采购需求A包

一、项目概况

1、项目内容：服务内容包含电子政务外网运维服务、网络安全技术体系优化服务、信息安全服务等方面。

2、采购预算：该预算包含电子政务外网运维服务、网络安全技术体系优化服务、信息安全服务费用，报价超出采购预算的视为无效报价。

3、服务期：自合同签订之日起提供3年相关服务。

4、服务地点:采购人指定地点。

5、付款方式:中标人与采购人协商(具体以合同约定为准)。

二、项目目标

本项目通过购买澄迈县政务外网服务，服务内容包含电子政务外网运维服务、信息安全服务、网络安全技术体系优化服务等方面，旨在为澄迈县政务网提供符合ITSS标准的运维服务，确保提供更稳定、更安全的电子政务外网运行环境，实现电子政务外网各业务系统的无缝集成，提升电子政务外网的相关系统及网络的可用性。本项目通过购买服务对全县电子政务外网、办公互联网进行安全改造，强化接入政务外网和办公互联网的安全能力，从而提升澄迈县政务外网和办公互联网安全保障整体水平。通过配套澄迈县电子政务外网的运维服务体系及运维管理系统，以切实提升澄迈县电子政务外网整体运维水平，达到标准化、智能化的政府服务能力，从而提高政府的工作效率和公众形象，电子政务外网运维的主要目标如下：

1、安全。通过健全和规范的安全制度，对电子政务网终端进行

有效管控，充分利用工具平台和自动化的特点，全程跟踪和控制运维全生命周期，做好事前、事中、事后的预防、应急和报告，配合业主完成电子政务网相关的信息安全监管要求。

2、高效。提升电子政务网整体运维效率，快速对变更、事件、服务请求进行响应，从而满足电子政务系统的快速响应需求，通过引入工具平台提升监控预警能力、事件跟踪处置效率。

3、标准。通过标准化操作文档，提供稳定的网络及信息系统服务，保障运维服务质量能始终如一。

三、服务需求

3.1 电子政务外网运维服务需求

电子政务外网运维服务需求包括:

1、运维体系建设服务

2、网络运维服务

3、运维驻场服务

4、网络架构优化提升服务

5、重要保障服务

6、应急响应服务

7、运维咨询服务

8、设备运维服务

3.2 信息安全服务需求

信息安全服务需求包括：

1、信息安全驻场服务

2、网络安全防护服务

3、安全防护体系运维服务

4、安全策略管理及优化服务

5、渗透测试服务

6、漏洞扫描服务；

7、安全加固指导服务；

8、安全检查服务

9、web 应用监控服务

10、代码审计服务

11、数据安全评估服务

12、网络安全应急服务；

13、网络安全预防与应急技巧培训服务。

3.3 网络安全技术体系优化服务

1、网络设备租赁服务；

2、安全设备租赁服务；

3、安全设备维保服务

四、项目服务内容

4.1 电子政务外网运维服务

4.1.1 电子政务外网运维服务范围

本项目电子政务外网运维服务范围如下：

序号	服务分类	服务内容	服务描述	服务模式	服务期限/频次
1	运维体系建设服务	1 名运维主管工程师驻场服务	现场派驻的 1 名运维主管工程师，负责现场运维保障及运维体系建设，运维团队日常管理并会同二线项目、流程、质量等专家团队负责提供 7*24 小时运维支持。	现场实施	3 年
		运维	运维流程执行包括服务级别管理、可用	现场	3 年

