**厦门大学嘉庚学院**

**信息系统等级保护咨询及服务与重大会议期间安全保障服务招标方案**

**一、项目背景**

根据《福建省教育厅福建省公安厅关于切实做好我省教育行业信息安全等级保护工作的通知》（闽教科[2016]95号）文件要求，通过公开招标方式，为厦门大学嘉庚学院提供信息系统安全等级保护安全评估建设咨询及服务与重要会议期间安全保障服务。

**二、项目目标**

根据信息安全等级保护相关法规要求，对厦门大学嘉庚学院信息系统进行定级并形成定级备案文档，继而通过等级保护安全评估服务，评估网络及信息系统技术安全现状和管理安全现状，发现当前网络及信息系统存在的各种安全风险，以及和国家等级保护相关标准的差距，提出解决方法并规划和形成分几段整改方案建议，最终取得公安部门颁发的信息系统安全等级保护备案证明。同时，提供在重要会议期间，安排专业服务人员和提供相应安全设备对网站相关资产进行安全巡检、安全加固服务，对重要网站实行7\*24小时不间断的监控，对突发事件进行应急响应，并提供定时通告与防护等服务。确保重要会议期间网站得到专业化的安全保障，重要业务正常顺利运行，同时提高管理人员应急处置保障能力。

**三、项目内容**

|  |  |
| --- | --- |
| 项目序号 | 服务名称 |
| 1 | 信息系统等保建设咨询服务 |
| 2 | 重保会议安全保障服务 |

**1、信息系统等保建设咨询服务：**

**1.1、等级保护备案**

根据《等级保护基本要求》，完成厦门大学嘉庚学院信息系统6个二级信息系统等级保护建设工作，最终取得公安部门等级保护的相关备案证明，备案地为漳州市。取得备案证明及等保建设咨询服务须在2017年7月30日前完成。

**1.2、资产分析阶段**

（1）资产调查：调查和统计信息资产，其中必须包括但不限于物理环境、网络设备、主机、应用软件、业务系统、数据、人员、标准流程等，明确其现有状况、配置情况和管理情况，并对所有信息资产按照一定标准进行资产赋值，绘制各业务系统的数据流图。具体的现状情况如主机系统，需明确其配置、存储空间（包括剩余空间，空间分配）操作系统平台、版本、补丁、IP地址、开放端口、服务和进程等配置管理信息。

（2）网络拓扑调查：包括对所有网络的拓扑结构进行调查，并按统一标准绘制成图。

（3）安全系统调查：包括但不限于明确现有安全设备的部署情况和使用情况，编制安全区域图。

**1.3、差距分析与整改**

（1）渗透性测试：在确保安全的前提下通过黑盒和白盒方式对指定的系统进行渗透攻击，发现该系统存在的安全隐患，并提出解决措施。

（2）漏洞评估：通过工具和人工方法，对信息系统及设备进行漏洞扫描评估。

（3）安全策略分析：对信息系统现有的安全策略进行分析，发现存在的安全隐患。

（4）安全管理评估：对信息系统管理现状进行评估，包括安全管理机构评估、安全管理制度评估、人员安全管理评估、系统建设管理评估、系统运维管理评估。

（5）差距分析报告：依据技术评估、管理评估、漏洞评估及渗透性测试结果完成等级保护差异分析和安全评估报告，该报告将作为等级保护整改重要依据。报告包括但不限于《物理安全差距分析表》、《网络安全差距分析表》、《主机安全差距分析表》、《应用系统差距分析表》、《数据安全差距分析表》、《人员安全管理差距分析表》、《安全管理制度差距分析表》、《安全管理机构差距分析表》、《系统建设管理差距分析表》、《系统运维管理差距分析表》、《防火墙等级保护安全检查》、《数据库系统等级保护安全检查》、《主机系统等级保护安全检查》、《应用系统渗透测试报告》、《网站渗透测试报告》等。

（6）整改与优化：按照不同等级的不同要求，根据差距分析报告，逐条、逐项对比、检测，针对不符合项，按照系统化、体系化设计思路，按照“缺什么补什么”的原则，帮助厦门大学嘉庚学院在管理制度建设和技术措施方面开展全面整改，对于风险评估过程中发现的安全漏洞和安全脆弱性情况，提出可行的安全加固方案，并协助完成加固工作，如果由于学校现实原因限制不能执行的，提供过渡方案以降低安全风险。

