台	第三级（S3A3G3）	46000043004-17012
4	全国学生资助管理信息系统（海南）	第三级（S3A3G3）	46000043009-17006
5	全国中等职业学校学生管理信息系统（海南）	第三级（S3A3G3）	46000043009-17007
6	全国教师管理信息系统（海南）	第三级（S3A3G3）	46000043009-17008

7	**海南省校舍安全管理信息系统**	第三级（S3A3G3）	46000043004-16008
8	**全国中小学学籍管理系统（海南）**	第三级（S3A3G3）	46000043009-18011
9	**国家学前管理信息系统（海南）**	第三级（S3A3G3）	46000043004-18011
10	**应用服务支撑服务平台**	第三级（S3A3G3）	46000043009-16003
11	**教育基础数据库管理与服务系统**	第三级（S3A3G3）	46000043009-16001

4.2 项目依据

4.2.1 政策法规

1. 《中华人民共和国网络安全法》
2. 《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；
3. 《互联网安全保护技术措施规定》（公安部令第 82 号）；
4. 《关于加强信息安全保障工作的意见》（中办发[2003]27 号）
5. 《信息安全等级保护管理办法》（公通字[2007]43 号）；
6. 《中华人民共和国政府信息公开条例》；
7. 《国务院办公厅关于进一步加强政府网站管理工作通知》（国办函【2011】40 号）；

8. 《关于进一步加强国家电子政务网络建设和应用工作的通知》（发改高技【2012】1986 号）；

9. 《关于进一步加强信息安全等级保护工作的通知》（琼等保办【2013】2 号）；

10. 《海南省信息化条例》；

11. 《国家网络安全检查操作指南》（中央网络安全和信息化领导小组办公室 2014 年 6 月）

12. 《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 号文）

13. 《关于印发<海南省党政机关、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》（琼公通[2015]371 号）

公安部、国家保密局、国家密码管理局和国务院信息化工作办公室于 2007 年 6 月联合发布了《信息安全等级保护管理办法》，标志着信息安全等级保护工作在全国范围内的全面推进。信息安全等级保护是国家信息安全保障工作的基本制度、基本策略、基本方法，是国家层面制定的信息安全工作标准。

2014 年 6 月中央网络安全和信息化领导小组办公室下发的《国家网络安全检查操作指南》中明确指出了相应的网络安全检查内容：安全检查工作通常包括检查工作部署、信息系统基本情况梳理、日常工作情况检查、年度重点工作检查、安全技术检测、检查总结整改等六个环节。

2017 年 6 月 1 日起施行的《中华人民共和国网络安全法》是国家在互联网领域及网络安全方面的基础法律，也是自党的十八大以来的又一部重要法律。分别从网络空间主权维护及治理，国家网络安全等级保护制度，关键信息基础设施保护，网络运营者、网络产品和服务提供者义务，保障网络信息安全、个人信息

保护，关键信息基础设施重要数据跨境传输，监测预警与应急处置等方面做出了详细要求及说明。

4.2.2 标准

14. 《信息系统安全等级保护实施指南》GB/T 25058-2010；

15. 《信息安全技术网络安全等级保护基本要求》GB/T 22239-2019；

16. 《信息安全技术信息系统安全通用技术要求》GB/T 20271-2006；

17. 《网络安全等级保护测评要求》GB/T 28448-2019；

18. 《网络安全等级保护测评过程指南》GB/T 28449-2018；

19. 《信息系统安全管理要求》GB/T 20269-2006

20. 《信息安全风险评估规范》GB/T 20984-2007

21. 《信息安全事件管理指南》GB/Z 20985-2007

22. 《信息安全事件分类分级指南》GB/Z 20986-2007

4.3 项目服务内容及要求

4.3.1 网络安全等级保护测评服务

投标人依据国家网络安全等级保护管理规定，按照有关管理规范和技术标准在 60 个工作日内对我单位海南省教育厅网站（第三级 S3A3G3)、海南省高考综合改革信息化平台（第三级 S3A3G3)等 12 个系统的进行等级测评，在完成测评后，针对信息系统测评的情况，出具相应的测评报告，并提出具有针对性的整改建议。

4.4.1 测评内容

1、对招标文件“用户需求书”中提供项目范围和服务内容进行确认、分析和梳理，提出详细的等级保护测评方案。

2、对信息系统的整体保护状况和信息系统组件，逐一进行安全等级保护测评，测评的内容包括但不限于以下内容：

（1）安全技术测评：包括安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心等五个方面的安全测评；

（2）安全管理测评：安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理等五个方面的安全测评。

3、完成测评工作后，出具符合海南省公安厅要求的网络安全等级保护测评报告，并提出具有针对性的整改建议。

4.4.2 测评实施

投标人在测评过程中，需按照《网络安全等级保护测评过程指南》等标准开展测评实施工作，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、报告编制活动。测评双方之间的沟通与洽谈应贯穿整个等级测评过程。

