项目采购需求

说明：

1.投标人提供的货物服务必须符合国家和行业标准。

2.标“★”为实质性参数要求和条件，投标人必须满足并在投标文件中如实作出响应，否则投标无效；标“▲”为重点指标；无标识的为一般指标。

3.投标人投标时必须在投标文件中对所有项目要求及技术需求内容、商务要求表中内容及附件内容（如有）逐条响应并一一对应。

4. 本项目采购所有分标标的对应的中小企业划分标准所属行业为：软件和信息技术服务业。

C 分标

一、技术参数、服务内容要求：			
序号	**标的名称**	**数量及单位**	**技术需求或者服务要求**
1	风险评估	1 项	1、项目内容: 根据《中华人民共和国网络安全法》及税务总局安全要求，由具有信息安全风险评估资质的机构对国家税务总局广西壮族自治区税务局的 8 个等保三级信息系统进行风险评估，对信息系统的资产、威胁、脆弱性进行识别分析，并对现有的管理制度和技术措施进行安全评估，提高重要信息系统防范风险的能力，风险评估出具的报告需具备产品质量评价、成果及司法鉴定，具有法律效力。 2、评估目标 （1）对现有的信息安全管理制度和技术措施的有效性进行风险评估。 （2）对信息系统的资产、威胁、脆弱性进行识别、分析。 （3）对信息系统的风险状况提出安全整改建议。 3、评估范围 包括：信息系统所涉及的物理环境、网络、主机、系统软件、应用软件、管理制度、人员等。 4、评估内容 （1）信息系统安全管理状况评估 评估国家税务总局广西壮族自治区税务局各种安全制度的建立情况。包括：终端计算机访问互联网的相关制度；终端计算机接入内网的相关制度；使用移动存储介质的制度；系统业务应用人员、系统的开发、维护、管理人员、维护人员相关的安全管理制度等。 （2）网络结构、网络安全设备状况评估

			评估范围包括：分析网络拓扑结构是否清晰划分网络边界；评估网络的访问控制措施。 （3）资产的脆弱性状况评估 评估内容包括机房评估，对机房环境，空调，防雷接地状况评估；网络评估，对交换机，路由器的口令设置和管理，配置文件的备份状况评估；安全评估，对防火墙、入侵检测系统、防病毒系统、桌面管理系统、审计系统评估；服务器评估，对服务器的口令、共享资源、系统服务安全、系统安全补丁、日志记录、木马检测进行评估。 （4）信息系统 评估信息系统，评估内容包括：数据库系统、应用数据、应用系统和数据库涉及到的主机操作系统。 5、评估依据 （1）适用的法律法规 （2）现有国际标准、国家标准、行业标准 （3）GBT 20984-2022 （信息安全技术 信息安全风险评估方法） （4）GB/T31509-2015 （信息安全技术 信息安全风险评估实施指南） （5）GB/T9361-2011 计算机场地安全要求 （6）GB17859-1999 计算机信息系统安全保护等级划分准则 （7）GB/T 18336.3-2015 信息安全技术 信息技术安全性评估准则 （8）GB/T 22081-2016 信息技术 信息安全管理实用规则 （9）国家税务总局对信息系统的安全要求和相关制度。 （10）信息系统本身的实时性或性能要求。
2	源代码审计	1 项	1、项目内容: 根据《中华人民共和国网络安全法》及税务总局安全要求，由具有软件系统检测资质的机构对 8 个等保三级信息系统进行应用系统源代码安全审计，从代码层面发现系统存在的安全缺陷，并形成源代码安全审计报告。 2、检测依据 安全检测主要依据以下标准: （1）GB/T 20271-2006《信息安全技术 信息系统安全通用技术要求》 （2）GB/T 34944-2017《Java 语言源代码漏洞测试规范》 （4）GBT 39412-2020《信息安全技术 代码安全审计规范》 （5）GB/T 28452-2012《信息安全技术 应用软件系统通用安全技术要求》 （6）GBT 20988-2007《信息安全技术 信息系统灾难恢复规范》 （7）GB/T 28458-2020《信息安全技术 网络安全漏洞标识与描述规范》 （8）GB/T 30279-2020《信息安全技术 网络安全漏洞分类分级指南》

