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。

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、商务要求表中内容及附件内容（如有）逐条响应并一一对应。

二、采购内容： 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="3">一、技术参数、服务内容要求：</td></tr>
<tr><td>服务名称</td><td>数量</td><td>服务内容及服务要求</td></tr>
<tr><td>安全设备维保及安全驻场服务</td><td>1项</td><td>
1、需要维保设备清单
本次维保项目包含广西税务局两个办公区相关核心网络安全设备的维保服务，同时向广西税务局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，以下为本次维保设备的详细清单：
1.1 民办、园办中心机房需维保的设备清单如下所示：
<table>
<tr><td>编号</td><td>位置</td><td>设备类型</td><td>数量</td><td>备注</td></tr>
<tr><td>1</td><td rowspan="5">广西税务民族办公区数据中心机房</td><td>千兆防火墙（启明天清汉马 USG-FW-2000D-GXLT）</td><td>46</td><td rowspan="5">维保服务期2年</td></tr>
<tr><td>2</td><td>千兆 IDS（启明天阗入侵检测 NT3000-LT-S-GXLT）</td><td>14</td></tr>
<tr><td>3</td><td>安全管理系统（启明泰合信息安全运营中心 TSOC-USM 标准版）</td><td>1</td></tr>
<tr><td>4</td><td>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）</td><td>1</td></tr>
<tr><td>5</td><td>防火墙（启明天清汉马 USG-FW-12600GP 万兆）</td><td>20</td></tr>
</table>
</td></tr>
</table>

		6		入侵检测系统（启明天阗入侵检测 NT12000-LT-B 万兆）	3	
		7		网络安全审计系统（启明天玥审计系统 CA6500ER）	2	
		8		漏洞扫描系统（启明天镜脆弱性扫描系统 CSNS-H3）	1	
		9		4A 审计系统（启明天玥堡垒机 OSM-7200）	2	
		10		奇安信新一代威胁感知系统 V4.0 A58（控制平台）	1	
		11		奇安信新一代威胁感知系统 V4.0 S56（探针）	2	
		12	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	
		13		防火墙(启明天清汉马 USG-FW-12600GP 万兆）	10	
		14		流量分析审计（启明天玥网络安全审计系统 FA3000SE-R）	1	
		15		数据库审计（深信服 DAS-4300-JM）	1	
		16		网页防篡改（网神 SecWAF3600WPS）	2	
		17		堡垒机（久安世纪 LS-SOP 1500）	2	
		18		上网行为管理系统（深信服 AC-4300-CP）	1	

1.2 园办中心机房需维保的设备清单如下所示：

编号	型号	用途	序列号
1	TopAudit	业务处理域网络审计系统	Q1604420311
2	NGFW4000-UF	业务处理域防火墙（备）	Q1604420031
3	NGFW4000-UF	业务处理域防火墙（主）	Q1604420032
4	NGFW4000-UF	外联网域（内）防火墙（备）	Q1406227638

		5	NGFW4000-UF	外联网域（内）防火墙（主）	Q1406227639	
		6	NGFW4000-UF	外联网域（外）防火墙（备）	K1101057523	
		7	NGFW4000-UF	外联网域（外）防火墙（主）	K1101057533	
		8	TopAudit	业务服务域网络审计系统	Q1604420260	
		9	NGFW4000-UF	业务服务-防火墙（备）	Q1604420157	
		10	NGFW4000-UF	业务服务域-防火墙（主）	Q1604420033	
		11	TopAudit	4A 审计 01	Q1604420264	
		12	TopAudit	4A 审计 02	Q1604420261	
		13	NGFW4000-UF	运行保障域-防火墙（主）	Q1604420091	
		14	NGFW4000-UF	运行保障域-防火墙（备）	Q1604420095	
		15	NGFW4000-UF	安全支撑域防火墙（主）	Q1604420066	
		16	NGFW4000-UF	安全支撑域防火墙（备）	Q1604420064	
		17	NGFW4000-UF	遗留系统用防火墙（主）	Q1604420019	
		18	NGFW4000-UF	遗留系统用防火墙（备）	Q1604420063	
		19	NGFW4000-UF	终端接入域防火墙（主）	Q1604420232	
		20	NGFW4000-UF	终端接入域防火墙（备）	Q1604420255	
		21	NGFW4000-UF	外联网域（外）防火墙（主）	Q131163231	
		22	NGFW4000-UF	外联网域（外）防火墙（备）	Q131163233	
		23	NGFW4000-UF	外联网域（内）防火墙（主）	Q131163232	
		24	NGFW4000-UF	外联网域（内）防火墙（备）	Q131163234	
		25	G30-TAX68	网神 SecGate3600 防火墙	SSOS132729	
		26	G30-TAX68	网神 SecGate3600 防火墙	SSOS132723	
		27	G30-TAX68	税库银防火墙（外）	SSOC112578	
		28	G30-TAX68	税库银防火墙（内）	SSOC110848	
		29	NS2200-F	天阗入侵检测与管理系统	10061102159953	
		30	NS2200-F	天阗入侵检测与管理系统	10061102159816	
		31	NS2200-F	互联网入侵检测系统 IDS 引擎	10061112301906	
		32	TSOC-FC-1900	园办互联网探针	NT00378552	
		33	SHJ0901-B	卫士通服务器密码机	EW1Z214050416	
		34	SHJ0901-B	卫士通服务器密码机	EW1Z214050413	
		35	SHJ0901-B	卫士通服务器密码机	EW1Z214050437	
		36	SHJ0901-B	卫士通服务器密码机	EW1Z214050351	
		37	SHJ0901-B	卫士通服务器密码机	EW1Z214050426	
		38	SHJ0901-B	卫士通服务器密码机	EW1Z214050436	
		39	签名校验服务器	签名校验服务器	51903357	
		40	签名校验服务器	签名校验服务器	51903356	
		41	签名校验服务器	签名校验服务器	51903212	
		42	签名校验服务器	签名校验服务器	51903210	
		43	签名校验服务器	签名校验服务器	51903211	
		44	签名校验服务器	签名校验服务器	51903213	
		45	签名校验服务器	签名校验服务器	51903354	
		46	签名校验服务器	签名校验服务器	51903355	

47	SRJ1302	普华签名验证服务器	201452026JP6VJL
48	SRJ1302	普华签名验证服务器	2014520W8J6DB49
49	SRJ1302	普华签名验证服务器	2015072403YGFUUM
50	SRJ1302	普华签名验证服务器	20150724RNWTQVXU
51	SRJ1302	普华签名验证服务器	20140520XP2BCQAZ
52	SRJ1302	普华签名验证服务器	20140520YDAKB85P
53	SRJ1302	普华签名验证服务器	20140520RXMCH2MC
54	AD9000	互联网域网闸负载均衡（主）	5101001522
55	AD9000	互联网域网闸负载均衡（备）	5101001524
56	AD8050	内网域网闸负载均衡（主）	5101003860
57	千兆网闸	内网与互联网数据交换网闸	G0097FUTH
58	千兆网闸	内网与互联网数据交换网闸	G0097FUTH
59	千兆网闸	内网与互联网数据交换网闸	G0097FUTH
60	千兆网闸	内网与互联网数据交换网闸	G0097FUTH