序号	服务分类	服务内容	服务描述	服务模式	服务期限/频次
		流程执行	性管理、持续性管理及能力管理等，最核心的是“多级支持”和“服务流程”两个模块，各流程相互贯穿和作用，形成有机整体。深入理解 ITIL、ITSM、BS15000、ISO20000 与 ISO9000 等国内外先进标准，涵盖服务管理体系、服务级别管理、服务台管理流程、突发事件管理、问题管理、变更管理、发布管理、配置管理等方面。	实施	
		运维流程监督	基于 ITSS 体系，对事件、故障、问题、配置、变更、发布和部署等流程环节进行监控，并督促在所规定的时限范围、质量要求内完成，确保运维整体质量及效率满足需求。	现场实施	3 年
		运维流程改进	运用流程优化、内控、质量管理的方法优化和完善业务流程、管理体系、角色和职责等，持续提升运维质量。	现场实施	3 年
		运维平台管理	运维平台是在 IT 运维管理过程中能够借助的用来提高服务质量和效率的工具，为推动运维服务的系统化和科学化管理，通过运维平台的辅助，可以极大提高工作效率、降低工作差错率、提升业务系统稳定性，更好地为业务保驾护航。	现场实施	3 年
		驻场服务管理	提供驻场团队服务整体管理，通过人员、技术、流程、制度等方面的管理投入，确保驻场整体服务满足需求。	现场实施	3 年
2	网络运维服务	1 名网络运维工程师驻场服务	现场派驻的 1 名网络工程师负责现场 5*8 小时网络运维保障，负责澄迈县电子政务外网核心级和汇聚级交换路由设备、各乡镇、委办局等接入交换机等网络系统的日常运维、监控及安全设备运维服务，并会同二线网络技术专家团队负责 7*24 小时技术支持。	现场实施	3 年
		网络监控运维服务	保障政务外网、互联网网络访问的畅通，实时监控网络通信流量情况；各乡镇及委办局接入级交换机的日常运维；政务云核心级和汇聚级交换机的日常运维；政务外网路由器和交换机的日常运维；	现场实施	3 年
		网络系统及设备例	定期对主干设备例行性安全健康检查，对设备的物理运行情况、清洁情况、系统运行情况、系统资源利用情况、系统运行日志、相应功能是否正常运行等进	现场实施	3 年

序号	服务分类	服务内容	服务描述	服务模式	服务期限/频次
		行巡检服务	行检查并记录，排除可能存在的安全问题和隐患。		
		网络配置及线路管理服务	掌握网络设备的配置及参数变更情况，备份各个设备的配置文件；掌握政务外网、互联网网络的线路连接情况，监督网络通信状况；	现场实施	3 年
		网络优化、升级咨询服务	为政务外网、互联网提供网络优化咨询服务；协助澄迈县电子政务外网迁移升级等工作，保障网络健康、可用。	现场实施	3 年
3	运维驻场服务	6 名现场运维工程师驻场服务	为电子政务外网运维服务提供 6 名驻场运维工程师，负责为澄迈县电子政务外网相应系统提供运维服务，包括系统软硬件日常运维、数据库运维、系统监控及巡检、桌面支持等工作。	现场实施	3 年
4	网络架构优化提升服务	网络工具定期巡检	定期对网络工具进行巡检，对设备的物理运行情况、清洁情况、系统运行情况、系统资源利用情况、系统运行日志、相应功能是否正常运行等进行检查并记录，排除可能存在的安全问题和隐患。	现场实施	3 年/每年 52 次
		网络工具升级	每年定期对网络工具进行软件版本升级，固件升级。	现场实施+远程实施	3 年/每年 12 次
5	重要保障服务	重要期维保障管及理	重要保障服务在国家重要会议或重大活动期间协助客户保障网络、基础设施、信息安全等，通过制定明确重要保障方案，落实重要保障任务的组织与实施，执行重要保障信息的通报，协助重要保障突发事件处置，使重要会议或重大活动期间的客户业务系统安全平稳运行。	现场实施	3 年/每年不少于 30 天
		重要期维保障专家值守	通过二线运维专家（网络、系统、设备等）在重保期间进行 7×24 值守，主要开展以下工作内容：重保检查、故障定位、排障处理及其他保障政务外网稳定可靠工作等。	现场实施+远程实施	3 年/每年不少于 30 天

