**采购招标文件**

**项目名称：海南广播电视大学信息系统安全等级保护测评服务**

**采购编号：琼电大信招-2020-0501**

**2020年5月**

文件目录

一、邀请函

二、项目需求

三、评分表

四、投标文件格式

第一部分 邀请函

根据《中华人民共和国政府采购法》的规定,现就海南广播电视大学信息系统安全等级保护测评服务项目进行询价采购，邀请符合资质条件单位前来报价投标。投标人必须对包内的所有内容进行报价，具体的服务要求详见项目需求。

一、项目名称：海南广播电视大学信息系统安全等级保护测评服务；

二、采购编号：琼电大信招-2020-0501；

三、采购方式：校内公开招标；

四、供应商资格要求：（投标人必须具备以下条件并提交相关证明资料）：

1、在中华人民共和国境内注册、具有独立承担民事责任能力的法人（提供工商营业执照副本、组织机构代码、税务登记证复印件或三证合一营业执照）；

2、具有较强的本地化服务能力，非本地投标人应在海南有分公司或办事处(需提供工商或商务部门注册资料，注册满二年)作为常驻服务和技术支持机构，配有较强的专业技术队伍，对故障响应能在4小时内到现场；

3、必须提供参加采购活动前三年内，在经营活动中没有重大违法记录的声明函（加盖公章）；

4、本项目不得转包、分包，不接受联合体投标。

五、联系人：

地址：海南省海口市美兰区海甸岛二西路20号海南广播电视大学信息办；联系人：陈龙，电话：66212521

六、投标截止时间：2020年5月 日17：30时（逾期或不符合规定的投标文件恕不接受）

海南广播电视大学

2020 年 5 月 日

**第二部分 项目需求**

项目A包：“钉钉”管理系统安全等保测评服务详见附件1；

项目B包：海南省干部在线学习中心安全等保测评服务 (2020)详见附件2

**第三部分 评分表**

|  |  |  |
| --- | --- | --- |
| 序号 | 评分细则 | 分值 |
| 1 | 具有省公安厅网络安全等级保护测评机构推荐证书，得20分，无得0分。 | 20 |
| 2 | 投标方案对需求响应情况，优：9-10分，良：7-8分，中：6，差：5分以下。（两个测评项目分别评分） | 10 |
| 3 | 拥有2017年以来全国网络安全等级保护测评机构先进单位证书情况，以最近时间得奖，得分高的原则评分，3个得10分，2个得8-9分，1个得6-4分（其中2019年得奖6分，2018年得奖5分，2017年得奖4分），无得0分。 | 10 |
| 4 | 投标者的测评合同中拥有最高等级测评为5级得25分，最高等级测评为4级得20分，最高等级测评为3级得16分，最高等级测评为2级得13分。（得分相同时，逐级对比其合同个数，可以作为选定中标者的主要参考） | 25 |
| 5 | 满足招标文件要求且价格最低的投标价为基准价，其价格分为满分。其他投标人的价格分统一按照下列公式计算：价格分=（基准价／最终报价）×30。 | 30 |
| 6 | 按照等级保护2.0标准测评项目的数量大于等于5个得5分；小于5个的，按项目个数评分，一个一分。 | 5 |
|  | 合计 | 100分 |
| 注：按照评分标准，如果两家或以上得分相同，由开标人员可以参考第4条的要求，讨论决定并提出建议中标者。 | | |

**第四部分 投标文件格式**

（正本/副本）

海南广播电视大学信息系统安全等级保护测评服务

投标文件

投标人：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_（盖单位章）

法定代表人或其委托代理人：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_（签字）

\_\_\_\_\_\_\_\_\_\_\_\_年\_\_\_\_\_\_月\_\_\_\_\_日

**目 录**

一、投标报价函（格式）

二、法定代表人身份证明（格式）

三、授权委托书（格式）

四、案例情况介绍

五、投标人诚信承诺书（格式）

六、公司资质及荣誉证书

七、技术方案

## 一、投标报价函

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_（招标人名称）:

1、根据已收到海南广播电视大学信息系统安全等级保护测评服务招标文件，我单位经研究招标文件中的所有内容后，我方就上述服务内容进行投标报价（两个系统分开报价，投标格式请勿修改）。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 系统名称 | 级别 | 服务内容 | 工期 | 报价 |
| “钉钉”管理系统安全等保测评服务 | 二级 |  |  |  |

投标单位： 日期

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 系统名称 | 级别 | 服务内容 | 工期 | 报价 |
| 海南省干部在线学习中心安全等保测评服务 (2020) | 二级 |  |  |  |

