第六章　项目采购需求

一、说明：

1.投标人提供的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投分标所有项目要求及技术需求内容、商务条款内容及附件内容（如有）逐条响应并一一对应。

二、采购内容：

本项目（A、B、C、D分标）采购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

<table>
<tr><td colspan="4">一、项目要求及技术需求</td></tr>
<tr><td>项号</td><td>服务名称
(标的名称)</td><td>数量及
单位</td><td>项目要求及技术需求</td></tr>
<tr><td>1</td><td>安全设备维保服务和驻场值守服务</td><td>1项</td><td>
一、服务内容
对国家税务总局广西壮族自治区税务局两个办公区相关核心网络安全设备提供自2024年10月14日起为期2年的维保服务，同时向采购人提供网络安全事件解决、网络安全隐患的排除及备份安全设备的相关数据库、操作系统等维护服务。
1.本次维保的相关核心网络安全设备：
（1）安全设备清单1
<table>
<tr><th>序号</th><th>位置</th><th>设备类型</th><th>数量</th><th>备注</th></tr>
<tr><td>1</td><td>广西税</td><td>千兆防火墙（启明天清汉马USG-FW-2000D-GXLT）</td><td>46台</td><td>提供自2024年</td></tr>
</table>
</td></tr>
</table>

				2	务民族办公区数据中心机房	千兆 IDS（启明天阗入侵检测 NT3000-LT-S-GXLT）	14 台	10 月 14 日起为期 2 年的维保服务	
				3		安全管理系统（启明泰合信息安全运营中心 TSOC-USM 标准版）	1 台		
				4		异常流量管理设备（启明天清异常流量管理与抗拒绝服务系统 ADM-GUARD-8800）	1 台		
				5		防火墙（启明天清汉马 USG-FW-12600GP 万兆）	20 台		
				6		入侵检测系统（启明天阗入侵检测 NT12000-LT-B 万兆）	3 台		
				7		网络安全审计系统（启明天玥审计系统 CA6500ER）	2 台		
				8		漏洞扫描系统（启明天镜脆弱性扫描系统 CSNS-H3）	1 台		
				9		4A 审计系统（启明天玥堡垒机 OSM-7200）	2 台		
				10		奇安信新一代威胁感知系统 V4.0 A58（控制平台）	1 台		
				11		奇安信一代威胁感知系统（探针）V4.0 S56	2 台		
				12		三未信安 SJJ1212	2 台		
				13	广西税务园湖办公区数据中心机房	下一代防火墙（H3C SecPath F5000）	2 台	提供自 2024 年 10 月 14 日起为期 2 年的维保服务	
				14		防火墙（启明天清汉马 USG-FW-12600GP 万兆）	10 台		
				15		流量分析审计（启明天玥网络安全审计系统 FA3000SE-R）	1 台		
				16		数据库审计（深信服 DAS-4300-JM）	1 台		
				17		网页防篡改（网神 SecWAF3600WPS）	2 台		
				18		堡垒机（久安世纪 LS-SOP 1500）	2 台		
				19		上网行为管理系统（深信服 AC-4300-CP）	1 台		

（2）安全设备清单 2

序号	品牌	型号	设备名称	数量	序列号
1	天融信	TopAudit	业务处理域网络审计系统	1 台	Q1604420311
2	天融信	NGFW4000-UF	业务处理域防火墙（备）	1 台	Q1604420031
3	天融信	NGFW4000-UF	业务处理域防火墙（主）	1 台	Q1604420032
4	天融信	NGFW4000-UF	外联网域（内）防火墙（备）	1 台	Q1406227638
5	天融信	NGFW4000-UF	外联网域（内）防火墙（主）	1 台	Q1406227639
6	天融信	NGFW4000-UF	外联网域（外）防火墙（备）	1 台	K1101057523
7	天融信	NGFW4000-UF	外联网域（外）防火墙（主）	1 台	K1101057533
8	天融信	TopAudit	业务服务域网络审计系统	1 台	Q1604420260
9	天融信	NGFW4000-UF	业务服务-防火墙（备）	1 台	Q1604420157
10	天融信	NGFW4000-UF	业务服务域-防火墙（主）	1 台	Q1604420033
11	天融信	TopAudit	4A 审计 01	1 台	Q1604420264
12	天融信	TopAudit	4A 审计 02	1 台	Q1604420261
13	天融信	NGFW4000-UF	运行保障域-防火墙（主）	1 台	Q1604420091
14	天融信	NGFW4000-UF	运行保障域-防火墙（备）	1 台	Q1604420095
15	天融信	NGFW4000-UF	安全支撑域防火墙（主）	1 台	Q1604420066
16	天融信	NGFW4000-UF	安全支撑域防火墙（备）	1 台	Q1604420064
17	天融信	NGFW4000-UF	遗留系统用防火墙（主）	1 台	Q1604420019