2、维保服务目标

以上安全设备生产厂家为北京启明星辰信息安全技术有限公司（以下简称“启明星辰”）、天融信网络安全技术有限公司（以下简称“天融信”）、深信服科技股份有限公司（以下简称“深信服”）、上海普华科技发展股份有限公司（以下简称“上海普华”）、网神信息技术(北京)股份有限公司（以下简称“网神”）、卫士通信息产业股份有限公司（以下简称“卫士通”），为确保能迅速解决广西税务局核心网络安全事件，排除网络安全隐患，保证广西税务局核心网络及其承载各项业务的稳定运行，建议运维供应商采购原厂维保服务。

针对中标供应商为本次项目提供 2 年安全设备维保服务，同时根据日常维护的数据和记录进行分析，更好的为采购人的信息化发展提供有力的保障。

维保服务要求中标供应商能对采购人现有的安全设备进行跟踪管理，及时掌握采购人的安全系统运行现状，反映出采购人全网络安全设备的可用性情况和健康状况，创建一个可知可控的安全运维环境,从而确保安全设备能为采购人税收业务系统提供可靠、高效、持续、安全的运行环境。

3、维保服务内容

3.1、一站式服务

要求中标供应商提供一站式服务模式，即采购人在维保服务期内以上列表中的安全设备出现故障后，只要拨打专用电话后，接下来的确认故障、预约上门时间、上门服务、满意度回访等工作。

服务过程记录

采购人信息中心一旦报故障一次，终端信息、故障信息、服务过程等信息就会被记录下来，今后如再次报故障，可以马上查找到相关错误信息和资料，指导工程师能做出有更针对性的服务。

快速派单

采购人信息中心报故障后，要求工程师判定后确定需要做出现场支持服务，马上派出相应的工程师前往解决。

服务过程监控

监控工程师是否在承诺的时间内做出响应，是否是指定工程师上门服务，修复时间是否符合标准等关键服务指标。

故障分析系统

根据采购人所报故障的信息和服务过程信息，根据需求做数据分析，并将常见故障、批量问题、使用问题等关键信息提取出来，供项目负责人做出分析和预防改进方案。

3.2、故障分级响应服务

3.2.1 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、二级故障外的其它软硬件故障，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。

3.2.2 报障与响应时间

要求运维服务的故障响应时间为 10 分钟，并于 2 小时内到达现场进行处理。

3.2.3 故障解决时间

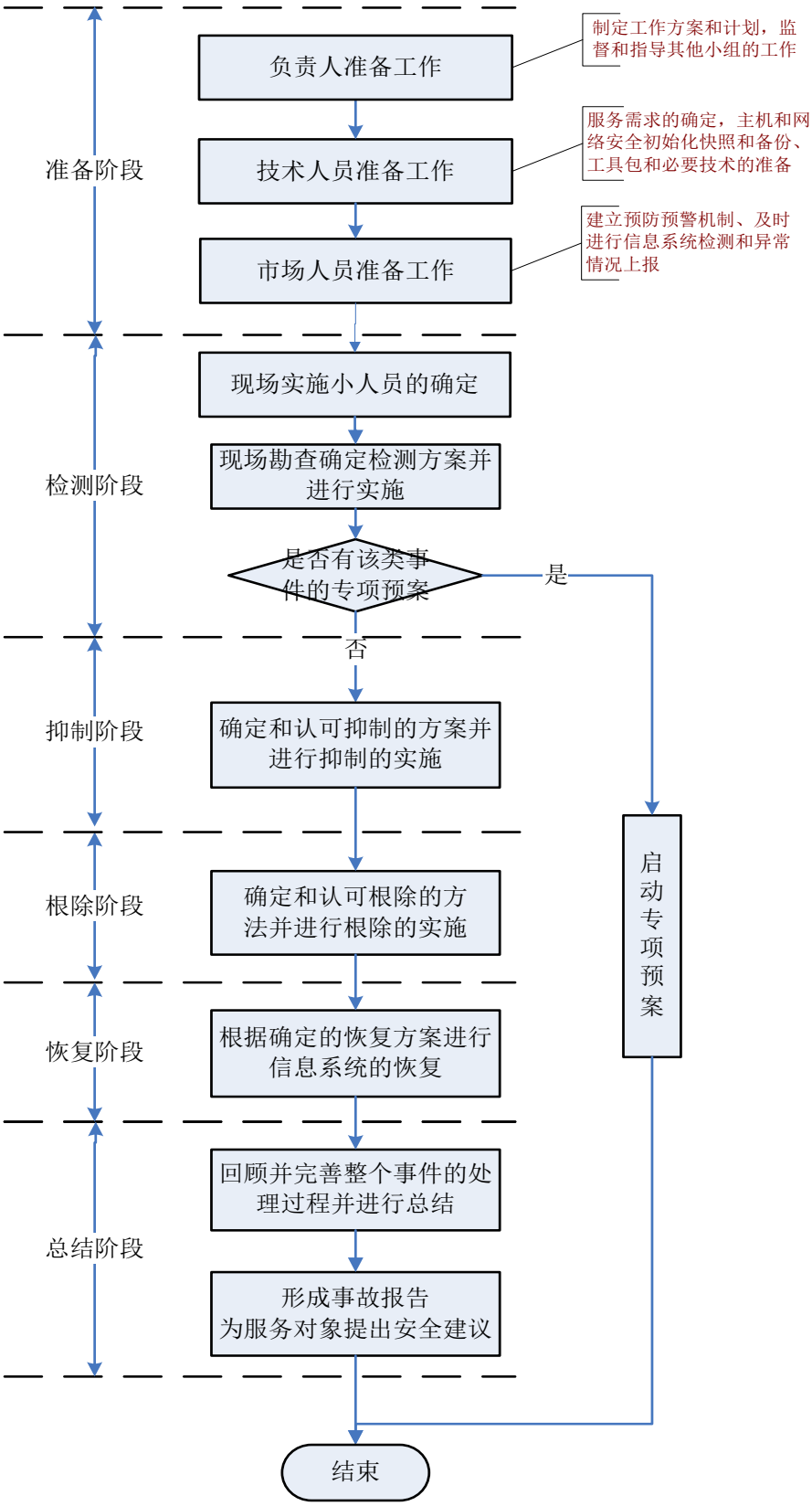
技术专家在规定时间到达现场，即开始不间断工作，直到故障排除。对于影响业务的一级故障，在进行故障处理时，要求运维服务必须优先考虑业务恢复，然后再彻底解决故障。

