

竞争性磋商公告

项目概况

成都体育学院 2021 年 SSL 证书服务、网络安全等级保护测评服务、网站漏扫服务采购项目的潜在供应商应在成都市高新区天府大道 1700 号新世纪环球中心 E3 门栋 6 楼 2-1-611-615 四川中意招标有限公司获取采购文件，并于 2021 年 6 月 4 日 10 点 00 分（北京时间）前提交响应文件。

一、项目基本情况

项目编号：ZY20210358QT-C

备案编号：

项目名称：成都体育学院 2021 年 SSL 证书服务、网络安全等级保护测评服务、网站漏扫服务采购项目

采购方式：竞争性谈判 竞争性磋商 询价

包数：本项目共计 3 包

预算金额：41.5 万元，其中第一包：1 万元；第二包：34 万元；第三包：6.5 万元。

最高限价（如有）：

采购需求：详见附件

合同履行期限：第一包：服务时间：2021 年 10 月 12 日-2022 年

10月11日。 第二包：服务时间：本项目需要在合同签订后90个工作日内完成安全等级测评服务及等保备案申报工作。 第三包：服务时间：1年（2021年12月15日-2022年12月14日）。

本项目（否）接受联合体。

二、申请人的资格要求：

1. 满足《中华人民共和国政府采购法》第二十二条规定；
2. 落实政府采购政策需满足的资格要求：无；
3. 本项目的特定资格要求：无。

三、获取采购文件

时间：2021年5月25日至2021年5月31日（磋商文件的发售期限自开始之日起不得少于5个工作日），每天上午9:00至12:00，下午14:00至17:00（北京时间，法定节假日除外）

地点：成都市高新区天府大道1700号新世纪环球中心E3门栋6楼2-1-611-615 四川中意招标有限公司

方式：请供应商通过以下流程进行磋商文件购买：

3、请供应商通过本单位网站（www.sczyzb.net）进行注册报名；具体操作流程详见该网站的“使用手册”。报名询问电话：028-87050033-0，网站技术电话：18628172742。

售价：人民币400元/份（磋商文件售后不退，磋商资格不能转让）。

四、响应文件提交

截止时间：2021年6月4日10点00分（北京时间）（从磋商文件开始发出之日起至供应商提交首次响应文件截止之日止不得少于10日；从谈判文件开始发出之日起至供应商提交首次响应文件截止之日止不得少于3个工作日；从询价通知书开始发出之日起至供应商提交响应文件截止之日止不得少于3个工作日）

地点：成都市高新区天府大道1700号新世纪环球中心E3门栋6楼2-1-611-615四川中意招标有限公司本项目开标室。

五、开启（竞争性磋商方式必须填写）

时间：2021年6月4日10点15分（北京时间）

地点：成都市高新区天府大道1700号新世纪环球中心E3门栋6楼2-1-611-615四川中意招标有限公司本项目开标室。

六、公告期限

自本公告发布之日起3个工作日。

七、其他补充事宜

无。

八、凡对本次采购提出询问，请按以下方式联系。

1. 采购人信息

名 称： 成都体育学院

地 址： 四川省成都市武侯区体院路 2 号

联系方式： 刘老师： 028-85097065

2. 采购代理机构信息（如有）

名 称： 四川中意招标有限公司

地 址： 成都市高新区天府大道 1700 号新世纪环球中心 E3

门栋 6 楼 2-1-611-615

联系方式： 028-87050033

3. 项目联系方式

项目联系人： 赵龙

电 话： 028-87050033 转 2040

附件：本项目技术要求：

第 1 包：SSL 证书服务

★一、服务要求

- 1、证书有效期 ≥ 1 年（上一次维保服务结束后一年；如果上一次维保已结束，则维保起始日期以签订合同时间为起始时间）。
- 2、证书品牌：Symantec、Digicert、Geotrust、Globalsign 其中之一。
- 3、证书类型：通配符（主域名+所有二级域名）同步防护，不限服务器类型和数量。
- 4、工程师协助部署（支持所有格式）。