				18	天融信	NGFW4000-UF	遗留系统用防火墙（备）	1 台	Q1604420063	
				19	天融信	NGFW4000-UF	终端接入域防火墙（主）	1 台	Q1604420232	
				20	天融信	NGFW4000-UF	终端接入域防火墙（备）	1 台	Q1604420255	
				21	天融信	NGFW4000-UF	外联网域（外）防火墙（主）	1 台	Q131163231	
				22	天融信	NGFW4000-UF	外联网域（外）防火墙（备）	1 台	Q131163233	
				23	天融信	NGFW4000-UF	外联网域（内）防火墙（主）	1 台	Q131163232	
				24	天融信	NGFW4000-UF	外联网域（内）防火墙（备）	1 台	Q131163234	
				25	网神	G30-TAX68	网神 SecGate3600 防火墙	1 台	SSOS132729	
				26	网神	G30-TAX68	网神 SecGate3600 防火墙	1 台	SSOS132723	
				27	网神	G30-TAX68	税库银防火墙（外）	1 台	SSOC112578	
				28	网神	G30-TAX68	税库银防火墙（内）	1 台	SSOC110848	
				29	启明星辰	NS2200-F	天阗入侵检测与管理系统	1 台	10061102159953	
				30	启明星辰	NS2200-F	天阗入侵检测与管理系统	1 台	10061102159816	
				31	启明星辰	NS2200-F	互联网入侵检测系统 IDS 引擎	1 台	10061112301906	
				32	启明星辰	TSOC-FC-1900	园办互联网探针	1 台	NT00378552	
				33	卫士通	SHJ0901-B	卫士通服务器密码机	1 台	EW1Z214050416	
				34	卫士通	SHJ0901-B	卫士通服务器密码机	1 台	EW1Z214050413	
				35	卫士通	SHJ0901-B	卫士通服务器密码机	1 台	EW1Z214050437	
				36	卫士通	SHJ0901-B	卫士通服务器密码机	1 台	EW1Z214050351	

				37	卫士通	SHJ0901-B	卫士通服务器密码机	1 台	EW1Z214050426	
				38	卫士通	SHJ0901-B	卫士通服务器密码机	1 台	EW1Z214050436	
				39	德安	签名校验服务器	签名校验服务器	1 台	51903357	
				40	德安	签名校验服务器	签名校验服务器	1 台	51903356	
				41	德安	签名校验服务器	签名校验服务器	1 台	51903212	
				42	德安	签名校验服务器	签名校验服务器	1 台	51903210	
				43	德安	签名校验服务器	签名校验服务器	1 台	51903211	
				44	德安	签名校验服务器	签名校验服务器	1 台	51903213	
				45	德安	签名校验服务器	签名校验服务器	1 台	51903354	
				46	德安	签名校验服务器	签名校验服务器	1 台	51903355	
				47	上海普华	SRJ1302	普华签名验证服务器	1 台	201452026JP6VJL	
				48	上海普华	SRJ1302	普华签名验证服务器	1 台	2014520W8J6DB49	
				49	上海普华	SRJ1302	普华签名验证服务器	1 台	2015072403YGFUUM	
				50	上海普华	SRJ1302	普华签名验证服务器	1 台	20150724RNWTQVXU	
				51	上海普华	SRJ1302	普华签名验证服务器	1 台	20140520XP2BCQAZ	
				52	上海普华	SRJ1302	普华签名验证服务器	1 台	20140520YDAKB85P	
				53	上海普华	SRJ1302	普华签名验证服务器	1 台	20140520RXMCH2MC	
				54	深信服	AD9000	互联网域网闸负载均衡（主）	1 台	5101001522	
				55	深信服	AD9000	互联网域网闸负载均衡（备）	1 台	5101001524	

56	深信服	AD8050	内网域网闸负载均衡（主）	1 台	5101003860
57	安赛	WIDS2090	Web 漏洞感知系统 1	1 台	907CA1B1
58	安赛	WIDS2090	Web 漏洞感知系统 2	1 台	0B155A1B

2.维保服务要求

（1）针对采购人此次参保的安全设备，提供自 2024 年 10 月 14 日起为期 2 年的维保服务。

（2）采购人的机房核心网络安全设备提供技术支持和运行检查服务。

▲（3）为安全设备清单中设备提供每日 1 次的巡检服务并每月出具详细的巡检报告。

（4）要求设置客户代表与支持团队：为本次项目专门设立客户代表与支持团队，根据采购人的安全设备特点制定服务计划，并在维保服务实施中负责相关协调。

（5）远程技术支持服务：要求安排支持团队（支持团队人员不少于 4 名，支持团队人员必须是中标人的正式人员，或是与中标人签订 1 年以上劳动合同且实际工作满 1 年的人员，具有计算机技术与软件专业技术资格证书或 CISP 认证证书的优先，具有 2 年相关岗位工作经验）受理问题，提供全天候无间断的产品技术咨询、故障申报受理、硬件维修受理以及服务政策咨询等服务内容。

▲（6）工程师快速现场支持服务：考虑到采购人的网络组网复杂，运行有重要业务及设备，在核心网络出现问题时，需要及时排查并能迅速解决；要求在重大法定节假日、重大网络故障事件，重要切换、上线、变更、切换演练等大型网络变动时，提供以下现场支持服务：