			（9）CVE(Common Vulnerabilities & Exposures)公共漏洞字典表 （10）OWASP 十大 Web 漏洞（Open Web Application Security Project） 本项目相关文档，包括开发实施合同、需求规格说明书、系统详细设计、部署安装详细说明说、操作手册和功能列表等 3、检测分析 （1） 静态安全性测试分析 通过对源代码进行分析，检查出源代码中的缺点和错误信息，分析并找到这些问题引发的安全漏洞，并提供代码修订措施和建议。要求使用源代码审计工具对源代码进行完整的自动化审计工作，并得出结果报告。 自动化审计的内容包括: 1）前后台分离的运行架构 2）WEB 服务的目录权限分类 3）认证会话与应用平台的结合 4）数据库的配置规范 5）SQL 语句的编写规范 6）WEB 服务的权限配置 7）对抗爬虫引擎的处理措施 （2） 人工审查 自动化审计完成后，再由专业检测人员进行人工判断、分析，分析排除源代码漏洞中的误报内容，同时检查真实存在漏洞代码的关联点，查看是否有漏报，分析排查后最终获得较为准确的软件代码安全问题结果，并生成报告导出，作为正式报告编写的参考内容。
3	数据安全风险评估	1 项	1、项目内容: 根据《中华人民共和国网络安全法》、《中华人民共和国数据安全法》及总局相关文件要求聘请具有信息安全风险评估资质的机构对广西税务局 8 个等保三级信息系统进行数据安全风险评估，围绕数据和数据处理活动，聚焦可能影响数据的保密性、完整性、可用性和数据处理合理性的安全风险，通过信息调研识别数据处理者、业务和信息系统、数据资产、数据处理活动、安全措施等相关要素，然后从数据安全管理、数据处理活动、数据安全技术、个人信息保护等方面识别风险隐患，分析数据安全风险，出具数据安全风险评估报告，并给出整改建议。 2、评估目标 （1）摸清 8 个重要信息系统数据种类、规模、分布等基本情况； （2）摸清 8 个重要信息系统数据处理活动的情况； （3）发现可能影响国家安全、公共利益或者个人、组织合法权益的数据安全问题和风险；

			（4）发现共享、数据交换、委托处理等处理活动的数据安全问题和风险； （5）提供数据安全保护措施建议，提升数据安全保护能力。 4、评估内容 开展数据安全风险评估，围绕数据安全管理、数据处理活动安全、数据安全技术、个人信息保护等方面开展评估。 （1）数据安全管理 **从制度流程、组织机构、分类分级、人员管理、合作外包管理、安全威胁和应急管理、开发运维、云数据安全等方面进行评估。** （2）数据处理活动安全 **从数据收集、数据存储、数据传输、数据使用和加工、数据提供、数据公开、数据删除等方面进行评估。** （3）数据安全技术 从网络安全防护、身份鉴别与访问控制、监测预警、数据脱敏、数据防泄漏、接口安全、备份恢复、安全审计等方面进行评估。 （4）个人信息保护 **从基本原则、告知同意、保护义务、主体权利、投诉举报、个人信息处理、敏感个人信息保护、大型网络平台等方面涉及内容进行评估。** 5、评估依据 （1）适用的法律法规 （2）现有国际标准、国家标准、行业标准 （3）GBT 20984-2022 信息安全技术 信息安全风险评估方法 （4）GB/T31509-2015 信息安全技术 信息安全风险评估实施指南 （5）GB/T 43697-2024 数据安全技术 数据分类分级规则 （6）GB/T 35273—2020 信息安全技术 个人信息安全规范 （7）TC260-PG-20231A 网络安全标准实践指南——网络数据安全风险评估实施指引 （8）行业主管部门对业务系统的要求和制度 （9）系统相关单位的安全要求 （10）系统本身的实时性或性能要求
二、★商务要求			
1	合同签订日期	中标通知书发出后 25 日内。	
2	合同履约时间、服务地点	合同履约时间：签订合同之日至 2025 年 12 月 31 日。其中 2024 年度、2025 年度分别完成 1 次风险评估服务（含信息系统风险评估和源代码安全审计服务等）。 服务地点：广西区南宁市青秀区民族大道 105 号。	