根据故障级别，分级响应的故障解决时间如下：

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

3.3、应急响应流程

以下服务流程并非一个固定不变的教条，需要应急响应服务人员在实际中灵活变通，可适当简化，但任何变通都必须纪录有关的原因。详细的记录对于找出事件的真相、查出威胁的来源与安全弱点、找到问题正确的解决方法，甚至判定事故的责任，避免同类事件的发生。



3.4、安装支持服务

当维保设备清单中的设备需要进行升级扩容时，中标供应商提供升级硬件的安装支持；提供操作系统或操作系统级相关软件的安装支持；安排的工程师将定期在设备配置信息库中更新相应记录。

3.5、硬件维保服务

		对维保设备清单中的硬件，一旦故障发生，将提供最高优先级的现场维护，准确地排除故障，恢复系统的正常运行。当采购人设备出现故障在规定的时间内不能修复，中标供应商要提供同等功能的设备供采购人使用，直至故障修复为止。在得到采购人确认后维保工程师才能离开现场 **3.6、远程支持服务** 对于现场值班人员不能解决的故障，在征得采购人同意后，通过二线技术专家远程接入手段，登录到故障设备或软件，进行故障诊断，查找故障出现的原因，指导现场维护人员处理故障。 **3.7、事件库升级支持服务** 在服务有效期内，中标供应商向采购人提供此次参保设备的一体化安全网关的事件库升级、入侵检查设备事件库升级，并根据升级内容制定详细的实施方案。 **3.8、定期巡检服务** 巡检目的 了解采购人设备使用状况，延长设备正常运行时间和质量，提高工作效率； 消除隐患，降低故障率，节约设备使用投入； 了解采购人的服务需求，不断改进服务质量，提供更加贴身的服务。 巡检内容 检查场地环境； 检查系统运行的历史记录及错误记录； 优化系统环境； 针对核心安全设备，检查接受服务的设备配置及状态情况； 运行诊断程序测试各部分子系统是否正常； 预防性维护回顾及相应的技术指导和建议； 对服务过程中发生故障的设备进行及时处理。 巡检计划 签订合同后一个月内对相关设备进行统计并建立档案，定制维护计划。 巡检记录 每次巡检都要做详细的记录。 巡检报告 巡检结束后，巡检人员要做进一步的数据分析，给出设备使用意见，并向信息中心提交巡检报告。 **4、维保服务要求** 针对广西税务局网络安全防护设备维保项目，要求提供如下维保服务： （1）针对广西税务局此次参保的安全设备，要求提供 2 年的安全设备维保服务。 （2）要求提供广西税务局民办、园办机房核心网络安全设备的技术支持和运行检查服务。 （3）要求提供设备维保清单中设备每日 1 次的巡检服务并每月出具详细的巡检报告。 （4）要求设置服务经理与支持团队：为本次项目专门设立客户服务经理与支持团队，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：要求安排专职维护团队受理问题，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，采购人要求提供现场技术支持时，提供以下现场支持服务：

		1）工程师快速到达现场支持； 现场故障诊断及故障排除； 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：在服务有效期内，要求向采购人提供此次参保设备中的一体化安全网关、入侵检测、漏洞扫描系统和威胁感知系统的特征库升级服务，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，确保以上安全设备的正常运行。** （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的正常运行。 （9）快速备件先行更换服务：要求提供及时周到的快速备件更换服务。一旦定位是硬件故障无法及时解决，要求提供备机服务，保证故障部件得到及时更换，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，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。 **5.安全驻场服务** （1）安全驻场服务目标 通过安全驻场服务，降低设备故障率，提高设备运行性能，提高采购人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； 网络故障排查 网络安全设备硬件状态检查 网络流量检测 安全策略配置及配置优化 网络安全设备资料整理，配置参数整理 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广西税务局机房（南宁市民族大道 105 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，重大时期配合其他安全厂商联合开展 7×24 小时安全值守服务。 （2）安全值守人员要求 本次值守人员要求至少配备 5 人，其中至少包含 2 名具有 CISP 认证的安全服务工程师。 （3）现场值守人员工作安排 3.1、现场值守每日工作 每日一次对广西税务两个办公区安全设备巡检。 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。 3.2、现场值守每周工作 负责升级现有 8 台 WAF 规则库和系统版本。 负责升级奇安信天擎系统的漏洞补丁和系统版本。 负责升级天融信态势感知系统的漏洞补丁。 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，负责每 2 天将 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。 3.3、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。 3.4、现场值守每季度工作 负责“众测”平台的人工渗透，每个季度开展一次并生成报告。 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。 6.其他要求 ★（1）信息安全保密要求 1）必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）项目人员需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)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，中标供应商应负有连带责任。 4)中标供应商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)项目人员必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）中标供应商运维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，由于中标供应商运维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。 ★（3）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，由中标供应商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。中标供应商无法判定问题根源的，由中标供应商承担全部责任。采购人将根据问题的轻重、中标供应商责任的大小，扣除不高于合同款 5%服务金额。
二、商务条款要求：		
★项目服务地点		广西区内采购人指定地点。
★项目服务期限		自合同签订之日起 2 年。
★付款方式		合同签订后 30 日内采购人支付合同金额的 25%；运维期满 1 年，支付合同金额的 35%；运维期满 2 年，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则条款进行考核，按考核结果对合同服务费进行核算后，30 日内支付合同相应的剩余款项。采购人付款前，中标供应商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供应商提供合格发票，并不承担延迟付款责任。
★验收方法		1.中标供应商履约完毕时，及时向采购人提出履约验收申请。 2.按照采购人的验收方案，中标供应商准备相关验收资料，随时准备接受验收。 3.中标供应商随时接受采购人在中标供应商履约过程中的工作监督、检查和指导。 4.本项目验收由采购人组织，中标供应商配合进行。
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：对项目需求理解、运行维护方案、实施方案、履约能力等。