（a）工程师快速到达现场支持；

（b）现场故障诊断及故障排除；

（c）现场软件升级。

本项目服务工程师到达现场的时间为 2 小时内到达。

★（7）特征库升级支持服务：在维保服务有效期内，要求向采购人提供防火墙、入侵检测系统、漏洞扫描系统、Web

			漏洞感知系统和威胁感知系统的特征库升级支持服务，升级内容包括但不限于特征库升级、威胁情报模块升级、威胁检测引擎版本升级和产品检测规则库升级等。 ▲（8）应急响应：要求为采购人提供重大安全事故和突发网络安全事件的随时应急响应服务。在采购人的核心网络因为安全设备故障发生网络瘫痪、网络入侵等重大安全事故时，必须第一时间提供现场应急技术支持。 要求 10 分钟内应急响应、2 小时内安全技术专家到达现场，处理问题并提出安全解决方案。由于硬件设备等原因不能立即解决的，提供临时解决方案建议，最大限度地保证采购人安全事件不升级及核心网络的正常运行。 ▲（9）快速原厂备件先行更换服务：要求提供及时周到的快速原厂备件更换服务。一旦定位是硬件故障无法及时解决，要求立即提供原厂备件服务，保证故障部件得到原厂备件的及时更换，以使采购人的业务在最短时间内恢复正常。 （10）要求为本项目指定一名客户代表（客户代表必须是中标人的正式人员，或是与中标人签订 1 年以上劳动合同且实际工作满 1 年的人员，具有 2 年相关岗位工作经验），针对本项目制定服务计划，联系服务资源，定期与技术人员交流，对维护情况进行回顾，组织和协调服务事宜，在现场服务时服从采购人的安排。 （11）要求在服务期内与采购人签订保密协议，承诺严格保护采购人的系统、数据、信息的安全，安排的工程师对工作过程中知悉的采购人资料和信息，除采购人作出相反的书面说明外，均视为采购人的商业秘密，未经采购人书面同意绝不向任何第三方泄漏。因违反保密义务而给采购人造成损失的将承担相应的赔偿责任。 ▲（12）维保设备档案管理服务：要求指定工程师收集并及时更新系统当前的设备资料，包括设备的型号、数量、序列号、硬件配置、操作系统版本、所安装软件及版本信息、系统配置脚本，建立设备资料库并提交给采购人，每次对设备改配后都对文档进行相应更新；建立维护历史资料库，记录每次维护的内容、处理方法、相关技术，与采购人共享这些资料，并在培训中对这些维护操作向采购人作详细介绍。 ▲（13）要求针对本次维保设备建立技术交流、培训机制。每年不定期地进行维保服务产品培训。培训内容主要针对实际维护工作，包括对产品系列的认识、日常管理、紧急故障处理办法、相关新技术的介绍等。 **3.安全值守运维服务要求** ▲（1）安全值守运维服务目标

			通过安全值守运维服务，降低设备故障率，提高设备运行性能，提高采购人的网络安全设备运行的稳定性、可靠性。以专业化运作模式解决采购人各类信息系统信息化发展的需求。需要提供故障诊断、远程支持、现场支持、软件升级、设备搬迁、网络优化、设备巡检、现场培训、技术交流、网络安全建议等服务。大体内容如下； （a）网络故障排查 （b）网络安全设备硬件状态检查 （c）网络流量检测 （d）安全策略配置及配置优化 （e）网络安全设备资料整理，配置参数整理 （f）网络安全设备使用状况趋势分析及建议 本次值守服务驻场地点为民族办公区机房和园湖办公区机房（南宁市青秀区民族大道 105 号、园湖南路 26 号），要求值守工程师按照采购人要求提供 7×8 小时的驻场运维服务（在重大关键时刻等特殊情况下，必须按照采购人要求提供 7×24 小时的驻场运维服务）。 （2）安全值守人员要求 本项目安全值守人员要求至少配备 5 名，安全值守人员必须是中标人的正式人员，或是与中标人签订 1 年以上劳动合同且实际工作满 1 年的人员，具有 CISP 认证证书的优先，具有 2 年相关岗位工作经验。 ▲（3）现场值守人员工作安排 （a）现场值守每日工作 对采购人的两个办公区机房安全设备每日一次巡检。 协助采购人每日开通防火墙、堡垒机的安全策略和梳理安全策略。 负责监控 IDS、WAF，封堵恶意 IP，解封误报 IP。 负责开通园办、民办办公终端入网申请和变更处理。 负责监控 360 天擎系统的违规外联，负责安全 U 盘运维。

			负责监控亚信虚拟终端运行情况。 负责监控国家税务总局安全保障网和“众测”平台的应用系统漏洞信息。 负责监控奇安信天眼威胁感知系统上的异常流量，提供恶意 IP 进行封堵。 负责监控 ITS 系统安全运行状况。 协助采购人各应用系统异常需要联调的各种工作。 （b）现场值守每周工作 负责提供防火墙、入侵检测系统、漏洞扫描系统、Web 漏洞感知系统和威胁感知系统的规则库升级工作。 负责升级奇安信天擎系统和安赛 Web 漏洞感知系统的补丁和系统版本。 负责升级金四安全管理平台的漏洞补丁。 负责升级亚信虚拟终端的漏洞补丁。 负责每周备份防火墙配置，负责定期将 WAF 安全日志导成 Excel 文件。 负责巡检园办安全设备、民办安全设备并每 2 天出具巡检报告。 （c）现场值守每月工作 安全设备每日巡检报告装订成册并提交。 负责 ITS 系统的审计报告生成，每个月出具一份。 负责启明泰合和安恒日志系统的每月分析报告生成。 负责奇安信天眼流量采集系统的每月分析报告生成。 负责安赛 Web 漏洞感知系统的每月分析报告生成。 负责打印每月安全策略申请单并随机抽验。 负责通过启明漏洞扫描系统开展每月的互联网应用漏扫并生成报告。 （d）现场值守每季度工作 负责“众测”平台的人工渗透，每 2 个月开展一次并生成报告。

负责启明泰合和安恒日志系统的每季度日志报告分析汇总。

负责启明漏洞扫描系统运维，每个季度开展一次全网漏扫并生成报告。

二、故障处理响应时间要求

故障级别	响应时间	到达现场时间	故障解决时间
一级故障	10 分钟	2 小时内	4 小时内
二级故障	10 分钟	2 小时内	8 小时内
三级故障	10 分钟	2 小时内	12 小时内