投标单位： 日期

## 二、法定代表人身份证明

投标人名称：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

单位性质：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

地址：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

成立时间： 年 月 日

经营期限：

姓名： 性别： 年龄： 职务：\_\_\_\_\_\_\_\_\_\_\_

系 （投标人名称）的法定代表人。

特此证明。

附：法定代表人身份证复印件

投标人：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_（盖单位章）

\_\_\_\_\_\_\_\_\_\_年\_\_\_\_月\_\_\_\_日

## 三、授权委托书

本人\_\_\_\_\_\_\_\_（姓名）系 （投标人名称）的法定代表人，现委托\_\_\_\_\_\_（姓名）为我方代理人。代理人根据授权，以我方名义签署、澄清、说明、补正、递交、撤回、修改 （标段名称） 投标文件、签订合同和处理有关事宜，其法律后果由我方承担。

委托期限：

代理人无转委托权。

附：代理人身份证复印件

投标人：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_（盖单位章）

法定代表人：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_（签字或盖章）

身份证号码：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

委托代理人：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_（签字或盖章）

身份证号码：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_年\_\_\_\_月\_\_\_\_日

## 

**四、案例情况介绍**

提供近3年从事信息系统安全等级保护测评服务项目案例清单，并提供相应安全等级的案例合同扫描件1份（每个安全等级合同扫描件不超过1份）。

|  |  |  |
| --- | --- | --- |
| 客户名称 | 合同金额 | 服务内容 |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**五、投标人诚信承诺书**

我单位在参加**海南广播电视大学信息系统安全等级保护测评服务**的投标活动中，郑重承诺如下：

1、我方在此声明，本次招标投标活动中申报的所有资料都是真实、准确完整的，如发现提供虚假资料，或与事实不符而导致投标无效，甚至造成任何法律和经济责任，完全由我方负责；

2、我方在本次投标活动中绝无资质挂靠、串标、围标情形，若经贵方查出，立即取消我方投标资格并承担相应的法律责任；

3、我方在以往的招标投标活动中，无重大违法、违规的不良记录；我方人员没有重大违法记录；

4、我方一旦中标，将严格按照投标文件中所承诺的报价、质量、工期、措施、项目负责人等内容组织实施；

5、我方一旦中标，将按规定及时与建设单位签订合同。

投标人名称： （盖公章）

法定代表人（或授权代理人）： （签字或盖章）

日 期：2020年 月 日

**六、公司资质及荣誉证书**

**七、技术方案**

**附件1**

“钉钉”管理系统安全等保测评服务要求

一、项目概述

通过委托专业信息安全等级测评服务机构，根据《信息安全技术网络安全等级保护基本要求》等相关文件及标准要求，对海南省脱贫致富电视夜校“钉钉”管理系统进行信息安全等级保护二级测评，并出具《信息系统安全等级保护测评报告》及整改指导、信息安全培训等服务。

二、服务要求

**（一）服务目标**

通过信息安全等级保护测评服务，对钉钉管理系统开展符合性测评，衡量该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。

**（二）信息系统安全等级保护符合性测评**

按照公安部制订的信息系统安全等级测评报告格式编制等级测评报告，报告中必须明确相应信息系统是否满足等级保护要求。

**（三）整改方案编制**

测评机构需根据测评结果，应针对性的提出整改建议方案。整改建议方案应具有可操作性，符合实际情况，且能够切实解决问题。

整改建议方案应明确设计依据、整改内容、整改方案、能够解决的问题、投资概算以及风险评估。

在整改实施过程中，测评机构应全力支持，负责技术把关、整改验收以及其他咨询工作。

**（四）交付成果和报告**

中标方需在45天内交付成果和报告，提交测评报告及安全整改方案，包括：

《海南省脱贫致富电视夜校钉钉管理系统等级保护测评报告》

《海南省脱贫致富电视夜校钉钉管理系统等级保护安全整改方案》

测评过程材料，包括调研表、技术测评记录等。

**（五）服务验收标准**

服务通过验收须满足以下所有条件：

1. 完成信息系统测评并出具《测评报告》；
2. 针对性的制定整改方案，并出具《整改建议方案》；
3. 提交调研表、技术测评记录等服务过程材料；
4. 符合省级以上公安部门提出的信息安全等级保护测评相关要求。

# 附件2 海南省干部在线学习中心安全等保测评服务 (2020)项目需求

## 一、项目名称

海南省干部在线学习中心安全等保测评服务 (2020)