B 分标

一、技术参数、服务内容要求：		
服务名称	数量	服务内容及服务要求
重大时期网络安全保障服务	1项	**一、服务目标** 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，减少广西税务局互联网测资产的暴露面和攻击面，提升广西税务局互联网侧防护能力，并通过提供重要时期安全值守服务，为广西税务局提供值守前期防护准备、值守期间安全监测及应急响应、值守结束的总结与整改支撑服务，专业的安全团队与广西税务局协同开展重要时期安全防护值守工作，全面提升广西税务局的安全监测防护能力，降低安全事件的发生概率，保障广西税务局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，强力提升采购人网络安全防护能力，需充分利用专业安全技术厂商的力量，协同做好重要时期安全值守服务。具体内容如下： ★1、提供不少于 5 名熟悉《奇安信天眼高级威胁分析系统》的网络安全工程师【其中至少有 2 人具有注册信息安全工程师-渗透测试专家(CISP-PTS)认证及 Web 应用安全专家（CWASP）认证）】，在重要时期对广西税务局互联网应用提供 7×24 小时安全值守服务，值守总时间不少于 60 天/年。 2、在安全值守前期，协助广西税务局做好准备工作，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；在安全值守前期供应商需提交《安全防护工作方案》。 3、对广西税务局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;协助区税务局积极开展安全自查与加固工作；统筹开展广西税务局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;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：安全服务商进行统筹协调，根据工作方案统筹开展区税务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区税务局的应用系统进行渗透测试，服务商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 小时的对广西税务局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。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、在每个安全值守阶段结束后，协助广西税务局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。需提交《安全值守总结报告》。 7.在安全值守保障期间，必须根据网络上所披露的 0day 漏洞，对广西税务局流量分析系统中的规则进行更新后，以实现对新漏洞的检测。 **三、其他要求**

		1. 中标供应商在服务期间的其他要求： ★1.信息安全保密要求 （1）必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）项目人员需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)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，中标供应商应负有连带责任。 （4)中标供应商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)项目人员必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.中标供应商运维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，由于中标供应商运维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。 ★3.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，由中标供应商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。中标供应商无法判定问题根源的，由中标供应商承担全部责任。采购人将根据问题的轻重、中标供应商责任的大小，扣除不高于合同款 5%服务金额。
二、商务条款要求：		
★项目服务地点		广西区内采购人指定地点。
★项目服务期限		自合同签订之日起 2 年。
★付款方式		合同签订后 30 日内采购人支付合同金额的 25%；运维期满 1 年，支付合同金额的 35%；运维期满 2 年，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则条款进行考核，按考核结果对合同服务费进行核算后，30 日内支付合同相应的剩余款项。采购人付款前，中标供应商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供应商提供合格发票，并不承担延迟付款责任。
★验收方法		1.中标供应商履约完毕时，及时向采购人提出履约验收申请。 2.按照采购人的验收方案，中标供应商准备相关验收资料，随时准备接受验收。 3.中标供应商随时接受采购人在中标供应商履约过程中的工作监督、检查和指导。 4.本项目验收由采购人组织，中标供应商配合进行。
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：对项目需求理解、项目实施方案、运行维护方案、履约能力等

C 分标

一、技术参数、服务内容要求：		
服务名称	数量	服务内容及服务要求
数字证书系统、双向安全交换系统和密码服务组件系统运维服务	1项	**一、税务数字证书系统** **(一)服务范围** 广西省税务数字证书系统主要包括： 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，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、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 16 台通用服务器、4 台签名验签服务器、10 台密码机。 2. 网络联通性检查 通过堡垒机远程登录的方式，检查各服务器之间、省局与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 每天通过监控日志的方式检查各证书子系统之间的服务情况，包括证书发行、证书同步、证书介质初始化和身份认证等服务日志，远程测试 RSA 算法、SM2 算法证书发行管理。 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. 技术咨询 对于国家税务总局广西壮族自治区税务局税务干部提供税务数字证书系统和密码服务组件系统的功能使用电话咨询服务。提供税务数字证书系统和密码服务组件系统的应

		用开发的技术咨询服务。使其在税务数字证书系统的使用过程中遇到的各类故障问题需要帮助进行定位和解决。 8. 现场支持 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。 9. 知识库的整理和总结 除上述服务内容外，中标供应商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，大大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 2 名专业运维人员远程参与广西壮族自治区税务数字证书系统和密码组件服务系统的运维服务工作，该人员具备胜任运维服务工作岗位的资质、能力和水平，具有 3 年及以上的证书系统运维服务经验。同时提供 1 名高级技术支持人员(远程参与），遇到重大问题时及时解决，具有 8 年及以上的证书系统运维服务经验，具有 CISP 证书。 **二、双向安全交换系统** **(一)服务范围** 双向安全交换系统、配套的通用服务器和安全设备 **(二)服务内容** 针对上诉服务范围，具体服务内容如下： 1.设备巡检监控 提供 5*8 为基础的设备现场监控和 7*24 小时的手机在线值班,以配合广西区税局的日常运营。 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，对系统运行的计算机存储资源进行监控，对系统日志信息进行整理分类分析，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的运行异常情况。及时报告“双向”交换系统的应用系统异常运行情况，以便及时处理。

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得到及时有效的跟踪和处置；参考各省“双向”交换系统的告警事件及时开展预防处置工作，以便提前预防类似事件的发生。

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统计报表，以便能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。

(三)服务产出物

为了让广西区税局充分了解网络中真正发生的事情,执行控制和管理关键操作的权利,并为正在发生的事情提供指导，驻场工程将根据责任矩阵向客户名称做定期或紧急报告，内容包括设备性能，故障或告警，操作，SLA 以及驻场服务的其他重要信息，例如：

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

驻场服务报告

驻场工程师将按照双方共同商定的格式每日，每周，每月，每季度或每年提交给广西区税局驻场服务报告，故障处理报告将包括分析根本原因和防止再次发生的建议。

(四)服务方式

采用驻场运维服务方式，保障双向安全交换系统的正常运行。

(五)服务人员

提供 1 名驻场运维人员在现场开展 7*8 小时的双向安全交换系统的运维服务工作，同时需要指派一个合格的运维团队（非驻场人员），包括但不限于项目经理、高级技术支持、售后技术服务支持人员等。现场支持人员要求至少具有 1 年双向安全交换系统

		的运维工作经验。 **三、其他要求：** ★1.信息安全保密要求 （1）必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）项目人员需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)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，中标供应商应负有连带责任。 （4)中标供应商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)项目人员必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.中标供应商运维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，由于中标供应商运维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。 ★3.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，由中标供应商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。中标供应商无法判定问题根源的，由中标供应商承担全部责任。采购人将根据问题的轻重、中标供应商责任的大小，扣除不高于合同款5%服务金额。
二、商务条款要求：		
★项目服务地点		广西区内采购人指定地点。
★项目服务期限		自合同签订之日起2年。
★付款方式		合同签订后30日内采购人支付合同金额的25%；运维期满1年，支付合同金额的35%；运维期满2年，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则条款进行考核，按考核结果对合同服务费进行核算后，30日内支付合同相应的剩余款项。采购人付款前，中标供应商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供应商提供合格发票，并不承担延迟付款责任。
★验收方法		1.中标供应商履约完毕时，及时向采购人提出履约验收申请。 2.按照采购人的验收方案，中标供应商准备相关验收资料，随时准备接受验收。 3.中标供应商随时接受采购人在中标供应商履约过程中的工作监督、检查和指导。 4.本项目验收由采购人组织，中标供应商配合进行。
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：对项目需求理解、运行维护方案、实施方案、履约能力等