注：故障级别分类

根据故障的严重程度和影响程度的不同，故障级别由低到高分为三级故障、二级故障、一级故障。当故障没有在规定时限内恢复或解决时，故障级别将自动升级。

一级故障(重大故障)：最紧急，指设备或软件在运行中出现服务器宕机或系统瘫痪等导致服务中断、业务停止、数据丢失的故障。

二级故障(严重/主要故障)：紧急，指设备或软件在运行中出现的直接影响服务，导致系统性能或服务能力部分丧失的故障（如设备关键部件故障，系统响应速度大幅下降）；或具有潜在的系统瘫痪或服务中断的危险，可能导致设备或软件的基本功能不能实现的故障（如冗余设备单侧故障）等。

三级故障(一般/次要故障)：一般，除一、二级故障外的其他软硬件故障，指设备或软件在运行中出现的，轻微影响系统功能和性能（性能降低小于 20%），但关键业务不受影响的故障。

★三、服务方式

7×8 小时硬件故障保修，硬件设备发生故障后提供原厂备件更换，提供定期硬件巡检服务；要求在采购人的机房派遣 5 名值守工程师提供 7×8 小时的驻场运维服务（在重大关键时刻等特殊情况下，必须按照采购人要求提供 7×24 小时的驻场运维服务）。

四、验收要求

			1.验收条件：本需求书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采购文件的规定要求。 2.验收标准：以本需求书中相关内容及其要求为依据，作为项目验收标准。中标人是否按照本需求书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，中标人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。 **五、安全保障和罚则要求** ★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 （1）中标人应要求供应链厂商严格落实供应链安全管理各项规定，包括按照国家相关法律法规开展的安全审查、安全评估、渗透测试等，并将供应链厂商落实情况作为项目验收的检查内容。 （2）中标人应要求供应链厂商严格遵守采购合同、协议、承诺书等文件中的安全相关条款，对供应链厂商履行网络安全责任不到位、造成安全事件或产生不良影响的行为，采购人将视安全事件严重情况按合同总金额的20%-30%的比例

			进行扣减。 ★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总金额的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.罚则条款 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。采购人将视问题轻重、中标人责任大小等情况，按不高于合同总金额的5%的比例进行扣减。
二、商务条款			
合同签订日期	中标通知书发出后30日内。		
★服务期限、服务地点	1.服务期限：2年，从2024年10月14日至2026年10月13日止。 2.服务地点：国家税务总局广西壮族自治区税务局民族办公区机房和园湖办公区机房（南宁市青秀区民族大道105号、园湖南路26号）。		
★报价要求	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。
★付款方式	自提供运维服务且收到发票 10 个工作日内，采购人向中标人支付合同总金额的 25%作为预付款；中标人按合同约定提供服务期满一年，经采购人验收合格后且收到发票 10 个工作日内，采购人向中标人支付合同总金额的 25%；中标人按合同约定提供服务期满一年六个月，经采购人验收合格后且收到发票 10 个工作日内，采购人向中标人支付合同总金额的 25%；中标人按合同约定提供服务期满二年，经采购人验收合格后且收到发票 10 个工作日内，采购人向中标人支付合同剩余款项。 采购人付款前，中标人应向采购人开具等额有效的增值税发票，采购人未收到发票的，有权不予支付相应款项直至中标人提供合格发票，并不承担延迟付款责任。

B 分标

一、项目要求及技术需求			
项号	服务名称（标的名称）	数量及单位	项目要求及技术需求
1	重大时期网络安全保障服务	1 项	**一、服务内容** 本项目的服务目标是，通过本项目的建设，依托互联网资产排查，减少采购人的互联网测资产的暴露面和攻击面，提升采购人互联网侧防护能力，并通过提供重大时期安全保障服务，为采购人提供值守保障前期防护准备、值守保障期间安全监测及应急响应、保障结束的总结与整改支撑服务，专业的安全团队与采购人协同开展重大时期安全防护值守保障工作，全面提升采购人的安全监测防护能力，降低安全事件的发生概率，保障采购人的业务系统安全稳定运行。 **二、服务任务** 为有效应对实战化状态下的网络安全攻击，强化采购人的网络安全防护、检测、响应能力，降低业务系统被攻击、被利用的风险，强力提升采购人的网络安全防护能力，中标人需协同做好重大时期网络安全保障服务。具体内容如下： ★1、提供不少于 5 名熟悉采购人现有全流量高级威胁检测系统及网络安全环境架构的网络安全工程师，在重大时期对采购人的互联网应用提供 7×24 小时安全值守保障服务，每年值守保障总时间不少于 60 天。 ▲2、在安全值守保障前期，协助采购人做好准备工作，建立安全防护工作组织，确定安全防护职责及工作分工；制定安全值守工作方案，明确值守工作的人员分工、防护内容、值守计划等；制定响应的应急预案；本阶段中标人需提交《安全防护工作方案》。 ▲3、对采购人的互联网敏感资产进行全面的检测发现，发现互联网未知资产及高风险资产；对相关敏感信息资产进行排查和发现；协助采购人积极开展安全自查与加固工作；统筹开展采购人的互联网应用的渗透测试工作，挖掘可能被攻击利用的安全漏洞及风险；本阶段中标人需提交《互联网敏感资产发现报告》、《渗透测试报告》以及在自查与加固阶段输出的各类安全评估报告、加固报告等。