★二、商务要求

- 1、服务时间：2021 年 10 月 12 日-2022 年 10 月 11 日
- 2、服务地点：成都体育学院
- 3、付款方式及条件：合同签订后，经采购人确认无异议且验收合格后，采购人在收到成交供应商提供的全额、正规普通增值税发票以及相关凭证之日起 30 日内，一次性支付合同款项。
- 4、验收标准：符合相关行业标准，按照成都体育学院校内制度《成都体育学院采购验收管理办法》（成体院【2017】149 号）的要求进行验收。供应商可在 <http://zcglc.cd.su.edu.cn/gzdz/cgzd/xxcgzd/2017-12-20-259.html> 查阅《成都体育学院采购验收管理办法》具体内容。

第 2 包：网络安全等级保护测评服务

1、网络安全等级保护清单

| 名称 | 定级 | 备注 |
|----------------------------|----|---------|
| 学校网站群系统 (含门户网站及校内各部门网站) | 三级 | 测评+备案证明 |

| | | |
|-------------|----|---------|
| 招生系统 | 三级 | 测评+备案证明 |
| 境内外学生管理服务平台 | 二级 | 测评+备案证明 |
| 在线采编平台 | 二级 | 测评+备案证明 |
| 包含项目产生的任何费用 | | |

2、项目需求：

2.1 项目背景

随着网络和信息技术的快速发展和信息化的深入应用，成都体育学院信息化程度不断提高，信息化已经成为提高教学管理和科研的不可或缺的重要手段。信息安全是信息系统提供各项业务服务的重要保障，而安全测评工作是信息系统安全保障建设的关键，其直接制约着成都体育学院的信息服务质量，以及教学管理等重要数据资源的机密性、完整性和可用性。

成都体育学院将请第三方机构对其重要信息系统进行安全测评工作，按照国家等级保护的要求依据成都体育学院信息系统实际情况进行安全测评相关工作，满足安全等级保护工作需求。

2.2 建设原则

2.2.1 安全保密原则

报价人在为成都体育学院提供安全服务的过程中，要严格遵守合同规定，执行国家《保密法》及有关保密的法律法规，服务过程中凡是涉及到的任何用户信息均属保密信息，不得泄露给第三方单位或个人，不得利用这些信息损害用户利益。

2.2.2 最小影响原则

报价人在成都体育学院开展的安全服务工作，要尽可能小的影响系统和网络的正常运行，不能对业务的正常运行产生显著影响（包括系统性能明显下降、网络阻塞、服务中断等），如无法避免，应对风险进行说明。

2. 2.3 规范性原则

报价人在成都体育学院开展的安全服务工作，要由专业的安全服务人员依照规范的操作流程进行，对操作过程和结果要有相应的记录，提供完整的服务报告。

2.2.4 可控性原则

报价人在成都体育学院开展的安全服务工作过程中采用的工具、方法和过程要在双方认可的范围之内，保证用户对于服务过程的可控性。

2.2.5 质量保障原则

报价人在成都体育学院开展的安全服务工作需特别重视项目质量管理，项目的实施需严格按照项目实施方案和流程进行，并由项目协调小组从中监督、控制项目的进度和质量。

3、本项目需实现的目标

依照 GB/T 22239-2019 开展相应等级的测评工作。通过安全等级测评，满足“公通字[2007]43号”、国家公安部、保密局、国家密码管理局、国务院信息化领导小组办公室于 2007 年联合颁布了 861 号文件《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》和《信息安全等级保护管理办法》等政策文件要求、同时发现信息系统潜在的威胁及风险点、为后续安全加固整改工作提供依据，同时落实国家信息安全等级保护政策、标准、成都市教育行业等级保护相关工作要求；全面加强成都体育学院自主应对信息系统的综合安全防护能力。降低成都体育学院信息系统安全风险；提升信息系统安全服务水平；加强成都体育学院对信息系统安全管理能力；完善安全综合防护能力和风险处置能力，降低和缓解现有信息安全风险，进一步健全和完善信息安全管理策略体系。满足技术和业务目标。

4、项目实施与组织管理要求等

依据国家各项相关标准法规和成都体育学院现有的规范、制度，同时结合项目实际需要，对信息安全等级保护项目工作中的定级、备案、测评（包括测评范围、测评方法等）、整改（包括整改方法、范围等）过程中，所需的产品、技术、制度、流程、建设要求和实施规范等方面，提供咨询、测评、整改建议以及整个建设过程的监督和管理等服务。所提供的整体方案需包括技术方案和实施方案。技术方案包括整体流程、技术方法和服务方案设计等，需要对每项技术方法的应

