

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 and 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。

A 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	等级保护测评服务	1 项	<p>1、总的要求</p> <p>由具备网络安全等级测评与检测资质的机构，依据《信息安全技术-网络安全等级保护基本要求》(GB/T 22239-2019) 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开展网络安全等级保护测评工作，并出具网络安全等级保护测评报告。</p> <p>2、标准依据</p> <p>《计算机信息系统安全保护等级划分准则》(GB 17859-1999)</p> <p>《网络安全等级保护基本要求》(GB/T 22239-2019)</p> <p>《网络安全等级保护测评要求》(GB/T 28448-2019)</p> <p>《网络安全等级保护测评过程指南》(GB/T 28449-2018)</p> <p>《网络安全等级保护设计技术要求》(GB/T 25070-2019)</p> <p>《网络安全等级保护测试评估技术指南》(GB/T 36627-2018)</p> <p>3、测评内容</p> <p>(1) 安全通用要求</p> <p>安全通用要求测评内容应包括安全技术和安全管理两大类。安全技术类应包括对安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心 5 个方面的测评。安全管理类测评应包括对安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理 5 个方面的测评。</p> <p>安全扩展要求</p> <p>本项目涉及等级保护对象涉及测评标准安全扩展要求(云计算、移动互联网、</p>

		<p>物联网、大数据、工业控制) 方面内容的, 投标人应该满足对被测评系统 2 个或以上网络环境的测评, 需根据实际情况选定适用的安全扩展要求测评内容开展本项目测评工作。</p> <p>4、测评方法</p> <p>在测评实施过程中, 应采用访谈、检查和测试、渗透测试等测评方法进行, 并与国家相关规范及标准的要求相符。</p> <p>访谈是指测评人员通过引导信息系统相关人员进行有目的的 (有针对性的) 交流以帮助测评人员理解、分析或取得证据的过程;</p> <p>检查是指测评人员通过对测评对象 (如管理制度、操作记录、安全配置等) 进行观察、查验、分析以帮助测评人员理解、分析或取得证据的过程;</p> <p>测试是测评人员使用预定的方法/工具使测评对象产生特定的行为, 通过查看和分析结果以帮助测评人员获取证据的过程;</p> <p>渗透测试是模拟黑客的攻击方法, 对受保护对象的应用系统、主机、网络进行攻击, 从而验证测评对象的弱点、技术缺陷或漏洞的一种评估方法。</p> <p>5、服务成果</p> <p>测评完成后, 对相应系统出具符合《网络安全等级保护基本要求》且公安机关认可的网络安全等级保护测评报告。</p> <p>6、服务团队</p> <p>至少提供项目经理 1 名【具备信息/网络安全等级测评证书(高级)】, 测评人员 6 人【具备信息/网络安全等级测评证书】, 测评人员具有 2 年或以上同类工作经验。</p>
二、★商务要求		
1	合同签订日期	中标通知书发出后 25 日内。
2	合同履行时间、服务地点	<p>合同履行时间: 签订合同之日起至 2025 年 12 月 31 日。其中 2024 年度、2025 年度分别完成 1 次等级保护测评服务。</p> <p>服务地点: 广西区南宁市青秀区民族大道 105 号。</p>
3	报价要求	<p>(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。</p> <p>(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</p>

		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	<p>①完成 2024 年度等级保护测评服务，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 年度等级保护测评服务，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。</p> <p>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。</p>
5	验收方式及标准	<p>(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。</p> <p>(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。</p> <p>(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。</p>
6	其他要求	<p>1. 信息安全保密要求</p> <p>(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。</p> <p>(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。</p> <p>(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。如出现泄密事件，中标人应负有连带责任。</p> <p>(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。</p> <p>(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。</p> <p>2. 供应链安全管理要求</p> <p>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：</p>

		<p>(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;</p> <p>(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;</p> <p>(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;</p> <p>(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;</p> <p>(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;</p> <p>(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;</p> <p>(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。</p> <p>3. 网络安全和数据安全管理要求</p> <p>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程度按合同金额的 20%-30%的比例进行扣减。</p> <p>安全事件具体内容主要包括(但不限于)以下内容:</p> <p>(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。</p> <p>(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。</p> <p>(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。</p> <p>4. 罚责条款</p> <p>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。</p>
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。