			▲4、渗透测试：中标人进行统筹协调，根据工作方案统筹开展采购人系统各业务的渗透测试工作，挖掘可能在演习中被攻击在利用的安全漏洞及风险。为确保在国家监管单位正式开展实战攻防演习前快速对采购人的应用系统进行渗透测试，中标人应充分利用自动化的渗透测试工具开展有关工作。 ★5、通过各类手段，对各类安全漏洞资讯进行整理和通告，做好安全预警工作；值守期间能 7×24 小时的对采购人的互联网应用的安全状态进行监控，并根据实际环境协助完善安全设备的告警规则，通过合理的规则配置，及时发现正在发生的安全事件以及现潜在的安全风险，并及时定位问题，处理问题。本阶段中标人需提交《安全预警通告》、《安全监测值守日报》、《应急响应处置报告》等。 ▲6、在安全值守保障期间，必须根据网络上披露的 0day 漏洞，实施更新采购人流量分析系统中的规则库，以实现对新漏洞的检测。 ▲7、在每个安全值守保障阶段结束后，协助采购人统一组织开展总结工作，报告中将详细记录保障过程、全面记录运行数据、深入总结保障经验、总结重点突出数据和经验，协助完善应急响应机制及预案，针对发现的安全漏洞及不足，制定技术方案进行整改加固。本阶段中标人需提交《安全值守总结报告》。 **★三、服务方式** 要求重大时期提供 7×24 小时的安全值守保障服务，每年值守保障总时间不少于 60 天，在安全值守期间能对网络攻击做预判分析，对安全事件能做溯源追踪，并完成相关安全事件报告。 **四、服务人员** 中标人提供重大时期网络安全保障服务，组建不少于 5 名网络安全工程师的运维团队提供安全值守保障服务，运维团队中人员必须是中标人的正式人员，或是与中标人签订 1 年以上劳动合同且实际工作满 1 年的人员，具有渗透测试相关资质认证（如 CISP-PTS 认证的安全服务工程师）或者计算机技术与软件专业技术资格证书优先，具有 2 年相关岗位工作经验；其中 1 名人员具有 Web 应用安全专家（CWASP）认证，1 名人员担任项目经理统筹和管理服务的实施。 **五、验收要求** 1.验收条件：本需求书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：以本需求书中相关内容及其要求为依据，作为项目验收标准。中标人是否按照本需求书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，中标人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。 **六、安全保障和罚则要求** ★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 （1）中标人应要求供应链厂商严格落实供应链安全管理各项规定，包括按照国家相关法律法规开展的安全审查、安全评估、渗透测试等，并将供应链厂商落实情况作为项目验收的检查内容。 （2）中标人应要求供应链厂商严格遵守采购合同、协议、承诺书等文件中的安全相关条款，对供应链厂商履行网络安全责任不到位、造成安全事件或产生不良影响的行为，采购人将视安全事件严重情况按合同总金额的 20%-30%的比例进行扣减。

			★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总金额的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.罚则条款 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。采购人将视问题轻重、中标人责任大小等情况，按不高于合同总金额的5%的比例进行扣减。
二、商务条款			
合同签订日期	中标通知书发出后30日内。		
★服务期限、服务地点	1.服务期限：2年，从2024年10月14日起至2026年10月13日止。 2.服务地点：南宁市青秀区民族大道105号。		
★报价要求	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。		

★付款方式	自提供运维服务且收到发票 10 个工作日内，采购人向中标人支付合同总金额的 25%作为预付款；中标人按合同约定提供服务期满一年，经采购人验收合格后且收到发票 10 个工作日内，采购人向中标人支付合同总金额的 25%；中标人按合同约定提供服务期满一年六个月，经采购人验收合格后且收到发票 10 个工作日内，采购人向中标人支付合同总金额的 25%；中标人按合同约定提供服务期满二年，经采购人验收合格后且收到发票 10 个工作日内，采购人向中标人支付合同剩余款项。 采购人付款前，中标人应向采购人开具等额有效的增值税发票，采购人未收到发票的，有权不予支付相应款项直至中标人提供合格发票，并不承担延迟付款责任。

C 分标

一、项目要求及技术需求			
项号	服务名称 (标的名称)	数量及 单位	项目要求及技术需求
1	数字证书系统运维服务	1 项	**一、服务范围** 国家税务总局广西壮族自治区税务局税务数字证书系统（含密码组件服务系统）主要包括： 1.RSA 算法税务数字证书注册系统 RA（内部）； 2.RSA 算法税务数字证书注册系统 RA（外部）； 3.RSA 算法税务数字证书发布系统（内部，包括 OCSP 和 LDAP）； 4.RSA 算法税务数字证书系统发布系统（外部，包括 OCSP 和 LDAP）； 5.SM2 算法税务数字证书注册系统 RA（内部）； 6.SM2 算法税务数字证书注册系统 RA（外部）； 7.SM2 算法税务数字证书发布系统（内部，包括 OCSP 和 LDAP）； 8.SM2 算法税务数字证书系统发布系统（外部，包括 OCSP 和 LDAP）； 9.SM2 算法税务 UKey 介质初始化系统； 10.RSA 算法签名认证系统； 11.SM2 算法签名认证系统。 12.密码服务组件系统。 以上所有子系统均在运维服务范围内。 **二、服务内容** 针对以上证书子系统，提供 7×8 小时的运维服务，具体运维内容如下：