用位置进行详细描述，对系统进行详细的测评，发现系统不足，明确安全风险隐患和差距，提出整改意见，协助成都体育学院信息安全管理人员进行整改；实施方案包括人员组织、时间安排、阶段性文档提交、验收标准、质量保证和风险规避措施等，需要明确每项工作的时间安排、操作时间和操作人员。报价人负责提供的服务内容至少应包括，但不限于以下各项：

(1) 服务提供商在信息安全等级保护测评和风险评估前应制定详细的技术方案，包括信息安全等级保护测评项目计划书、测评实施方案以及人员安全培训计划等，并提交成都体育学院审核。

(2) 信息安全等级保护测评包括但不限于以下对象：网络结构、网络服务、主机系统、存储备份系统、数据库、中间件、应用系统、数据安全、安全系统、系统安全策略等。

(3) 服务提供商应描述测评服务的技术方案，包括准备工作、技术措施、人员安排、时间进度、可能对系统造成的影响等。

(4) 安全测评工作应尽量选择在非业务繁忙时段进行，将对被测系统可能带来的影响减至最小。

(5) 服务提供商应书面承诺能够积极与成都体育学院协作，共同完成本项目的测评工作，项目实施过程中出现问题不得互相推诿，双方应主动进行沟通，并及时解决问题，确保项目顺利实施。

★5、采购项目服务时间

服务时间：本项目需要在合同签订后 90 个工作日内完成安全等级测评服务及等保备案申报工作。

6、实施团队要求：

报价人须为本项目组建稳定的、专业的、独立的项目团队，专门负责本项目服务实施工作，进行相关的项目管控和随时调整项目实施方向。针对本项目成立专门的项目组，确保人力、物力的投入，项目组成员必须稳定，项目实施团队成员在项目终验前如果人员退出或更换，需要征得采购人同意。

项目经理至少具有 3 年以上安全集成或安全服务项目实施经验，并具有类似工程的项目经历。项目经理需具备具有高级信息安全等级测评师证书，需提供高级信息安全等级测评师证书复印件及个人简历。

7、组织管理要求

要求给出切实可行的项目实施方案，方案中要包含风险管理、进度管理、变更管理、沟通管理、文档管理、质量管理、技术保障措施、组织保障措施等内容。

在项目实施的全过程中，采购人有对项目进度、质量进行监督控制的职责和权利，报价人应全面配合，定期向采购人提交项目进展情况报告。

★8、项目验收标准

(1) 验收：交付后，采购人将根据招标技术需求各项指标进行验收，经双方确认完成验收，签署验收报告。

(2) 需提交的验收文件资料主要包括：

网络安全等级保护测评报告（每系统一份）；

渗透测试报告（每系统一份）；

漏洞扫描报告（每系统一份）；

项目验收申请表；

项目设计方案及工程过程文档；

项目建设合同和有关修改、调整情况的纪要文件；

项目的技术报告和工作总结报告；

项目建设的技术资料及各阶段成果及过程记录文档；

★9、保密要求

报价人要严格遵守国家《保密法》及有关保密的法律法规，选派具有良好职业道德的人员参与和从事本项目工作，教育相关人员恪守职业道德，服从采购人的管理，严格遵守采购人的保密规定和工作制度，并承担相应的保密责任。

所有参与本项目的服务人员自觉接受采购人的安全保密监督和管理，如违反安全保密条款，采购人将追究其责任，对重大的泄密事件将移交司法部门追究其法律责任；对泄露系统资料，造成伤害的，除依据有关规定追究有关责任人员法律责任外，还将依法承担相应的民事责任。

10、技术支持及售后服务需求

报价人应针对本项目提供详细的技术支持及服务方案，方案包括完善的技术支持体系、服务响应流程、响应时间、服务热线、服务保障措施、应急处置措施等内容。

服务期间内，报价人需成立专门技术队伍，按采购人要求对测评服务期间安全技术问题解答，报价人需提供 7*24 小时热线电话服务响应，对服务期间发生的问题在 1 小时内给予响应，若电话不能解决需 2 小时到现场进行分析处理。