**1.4、 安全规划**

中标服务商需根据厦门大学嘉庚学院网络安全现状，结合等级保护要求，在充分考虑信息系统正常运行的状况下进行安全域设计，分析安全需求得出安全控制措施，并对安全控制的相关性、紧迫性、可实施性、难易程度和预期效果等进行分析，对厦门大学嘉庚学院未来3-5年信息安全工作进行规划，提出可行的安全解决方案和安全规划。

**1.5、 等级保护预测评**

（1）预测评方案制订：根据等级保护要求，制订《安全预测评方案》，《安全预测评现场计划》，《安全预测评作业指导书》，方案和作业指导书中必须明确采用的技术手段、人工方法和使用的工具，明确预评估的具体内容，方案和作业指导书经采购人批准后实施。

（2）技术预评估：包括物理安全、网络安全评估、主机系统安全评估、应用安全评估、数据安全评估等。预测评应当覆盖等级保护技术要求，在方案和作业指导书中应对此加以说明。

（3）设备预测评：根据等级保护的相关标准和要求，分析主机、网络及安全设备面临的威胁，测评现有系统的存在的弱点，明确现有网络面临的安全风险和隐患。

（4）网络安全预测评：根据现有网拓扑结构和网络设备配置情况，分析整体网络拓扑结构的合理性和可靠性；分析业务系统和网络结构部署关系，指出系统存在的安全风险和隐患。主要包含结构安全与网段划分、网络访问控制、拨号访问控制、网络安全审计、边界完整性检查、网络入侵防范、恶意代码防范、网络设备防护等方面。

**1.6、 报告文档编制**

（1）信息系统资产清单（包括但不限于服务器、网络设备、信息系统的详细情况）；详细网络拓扑图、数据流图、安全域图；信息系统定级报告；等级化安全评估报告；渗透性测试报告；主机、网络设备及应用系统风险分析报告；加固建议报告；等级安全体系框架建议；等级保护体系安全规划建议；等级保护整改建议方案；信息系统运维管理系统建议方案。

（2）根据实际情况结合等级保护相关要求协助制定各类等级保护安全管理制度，包括但不限于：《安全管理日常维护细则》、《安全审计管理制度》、《第三方人员管理制度》、《防病毒紧急响应流程》、《机房监控与管理流程》、《机房运行管理规范》、《服务器运维管理规范》、《软件开发环境使用管理要求》、《系统交付管理规范》、《资产安全管理规范》、《安全事件报告和处置管理规范》、《人员安全管理规范》、《信息系统安全运维管理规范》等。

**1.7、 技术资料要求**

包含但不限于下述文档：《信息系统资产清单》、《安全评估方案》，《安全评估现场计划》，《安全评估作业指导书》、《物理安全差距分析表》、《网络安全差距分析表》、《主机安全差距分析表》、《应用系统差距分析表》、《数据安全差距分析表》、《人员安全管理差距分析表》、《安全管理制度差距分析表》、《安全管理机构差距分析表》、《系统建设管理差距分析表》、《系统运维管理差距分析表》、《防火墙等级保护安全检查》、《数据库系统等级保护安全检查》、《主机系统等级保护安全检查》、《应用系统渗透测试报告》、《网站渗透测试报告》、《安全管理日常维护细则》、《安全审计管理制度》、《第三方人员管理制度》、《防病毒紧急响应流程》、《机房监控与管理流程》、《机房运行管理规范》、《服务器运维管理规范》、《软件开发环境使用管理要求》、《系统交付管理规范》、《资产安全管理规范》、《安全事件报告和处置管理规范》、《人员安全管理规范》、《信息系统安全运维管理规范》。

**2、重大会议期间安全保障服务：**

为保障学校信息系统在厦门重大会议期间正常、稳定、持续的运行，需要安全服务商配合做好会议期间信息系统的安全保障工作。

**2.1外网网站渗透测试服务**

提供外网网站渗透测试服务，通过渗透测试发现服务的外网网站中存在的安全漏洞，并提供修复建议，配合修复验证。避免网站中存在的安全漏洞被不法分子利用，导致网站遭到篡改，挂马等破坏，从而引发重大的安全事故。