			▲1.硬件巡检 每天对广西壮族自治区税务局税务数字证书系统涉及的通用服务器（含虚拟机）、签名验签服务器和密码机等设备进行硬件巡检，主要包括CPU、磁盘空间、内存使用率等。包括47台通用服务器（含虚拟机）、4台签名验签服务器、16台密码机。 2.网络联通性检查 通过堡垒机登录的方式，检查各服务器之间、采购人与国家税务总局之间的网络联通情况，对出现的网络问题及时进行排查修复。 ▲3.各证书子系统服务巡检及测试 每天通过监控日志、系统登录测试、功能自测等方式检查各系统的服务情况，包括证书发行、证书同步、证书介质灌装初始化和身份认证、签名验签、密码服务模块、协同签名模块等服务日志。 ▲4.数据备份巡检 每天定时检查各子系统之间的数据备份情况，对备份结果进行验证，防止因人员操作失误或服务器宕机造成数据丢失。 ▲5.补丁升级 根据网络安全需求，对国家税务总局下发的关于功能修复、优化的补丁进行升级。包括RA、OCSP、LDAP、签名服务器、密码机、密码服务资源管理模块、协同签名模块等相关补丁。 ▲6.漏洞修复 为保证数字证书系统安全运行，需对存在的漏洞进行补丁升级，如常见的弱口令、OpenSSH漏洞、中间件反序列化漏洞、strus漏洞、oracle数据库漏洞等。 7.组织培训 按照采购人要求，不定期组织系统培训服务，解答系统相关问题，便于采购人的工作人员学习掌握系统使用。 ▲8.知识库的整理和总结

			在提供税务数字证书系统运维服务过程中做好问题记录，不断更新、完善、整理常见问题，形成运维服务知识库，作为运维服务过程中重要的技术资料储备库，汇集在工作中遇到的典型案例归纳总结的知识要点和全面实用的资料手册，提高运维服务质量和效率。 **三、服务产出物** 《税务数字证书系统运维服务月报》 《月度税务数字证书系统巡检记录表》 《月度故障问题处理表》 《月度补丁升级记录表》 《月度电话技术咨询记录表》 **★四、服务方式** 采用远程运维服务方式，包括但不限于电话支持、网络支持以及现场支持等。 1.电话支持。每周 7 天，每天 8 小时的电话支持，对服务请求进行响应和答复，解决税务数字证书系统证书办理、证书使用过程中遇到的问题。 2.网络支持。通过电子邮件、微信在线交流等方式，解答税务数字证书系统和证书应用相关问题。 3.现场服务。遇到重大突发事件或远程无法解决的故障问题时，在服务期内不限次数派专业技术人员及时到现场予以解决。 **五、服务人员** 提供 3 名运维人员远程开展广西壮族自治区税务数字证书系统（含密码组件服务）的运维服务工作，运维人员必须是中标人的正式人员，或是与中标人签订 1 年以上劳动合同且实际工作满 1 年的人员，具备胜任运维服务工作岗位的资质、能力和水平，具有计算机技术与软件专业技术资格证书或 CISP 认证证书的优先，具有 3 年数字证书系统运维服务经验。同时提供 1 名高级技术支持人员，高级技术支持人员必须是中标人的正式人员，或是与中标人签订 1 年以上劳动合同且实际工作满 1 年的人员，遇到重大问题时及时解决，具有 8 年数字证书系统运维服务经验，具有 CISP 认

			证证书的优先。 **六、验收要求** 1.验收条件：本需求书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：以本需求书中相关内容及其要求为依据，作为项目验收标准。中标人是否按照本需求书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，中标人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。 **七、安全保障和罚则要求** ★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 （1）中标人应要求供应链厂商严格落实供应链安全管理各项规定，包括按照国家相关法律法规开展的安全审查、安全评估、渗透测试等，并将供应链厂商落实情况作为项目验收的检查内容。

			（2）中标人应要求供应链厂商严格遵守采购合同、协议、承诺书等文件中的安全相关条款，对供应链厂商履行网络安全责任不到位、造成安全事件或产生不良影响的行为，采购人将视安全事件严重情况按合同总金额的 20%-30%的比例进行扣减。 ★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总金额的 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.罚则条款 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。采购人将视问题轻重、中标人责任大小等情况，按不高于合同总金额的 5%的比例进行扣减。
2	双向安全交换系统运维服务	1 项	**一、服务范围** 双向安全交换系统、配套的通用服务器及安全设备。 **二、服务内容** 针对上述服务范围进行运维服务，具体服务内容如下： ▲1.设备巡检监控 提供 5×8 小时的设备现场监控和 7×24 小时的手机在线值班，以配合采购人的日常运营。驻场工程师的现场监控

任务不仅仅是简单的“告警监控”，而是参考警报和性能指标，通过不同的方式和性能数据进行诊断，以更有效地识别问题，挖掘故障根因，以确保可以快速、专业地处理可能发生的任何故障和告警。

2.系统维护

开展“双向”交换系统的日常运行维护工作，需开展常态化日常监控工作，对系统运行的计算存储资源进行监控，对系统日志信息进行整理分析，对系统配置和性能进行调优，开展系统健康检查，处理系统故障；负责系统的补丁升级工作；确保已经接入交互通道应用系统的稳定运行，并负责新建应用系统的交互通道接入；在应用系统出现故障时，配合应用系统进行故障排查。

▲3.接入双向的应用系统监控

对接入“双向”交换系统的应用系统运行情况进行监控，及时报告和处理应用系统在交互通道内的运行异常情况。及时报告各省“双向”交换系统的应用系统异常运行情况，以便通知各省及时处理。