测评准备活动

测评准备工作包括工作启动、信息收集和分析、工具和表单准备。

详细要求见下表：

项目内容	工作内容	成果输出
工作启动	1.组建测评项目组	向用户提交《项目计划书》《提供资料清单》
	2.编制《项目计划书》	
	3.确定测评委托单位应提供的资料	
信息收集	1.整理调查表单	《等级保护对象调查表》

分析	2.发放调查表单给测评委托单位	
	3.协助测评委托单位填写调查表	
	4.收回调查结果	
	5.分析调查结查	
工具和表单准备	1.调试测评工具	确定测评工具(测评工具清单)、《现场测评授权书》、《测评结果记录表》、《文档交接单》
	2.模拟被测定级对象搭建测评环境	
	3.模拟测评	
	4.准备打印表单	

方案编制活动

方案编制活动包括测评对象确定、测评指标确定、测评内容确定、工具测试方法确定、测评指导书开发及测评方案编制等六项主要任务。

详细要求见下表：

工作内容	工作详细任务	输出成果
测评对象确认	识别并描述被测定级对象等级 识别并描述被测定级对象的整体结构 识别并描述被测定级对象的边界 识别并描述被测定级对象的网络区域 识别并描述被测定级对象的重要节点和业务应用 识别并描述被测定级对象的主要设备 确定测评对象	《测评方案》的测评对象部分
测评指标确定	识别被测定级对象业务信息和系统服务安全保护等级	《测评方案》的测评指标部分
	选择对应等级的SAG三类安全要求作为测评指标	
	根据被测定级对象确定不适用测评指标、特殊	

	测评指标	
	确定基本测评指标和特殊测评指标进行描述,并分析给出指标不适用的原因	
测试内容确定	识别每个测评对象的测评指标	《测评方案》的测评实施部分
	识别每个测评对象对应的每个测试指标的测试方法	
工具测试方法确定	确定工具测试的测评对象 选择测试路径 确定测试工具的接入点 **本次项目测评需要使用到如下工具：** 漏洞扫描工具； Windows 主机安全配置检查工具； Linux 主机配置检查工具； 网络及安全设备配置检查工具； 病毒检查工具； 木马检查工具； 网站恶意代码检查工具； 在线检查工具（网站安全检查工具）； 终端安全检查工具； 口令破解工具； 渗透测试工具； SQL 注入验证检查工具； 在线数据库安全检查工具；	《测评方案》的 的工具测试方法及内容部分
测评指导书开发	描述单个测评对象，内容包含名称、位置信息、用途、管理人员等信息	测评指导书、测评结果记录表格
	确定测评活动,包括测评项、测评方法、操作	

	步骤和预期结果等四部分	
	设计单项测评、整体测评表述形式	
	根据测评指导书,形成测评结果记录表格	
测评方案编制	描述测评项目基本情况和工作依据	向用户提交《测评方案》、《风险规避实施方案》
	描述测评协议书和被测定级对象情况,估算现场测评工作量	
	描述测评项目组成员安排,编制工作安排情况	
	汇总上述内容及方案编制活动的其他任务获取的内容形成测评方案文稿	
	评审和提交测评方案	
	根据测评方案制定风险规避实施方案	

现场测评活动

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，然后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。

详细要求见下表：

工作内容	工作详细任务	输出
现场测评准备	现场测评授权书签署	会议记录,测评方案,现场测评工作计划和风险告知书,现场测评授权书
	召开现场测评启动会	
	双方确认测评方案	

	双方确认配合人员、环境等资源	
	确认等级保护对象已经备份	
现场测评和结构记录	依据测评指导书实施测评	《测评指导书》 《文档交接/规划记录单》（已更新） 访谈结果：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、安全运维管理安全测评的测评结果记录或录音 ； 文档审查结果： 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、安全运维管理测评的测评结果记录； 配置核查结果： 安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心测评结果记录表格 工具测试结果： 安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心测评结果记录，工具测试完成后的电子输出记录，备份的测试结果文件 实地察看结果： 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、安全运维管理测
	记录测评获取的证据、资料等信息	
	汇总测评记录，如果需要，实施补充测评	
结果确认和资料归还	召开现场测评结束会	
	测评委托单位确认测评过程中获取的证据和资料的正确性，并签字认可	
	测评人员归还借阅的各种资料	

		评结果记录 测评结果确认： 现场核查中发现的问题汇总、证据和证据源记录、被测单位的书面认可文件

报告分析及编制活动

在现场测评工作结束后，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项测评结果后,还需进行单元测评结果判定、整体测评、系统安全保障评估,经过整体测评后,有的单项测评结果可能会有所变化,需进一步修订单项测评结果,而后针对安全问题进行风险评估,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、系统安全保障评估、安全问题风险评估、等级测评结论形成及测评报告编制七项主要任务。。