B 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	商用密码应用安全性评估服务	1 项	<p>一、总体要求</p> <p>依据《中华人民共和国密码法》、《信息安全技术 信息系统密码应用基本要求》(GB/T39786-2021) 要求和系统自身的安全需求分析,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开展商用密码应用安全性评估,为重要网络和信息系统的密码安全提供科学评价,逐步规范网络运营者的密码使用和管理行为。</p> <p>二、技术标准</p> <ol style="list-style-type: none"> 1. GB/T 39786—2021 《信息安全技术信息系统密码应用基本要求》 2. GM/T 0115—2021 《信息系统密码应用测评要求》 3. GM/T 0116—2021 《信息系统密码应用测评过程指南》 4. 《信息系统密码应用高风险判定指引》 5. 《商用密码应用安全性评估量化评估规则》 <p>三、服务内容</p> <p>(一) 信息系统应用方案商用密码应用性评估</p> <p>依据中国密码学会密评联委会发布的《商用密码应用安全性评估报告模板》(2023 版)对信息系统商用密码应用方案开展评估工作,并逐一出具《密码应用方案评估报告》。</p> <p>方案评估要点:</p> <ol style="list-style-type: none"> 1. 文档结构是否完整 2. 系统基本情况是否梳理充分 3. 密码应用需求是否清晰明确 4. 密码应用技术框架中密码协议、防护机制、密钥管理、密码应用子系统设计是否合理,能否满足安全需求和保障要求 5. 密码产品应用和部署设计是否合理、正确 6. 安全管理方案是否覆盖密码安全相关人员、制度、实施、应急等内容 7. 实施保障方案中实施计划是否科学、合理,组织管理方法和保障是否合理有效 <p>(二) 信息系统商用密码应用安全性评估</p> <p>依据《信息安全技术 信息系统密码应用基本要求》(GB/T39786-2021)等技术标准对国家税务总局广西壮族自治区税务局三级信息系统(每年测评系统数量不少于 8 个)进行商用密码应用安全性评估工作,并出具符合要求的《商用密码应用安全性评估报告》。</p> <p>1. 实施方式</p> <p>系统测评:及时发现系统脆弱性,识别变化的风险,了解系统安全状况,对照密码应用方案对系统开展测评。根据被测评对象的实际情况、所属</p>

		<p>行业及系统使用的密码产品情况，选择并确定测评依据。在系统真实环境下进行测评，以测评密码保障是否安全有效，密码使用是否合规、正确、有效。并通过测评发现系统存在的安全隐患和风险，提出可行性完善建议。</p> <p>密码技术应用测评：物理安全密码测评、网络安全密码测评、主机安全密码测评、应用安全密码测评、数据安全及备份恢复密码测评。测评验证不同安全等级信息系统的商用密码应用是否达到具有相应安全等级的安全保护能力，是否满足相应安全等级的保护要求。</p> <p>密钥管理测评：检测信息系统密钥管理各环节，包括对密钥的生成、存储、分发、导入、导出、使用、备份、恢复、归档与销毁等环节进行管理和策略制定的全过程是否符合要求。</p> <p>安全管理测评：对制度、人员、实施和应急等四个方面安全管理的测评，并协助完善商用密码应用安全性管理制度，协助完善密码相关系统运维管理制度。</p> <p>2. 评估成果</p> <p>针对被评估系统编制密码应用安全性评估报告，报告按照国家密码管理局要求包含的内容编制或参考模板编制。报告中应协助被评估单位认清风险，查找漏洞，找出差距，提出有针对性的加强完善密码安全管理和防护建议，并逐一出具商用密码应用安全性评估报告。</p> <p>（三）服务团队</p> <p>至少提供项目经理一名，测评人员 4 人，且具有 2 年以上同类工作经验，二线专家 2 人。</p>
二、★商务要求		
1	合同签订日期	中标通知书发出后 25 日内。
2	合同履行时间、服务地点	<p>合同履行时间：签订合同之日起至 2025 年 12 月 31 日。其中 2024 年度、2025 年度分别完成 1 次商用密码应用安全性评估服务。</p> <p>服务地点：广西区南宁市青秀区民族大道 105 号。</p>
3	报价要求	<p>（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。</p> <p>（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</p>

		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	<p>①完成 2024 年度商用密码应用安全性评估服务，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 年度商用密码应用安全性评估服务，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。</p> <p>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。</p>
5	验收方式及标准	<p>(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。</p> <p>(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项目管理开展各项工作，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。</p> <p>(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。</p>
6	其他要求	<p>1. 信息安全保密要求</p> <p>(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。</p> <p>(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。</p> <p>(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。</p> <p>(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。</p> <p>(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。</p>

	<p>2. 供应链安全管理要求</p> <p>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：</p> <p>(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；</p> <p>(2) 中标人销售产品满足业务持续稳定运行时需求的使用授权；</p> <p>(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；</p> <p>(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；</p> <p>(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；</p> <p>(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；</p> <p>(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。</p> <p>3. 网络安全和数据安全管理要求</p> <p>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程度按合同金额的 20%-30%的比例进行扣减。</p> <p>安全事件具体内容主要包括(但不限于)以下内容：</p> <p>(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。</p> <p>(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。</p> <p>(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。</p> <p>4. 罚责条款</p> <p>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。</p>
<p>三、其他要求</p>	