序号	服务分类	服务内容	服务描述	服务模式	服务期限/频次
6	应急响应服务	应急预案及实战化演练	应急响应服务根据应急预案对发生的安全事件快速作出响应，根据安全事件等级，第一时间采用现场或远程的方式高效、准确、及时应对突发事件，并快速处理，及时恢复，将影响范围将至最低。该阶段主要为制订与完善网络、系统及数据中心机房基础设施系统的应急预案，组织落实以上系统的演练计划，确保应急预案完整、应急手段有效，保证在紧急情况下能够发挥正确作用。	现场实施+远程实施	3年/每年12次
		应急响应执行	通过二线运维专家（网络、系统、设备等）7*24小时不间断执行以上系统的应急响应及处置，控制系统故障影响范围，确保业务连续性和系统可用性，保障甲方业务平稳、健康运行。	现场实施+远程实施	3年/每年24次
7	运维咨询服务	ITIL流程咨询；智能绿色数据中心；服务器/虚拟化/云平台运维咨询；其他需要的咨询服务	通过二线运维专家（网络、系统、设备等）、三线厂商资源，协助跟踪业界新技术、新产品、新应用并提供相应的5*8小时咨询服务，针对客户需求提供解决方案、开展技术培训和交流研讨等。	现场实施+远程实施	3年
8	设备运维服务	硬件设备例行检查及维护	系统硬件设备工作状态例行检查和维护，向客户汇报任何异常情况，并提出解决方案，确保设备稳定运行；	现场实施+远程实施	3年
		协助在保硬件	在保设备维修服务处于保修期内的故障设备，协助在客户授权的范围内代表客户协调产品供货商予以维修，并监督维	现场实施+远程	3年

序号	服务分类	服务内容	服务描述	服务模式	服务期限/频次
		设备维修送保服务	修时效和质量；	实施	
		过保硬件设备维修保障服务	过保设备维修服务：本项目服务设备清单（参见《五、项目服务内容→4.1.2 电子政务外网运维服务清单→4.1.2.1 网络及安全设备清单》）中处于保修期外的设备需要维修时，服务提供单位负责协调符合要求的供应商给予维修，并确保维修时效及质量。	现场实施+远程实施	3 年

以上服务范围为整体服务内容，投标方必须提供包括且不限于上述范围的运维服务内容。

4.1.2 电子政务外网运维服务清单

4.1.2.1 网络及安全设备清单

需要运维的网络及安全设备清单如下：

序号	应用类型	数量	单位	品牌型号
1	政务边界墙 1	1	台	华为 USG6655E
2	政务边界墙 2	1	台	华为 USG6655E
3	澄迈县政务云边界墙 1	1	台	华为 USG6655E
4	澄迈县政务云边界墙 2	1	台	华为 USG6655E
5	核心交换机-主用	1	台	华为 S9312
6	核心交换机-备用	1	台	华为 S9312
7	委办局、乡镇接入交换机	47	台	Quidway S5328C-EI

4.1.2.2 政务数据中心设备管理清单

需要进行设备管理的清单如下：

序号	系统及类别	设备类型	品牌型号	设备位置
1	政务边界墙 2	网络设备	华为 USG6655E	2A-7-0(03U)
2	政务边界墙 1	网络设备	华为 USG6655E	2A-7-0(05U)
3	澄迈县政务云边界墙 2	网络设备	华为 USG6655E	2A-7-0(07U)
4	澄迈县政务云边界墙 1	网络设备	华为 USG6655E	2A-7-0(09U)

5	波分设备	网络设备	HUAWEI Optix OSN 9600M24	2A-7-0(14U~32U)
6	电源模块	电源设备	DPD63-8-8	2A-7-0(33U~35U)
7	电源模块	电源设备	华为 SMU11B	2A-7-0(38U)
8	电源模块	电源设备	华为 SMU11B	2A-7-0(40U)
9	核心汇聚交换机-主用	网络设备	华为 S9312	2A-7-1(2U~16U)
10	视频监控服务器 2	服务器	海康威视	2A-7-1(19U~20U)
11	视频监控服务器 3	服务器	海康威视	2A-7-1(22U~23U)
12	U2000 网管服务器	服务器	IBM x3850 X5	2A-7-1(25U~28U)
13	天融信防火墙（县营商环境建设局）	网络设备	天融信 1508	2A-7-1(30U)
14	锐捷防火墙	网络设备	RG-WALL 1600-M6600	2A-7-1(32U)
15	堡垒机-明御	网络设备	明御	2A-7-1 （34U)
16	深信服上网行为（流控）	网络设备	深信服 SG 6500	2A-7-1(36U~37U)
17	互联网出口防火墙-主用	网络设备	华为 Eudemon1000E	2A-7-1(40U)
18	核心汇聚交换机-备用	网络设备	华为 S9312	2A-7-2(2U~16U)
19	视频监控服务器 4	服务器	海康威视	2A-7-2(22U~23U)
20	KVM+显示器	服务器	运维专用工具	2A-7-2(25U)
21	互联网出口防火墙-备用	网络设备	华为 Eudemon1000E	2A-7-2(36U)
22	交转直电源模块	电源	华为 SMU10B	2A-7-2(38U)
23	交转直电源模块	电源	华为 SMU11B	2A-7-2(40U)
24	天融信防火墙（政务中心）AF 1720	网络设备	天融信	2A-7-3(01U)
25	硬件防火墙（县营商环境建设局）	网络设备	深信服 AF-1180	2A-7-3(03U)
26	接入交换机	网络设备	华为 S5300	2A-7-3(05U)
27	电信短信服务器	服务器	IBM X3250 M2	2A-7-3(07U)
28	澄迈电子公文归档管理系统 IMM2 口	服务器	IBM X3650 M4	2A-7-3(09U~10U)