**2.2网站监控服务**

提供网站监测服务，通过网站安全监测平台对需要监控的网站进行不间断的监测，结合安全专家的专业分析，及时发现网站存在的安全隐患和问题，第一时间通知安全管理员进行处理，并提供安全建议，降低风险，减少损失。同时定期提供网站安全监测报告，使安全管理员了解峰会期间网站的安全状况和安全趋势，必要时采取措施，控制风险。监控内容包括网站漏洞扫描、网页挂马检查、网页敏感内容实时监测、可用性监测、网页篡改监测、网站域名解析监测、钓鱼网站监测等。

**2.3资产漏洞全生命周期管理**

在初步梳理服务基础之上，建立漏洞管理库，根据不同维度，对资产及漏洞进行统一管理、统一分析。根据数据模型为安全管理提供管理及考核依据。通过资产定级管理、漏洞修复管理等活动的梳理，建立网络部漏洞管理流程，包括：管理方针、规范、作业指导书、具体执行表单等四级文档以及流程活动说明等。

**2.4漏洞（包括系统、web、应用）初步梳理服务**

对常见高中风险系统安全漏洞的分析整理和归类，并分专业建立漏洞跟踪表模板；

整理常见高中风险系统安全漏洞的详细加固步骤形成指引性操作文档。

**2.5互联网资产暴露核查**

对互联网暴露面资产开展稽核，针对发现的IP资产进行扫描，服务开始和重保期封网前各开展一次。

**2.6日常性集中系统漏洞（包括系统、web、应用）治理支撑服务**

进行网络设备中高中风险漏洞的加固指导和漏洞整改后的人工复查和验证工作。并提供漏洞加固过程必要的补丁下载、验证、测试和现场加固保障服务。

提供设备自动化登陆扫描验证服务。建立登陆扫描的手段，定期更新漏洞库，每周对网络资产进行登陆扫描及验证工作，提高目前漏洞识别的准确性。

漏洞加固支撑服务，要求督促各厂商及时、准确、高效的开展漏洞加固、整改、复查工作，形成风险闭环，必要时提供现场安全培训工作。

**2.7互联网业务梳理和范围检查**

针对对外开放的WEB、APP业务和应用系统，每月对全校IP地址进行跟踪和反向解析，确认是否开放网站和APP等业务，发现未上报的资产进行通报和情况反馈。

**2.8防护手段**

针对重大会议安全保障的要求，服务商需提供有软、硬件产品支撑的各种防护，包括但不限于以下：网站安全监测与防护、DDOS监测与防护、入侵监测与防护、APT监测与防护、DNS域名修正和防篡改、综合安全态势的预警防御等等。投标人需提供详细的防护方案，包括软、硬件产品的型号和功能说明等。

**2.9应急演练**

拟定的安全预案模拟各类安全攻击和演练场景进行演练操作，包括信息安全、网络安全、业务安全等，并组织相应的人员进行排练。

**2.10威胁情报通报**

提供最新安全动态、技术和定制的安全信息，包括实时安全漏洞通知、定期安全通告汇总、临时安全解决方案和安全知识库更新等。

**2.11现场值守服务**

重大会议期间，服务商派出至少1名资深安全专家配合客户进行7\*24小时的现场防护和应急处理服务。

现场值守工程师对客户网络中的安全设备运行状态进行例行检查，并持续监控网内的安全事件，针对信息安全预警、安全防护、系统监控等方面的运行状况进行安全检查，监控各安全设备的运行状态，及时收集各安全设备的运行数据，在第一时间发现可能出现的各种网络安全问题，并及时通知加以防范。同时，保障期间每天需针对各系统的运行情况整理系统运行安全日报。

**2.12一键封堵**

为保障在遭遇突发安全攻击事件时，能在最短时间内控制事态的扩散，服务商需承诺可提供分钟级别的解决方案，在互联网出口层面可通过监测与防御能力的设备与平台，分析出的真实攻击事情，快速下发指令，对攻击事件进行分钟级自动响应，避免安全事件产生重大影响。投标人需提供详细的解决方案，其中包括突发安全攻击事件的故障环节以及稳定恢复学院网络性能和线上业务的运行保障。

**2.13安全保证承诺**

服务进行阶段中，服务商需及时将存在的问题告知校方，包括人工修复问题和产品缺失问题，校方会根据问题及时安排后续修复及采购计划。如因时间问题，针对缺失需采购的产品，校方未能如期采购，**服务商需在投标文件中明确承诺，无偿提供项目所需的全部产品，配合校方安全渡过重大会议，会议结束后立即归还产品。未有明确承诺的，视为无效投标。**