▲4.告警事件处置

监测“双向”交换系统告警事件，对告警事件进行及时的报告和处理，保障每一个告警事件都能够得到及时有效的跟踪和处置。

5.统计报表

定期对“双向”交换系统内应用系统的运行情况出具报表，以便国家税务总局能够全面掌握应用系统的整体运行情况，报表周期为每月、季度、半年和整年。

定期对税务系统“双向”交换系统运维工作情况出具统计报表，报表周期为每月、季度、半年和整年。

三、服务产出物

序号	报告内容	频率
1	设备性能/容量报告	每周
2	设备告警报告	每周
3	配置变更报告	每月

4	预防性维护报告	每月
5	容灾演练复盘报告	半年
6	故障处理报告	按事件
7	月度工作总结报告	每月

★四、服务方式

采用驻场的服务方式，保障双向安全交换系统的正常运行。

五、服务人员

提供 1 名驻场运维人员开展 7×8 小时双向安全交换系统的运维工作，同时需指派一个合格的运维团队（人数不少于 3 名），包括但不限于项目经理、高级技术支持人员、售后技术支持人员等。驻场运维人员和运维团队人员，必须是中标人的正式人员，或是与中标人签订 1 年以上劳动合同且实际工作满 1 年的人员，具有 1 年双向安全交换系统运维工作经验，具有计算机技术与软件专业技术资格证书或 CISP 认证证书的优先。

六、验收要求

1.验收条件：本需求书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：以本需求书中相关内容及其要求为依据，作为项目验收标准。中标人是否按照本需求书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，中标人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。

七、安全保障和罚则要求

★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 （1）中标人应要求供应链厂商严格落实供应链安全管理各项规定，包括按照国家相关法律法规开展的安全审查、安全评估、渗透测试等，并将供应链厂商落实情况作为项目验收的检查内容。 （2）中标人应要求供应链厂商严格遵守采购合同、协议、承诺书等文件中的安全相关条款，对供应链厂商履行网络安全责任不到位、造成安全事件或产生不良影响的行为，采购人将视安全事件严重情况按合同总金额的 20%-30%的比例进行扣减。 ★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总金额的 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.罚则条款 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。采购人将视问题轻重、中标人责任大小等情况，按不高于合同总金额的5%的比例进行扣减。
二、商务条款			
合同签订日期			中标通知书发出后30日内。
★服务期限、服务地点			1.服务期限：2年，从2024年10月13日起至2026年10月14日止。 2.服务地点：国家税务总局广西壮族自治区税务局。
★报价要求			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。
★付款方式			自提供运维服务且收到发票10个工作日内，采购人向中标人支付合同总金额的25%作为预付款；中标人按合同约定提供服务期满一年，经采购人验收合格后且收到发票10个工作日内，采购人向中标人支付合同总金额的25%；中标人按合同约定提供服务期满一年六个月，经采购人验收合格后且收到发票10个工作日内，采购人向中标人支付合同总金额的25%；中标人按合同约定提供服务期满二年，经采购人验收合格后且收到发票10个工作日内，采购人向中标人支付合同剩余款项。 采购人付款前，中标人应向采购人开具等额有效的增值税发票，采购人未收到发票的，有权不予支付相应款项直至中标人提供合格发票，并不承担延迟付款责任。

D 分标

一、项目要求及技术需求			
项号	服务名称（标的名称）	数量及单位	项目要求及技术需求
1	金四网络安全管理平台运维服务	1 项	**一、项目背景** 为降低互联网办税系统遭受境内外网络攻击导致数据泄漏的风险，提升网络安全风险感知和预警处置能力，需开展“金四网络安全管理平台”的监测预警工作，要求采购 7×24 小时网络安全监控服务，提供不少于 5 名的驻场技术人员通过“金四网络安全管理平台”对各应用系统进行监控，及时发现并处置各种威胁行为；同时提供由不少于 8 名技术人员组成的后台运维支撑团队，每 2 个月开展一次安全资讯服务以及特殊时期的远程安全网络事件技术支撑服务。 **二、服务内容** 针对广西壮族自治区税务局金四安全管理平台运维服务，具体运维内容如下： （一）平台技术服务 提供“金四网络安全管理平台”产品使用咨询、配置变更、问题处理及日常维护等技术支持；提供平台的版本变更升级（补丁版本及功能性版本等）；提供“金四网络安全管理平台”定期巡检、周期性调整，推动故障处理，定期形成报告输出。 （二）安全运营服务 ▲1、资产识别与梳理：借助安全工具对用户及资产进行识别，并在后续服务过程中触发资产变更等相关服务流程，确保平台中资产信息的准确性和全面性。 ▲2、脆弱性管理：通过漏洞扫描工具及其他接入信息，对识别的漏洞进行优先级排序，协助采购人完成漏洞修补工作。 ▲3、策略管理：每月对安全组件上的安全策略进行统一管理工作，确保安全组件上的安全策略始终处于最优水平，

针对威胁能起到最好的防护效果。

▲4、持续攻击对抗：通过攻击日志分析，发现持续性攻击。

▲5、事件分析与处置：实时针对异常流量分析、攻击日志和病毒日志分析，聚合发现安全事件。针对分析得到的勒索病毒、挖矿病毒、篡改事件、webshell、僵尸网络等安全事件，通过工具和方法对恶意文件、代码进行根除，帮助采购人快速恢复业务，消除或减轻影响。

▲6、应急响应：通过事件检测分析，提供抑制手段，降低入侵影响，协助快速恢复业务，同时还原攻击路径，分析入侵事件原因，指导用户进行安全加固、提供整改建议、防止再次入侵。