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。
---	------	---

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	<p>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。</p> <p>2、评估目标 (1) 对现有的信息安全管理制度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。</p> <p>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。</p> <p>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</p>

		<p>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。</p> <p>5、评估依据</p> <p>(1) 适用的法律法规</p> <p>(2) 现有国际标准、国家标准、行业标准</p> <p>(3) GBT 20984-2022 (信息安全技术 信息安全风险评估方法)</p> <p>(4) GB/T31509-2015 (信息安全技术 信息安全风险评估实施指南)</p> <p>(5) GB/T9361-2011 计算机场地安全要求</p> <p>(6) GB17859-1999 计算机信息系统安全保护等级划分准则</p> <p>(7) GB/T 18336.3-2015 信息安全技术 信息技术安全性评估准则</p> <p>(8) GB/T 22081-2016 信息技术 信息安全管理实用规则</p> <p>(9) 国家税务总局对信息系统的安全要求和相关制度。</p> <p>(10) 信息系统本身的实时性或性能要求。</p>
2	源代码审计	<p>1、项目内容:</p> <p>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。</p> <p>2、检测依据</p> <p>安全检测主要依据以下标准:</p> <p>(1) GB/T 20271-2006 《信息安全技术 信息系统安全通用技术要求》</p> <p>(2) GB/T 34944-2017 《Java 语言源代码漏洞测试规范》</p> <p>(4) GBT 39412-2020 《信息安全技术 代码安全审计规范》</p> <p>(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》</p> <p>(6) GBT 20988-2007 《信息安全技术 信息系统灾难恢复规范》</p> <p>(7) GB/T 28458-2020 《信息安全技术 网络安全漏洞标识与描述规范》</p> <p>(8) GB/T 30279-2020 《信息安全技术 网络安全漏洞分类分级指南》</p> <p>(9) CVE(Common Vulnerabilities & Exposures)公共漏洞字典表</p> <p>(10) OWASP 十大 Web 漏洞 (Open Web Application Security Project)</p> <p>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、部署安装详细说明书、操作手册和功能列表等</p> <p>3、检测分析</p> <p>(1) 静态安全性测试分析</p> <p>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。</p>

		<p>自动化审计的内容包括：</p> <ol style="list-style-type: none"> 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 <p>(2) 人工审查</p> <p>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。</p>
3	数据安全风险评估	<p>1、项目内容：</p> <p>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、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。</p> <p>2、评估目标</p> <ol style="list-style-type: none"> (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。 <p>4、评估内容</p> <p>开展数据安全风险评估，围绕数据安全、数据处理活动安全、数据安全、数据安全技术、个人信息保护等方面开展评估。</p> <p>(1) 数据安全</p> <p>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。</p> <p>(2) 数据处理活动安全</p>

		<p>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。</p> <p>(3) 数据安全技术</p> <p>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。</p> <p>(4) 个人信息保护</p> <p>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。</p> <p>5、评估依据</p> <p>(1) 适用的法律法规</p> <p>(2) 现有国际标准、国家标准、行业标准</p> <p>(3) GBT 20984-2022 信息安全技术 信息安全风险评估方法</p> <p>(4) GB/T31509-2015 信息安全技术 信息安全风险评估实施指南</p> <p>(5) GB/T 43697-2024 数据安全技术 数据分类分级规则</p> <p>(6) GB/T 35273—2020 信息安全技术 个人信息安全规范</p> <p>(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</p> <p>(8) 行业主管部门对业务系统的要求和制度</p> <p>(9) 系统相关单位的安全要求</p> <p>(10) 系统本身的实时性或性能要求</p>
二、★商务要求		
1	合同签订日期	中标通知书发出后 25 日内。
2	合同履行时间、服务地点	<p>合同履行时间：签订合同之日起至 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）。</p> <p>服务地点：广西区南宁市青秀区民族大道 105 号。</p>
3	报价要求	<p>(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。</p> <p>(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</p>

		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	<p>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</p> <p>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。</p>
5	验收方式及标准	<p>（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。</p> <p>（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。</p> <p>（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。</p>
6	其他要求	<p>1. 信息安全保密要求</p> <p>（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。</p> <p>（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。</p> <p>（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。</p> <p>（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。</p> <p>（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。</p> <p>2. 供应链安全管理要求</p> <p>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：</p>

		<p>(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;</p> <p>(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;</p> <p>(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;</p> <p>(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;</p> <p>(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;</p> <p>(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;</p> <p>(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。</p> <p>3. 网络安全和数据安全管理要求</p> <p>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程度按合同金额的 20%-30%的比例进行扣减。</p> <p>安全事件具体内容主要包括(但不限于)以下内容:</p> <p>(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。</p> <p>(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。</p> <p>(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。</p> <p>4. 罚责条款</p> <p>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。</p>
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。