**2.14保障时间**

保障时间：2017年8月1日至厦门会晤结束。

**四、服务要求**

1．本项目要求本地化服务、本地化实施，服务提供商应为本项目配备高水平的技术团队，并在响应文件中提供技术人员的劳动合同及社保缴交证明文件复印件。

2．服务提供商应提供近年来相同或相近项目的用户名单表，并附上合同或其他相关证明材料。

3．服务提供商应为符合政府采购法等法律法规的合格供应商，报价时应提供服务提供商依法纳税情况、社保缴纳情况、财务状况（银行资信证明或上一年度财务报表）、近一年内经营活动没有重大违法记录、信誉状况及相关项目经营业绩（提供合同、验收报告、用户证明等）等有效证明文件。

4．供应商认为有利于采购人的采购要求之外的优惠条款应单独列明。

**五、投标人应具备的资格以及应提供的资格证明文件**

投标人应在中华人民共和国合法注册、登记，符合政府采购法第二十二条第一款的法定条件，并符合以下特定条件：

1、投标人应具备独立的法人资格，相应的生产经营范围，并提供合法有效的法人营业执照副本及税务登记证副本复印件。（需提供相关材料复印件并加盖公章，原件备查）。

2、投标人必须提供法定代表人对服务商代表的授权书原件（服务商代表不是法定代表人的）及服务商代表的身份证复印件。

3、投标人取得《信息安全等级保护安全建设服务机构能力评估合格证书》以及《国家信息安全测评信息安全服务资质证书》。

4、本项目不接受联合体参加投标。

**说明：**投标人的资格条件在评审时进行检查。投标人应在响应文件中按招标文件的规定和要求附上所有的资格证明文件，提供的复印件必须加盖投标人公章，并在必要时提供原件备查。若投标人提供的资格证明文件不全或不实，其投标文件将按无效文件或成交资格被取消处理。

**六、评分参考**

按照评标程序的规定对各投标人的资格性以及符合性做出评审，只有资格性检查和符合性检查合格的投标文件才能进入综合评分。评标专家依据评分标准以及各项权重，就每个合格投标人的投标文件及其对招标文件要求的响应情况进行综合比较和评价，统计每个通过审核的投标人的技术、商务得分。

**（一）具体的评标标准。**

**1、通过评标专家资格性、符合性审核，有三家或三家以上符合专业条件**

**要求并对招标文件作实质性响应的投标人，则依照以下标准进行评分：**

**（一）技术评分（50分）**

|  |  |  |
| --- | --- | --- |
| 序号 | 评分界定 | 满分分值 |
| 1-1 | 对投标人的项目实施队伍人员情况进行评价：  每拥有一名CISP 认证信息安全专业人员（须提供认证证书  复印件并加盖投标人公章，以及最近1年投标人为其缴交社  保的证明材料复印件）的得5分，满分10分。 | 10 |
| 1-2 | 针对网络安全服务的执行能力进行评价：  ① 具备对各类信息系统在线运行于内部网络或互联网网络  的系统安全脆弱性分析与检测能力。5分  ② 具备对各类信息系统的漏洞扫描、代码级安全分析、信  息安全攻防的能力。3分  ③ 具备完整的、合理的、可行性高的安全检测技术与检测流程。3分  ④ 服务中提供的专业扫描或检查工具的知名度及先进性。(提供工具装备设施的有效证明)。4分  注：投标人提供安全漏洞检测设备，并提供设备的功能截图、投标人需掌握配置和使用方法，列出在整个服务周期中将使用的安全工具和装备及有关配套设施，并标明其每个在服务周期中的用途。  **备注：提供机构认证证明，或者购买合同证明。** | 15 |
| 1-3 | 对投标人第三级系统项目实施业绩评价：  投标人每提供一个高校等级保护（第三级系统）安全测评成功案例证明文件（要求提供等级保护安全测评报告相关页面复印  件并加盖投标人公章，且测评结果为基本符合）的；同时，  须提供该案例项目以下资料复印件并加盖投标人公章：  ①合同复印件（含设备清单页复印件）；  ②中标（成交）公告（提供相关网站中标或成交公告的下载网页及其网址）；  ③中标（成交）通知书；  ④提供测评通过证书，如未完工请提供项目进度表，项目进度表须附高校主要负责老师联系方式，以便核实；  ①、②、③、④四项缺一不可。上述材料中须能体  现案例简要说明、采购人联系方式，否则投标人须另页说明；  如未按照招标文件要求提供该项业绩完整资料的，专家对该项业绩将不予采信。每个有效案例得5分，满分10分。 | 10 |
| 1-4 | 根据服务商提供的服务方案整体合理性的评价，包括:   1. 对项目方案调研熟悉情况描述；项目组织结构、人员职责、人员资质和经验、服务计划和服务时间等内容进行评价，优得3分，良得2分，一般得1分。 2. 服务商提供的服务方案与我院所提出的安全保障服务要求内容的响应和契合度，优得3分，良得2分，一般得1分。 3. 重保会议安全保障服务中，是否明确承诺，无偿提供项目所需的全部软硬件产品，提供者得9分，无提供者不得分。 | 15 |
| 说明：报价人应提供证明材料并标注对应关系，未按要求提供证明材料的，认定该项技术指标不得分；报价人应如实表述其货物的技术指标，如报价人复制采购文件的磋商内容作为其报价文件组成内容的，磋商小组将对其作出不利的评审。 | | |