▲7、主动分析与响应：每月主动分析病毒类、攻击类、漏洞利用类、失陷类的安全事件，并提供相应解决方案。

▲8、威胁通告与排查：结合威胁情报，安全专家排查是否对用户资产造成威胁并通知用户，协助及时进行安全加固。

（三）安全技术服务

协助采购人完成“金四网络安全管理平台”内部的安全事件分析、风险处置建议、安全事件应急响应、事件回溯等工作。

（四）重保服务

针对大征期、重要节庆日提供“金四网络安全管理平台”的 7×24 小时全面保障服务，制定专项保障方案，提升巡检和监控频率，专人值守及时解决问题，编写重保报告。

三、服务响应时间

按照下表要求对使用单位的系统软件故障技术支持服务请求进行响应：

序号	故障级别（严重程度）	响应时间	故障解决时间
1	系统瘫痪，“金四网络安全管理平台”不能运转的	0.5 小时内	1 小时内
2	系统部分出现故障，“金四网络安全管理平台”仍能运转	1 小时内	2 小时内
3	初步诊断为系统软件问题，只造成“金四网络安全管理平台”性能下降	1 小时内	4 小时内

			★四、服务方式 本项目采用驻场运维服务方式+后台运维支撑服务方式。提供不少于5名的驻场技术人员提供7×24小时驻场服务，通过“金四网络安全管理平台”对各应用系统开展7×24小时监控，及时发现并处置各种威胁行为；同时提供不少于8名技术人员的后台运维支撑团队，每2个月开展一次安全资讯服务以及特殊时期的远程安全网络事件技术支撑服务。 **五、服务人员** 提供不少于5名的驻场技术人员提供7×24小时驻场服务，提供不少于8名的后台运维支撑团队。驻场技术人员和后台运维支撑团队人员，必须是中标人的正式人员，或是与中标人签订1年以上劳动合同且实际工作满1年的人员，具备胜任运维服务工作岗位的资质、能力和水平，具有计算机技术与软件专业技术资格证书或CISP认证证书的优先，具有2年相关岗位工作经验。 **六、投入技术人员要求** （一）驻场技术人员要求 要求驻场技术人员数量不少于5名，需提供7×24小时驻场运维服务，具体人员要求如下： （1）熟悉linux操作系统，具备服务器、存储等计算机知识，了解计算机体系架构， 内外部设备， 网络知识； （2）熟悉java、python、shell语言，有相关项目经验； （3）有分析和定位问题的能力，有独立解决问题能力，有较好的沟通能力；能顺利完成“金四网络安全管理平台”的资产录入、安全监控、安全响应和“金四网络安全管理平台”的运维升级、漏洞扫描、补丁发布等相关技术工作，能及时完成国家税务总局绩效考核相关技术要求工作。 （二）后台运维支撑团队要求 要求后台运维支撑团队人员数量不少于8名，需提供紧急现场支持服务，能在发生紧急安全事件时及时到达现场快速完成网络安全攻击定位、阻断拦截、溯源分析、威胁清除等工作，并出具网络安全事件分析报告；能针对现有环境下的安全威胁和安全隐患提出切实有效的整改建议；每2个月开展一次安全资讯服务以及特殊时期的远程安全网络事件技术支撑服务。出具服务报告的内容包含定期收集和整理安全漏洞信息、网络病毒活动信息和安全舆情信息，并

			进行整理和分析，编制《安全通告》并就如何有效开展威胁定位和威胁消除提出具体工作建议等内容。 **七、验收要求** 1.验收条件：本需求书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：以本需求书中相关内容及其要求为依据，作为项目验收标准。中标人是否按照本需求书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，中标人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。 **八.安全保障和罚则要求** ★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 （1）中标人应要求供应链厂商严格落实供应链安全管理各项规定，包括按照国家相关法律法规开展的安全审查、安全评估、渗透测试等，并将供应链厂商落实情况作为项目验收的检查内容。

			（2）中标人应要求供应链厂商严格遵守采购合同、协议、承诺书等文件中的安全相关条款，对供应链厂商履行网络安全责任不到位、造成安全事件或产生不良影响的行为，采购人将视安全事件严重情况按合同总金额的20%-30%的比例进行扣减。 ★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总金额的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.罚则条款 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。采购人将视问题轻重、中标人责任大小等情况，按不高于合同总金额的5%的比例进行扣减。
二、商务条款			
合同签订日期			中标通知书发出后30日内。
★服务期限、服务地点			1.服务期限：2年，具体时间以合同签订时间为准。 2.服务地点：国家税务总局广西壮族自治区税务局民族办公区机房（南宁市青秀区民族大道105号）。

★报价要求	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。
★付款方式	自提供运维服务且收到发票 10 个工作日内，采购人向中标人支付合同总金额的 25%作为预付款；中标人按合同约定提供服务期满一年，经采购人验收合格后且收到发票 10 个工作日内，采购人向中标人支付合同总金额的 25%；中标人按合同约定提供服务期满一年六个月，经采购人验收合格后且收到发票 10 个工作日内，采购人向中标人支付合同总金额的 25%；中标人按合同约定提供服务期满二年，经采购人验收合格后且收到发票 10 个工作日内，采购人向中标人支付合同剩余款项。 采购人付款前，中标人应向采购人开具等额有效的增值税发票，采购人未收到发票的，有权不予支付相应款项直至中标人提供合格发票，并不承担延迟付款责任。