福建省民族与宗教事务厅办公室

关于福建省民族与宗教事务厅网站和信息系统安全服务项目询价函

各报价单位：

我单位以询价采购方式进行下列物品的采购。请你单位就以下采购项目内容进行书面报价。

一、采购询价表

项目名称	服务内容	规格参数	年限
福建省民族与宗教事务厅网站和信息系统安全服务项目	福建省民族与宗教事务厅门户网站、福建省民族事务管理系统和福建省宗教事务管理系统及其支撑环境的保障服务。	详见询价文件附件“询价内容及具体要求”	2025.1.1－2027.12.31

二、相关要求

1.报价单位必须在中华人民共和国境内注册，具备独立法人资格，是省网信办认可的福建省信息网络服务安全支撑单位。

2.报价文件内容（须加盖公章）：

（1）报价文件;

（2）公司营业执照或副本复印件；

（3）提供近五年来省内企事业单位安全服务案例。

3. 请按本次询价采购的要求向我单位提交密封报价单及相关服务承诺等资料。报价文件请于2024年11月13日17点前以快递或直接送达方式送达（拒绝接受超时送达的报价单）。

4. 采购单位按照满足服务质量且报价合理的原则，由厅采购小组研究决定确定成交供应商。

5. 合同签订：成交单位接到成交通知书后三日内，到采购单位签订采购合同。询价文件、成交单位报价单和其他更优承诺等为签订合同的依据，按承诺时间供货和提供服务，如有违约行为，供应商将承担法律责任。

6. 具体违约条款及其它未尽事宜，将在双方签订合同时约定。

联系人：程建辉　87668723

福建省民族与宗教事务厅办公室

2024年11月6日

附件：询价内容及具体要求

服务项目	服务内容		服务提供方式
安全检测	网络安全检测	1、网络拓扑情况检查，包括网络拓扑设计的合理性，以及是否符合相关规定要求。	每季度一次 提供安全检测报告
		2、网络设备运行情况检查，确认网络设备是否运行良好	
		3、网络与信息安全产品运行检查，检查防火墙、入侵检测、入侵防御、数据库审计等产品的运行情况，确保网络安全产品正常运行，防护规则更新及时，防护策略有效配置。	
	服务器安全检测	1、服务优化，检查主机运行的服务是否遵循最小化原则，确保关闭不必要的服务，降低业务风险。	
		2、操作系统补丁检查，检查操作系统补丁是否按时更新，是否存在安全漏洞。	
		3、检查主机是否安装防病毒系统，病毒库是否为最新版本且定时升级，是否定期展开病毒查杀。	
		4、授权管理和访问控制检查，确认主机是否制定详细的授权管理和访问控制策略。	
		5、身份鉴别措施检查，检查主机是否合理配置口令的复杂度及锁定策略等，能否有效降低被暴力破解的可能性。	
		6、检查非必须的默认账号是否关停	
		7、通过漏洞扫描的方式检查服务器、操作系统和数据库是否存在安全漏洞和危险应用。	
	Web 安全检测	1、对所有对外网站进行安全漏洞扫描和验证，漏洞包括：sql 注入、xss 注入、恶意文件上传、命令执行等。	
		2、检查 WEB 应用防火墙日志，确保 WEB 应用防火墙良好运行无异常，对可疑的入侵事件进行排查和确认。	

		3、检查防篡改日志，确保网页防篡改系统良好运行无异常，对可疑的入侵事件进行排查和确认。	
		4、对网站进行 webshell 检查，确保网站没有被上传网页木马。	
		5、恶意外链检查，确保网站没有存在恶意外链。	
		6、系统后门检查：网站被入侵潜伏后，通常存在隐藏比较深的系统后门，重点发现绕过杀毒软件的系统后门。	
	帐号安全检测	1、检查操作系统是否存在多余默认账号和弱口令	
		2、检查数据库是否存在多余默认账号和弱口令	
	信息系统安全巡检	检测信息系统安全缺陷及风险，包括源代码危险函数使用、系统中身份认证安全、会话管理安全、上传下载、信息泄漏、数据验证等方面，评估系统在信息泄漏、数据破坏、身份仿冒等方面的安全风险。	
安全加固	网络结构及配置安全加固	针对安全巡检中发现的安全问题及突发性的安全漏洞对 WEB 源代码安全加固、网络结构及配置、服务器主机、数据库及应用系统进行全面加固，提高整体安全性能。	每季度一次 提供加固报告
	主机安全加固		
	数据库安全加固		
	信息系统安全加固		
日常监测	日常监测	对网站及信息系统页面可用性、篡改挂马、敏感信息、域名劫持、暗链接检测等提供 7*24 监测，发现问题及时响应。	7*24 小时

渗透测试	渗透测试	通过前期交互、情报搜集、威胁建模、漏洞分析、渗透攻击、后渗透攻击、报告等完整的渗透测试流程，模拟黑客攻击的方式验证甲方各信息系统的有效性；	每季度一次
风险评估	风险评估	对信息系统和现有的安全体系进行全面的安全风险评估，并提供整改建议。资产识别、脆弱性识别、漏洞扫描、威胁识别，风险分析，并撰写风险评估报告，拟定风险处理计划，提出整改方案。	每半年一次
应急演练	应急演练	根据信息安全应急预案制订信息安全应急预案演练方案，并根据应演练方案开展信息安全演练，演练内容包括安全漏洞爆发、web 入侵事件、系统入侵事件、拒绝服务攻击等常见的安全事件类型，按照应急预案实施应急响应完整过程并提供报告。	每半年一次
应急响应	应急响应	出现信息安全事件时，安排工程师到达现场提供信息安全技术支撑，协助甲方快速定位问题、消除事件影响、协助事件取证并提供如何避免类似事件的建议。	接到甲方通知后 2 小时内到达现场处理（重大安全事故 30 分钟内完成故障问题定位）
安全咨询、技术支持服务	安全防护	根据等保等要求协助做好相关网络安全制度、应急预案的制订、修订工作；派出技术人员协助内部网络安全及保密检查。	5*8 小时
	远程安全咨询服务	以电话或远程维护方式建立联系，提供 5*8 小时技术服务支持。	
重大活动安全保障	重大活动期间如数字中国、两会等安全保障	1、在遇到安全检查/敏感时期时，提前为甲方进行安全检查并加固网站及信息系统，调整安全防护措施，确保顺利通过安全检查/重大活动时期。	安全检查/重大活动时期
		2、在遇到安全检查/重大活动时期时，提前为甲方进行安全预演(即攻防演练)，确保甲方各部门、各科室明确遇到问题时，在第一时间该如何处置。	

		3、在甲方遇到主管或监管单位安全检查时，安全技术人员到场协助应对，确保检查顺利通过。	
		4、在重大活动期间安排值守人员提供 7*24 小时热线支撑，一旦发生安全事件立即响应，必要时到现场进行支撑。	
		5、在重大活动期间每天对甲方的信息系统进行安全状况检查，确认系统安全状况并提供报告。	

报 价 单

福建省民族与宗教事务厅办公室:

我方已认真阅读了贵单位发布的“福建省民族与宗教事务厅网站和信息系统安全服务项目”采购询价函，根据贵方提出的各项询价要求，现参与报价。详见附表。

报价单位:（盖章）

联系人:

联系电话:

时间: 年 月 日