D 分标

一、技术参数、服务内容要求：		
服务名称	数量	服务内容及服务要求
网络安全态势感知驻场运维服务	1项	**一、项目背景和工作目标** 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，提升网络安全态势感知和预警处置能力，需开展态势感知平台监测预警工作，要求采购 7×24 小时网络安全监控服务，提供不少于 5 名技术人员通过态势感知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团队，每 2 个月开展一次网络安全专业检测服务以及重要时期安全技术支撑服务。 **二、服务内容** 针对广西壮族自治区税务局态势感知平台监测预警驻场运维服务项目，具体运维内容如下： （一）资产监控管理服务 通过使用态势感知平台发现资产，对资产进行识别、分类以及标记管理，对网络中可能存在的未知资产进行动态识别。通过对已知资产的管理、未知资产的及时检测与发现相结合，动态绘制资产台帐，完善资产信息表。 （二）网络安全监测和分析服务 技术人员每日对态势感知平台发现的安全告警通过平台提供的一系列线索进行深度分析，并结合威胁情报进行综合研判，判断攻击是否成功，并对确定性的攻击事件进行有效的处置包括：风险控制、影响面调查、攻击链展现、攻击溯源等过程，每周出具《监测分析周报》。 （三）网络安全响应服务 技术人员每日通过态势感知平台对攻击行为进行监测发现、分析研判、应急处置、确认消除，出具《安全事件分析报告》，从而形成安全事件从发生到消除的闭环管理，实现安全事件管理机制。 （四）网络安全态势分析服务 技术人员按照信息系统等级保护的相关要求，通过态势感知平台收集、汇总、分析的安全风险对现有的税务信息系统的安全现状进行全局性的评估，分析信息资产存在的安全漏洞，分析信息资产面临的安全威胁及威胁发生的可能性，检查现有安全措施的有效性，从而识别出信息资产中存在的安全风险点，协助安全管理人员对税务信息资产所面临的风险程度做出准确的评价，提供相关整改修复加固建议，每月出具《安全态势分析月报》。 （五）漏洞管理服务 技术人员通过使用态势感知平台中的漏洞扫描模块主动发现资产存在的漏洞，并通知、协助相关部门对漏洞进行加固。加固结束后，安全运营人员通过平台验证加固情况，以确认风险是否被消除。对于新爆发的漏洞，安全运营人员会启动预警动作，并利用平台对新漏洞进行及时检测与处置。每月出具《漏洞扫描月报》。 （六）态势感知平台运维服务 技术人员每天对态势感知平台相关安全设备进行硬件巡检，以保证平台相关设备健康运行；定期配合研发对平台及相关设备进行软硬件升级，以确保平台功能和安全策略满足运营需求。每天出具《平台运维日报》。 （七）数据安全风险监控和处置服务 1.根据态势感知平台数据安全模块记录的应用登录、数据查询及导出、数据维护等风险识别信息，定义或优化异常行为规则，建立优化数据安全风险模型，分析确认异常

		行为并组织开展风险处置。 2.及时开展后台异常运维类数据安全风险监控和处置。预先定义异常行为规则，并在态势感知平台中设置相应数据安全风险模型，审核运维账号在数据库后台进行数据维护（增、删、改、查、拷）的记录，重点审计数据库后台登录和查询拷出记录，对照运维工作职责范围，确定是否存在异常后台操作的情况。对于触发数据风险模型产生告警的，按风险处置流程进行处置。 3.定期开展前台异常使用类数据安全风险监控和处置。 一是及时发现并分析处置前台异常访问。根据业务实际，预先定义异常访问行为规则，并在态势感知平台中设置相应数据安全风险模型，对于触发前台异常数据访问风险模型告警的，应审核用户账号登录和用户终端 IP 地址所属物理位置，对照用户工作岗位权限，确定是否存在跨区域操作、冒用盗用他人账号进行前台操作或未经授权、超职责范围操作及其它不符合规定的前台操作并进行相应处置。 二是严格审核确认并处置前台异常查询导出数据行为。定期（如每 15 日）汇总“前台异常查询导出数据”的监控记录，对照用户工作岗位职责，逐条审核用户账号登录和查询及导出数据的记录，确定是否存在前台超范围、超数量等异常查询及导出的情况。经相关业务部门核验确认属于异常行为的要立即开展异常风险处置工作；属于合理业务需求的，应提出相关异常行为规则设置建议，对数据安全风险模型优化完善。 **三、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。 **★四、服务人员** 提供不少于 5 人的驻场技术人员提供 7×24 小时驻场服务，提供不少于 8 人的后台运维支撑团队，该人员具备胜任运维服务工作岗位的资质、能力和水平。 **五、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 人，需提供 7×24 小时驻场运维服务，人员要求： （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；能顺利完成网络安全态势感知平台的资产录入、安全监控、安全响应态势感知平台运维升级、漏洞扫描、补丁发布等相关技术工作，能及时完成税务总局绩效考核相关技术要求工作。 （二）后台远程运维支撑团队要求 要求后台运维支撑团队人员数量不少于 8 人，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；要求后台运维支撑团队每 2 个月开展一次安全巡检，出具巡检报告的内容包含对网络安全态势感知平台上收集到的攻击行为进行深入分析，深入检查攻击中是否有 APT 攻击，是否有来自内部的威胁，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。 **六、服务时间、服务地点、服务期限和响应时间** （一）服务时间：合同签订之日起提供 17 个月的运维服务。 （二）服务地点：广西壮族自治区税务局。 （三）服务期限：对网络安全态势感知平台提供 17 个月的运维服务。 （四）服务响应时间

<table>
<tr><td></td><td></td><td>
要求 2 小时内做出实质性响应，并且按照下表要求对采购人的系统软件故障技术支持服务请求进行响应：
<table>
<tr><td>序号</td><td>故障级别（严重程度）</td><td>响应时间</td><td>故障解决时间</td></tr>
<tr><td>1</td><td>系统瘫痪，态势感知平台不能运转的</td><td>0.5 小时内</td><td>1 小时内</td></tr>
<tr><td>2</td><td>系统部分出现故障，态势感知平台仍能运转</td><td>1 小时内</td><td>2 小时内</td></tr>
<tr><td>3</td><td>初步诊断为系统软件问题，只造成态势感知平台性能下降</td><td>1 小时内</td><td>4 小时内</td></tr>
</table>
七、项目数据安全和保密要求
★1.信息安全保密要求
（1）必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）项目人员需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)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，中标供应商应负有连带责任。
（4)中标供应商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)项目人员必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.中标供应商运维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，由于中标供应商运维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。
★3.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，由中标供应商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。中标供应商无法判定问题根源的，由中标供应商承担全部责任。采购人将根据问题的轻重、中标供应商责任的大小，扣除不高于合同款 5%服务金额。
</td></tr>
<tr><td colspan="3">二、商务条款要求：</td></tr>
<tr><td colspan="2">★项目服务地点</td><td>广西区内采购人指定地点。</td></tr>
<tr><td colspan="2">★项目服务期限</td><td>自合同签订之日起 17 个月。</td></tr>
</table>