29	就业局 2 服务器	服务器	IBM X3650 M3	2A-7-3(12U~13U)
30	就业局 1 服务器	服务器	IBM X3650 M3	2A-7-3(15U~16U)
31	互联网出口保密检测器	网络设备	蓝盾	2A-7-3(18U~19U)
32	乡镇联网综合安全网关（省纪委）	网络设备	天融信	2A-7-3(21U)
33	管理服务器 3(政务中心)	服务器	IBM X3550 M3	2A-7-3(23U~24U)
34	杀毒服务器	服务器	IBM X3610	2A-7-3(26U~27U)
35	数据库（政务中心）	服务器	IBM X3550 M3	2A-7-3(29U~30U)
36	网控服务器	服务器	IBM X3610	2A-7-3(32U~33U)
37	应用服务器 2(政务中心)	服务器	IBM X3550 M3	2A-7-3(35U~36U)
38	深信服防火墙（县营商环境建设局）	网络设备	深信服 AF-1820	2A-7-3(38U~39U)
39	视频监控服务器 1	服务器	海康威视	2A-7-4(01U~03U)
40	政务网（主干）交换机	网络设备	H3C S3600V2	2A-7-4(05U)
41	730055134100000033 服务器	服务器	IBM X3650 M4	2A-7-4(07U~08U)
42	730055134100000032 服务器	服务器	IBM X3650 M4	2A-7-4(10U~11U)
43	电子公章服务器	服务器	IBM X3250 M2	2A-7-4(13U)
44	虚拟化服务器	服务器	IBM X3550 M4	2A-7-4(15U)
45	办公 OA 数据 1	服务器	IBM X3550 M3	2A-7-4(17U)
46	办公 OA 数据 2	服务器	IBM X3550 M3	2A-7-4(19U)
47	接入交换机	网络设备	H3C 5100	2A-7-5(1U)
48	视联动力 Visionvera	网络设备	Visionvera	2A-7-5(3U)
49	RG-S2910-24GT4XS-E	网络设备	锐捷	2A-7-5(5U)
50	视联动力 Visionvera	网络设备	Visionvera	2A-7-5(7U)
51	政务外网备用出口路由器	网络设备	华为 NE08E	2A-7-5(09U~10U)
52	政务外网电信出口路由器	网络设备	华为 NE08E	2A-7-5(12U~13U)
53	政务外网移动出口路由器	网络设备	华为 NE08E	2A-7-5(15U~16U)

54	政务外网交换机 1	网络设备	华为 S5720-56C-EI	2A-7-5(18U)
55	政务网路由器	网络设备	H3C MSR5040	2A-7-5(20U~22U)
56	政务汇聚网（主干）交换机	网络设备	H3C 5600	2A-7-5(24U)
57	网御	网络设备	网御	2A-7-5(29U)
58	交转直电源模块	电源	华为 SMU01C	2A-7-5(35U)
59	交转直电源模块	电源	华为 SMU01C	2A-7-5(37U)
60	交转直电源模块	电源	华为 SMU01C	2A-7-5(39U)

4.1.2.3 数据库及操作系统清单

需要提供运维的数据库及操作系统清单如下：

序号	名称	用途	数量	备注
1	Centos 6.5	澄迈县党政办公信息系统-应用服务器、操作系统/数据库管理系统	1	
2	Windows Server 2003	澄迈县党政办公信息系统-电子公章服务器、操作系统/数据库管理系统	1	
3	Centos 6.5/Oracle 10G	澄迈县党政办公信息系统-数据库服务器、操作系统/数据库管理系统	1	