**（二）商务评分：30分**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 评分界定 | | 满分分值 |
| 2-1 | 投标人的基本情况 | 1. 投标人的企业经营年限进行评价：企业成立   8年及以上的得2分，5年及以上8年以下的  得1分，5年以下的不得分，提供相关证明文件，  否则不得分。 | 2 |
| ②投标人注册资金：注册资金≥人民币2000万元  的得2分，人民币1000万元≤注册资金＜人民  币2000万元的得1分，注册资金小于1000万  元的不得分。 | 2 |
| 2-2 | 投标人具有ISO27001信息安全管理体系认证证书，提供证书  复印件，否则不得分。 | | 3 |
| 2-3 | 公安部颁发的信息安全等级保护安全建设服务机构能力评估合格证书，提供者得4分，没有不得分，提供相应证书复印件作为考评依据，原件备查。 | | 4 |
| 2-4 | 投标人需提供中国信息安全认证中心（ISCCC）认证的信息安全风险评估服务资质，风险评估服务一级得3分，二级得2分，三级得1分。不满足以上者不得分，提供相应证书复印件作为考评依据，原件备查。 | | 3 |
| 2-5 | 投标人需提供中国信息安全认证中心（ISCCC）认证的信息安全应急处理服务资质，应急处理服务一级得3分，二级得2分，三级得1分。不满足以上者不得分，提供相应证书复印件作为考评依据，原件备查。 | | 3 |
| 2-6 | 投标人具备安全研究能力，具备漏洞独立发现能力并在从2014年至今向CNVD、CNNVD、CVE等信息安全漏洞共享平台报送漏洞数量在100个或以上，得3分；100个>报送漏洞数量≥20个，得2分；20个>报送漏洞数量>0个，得1分；未提供或没有发布过漏洞的不得分。注：投标人应提供其发布过的漏洞的有效证明材料。 | | 3 |
| 2-7 | 服务商须具有应急支撑服务能力，需取得《国家级应急服务支撑单位》（1分）或《福建省网络与信息安全应急处置技术支撑单位》（1分）或《省级应急服务支撑单位》（1分）证书，取得一个证书得1分，同时具备得3分，不具备该资质得0分。提供相关证明资料，加盖服务商公章。 | | 3 |
| 2-8 | 投标人具备涉及国家秘密的计算机信息系统集成资质证书，取得甲级以上，得3分，取得乙级，得1分，其他不得分，提供相应证书复印件作为考评依据，原件备查。 | | 3 |
| 2-9 | 根据投标文件是否完整响应招标文件要求，提供的资料是否详实、充分，以及服务商承诺的其他有利于采购人的条件。优得4分、良得3分、一般得1分。 | | 4 |

**（三）价格评分：20分**

**各有效投标人的综合得分＝技术因素分+商务因素分+价格因素分**

**备注：**

**1、由于评分主要根据投标文件提供的资料进行，投标人须针对各项评分标准做出相关详细说明，须自行承担由于资料提供不全、错漏、或者无效而导致的不利评审，并对自身提供的投标文件、资料的真实可靠性负责，所有证明材料均应加盖投标人公章。若因投标人提供的投标文件资料存在弄虚作假情况，评标专家有权取消其中标资格。**

2、评标专家对所有投标人的投标文件的评审，都采用相同的程序和标准。

3、参加评标的相关人员，不得将有关投标文件的审查、澄清、评估和比较以及会影响评标工作的一切情况，透露给任何一位投标人或与上述评标工作无关的人员。