★付款方式	合同签订后 30 日内采购人支付合同金额的 25%；运维期满 12 个月，支付合同金额的 35%；运维期满 17 个月，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则条款进行考核，按考核结果对合同服务费进行核算后，30 日内支付合同相应的剩余款项。 采购人付款前，中标供应商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供应商提供合格发票，并不承担延迟付款责任。
★验收方法	1.中标供应商履约完毕时，及时向采购人提出履约验收申请。 2.按照采购人的验收方案，中标供应商准备相关验收资料，随时准备接受验收。 3.中标供应商随时接受采购人在中标供应商履约过程中的工作监督、检查和指导。 4.本项目验收由采购人组织，中标供应商配合进行。
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：对项目需求理解、运行维护方案、实施方案、履约能力等

E 分标

<table>
<tr><td colspan="3">一、技术参数、服务内容要求：</td></tr>
<tr><td>服务名称</td><td>数量</td><td>服务内容及服务要求</td></tr>
<tr><td>信息系统应用不间断监控排障技术服务</td><td>1 项</td><td>
一、监控方案要求
（一）监控对象及分级
按照现状，目前已加入日常监控的系统(不包括子系统)约 60 个，采购人可根据工作需要进行调整。根据不同的系统影响力、重要性等因素，设置对应的服务内容和标准。下表为开展不间断监控的对象和级别：
<table>
<tr><td>系统级别</td><td>监控对象</td></tr>
<tr><td rowspan="4">特级</td><td>电子税务局</td></tr>
<tr><td>金税三期核心征管系统</td></tr>
<tr><td>税库银系统</td></tr>
<tr><td>增值税发票系统</td></tr>
<tr><td rowspan="4">一级</td><td>出口退税系统</td></tr>
<tr><td>社保费系统</td></tr>
<tr><td>ITS 系统</td></tr>
<tr><td>其他一级系统（堪场提供）</td></tr>
<tr><td rowspan="4">二级</td><td>绩效控制台信息系统</td></tr>
<tr><td>外部信息交换系统</td></tr>
<tr><td>安全策略二包</td></tr>
<tr><td>其他二级系统（堪场提供）</td></tr>
<tr><td rowspan="4">三级</td><td>人事系统</td></tr>
<tr><td>纪检监察</td></tr>
<tr><td>数字人事系统</td></tr>
<tr><td>其他三级系统（堪场提供）</td></tr>
</table>
以上监控服务对象会根据具体工作安排随时调整。
（二）特级系统监控方案
按照核心征管、电子税务局、税库银系统和增值税发票系统监控方案为主，综合运用各类监控手段和工具，对特级系统的运行数据和服务能力等相关技术指标进行监测和收集，实时掌握特级系统运行情况。值班人员负责监控值守、告警响应、信息提报等工作，及时发现系统运行问题，并推送相关部门进行分析处置，消除隐患。每月 5 日前形成特级系统月度运行监控工作报告（应包括特级系统基础环境监控、系统运行情况以及业务成交量等数据），报采购单位。
根据电子税务局系统业务特点和运维工作要求，监控系统对电子税务局实现 7×24 小时监测，监控数据采集频率不得低于 5 分钟/次。
本项目中的监控对象是指用于支撑特级系统运行的相关软硬件资源，主要包括：服务器、小型机、云计算资源、存储设备、网络及安全设备、操作系统、中间件、数据库、应用程序、依赖关联系统等。此外，还应对特级业务性能及用户行为进行监控，监控指标体系主要如下：
服务器监控主要包括：CPU 使用率、内存使用率、文件系统使用率、磁盘和网络 I/O 性能、服务器可用性、操作系统日志等。
中间件监控主要包括：服务端口可用性、中间件内存使用率、线程使用率、队列长度、中间件日志等。
</td></tr>
</table>

		数据库监控主要包括：服务端口可用性、表空间使用率、数据库 I/O、TopSQL 监控、数据库日志等。 网络监控主要包括：网络带宽使用率、网络响应延迟、丢包率等。 应用系统性能监控主要包括：应用系统可用性、并发访问数、每秒事物数、服务请求响应耗时、交易链路监控、应用系统日志分析等。 关联系统监控主要包括：关联系统可用性监控、关联系统服务接口调用响应时间。 业务监控主要包括：业务健康度、业务量（异常变化）、当月业务完成度、业务处理成功率、业务处理时间等。 用户行为监控通过是对纳税人的来源、访问页面、停留时间、操作模块、操作次数等行为进行监控和分析，实现对特级整体运行情况和服务能力的感知。 监控指标和阈值实行分类管理。系统监控数据应至少保留 1 个月，关键业务系统监控数据应至少保留 3 个月。 （三）一级系统监控要求 针对一级系统设置了 30 秒的软件自动检测可用性的监控间隔;每半小时值班人员主动实施应用的各项关键指标的健康检查；每周出具巡检报告。 （四）二级系统监控要求 “二级系统”包含了 23 个重要系统，如门户网站、车购税系统、自助办税系统等。针对二级系统设置了 60 秒的软件自动检测可用性的监控间隔;每小时值班人员实施应用的各项关键指标的健康检查；每月出具巡检报告。 （五）三级系统监控要求 “三级系统”包含 20 个重要系统，如数字人事、人事系统等。针对三级系统设置了 120 秒软件自动检测可用性的监控间隔；每 2 小时值班人员实施应用的各项关键指标的健康检查；每季度出具巡检报告。 二、值班工作要求 值班工作分为一线值班工作和二线值班工作。一线值班工作为：7×24 值班服务，二线值班工作为：5×8 工作方式开展工作，电话 7×24 提供支持。以下为具体要求： （一）一线值班工作要求 1.日常监控 对监控对象进行 7×24 小时监控； 对于特级系统：总局监控的三大核心系统（金税三期核心征管系统、金税三期税库银系统、广西税务电子税务局），实时监控应用可用性情况、告警信息情况、业务量统计情况，当应用可用性下降时，按照规范流程，通过及时通讯软件、电话做出 7×24 小时反馈和处理；从下降时点计时，五分钟内发布首次故障汇报，15 分钟内进行初步问题排查，准确定位故障点（需定位到模块、拨测位置、服务器 ip，端口；数据库 ip、实例名等具体位置），发布经初步排查故障原因后的二次故障汇报，恢复后五分钟内发布故障恢复汇报，持续未恢复的，按照应急处理机制通知相关人员。对于一、二、三级系统，利用现有的监控软件平台、监控脚本、人工检查方式检测信息系统可用性，做到发现系统故障及时反馈处理。 2.故障、告警信息分析定位 应用系统在运行过程中因项目环境的数据库、网络、服务器、防火墙等原因出现故障，针对特级系统，服务人员需针对应用出现可用性异常时的关键业务模块可用情况、告警信息情况、对应进行系统环境检查，进行初步故障原因分析，准确故障定位。记录和整理知识库。 对基础层告警信息进行分析，对影响系统可用性或者虽未影响系统可用性但是对系统产生较大风险的告警信息进行筛查和分析，并准确定位受影响业务、范围、节点等。