4.2 信息安全服务

本项目信息安全服务范围如下：

序号	服务项	服务子项	需求描述	服务方式	服务期限/频次
1	信息安全驻场服务需求	3 名网络信息工程师驻场服务需求	针对系统面临的日常风险，提供 3 名安全驻场服务人员，对澄迈政务外网网络安全保障管理进行服务。针对系统面临的日常风险，安全驻点服务主要以人员驻场为主，对日常安全问题以及故障事件能快速的响应处理，保障澄迈政务外网信息系统安全、稳定运行。针对重要信息系统、阶段性安全检查，对重要业务突发的重要安全事件、故障问题进行响应、定位、分析、协调、处理，迅速响应分析、统一协调、有效处理来保障重要业务系统的正常运行。	现场	3 年

			依据《中华人民共和国网络安全法》第十条、第二十一条第三小节、第六十条第三小节之规定及要求。需要随时或定时知道自己资产的网络安全情况的，那么就需要安全巡检服务，定期提供网络安全情况报告。定期对指定的安全系统及设备进行巡检，对设备的物理运行情况、清洁情况、系统运行情况、系统资源利用情况、系统运行日志、相应功能是否正常运行等进行检查并记录，排除可能存在的安全问题和隐患。	现场	3 年
			提供对指定安全防护系统日常告警监控，针对设备安全事件告警进行识别、处置。根据需要定期梳理报表，根据日常监控情况与实际需要实时调整安全防护策略	现场	3 年
			对部署的流量安全管控工具、未知威胁监测工具、入侵防御工具、运维审计工具、日志审计工具、网络行为管控工具等工具平台进行管理。	现场	3 年
			协助应急处置，对安全事件进行评估影响范围、协助进行事件抑制、溯源分析安全事件，并使用漏洞验证工具对处置结果进行验证，并针对安全事件提供有效的整改意见。	现场	3 年
2	网络安全防护服务需求		根据《中华人民共和国网络安全法》、等级保护等政策要求，明确要求对网络区域边界采取安全防护措施，网络区域边界安全防护措施是实现纵深防御的重要防护措施。通过对边界防护、访问控制、入侵防范、恶意代码和垃圾邮件防范、安全审计、可信验证采取技术措施,实现保护网络的区域边界安全。结合 2022 年三级等级保护测评结果分析,由此引出几点需求：	远程实施	3 年
			访问控制需求：		3 年
			针对跨安全域访问网络的行为，需要通过基于应用协议和应用内容的细粒度安全访问控制措施来解决，以实现网络访问行为可控可管。		3 年
			提高相关信息系统对网络区域边界相关的网络隔离与访问控制能力，实现区域间的合理访问控制，禁止未授权的会话连接。		3 年
			入侵防范需求：		3 年

		针对利用网络协议、操作系统或应用系统存在的漏洞进行恶意攻击（如碎片重组，协议端口重定位等），尤其是新型攻击行为，需通过网络入侵检测和防范等技术措施来解决，防止或限制从内、外部发起的网络攻击行为，对内、外部发起的网络攻击行为实时监测和拦截。		3 年
		恶意代码防范需求：		3 年
		针对通过恶意代码（蠕虫、挖矿等）传播对主机、应用系统和个人隐私带来的安全威胁，需要通过恶意代码防护技术手段解决。		
3	安全防护体系运维服务需求	通过安全防护体系运维服务将复杂的防护配置、策略调优与日常运维等繁杂工作交由专业、高效的安全运维专家团队处置，通过深入调研网络环境与理解内部事件处置流程，更好的响应客户的安全防护需求，满足监管单位的合规要求与各类合规安全检查。	远程实施	3 年/1 年 24 天
4	安全策略管理及优化服务需求	定期对安全设备业务访问策略进行梳理分析，发现过期、冗余、无效、不明确用途等策略，根据分析结果提供优化调整建议。	远程实施	3 年/1 年 24 天
5	渗透测试服务需求	依据《中华人民共和国网络安全法》及等保标准及相关规范开展渗透测试服务，渗透测试是指在获取用户授权后，通过真实模拟黑客使用的工具、分析方法来进行实际的漏洞发现和利用的安全测试方法。在测试过程中，用户可以选择渗透测试的强度，例如不允许测试人员对某些服务器或者应用进行测试或影响其正常运行。通过对某些重点服务器进行准确、全面的测试，可以发现系统最脆弱的环节，以便对危害性严重的漏洞及时修补，以免后患。	远程实施	3 年/1 年 24 天
		渗透测试服务通过模拟恶意黑客的攻击方法，深度评估网络系统安全的一种非破坏性的评估方法。根据测试对象目标不同，可分为：Web、APP、微信小程序、H5、API 接口、SDK、WiFi 等渗透测试服务。		3 年/1 年 24 天
6	漏洞扫描服务需求	根据《信息安全技术-网络安全等级保护基本要求》（GB/T 22239-2019）中 8.1.10.5 漏洞和风险管理中要求需要定期对信息系统的补丁、漏洞、恶意代码、备份及运行情况等方面的测试和安全检查；	远程实施	
		以等级保护测评标准为基线，通过使用自动化检测工具、人工分析等手段，针对 Web 漏		3 年/1 年 24 天