## 二、项目背景

依据《中华人民共和国计算机信息系统安全保护条例》（中华人民共和国国务院令第147号）、《国家信息化领导小组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）、《中华人民共和国网络安全法》等法律法规和相关文件要求，海南广播电视大学将于2020年开展信息安全等级保护测评工作。

## 三、项目内容

通过委托专业信息安全等级测评服务机构，根据《信息系统安全等级保护实施指南》等相关文件及标准要求，对海南省干部在线学习中心进行二级等保测评服务，并出具《信息系统安全等级保护测评报告》及整改指导、信息安全培训等服务。

## 四、服务实施

**（一）服务目标**

通过信息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。

**（二）测评依据**

《信息系统安全等级保护基本要求》

《信息系统安全等级保护测评要求》

《信息系统安全等级保护测评过程指南》

**（三）实施团队要求**

提供完整的测评实施团队名单及职责分工，所有人员必须属于测评机构在册员工（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》。

**（四）服务内容**

服务期内，测评机构须提供以下服务。

**1、等级保护培训咨询服务**

1）等级保护政策/标准咨询

随着国家信息安全等级保护的推进工作，信息安全等级保护政策、法律法规和标准体系也会相应的发布和更新，应针对本项目设立信息安全等级保护咨询平台，明确较为固定的咨询服务人员，并根据咨询要求提供正式的答复资料和文档。咨询内容包括但不限于信息安全等级保护国内外发展动态、等级保护政策、法律法规和标准体系咨询服务。

2）信息系统等级变更咨询

在信息系统出现等级变更时，协助用户单位对信息系统进行分析，明确信息系统边界和定级对象，对信息系统的子系统进行划分，确定信息系统以及子系统的安全等级。

3）等级保护建设整改咨询

按照信息系统安全总体方案要求，结合信息系统安全建设项目计划，根据信息安全等级保护相关标准和规定，对用户单位等级保护建设整改工作提供全面的安全方案的详细设计咨询，结合用户单位的实际情况，协助用户单位进行分布或分期地落实安全技术与管理措施，并根据预期实现的安全目标，全程提供在建安全设备和系统的测试、验收工作等咨询服务。

4）信息系统安全检查咨询

在用户单位开展信息系统安全检查时，全程提供咨询服务，包括检查范围、检查方法、检查结果分析以及整改措施制定等。

5）等级保护测评咨询

测评过程中，协助用户单位参照《信息系统安全等级保护测评要求》中评估内容和方法，对测评过程中所涉及到的评估项及测评过程中所编制相关表格、填写项提供全程咨询服务，确保测评工作的顺利开展。

**2、等级保护测评服务**

依据《信息系统安全等级保护基本要求》，对用户单位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《信息系统安全等级保护测评报告》，并提出具有针对性的整改建议。

1）测评内容

（1）对本单位已备案信息系统进行摸底、分析和梳理，提出详细的等保测评方案。

（2）逐一对信息系统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：包括物理安全、网络安全、主机系统安全、应用安全和数据备份及恢复等五个方面的安全测评；

② 安全管理测评：安全管理机构、安全管理制度、人员安全管理、系统建设管理和系统运维管理等五个方面的安全测评。

（3）完成测评工作后，提出整改建议；最后出具符合公安部门要求的信息系统安全保护等级测评报告，并在后期整改实施过程中提供全程咨询服务。

2）测评实施

信息安全测评项目过程需按照《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应贯穿整个等级测评过程。

（1）测评准备活动

测评准备工作包括编制项目启动、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 |
| 项目启动 | 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.确定用户单位应提供的资料 |
| 信息收集分析 | 定级报告及整改方案分析 | 《系统基本情况分析报告》 |
| 1.整理调查表单 |
| 2.发放调查表单给用户单位 |
| 3.协助用户单位填写调查表 |
| 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.模拟被测系统搭建测评环境 |
| 3.模拟测评 |
| 4.准备打印表单 |