★11、商务要求

服务期限要求：供应商在合同签订后 90 个工作日内完成安全等级测评服务及等保备案申报工作。采购人收到供应商反馈的等保测评备案证明后，服务结束。

付款方式：本项目服务完成且验收合格后，采购人在收到供应商提供的足额、正规发票以及相关凭证资料后的 30 日内，向成交供应商一次性支付合同款。

报价人应具备“国家网络安全等级保护工作协调小组办公室”颁发的《网络安全等级保护测评机构推荐证书》。

第 3 包：网站漏扫服务

1 总体要求

本项目建设为极简网络设计，采用旁路接入组网方案。漏洞扫描系统通过预设的扫描 IP 接入，主要通过采集信息、执行漏洞检测脚本对学校网站群进行实时安全监控预警，并对指定计算机系统、应用程序、数据库、WEB 服务、网络设备、安全设备的安全脆弱性进行检测，发现可被利用漏洞、不安全配置并实时预警。涵盖系统漏洞检测、网站监控预警、数据库漏洞检测、基线配置检查、弱口令检测和等保合规检查等功能模块。对学校各网段系统进行定期的安全检查，并输出相关的漏洞检测报告，提供安全解决方案建议。

能够全面发现学校信息系统中存在的各种脆弱性问题，包括各种安全漏洞、安全配置问题、不合规行为等进行 24 小时不间断监测、实时预警，形成整体安全评估报告，对安全状况进行可视化展示，有效提升学校信息安全保障能力和水平。

2 具体技术指标及性能要求

| 项目 | | 技术参数 |
|--------|----------|-------------------------------------------------------------------------------------------------------|
| 授权域名个数 | | >=52 个 |
| 漏扫服务对象 | | 学校主网站、各部门网站、专题网站 |
| 实时监测 | DNS 解析检测 | ▲实时监测各省主要运营商的 DNS 缓存服务器及被监测域名的授权服务器对被监测域名的解析结果是否正确。包括 A 记录、CNAME 记录、NS 记录、MX 记录、SOA 记录、PTR 记录（提供截图证明） |

| | | |
|-------|----------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| | 搜索引擎检测 | 搜索引擎监测，设置关键词，对至少 3 个主流搜索引擎的至少前 100 个搜索结果进行检查 |
| | 业务可用性监测 | 支持网站存活监测，通过固定的频率探测被监控主机或站点存活状态，监控不同地域和运营商的联通性、丢包率、网络时延。 |
| | | 支持页面响应监测，通过固定的频率模拟用户请求访问被监控站点，实时获取站点的响应状态和请求详情，精准的探测出网站的各种异常 5 分钟检测一次，当连续 3 次访问失败时判断为业务不可用 ▲实时监测目标站点的访问速度、页面加载时间等网站性能参数（提供截图证明） |
| | 篡改监测 | ▲对目标站点的关键页面进行实时篡改监测，分钟级篡改发现，第一时间通过微信、短信进行实时告警，并提供主动电话告警。（提供微信、短信告警截图证明） |
| | | 支持篡改处置服务，对业务系统已经发生页面篡改、敏感词的紧急事件进行应急处置，把访客的访问进行重定向至云端预置的站点维护界面，避免安全事件的扩大。 |
| | 黑链监测 | 支持对目标站点提供 7×24 小时网页黑链监测能力。发现网页黑链事件第一时间通过微信、邮件、电话、短信等方式通知用户，监测内容能够在报告中呈现。 |
| 敏感词监测 | 支持对目标站点提供 7×24 小时网页敏感词检测能力。发现网页敏感词事件第一时间通过微信、邮件、电话、短信等方式通知用户，监测内容能够在报告中呈现。 | |
| 及时告警 | 短信告警 | ▲支持以短信的方式对篡改、挂马、网站不可用等安全事件进行实时告警，支持微信端内容的及时推送（提供截图证明） |
| | 微信告警 | ▲支持以微信的方式对篡改、挂马、网站不可用等安全事件进行实时告警，支持微信端内容的及时推送（提供截图证明） |
| | 邮件告警 | 支持邮件的方式推送安全事件报告、月报 |
| 网站防御 | 网站防御 | 支持识别恶意请求含：跨站脚本(XSS)、注入式攻击(包括 SQL 注入、命令注入、Cookie 注入等)、跨站请求伪造等应用攻击行为 |
| | | 支持对用户上传的文件后缀名和文件内容进行全方面检查，杜绝 Webshell 的上传和访问 |
| | | 支持对 WEB 服务器容器、应用中间件、CMS 系统等第三方组件漏洞进行有效防护 |
| | | 支持智能识别攻击者，对网站连接发起攻击的 IP 地址进行自动锁定禁止访问被攻击的网站 |