		洞、系统软件漏洞进行检测。包括但不限于网站、网络设备、安全设备、操作系统、数据库、中间件、终端及其它系统软件等；对网络系统等实施交叉扫描验证，对扫描结果实施安全分析,及时掌握信息系统安全状况，发现存在的主要安全问题和薄弱环节，建立信息安全长期保障机制，降低安全风险，促进信息系统持续安全稳定运行；并提供详细的安全评估报告，对所有漏洞弱点的相关背景提供详细描述、引用，以及相应的修复和改进建议。		
7	安全加固指导服务需求	安全加固针对安全漏洞事件、安全检查事件、网络攻击事件、安全检查工作结果，收集加固方法及验证方法，协助相关供应商保障人员进行漏洞修复。	远程实施	3 年/1 年 24 天
		针对信息安全漏洞进行的加固，可采用的加固方法包括安装修复补丁彻底修复程序漏洞；关闭漏洞依据的相关服务使用漏洞没有利用条件；使用安全防护设备进行外部过滤防护。		3 年/1 年 24 天
8	安全检查服务需求	针对重要系统的主机配置检查服务、主机脆弱性扫描服务、系统风险点复查服务，系统上线主机及 web 应用安全检查服务，降低服务器及系统安全风险，确保信息系统持续安全稳定运行。	远程实施	3 年/1 年 12 天
9	web 应用监控服务需求	（根据客户）提供的重要（互联网）系统的 web 应用监控服务，监控重要系统的网站信息不被恶意篡改，出现挂马、黑链、非法植入敏感信息、赌博色情等不良内容，确保重要系统安全、高效运行，避免政府系统出现非法及不良信息。客户指定的不超过 3 个核心应用系统。	远程实施	3 年
10	代码审计服务需求	针对系统代码的审计服务，包括系统源代码审计服务、代码安全脆弱性加固辅导服务及系统配置项检查服务，避免系统代码安全问题，保障系统信息及数据安全。	远程实施	3 年
11	数据安全评估服务需求	通过查阅系统的数据字典、架构、接口、数据类型、账号权限、安全措施等，针对被评估系统，展开涉及人员、账号、日志等内容的评估，全面分析数据全生命周期的安全措施，找出数据安全风险，并提供完善有效的数据安全整改建议。	远程实施	3 年
12	网络安全应急需求	根据《网络安全法》、《网络安全等级保护制度》以及其他行业监管单位相关要求，结	远程实施	3 年/1 年 24 天

		合实际情况，建立分层次的应急预案体系，制定网络安全应急预案并针对预案定期开展网络安全应急演练。通过安全应急演练不断根据业务实际情况调整优化方案可提高组织应对突发网络安全能力，维护网络安全和社会稳定，保障各项工作正常开展。由专业信息安全服务机构负责制定应急演练方案并参与演练，协助编制演练总结报告。制定安全应急预案并通过安全应急演练不断根据业务实际情况调整优化方案可提高组织应对突发网络安全能力，维护网络安全和社会稳定，保障各项工作正常开展。		
13	网络安全预防与应急技巧培训需求	提供相关配套的应急教育培训，使各级人员了解应急事件可能产生的后果，各项应急预案内容、程序，熟悉应急方案流程、应急设备的操作方法等，贯彻落实应急预案的可操作性。	远程实施	3年/1年6天