3	报价要求	（1）本次报价须为人民币报价，只要填报了一个确定数额的总价，无论分项价格是否全部填报了相应的金额，报价应被视为已经包含了但并不限于本项目各项购买服务及相关服务等的费用和所需缴纳的所有价格、税、费。对于本文件中明确列明须报价的服务，供应商存在漏报的，将导致投标被否决。对于本文件中未列明，而供应商认为必需的费用也需列入总报价。在合同实施时，采购人将不予支付中标人没有列入的项目费用，并认为此项目的费用已包括在总报价中。 （2）超出采购预算价的，作无效标处理。评标委员会认为投标人的报价明显低于其他通过符合性审查投标人的报价，有可能影响产品质量或者不能诚信履约的，应当要求其在评审现场合理的时间内提供书面说明，必要时提交相关证明材料；投标人不能证明其报价合理性的，评标委员会应当将其作为无效投标处理。
4	付款方式	①完成 2024 年度风险评估服务（含信息系统风险评估和源代码安全审计服务等），并经采购人验收合格后，采购人向中标人支付合同总金额的 50%；完成 2025 年度风险评估服务（含信息系统风险评估和源代码安全审计服务等），采购人对项目进行验收，并根据项目验收标准及本项目合同罚责条款进行考核，按考核结果对合同服务费进行核算后，30 日内支付合同剩余款项 ②采购人付款前，中标人在申请付款时将同等金额、合法有效的发票开具给采购人，采购人在收到付款申请和发票后于 10 个工作日内支付。否则采购人有权顺延付款，并不承担延迟付款责任。
5	验收方式及标准	（1）验收条件：项目采购需求中包含的服务需求内容按期完成。服务内容、服务质量、服务成果以及组织管理和项目文档满足本采购文件的规定要求。 （2）验收标准：以本技术需求书中相关内容及其要求为依据，作为项目验收标准。供应商是否按照项目采购需求中定义的各项服务内容和服务管理开展各项工作，工作流程和结果是否符合采购人质量管理要求，是否在规定时间内提交相关工作文档。 （3）验收流程：符合项目验收条件后，供应商可提出项目验收书面申请，向采购人提交验收申请，向采购人整理提交项目相关管理、技术文档。采购人对项目工作内容及文档进行验收，项目验收通过后，采购人出具项目验收报告。
6	其他要求	1.信息安全保密要求 (1) 中标人须严格遵守国家税务总局广西壮族自治区税务局的安全保密制度。 (2) 中标人投入的项目人员须保证遵守国家有关版权和知识产权保护的政策、法律、法规和制度。 (3) 中标人投入的项目人员应对本项目中接触到的国家税务总局广西壮族自治区税务局所有的知识产权、商业秘密、技术成果等信息负保密义务。未经国家税务总局广西壮族自治区税务局书面同意，不得向社会公众或第三方通过任何途径出示、泄露，不得许可使用，不得对上述信息进行复制、传播、销售；保证不向外泄

		漏任何相关数据，不向外泄漏任何保密的技术资料。如出现支持人员泄密事件，中标人应负有连带责任。 (4) 中标人须与国家税务总局广西壮族自治区税务局签署合同项目实施期间的信息保密协议。 (5) 中标人投入的项目人员须与国家税务总局广西壮族自治区税务局签署合同项目实施期间的信息保密承诺书。 2.供应链安全管理要求 在项目采购需求中，中标人必须严格按照税务系统供应链安全管理的各项规定要求开展运维服务，包括但不限于: (1) 中标人销售的产品具备销售许可证、满足国家认可的网络安全规范和认证要求; (2) 中标人销售产品满足业务持续稳定运行时限需求的使用授权; (3) 中标人采用安全可控的方式、渠道，交付产品或开展服务等; (4) 中标人必须明确产品安全性，如不可利用产品的便利条件非法获取用户数据、控制和操纵用户系统和设备，不得在未授权情况下对产品进行升级或更新换代等; (5) 中标人必须明确安全责任和义务，如供应商对软硬件产品和服务的设计、研发、生产、交付等关键环节加强安全管理; (6) 中标人必须按照国家法律法规开展的安全审查、安全评估、渗透测试等; (7) 中标人必须设置声明条款，说明采购第三方产品、开源限制性、知识产权等情况。 3.网络安全和数据安全管理要求 中标人投入的项目人员在合同期间应严格按采购人的网络安全和数据安全相关规定开展工作，由于中标人投入的项目人员网络安全工作落实不到位引发安全事件的，采购人将视安全事件严重情况按合同金额的20%-30%的比例进行扣减。 安全事件具体内容主要包括(但不限于)以下内容: (1) 因补丁升级、漏洞修复、系统杀毒、数据备份、应用监控、网络监控等工作未落实到位，发生服务器被控制和应用系统被攻破的安全事件，被主管部门通报的。 (2) 因违规进行税费数据查询、导出和拷出等操作造成敏感数据泄漏，以及发生非法窃取数据行为。 (3) 因运维操作处置不当导致重要应用系统发生严重卡顿、停用的重大事件。 4.罚责条款 项目建设和运维过程中，因系统在对接、运行等服务中，导致其他系统受到影响的，由中标人负责组织相关服务厂商共同排查，明确问题根源、责任并报告采购

		人。中标人无法判定问题根源的，由中标人承担全部责任。采购人将根据问题的轻重、中标人责任的大小，扣除不高于合同总金额 5%的服务费用。
7	人员要求	至少提供项目经理 1 名；测评人员 5 人且具有 2 年或以上同类工作经验。
三、其他要求		
1	其他要求	投标人可以根据项目要求，在投标文件中提供包括但不限于：项目需求理解方案、实施方案、验收方案、人员、相关证书等。