| | | |
|--------------|-------------------------------------------|-------------------------------------------------------------------------------------------------------|
| 漏洞评估 | 暴露面检测 | 支持关键系统域名发现，自动发现客户所填入域名相关的所有子域名 |
| | | 支持检测网站服务器端口开放情况，比如数据库端口、Ftp 服务端口等，网站后台暴露，支持检测网站管理后台向互联网开放情况 |
| | 漏洞脆弱性检测 | 支持对 Web 漏洞进行扫描，覆盖通用漏洞和常规漏洞。支持 SQL 注入、XSS、安全配置错误、已知漏洞组件包含、敏感信息泄露等常见漏洞的检测 |
| | | 支持信息泄漏检测，能够检测网站源码、数据库备份文件、SVN 文件、系统重要配置、日志文件向外网泄漏、WebShell 检测 |
| 高危 Oday 事件告警 | 支持系统弱口令检测，对服务器对外提供的 rdp, ssh 等远程服务进行弱口令检测 | |
| 可视化展示 | 风险展示界面 | 支持高危 Oday 实时检测，出现 ODAY 漏洞时，主动对所监控用户业务做扫描发现，重要网络安全事件和安全漏洞快速预警通告和检测，检测结果第一时间定向推送到客户，能够支持手机微信、短信实时推送告警信息 |
| | | 支持提供可视化的监测界面，首页可直观进行安全风险的展示，至少包含：篡改通报、挂马通报、断网通报、紧急漏洞、高危漏洞在内的预警监控展示，业务系统安全状况 TOP3 展示等，便于实时掌握业务风险情况 |
| | 报告 | 支持用户端管理界面进行网站风险的管理，支持通过界面自行对域名进行增加和删除操作，支持管理网站业务的所有报表 |
| | | 支持每月定期生成网站安全评估，并生成安全评估报告，报告应至少包含扫描站点信息、风险分布情况、漏洞的风险描述、影响范围、解决方案和具体的攻击举证进行详细的展示 |
| | | 支持每日生成安全运营日报，每月生成安全运营月报，并针对安全事件实时生成安全事件报告 |

★3 商务要求

3.1、服务时间：1 年（2021 年 12 月 15 日-2022 年 12 月 14 日）

3.2、售后服务及授权：接到故障电话后半小时内响应用户要求，2 小时处理基本故障，4 小时内现场维护处理并在 24 小时内排除故障修复使用。签订合同前，提供原厂商针对该项目的授权书和售后服务承诺函，若不能提供，则采购人有权认定为供应商无法时限本项目的服务要求，采购人有权不予签订合同，由此造成的一切损失由成交供应商承担。

3.3 验收标准：供应商所提供服务应符合相关行业标准，符合采购文件要求，

本项目成交人与采购人将参照《财政部关于进一步加强政府采购需求和履约验收管理的指导意见》(财库〔2016〕205号),以及按照成都体育学院校内制度《成都体育学院采购验收管理办法》(成体院【2017】149号)的要求进行验收。供应商可在 <http://zcgjc.cd su.edu.cn/gzzd/cgzd/xxcgzd/2017-12-20-259.html> 查阅《成都体育学院采购验收管理办法》具体内容。

3.4 服务地点: 成都体育学院

3.5 付款方式: 本项目在验收合格后,采购人在收到成交供应商提供的全额、正规的普通增值税发票以及相关验收凭证等资料后的30日一次性完成合同款项的支付。

注: 本章中“★”项为实质性要求, 供应商不得负偏离, 否则视为无效响应。