（2）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、测试工具接入点确定、测评内容确定、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 |
| 一、测评对象确认 | 识别被测系统等级  识别被测系统的整体结构  识别被测系统的边界  识别被测系统的网络区域  识别被测系统的重要节点和业务应用  确定测评对象 | 《测评方案》的测评对象部分 |
| 二、测评指标确定 | 识别被测系统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ASG三类安全要求作为测评指标 |
| 就高原则调整多个定级对象共用的某些物理安全或管理安全测评指标 |
| 三、工具测试点确定 | 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 | 《测评方案》的测试工具接入点部分 |
| 四、测试内容确定 | 识别每个测评对象的测评指标 | 《测评方案》的单项测评实施和系统测评实施部分 |
| 识别每个测评对象对应的每个测试指标的测试方法 |
| 五、测评指导书开发 | 从已有的测评指导书中选择与测评对象对应的手册 | 《测评方案》的测评实施手册部分 |
| 针对没有现成测评指导书的测评对象，开发新的测评指导书 |
| 六、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》 |
| 描述被测系统的整体结构、边界和网络区域 |
| 描述被测系统的重要节点和业务应用 |
| 描述测评指标 |
| 描述测评对象 |
| 描述测评内容和方法 |

（3）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 |
| 1.现场测评准备 | 现场测评授权书签署 | 会议记录、确认的授权委托书、更新后的测评计划和测评方案 |
| 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 |
| 确认信息系统已经备份 |
| 测评方案、结构记录表格等资料更新 |
| 2.现场测评和结构记录 | 依据测评指导书实施测评 | 访谈结果：技术安全和管理安全测评的测评结果记录或录音 文档审查结果： 管理安全测评的测评结果记录 配置检查结果： 技术安全测评的网络、主机、应用测评结果记录表格 工具测试结果： 技术安全测评的网络、主机、应用测评结果记录，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： 技术安全测评的物理安全和管理安全测评结果记录 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 |
| 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 |
| 3.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 |

（4）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。详细要求见下表：

|  |  |  |
| --- | --- | --- |
| 工作内容 | 工作详细任务 | 工作依据（模版) |
| 1.单项测评结果判定 | 分析测评项所对抗威胁的存在情况 | 等级测评报告的单项测评结果部分 |
| 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 |
| 2.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 | 等级测评报告的单项测评结果汇总分析部分 |
| 判定每个测评对象的单元测评结果 |
| 3.整体测评 | 分析不符合和部分符合的测评项与其他测评项（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 | 等级测评报告的系统整体测评分析部分 |
| 分析被测系统整体结构的安全性对结果的影响情况 |
| 4.风险分析 | 整体测评后的单项测评结果再次汇总 | 等级测评报告的风险分析部分 |
| 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 |
| 为被测系统面临的风险进行赋值 |
| 评价风险分析结果 |
| 5.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 | 等级测评报告的等级测评结论部分 |
| 形成等级测评结论 |
| 6.测评报告编制 | 概述测评项目情况 | 等级测评报告 提交用户 |
| 描述被测系统情况 |
| 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 |

**3、制定内部安全管理制度和操作规程**

以建立健全信息安全管理体系为目的，从用户信息安全管理的现状入手，对国际和国内信息安全标准的情况进行了梳理，在理解信息安全管理模型的基础上，提供相应的安全管理制度模板，完成安全管理制度编，确定网络安全负责人，落实网络安全保护责任。

**（五）服务要求**

**1、信息系统安全等级保护符合性测评**

按照公安部制订的信息系统安全等级测评报告格式编制等级测评报告，报告中必须明确相应信息系统是否满足等级保护要求。

**2、整改方案编制**

根据测评结果，应针对性的提出整改建议方案。整改建议方案应具有可操作性，符合用户单位实际情况，且能够切实解决问题。

整改建议方案应明确设计依据、整改内容、整改方案、能够解决的问题、投资概算以及风险评估。

在整改实施过程中，应全力支持，负责技术把关、整改验收以及其他咨询工作。

**3、交付成果和报告**

（1）《信息系统安全等级保护测评报告》

（2）《安全管理制度》

（3）《整改建议方案》

（4）测评过程材料，包括调研表、技术测评记录、会议纪要等。

**4、服务验收标准**

服务通过验收须满足以下所有条件：

（1）完成信息系统测评并出具《测评报告》

（2）完成安全管理制度编制/修订并出具《安全管理制度》

（3）针对性的制定整改方案，并出具《整改建议方案》

（4）提交调研表、技术测评记录、会议纪要等服务过程材料

## 四、售后服务

提供详细的保修期内技术支持和服务方案，技术支持和服务方案包括（但不限于）：

（1）如在测评中出现不符合项，提供相应的整改建议及相关方案。对于测评中发现的主机和网络设备漏洞，应提供项目验收后一年的跟踪服务（验收通过之日起计算）。

（2）提供一年7×24小时技术支持和服务，8小时内实质性响应，对重大问题提供现场技术咨询支持，24小时内到达指定现场。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、问题解决中使用的方法及造成的损失等情况。