		3.故障反馈及跟踪 反馈：对监控发现的故障、异常按采购人规定的时效及时进行反馈，并协助系统管理员快速处理故障；（2）事件跟踪；（3）恢复测试；（4）事件总结。服务人员需及时反馈各系统管理员 4.解答服务 解答服务主要是针对金税工程运维服务管理平台的用户提供技术支持服务。主要工作内容为：（1）接收问题；（2）查询知识库；（3）分析处理问题；（4）反馈解决方案；（5）记录问题；（6）问题转出。 5.工作报告 本项目涉及监控的系统较多，考虑到服务人员工作量及工作饱和度，因此根据各应用系统的级别采取每日、周、月、季度、年度分别提供不同系统的工作报告。具体的工作报告时限及内容另行拟定。 （二）二线支持工作要求 1.日常监控。指导一线进行故障排查，对一线无法分析、定位的异常情况、故障原因进行二线技术支持；优化可用性监控问题排查、基础层告警信息分析方式方法，相应制定、更新手册；定期对一线值班工作人员进行培训； 2.日志、流量分析 日志分析、流量分析，对指定系统抓取的日志、流量进行分析，定位日志报错，流量异常等信息，更有效准确定位系统故障、排查原因。主要包含但不限于系统级别为特级类系统，采购人可指定系统进行日志分析。 3.协助管理综合监控平台 31 个拨测关键业务模块、32 个监控指标、209 个监控对象、1759 个监控任务及阈值； 4.了解、掌握和维护三大核心系统的部署架构、资源占用情况等资料（含应用系统使用的设备、所在网络域、使用到的数据库、涉及的网络设备、安全设备、安全策略）；根据以上部署架构、资源占用情况及时更新三大核心系统整体架构图，以备系统出现异常时做排查原因及决策使用；维护系统资源采集表（含服务器、数据库、中间件使用情况）； 5.了解、掌握和应用可用性相关的三大核心系统的 31 个关键业务模块，维护系统业务关键业务模块的数据走向，及时更新 HP Business Process Monitor(BPM)拨测路径及拨测脚本，保证应用可用性监控的准确性； 6.协助优化应用系统监控机制。按照目前的监控机制进行实施，逐步分析优化监控机制，探索最优的监控方案、应急处理办法；协助更新可用性异常的问题排查方法方法，更新排查手册，保证出现可用性异常时能快速准确定位故障原因及故障点； 7.各工具使用内容：熟练掌握金税工程运维服务-综合监控系统、HP Operations Orchestration central(OO)自动控制系统、综合展示系统、HP SiteScope、HP Business Process Monitor(BPM)、BSM Gateway、BSM DP 等监控工具的使用，熟悉服务器、数据库和中间件等基础资源问题排查，包括 linux 系统、aix 系统、oracle 数据库、weblogic、MQ 等。 8.故障特征分析，研判系统运行趋势 每季度抽取各系系统监控数据进行分析，了解引起可用性下降的业务模块响应时长、网络服务器连通性、中间件性能指标、关联第三方系统或接口稳定性等因素，形成分析报告，联络和跟踪厂商应对处置结果。 9.整合监控资源，构建综合监控体系 整合现有系统运行监控资源，构建以总局统推的综合监控平台为主，系统运维厂商、基础资源运维厂商自有监控软件为辅的系统运行综合监控平台，统一监控参数标准，

组建综合监控团队。

（三）人员考勤管理

1. 考勤范围

服务团队所有人员。

（1）7×24 值班服务

每月前排班，排班结果经采购方审核批准后执行。

岗位	上下班时间	人员安排
早班岗	7:30—14:30	每班安排一人
中班岗	14:30—22:00	每班安排一人
晚班岗	22:00—7:30	每班安排一人

(2)二线支持人员

按 5×8 工作方式开展工作，电话 7×24 提供支持。

2.考勤要求

服务人员在规定的上班时间晚到办公室打卡按迟到记录；服务人员在规定的上班时间提前离开办公室按早退记录；服务人员无故缺勤按旷工记录；服务人员回公司、请假、调休需提前向管理人员告知或申请。

3.考勤统计

每月统计服务人员考勤记录，填写《服务人员考勤表》提交管理人员。

三、综合监控体系要求

针对目前系统监控信息共享不畅，反馈不及时，问题定位过于片面等突出问题，整合现有系统运行监控资源，构建以总局统推的综合监控平台为主，系统运维厂商、基础资源运维厂商自有监控软件为辅的系统运行综合监控平台，统一监控参数标准，组建综合监控团队，实现运行环境全要素覆盖，故障原因多角度研判，故障处置高效率执行，在监控环节达成系统运维的提质增效。

（一）整合范围

为实现任务目标，整合包括但不限于以下监控平台：总局的监控平台基础层监控，可用性拨测监控，流量监控，日志分析等工具；电子税务局自行建设的监控系统；税库银库银社保费相关自行建设的流量监控；网络设备的自带的监控；安全设备的自带的监控；服务器、虚拟机性能监控；中间件、数据库性能监控；项目服务单位在运维平台基础上自主研发的主动告警、问题定位辅助平台。

（二）任务措施

1.掌握收集在用的监控工具的名称、地址、账号密码、使用手册、监控对象等信息，编制监控系统使用情况表。

2.分析研究各个监控系统监控内容、监控方式、使用对象、部署环境等运行情况，参照总局监控平台,确定监控环节，统一监控指标。

3.构建系统运行综合监控平台，首先进行自有系统的界面集成，统一登录入口；然后进行接口、数据层面集成，融合各监控环节数据，实现系统全要素监控；最后研究监控环节之间的数据关系和逻辑，建立系统运行智能化监控模型，实现运行趋势预测。