详细要求见下表：

工作内容	工作详细任务	工作依据（模版）
单项测评结果判定	分析测评项所对抗威胁的存在情况	测评报告的单项测评结果记录部分
	分析单个测评项是否有多方面的要求内容，依据“优势证据”法选择优势证据，并将优势证据与预期测评结果相比较	
	综合判定单个测评项的测评结果	
单元测评结果判定	汇总每个测评对象在每个测评单元的单项测评结果	测评报告的单元测评小结部分
	判定每个测评对象的单元测评结果	
整体测评	分析不符合和部分符合的测评项与其	测评报告的整体测评

	他测评项（包括单元内、层面间、区域间）之间的关联关系及对结果的影响情况	部分
	分析被测定级对象整体结构的安全性对结果的影响情况	
系统安全保障评估	整体测评后的单项测评结果汇总	测评报告的系统安全保障评估部分
	分析整体测评结果，分析被测定级对象的有效保护措施和存在的主要安全问题	
	评估系统安全保障情况	
安全问题风险分析	整体测评后的单项测评结果再次汇总	测评报告的安全风险分析部分
	分析部分符合项或不符合项所产生的安全问题被威胁利用的可能性	
	分析威胁利用安全问题后造成的影响程度	
	为被测定级对象面临的风险进行赋值	
	评价风险分析结果	
等级测评结论形成	统计再次汇总后的单项测评结果为部分符合和不符合项的项数	测评报告的等级测评结论部分
	形成等级测评结论	
测评报告编制	概述测评项目情况	向用户提交《网络安全等级测评报告》
	描述被测定级对象情况	
	描述测评范围和方法	
	描述整体测评情况	
	汇总测评结果	
	描述风险情况	
	给出等级测评结论和整改建议	

4.3.2 网络安全巡检服务

投标人自合同生效之日起一年内对我单位的系统提供 4 次的安全巡检工作，具体的工作内容包括网络安全巡检、主机安全巡检、数据备份与恢复巡检、网络防病毒巡检、物理机房环境巡检和安全管理制度落实检查，并包含对相关设备的维保信息和授权进行检查，提交相应的《安全巡检报告》。

安全巡检服务是根据《信息安全等级保护管理办法》（公通字[2007]43 号）、《信息安全技术网络安全等级保护基本要求》GB/T 22239-2019；，结合实际安全需求，通过定期开展信息系统安全巡检服务，及时发现存在的安全问题和薄弱环节，分析面临的安全威胁和风险，对发现的安全隐患提供改善建议，协助指导本单位落实防范对策和改进措施，并配合协调相关系统开发商和安全服务商及时对发现的问题进行整改，以加强网络与信息系统安全管理和技术防护，促进安全防护能力和水平提升，预防和减少重大信息安全事件的发生。

4.3.3 网络安全培训服务

1、投标方针对本项目为招标人提供1次的现场培训。

2、投标方应提供详细的培训方案（包括培训内容、时间、人数等）。

3、培训的内容包括但不限于：信息安全意识教育；信息安全事件动态及解读；信息安全基本防护技能；《网络安全法》和网络安全等级保护 2.0 要求解读。

服务成果：

通过信息安全等级保护培训服务，提高人员安全意识。

服务收益：

- 信息安全意识宣讲，提升全员信息安全意识；；
- 了解信息安全态势，及时掌握信息安全变化方向
- 掌握信息安全基本防护技巧，落实日常信息安全防护工作；

4.4 项目的实施要求

项目实施过程中，投标方应遵循国家标准、行业标准。

(1)项目实施要求

在项目实施中投标方必须做到：

1.提供项目实施组织架构；

2.提供详细的项目实施方案和计划进度说明书；

3.中标方项目经理在项目期间每周至少来招标方现场 1 次进行工作汇报，且电话要保持 7*24 小时通畅；

4.对于招标方的电话咨询和常规服务请求在 30 分钟内予以答复，紧急服务请求在 2 小时内到达招标方现场；

5.项目实施完成后提供可靠的后期维护工作；

6.严格按照双方确定的计划进度保质保量完成工作；

(2)实施团队要求

为保障项目服务质量和售后响应速度，投标人应承诺在本项目服务期内在本地部署不少于 10 人的测评师团队，投标人须在投标文件中提供完整的实施团队名单及职责分工，所有人员必须属于投标单位在册员工（以社保缴纳证明为认定依据）。实施测评工作的技术人员必须具备公安部信息安全等级保护评估中心颁发的《信息安全等级测评师证书》。实施团队名单中所列人员的社保缴纳证明和《信息安全等级测评师证书》复印件需在投标文件中提供，并加盖公章，同时提供原件核对。

(3)项目验收

投标方必须书面通知招标方所完成的工作和准备进行验收的项目种类及验收开始时间，此通知书需经招标方认定后方可执行。

(4)验收组织

成立由招标方、中标方以及其他有关人员组成的验收小组，负责对项目进行全面的验收。

(5)验收标准

- 完成每年的网络安全等级保护测评工作；
- 按系统提交《网络安全等级保护测评报告》；
- 提交项目实施阶段所有的过程文档。

4.5 工作完成后要求

1、要向海南省电化教育馆提供等保测评总结测评报告资料一份

2、根据测评报告出据整改建议，整改意见建议一式三份