4.成立监控团队，搭建运维监控指挥室，依托系统运行综合监控平台对主要运行系统进行实时监控。

综合监控体系建设因遵循以下原则：

（1）实时性。第一时间抓取系统可用性下降并告警，解决总局综合监控平台不主动提示问题；

（2）及时性。告警信息出现后监控团队全员可看，故障信息全员可知，快速定位故障原因，解决以往推送信息延迟，反馈结果不全面问题。

（3）时效性。平台主动显示系统厂商的工单、告警任务，综合团队人员当日办当日结，提高回复效率。

四、技术人员要求

不同岗位所需技术人员（项目经理、驻场人员等）的专业等级、数量、资质及工作经验要求等。

本项目须配置 6 名以上（含 6 名）技术工程师组成技术服务小组：

7×24 值班轮换 5 人；

5×8 二线支持、技术研究 1 人（7×24 电话支持）。

服务人员需要具备技术服务所需的相关知识，具体要求如下：

（1）服务人员需要具有一定的税收系统理解，同时具有一定的中间件（Weblogic、Tomcat、Linux）运维知识，熟悉 Weblogic 系统部署等知识，掌握数据库基础维护知识和数据查询，了解网络结构；熟识各系统后台登陆及常用功能操作，掌握系统常见故障问题解答方法。

（2）熟识税务局驻场日常维护工作流程。

（3）通过系统用户手册学习或相关系统管理人员培训后，掌握系统功能操作，熟练解决各类常见问题。

对应的服务工程师要求如下：

岗位	人员配置	人员要求	职责
值班岗 7×24（不间断监控）	3 人（A 岗）	一年以上系统监控运维服务经验，持有 Linux、软件中级类、OCP/OCM、H3C 等资格认证之一。 根据各级技术服务人员岗位对知识储备和工作经验的要求，对于值班岗位技术服务人员，具有本科以上学历，一年以上工作经验。能够熟练使用监控系统，熟练掌握相关系统软件的使用操作流程、监控的相关业务及常见问题的解决方法，独立接听、解答用户所提出的各种问题并进行相应的问题及回复记录。	负责应用日常监控、故障定位、问题处理； 负责数据的采集记录； 负责业务系统数据统计分析； 突发事件应急处理； 协助主管部门完成项目所需各项数据和报告。
	2 人（B 岗）	二年以上系统监控运维服务经验，软件初级、网络工程师、软件工程师类以上资格认证。 根据各级技术服务人员岗位对知识储备和工作经验的要求，对于值班岗位技术服务人员，具有本科以上学历，二年以上工作经验。熟悉监控相关的认识，能够将各类相关系统软件使用中出现的各种问题提炼、加工、深化成为知识，不断完善培训资料，制作文字文档或音视频教程，供税务机关下载使用。	负责应用日常监控、故障定位、问题处理； 负责数据的采集记录； 负责业务系统数据统计分析； 负责应用系统电话支持； 突发事件应急处理； 其他运行维护工作。 整合监控资源，管理综合监控平台

二线岗5×8（二线支持、技术研究）	1人	根据各级技术服务人员岗位对知识储备和工作经验的要求，对于二线岗位技术服务人员，具有本科学历，熟识JAVA开发语言，熟悉网络、IO/JDBC等技术，中间件维护，SQLServer、Mysql或Oracle等一种以上大/中型数据库系统和以及windows或unix操作经验。一年以上同类项目运维监控服务经验，熟练掌握监控软件的理论和日常操作。能编写监控脚本，处理监控工具的故障。能够解决相关业务系统紧急、重大、疑难等问题，熟悉各业务系统内部运行维护技术培训工作，熟悉运维平台运行环境的保障、数据的完整性、数据检验、数据的及时性，保证系统数据核查分析系统的正常运行。能够指导数据库管理、数据抽取的工作，开展各类数据集中统计分析技术方案的编制、论证，优化需求分析中的各种数据库脚本，安排协调和实施控制数据补偿、历史数据迁移、数据统一结构转换工作。	1.负责运维平台系统的操作技术支持； 2.协助完成主管部门安排的各项工作； 3.通过自身技术能力实现各系统数据分析报告； 4.自主开发适用于监控工作的辅助软件，提供可用性下降实时告警提示和报告； 5. 针对本项目面向主管部门不定期开展技术培训； 6. 分享运维平台经验，每季度技术研究成果，形式知识文档； 7. 协助运维平台重大安全漏洞补丁升级； 8. 定期汇总各系统可用性下降报告数据，协助主管部门促进系统厂商优化改善系统稳定性； 9.负责考勤管理； 10. 参与整合监控资源，提供可行性需求建议，构建综合监控体系。
团队管理	1人（不列入队伍配置）	具备软件中级类以上资格认证、软件项目经理认证、ITIL认证至少一项。对项目组的各项服务指标，进行人员绩效考核、工单分配、工单审核、工单处理过程的管控等。能够针对重大紧急监控事件制定监控响应策略、操作规程、规章制度和响应措施，做到程序化、周期化的评估、改善和提升，能够组织建立监控排障体系。	公司负责团队管理领导接受客户投诉和监督，依据客户需求调整人员。

注：因为值班工作轮换特殊性，建议服务单位预备至少1人作为灵活替换人员。

五、其他要求。

供应商应具备同类项目至少一年以上驻场服务经验,且团队成员稳定维持3人以上；

六、服务方式

服务地点：广西税务局；

服务期限：2022年10月-2024年9月（根据合同签订生效时间顺延）；为保证本项目的不间断监控的属性，应当充分预留新老项目的时间衔接，合理设置服务期限，防止出现服务期空档。

七、验收方式及标准

验收方式采取初验和终验两次，阶段性验收每三个月一次，终验综合阶段性验收成果整体验收。验收标准根据项目业务内容实施分项验收。

		八、其他要求： ★1.信息安全保密要求 （1）必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）项目人员需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)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，中标供应商应负有连带责任。 （4)中标供应商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)项目人员必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.中标供应商运维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，由于中标供应商运维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。 ★3.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，由中标供应商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。中标供应商无法判定问题根源的，由中标供应商承担全部责任。采购人将根据问题的轻重、中标供应商责任的大小，扣除不高于合同款5%服务金额。
二、商务条款要求：		
★项目服务地点		广西区内采购人指定地点。
★项目服务期限		自合同签订之日起23个月。
★付款方式		合同签订后30日内采购人支付合同金额的25%；运维期满12个月，支付合同金额的35%；运维期满23个月，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则条款进行考核，按考核结果对合同服务费进行核算后，30日内支付合同相应的剩余款项。 采购人付款前，中标供应商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供应商提供合格发票，并不承担延迟付款责任
★验收方法		1.中标供应商履约完毕时，及时向采购人提出履约验收申请。 2.按照采购人的验收方案，中标供应商准备相关验收资料，随时准备接受验收。 3.中标供应商随时接受采购人在中标供应商履约过程中的工作监督、检查和指导。 4.本项目验收由采购人组织，中标供应商配合进行。
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：对项目需求理解、运行维护方案、售后服务方案、履约能力等