4.3 网络安全技术体系优化服务

租赁设备参数指标如下：

序号	设备类型	技术指标	单位	数量
1	互联网专线接入交换机	1、交换容量不低于 330Gbps，包转发率不低于 120Mpps； 2、为了提高设备供电的可靠性，支持电源 1+1 主备； 3、提供不少于 24 个千兆电口，4 个万兆光口； 4、支持统一用户管理功能，支持 802.1X/MAC/Portal 等多种认证方式； 5、支持 4K VLAN，支持 Voice VLAN、支持端口 VLAN、协议 VLAN、IP 子网 VLAN； 6、支持静态路由、RIP、OSPF、RIPng、OSPFv3，ISIS，ISISv6，BGP，BGP4+，VRRP； 7、支持 MAC 表项不少于 16K，IPv4 路由表不少于 8K，IPv6 路由表不少于 3K； 8、支持防 ARP 攻击、DOS 攻击、ICMP 防攻击、CPU 保护； 9、支持 G.8032（ERPS）标准以太环网协议，故障倒换收敛时间小于 50ms； 10、支持堆叠，主机堆叠数不小于 9 台； 11、支持 IPv6、支持 IPv4/IPv6 双栈； 12、支持基于第二层、第三层和第四层的 ACL、支持双向 ACL； 13、支持 SNMP v1/v2/v3、Telnet、RMON、SSHv2，支持通过命令行、Web、中文图形化配置软件等方式进行配置和管理； 14、支持能效以太网 EEE 节能环保； 15、配置：2 块千兆单模光模块，1 根 3M 万兆堆叠线缆，3 年维保服务。	台	2
2	互联网核心交换机	1、交换容量不低于 1.2Tbps，包转发率不低于 460Mpps； 2、提供不少于 48 个千兆电口，4 个万兆光口，不少于 1 块业务扩展槽位；	台	2

		3、可扩展支持 4 个 40GE QSFP+端口； 4、支持静态路由、RIPv1/v2、OSPF、BGP、ISIS、RIPng、OSPFv3、ISISv6、BGP4+； 5、支持 MAC 地址规格不少于 32K，ARP 表项规格不少于 20000，Ipv4 路由表不少于 8K，Ipv6 路由表不少于 4K，ACL 规格表不少于 1K； 6、支持 4K VLAN，支持 QinQ，灵活 QinQ、支持端口 VLAN、协议 VLAN、IP 子网 VLAN； 7、支持 DHCPv6 Snooping，DAI，SAVI 等安全特性； 8、支持 IPv4/IPv6 双协议栈，支持 6to4、ISATAP、手动配置 tunnel； 9、支持对端口接收报文速率和发送报文速率进行限制，支持 SP、WRR、SP+WRR、DRR、SP+DRR 等队列调度算法； 10、支持以太网环网保护协议 ERPS，故障倒换时间小于 50ms； 11、支持 40G 端口堆叠，主机堆叠数不小于 9 台； 12、支持 CPU 保护功能 13、支持 SNMP v1/v2/v3、Telnet、RMON、SSHv2； 14、支持通过命令行、Web、中文图形化配置软件等方式进行配置和管理； 15、配置：双电源，2 块千兆单模光模块，1 根 3M 万兆堆叠线缆，3 年维保服务。		

3	政务外网安全管理接入	1、交换容量不低于330Gbps，包转发率不低于120Mpps； 2、为了提高设备供电的可靠性，支持电源1+1主备； 3、提供不少于24个千兆电口，4个万兆光口； 4、支持统一用户管理功能，支持802.1X/MAC/Portal等多种认证方式； 5、支持4K VLAN，支持Voice VLAN、支持端口VLAN、协议VLAN、IP子网VLAN； 6、支持静态路由、RIP、OSPF、RIPng、OSPFv3，ISIS，ISISv6，BGP，BGP4+，VRRP； 7、支持MAC表项不少于16K，IPv4路由表不少于8K，IPv6路由表不少于3K； 8、支持防ARP攻击、DOS攻击、ICMP防攻击、CPU保护； 9、支持G.8032（ERPS）标准以太环网协议，故障倒换收敛时间小于50ms； 10、支持堆叠，主机堆叠数不小于9台； 11、支持IPv6、支持IPv4/IPv6双栈； 12、支持基于第二层、第三层和第四层的ACL、支持双向ACL； 13、支持SNMP v1/v2/v3、Telnet、RMON、SSHv2，支持通过命令行、Web、中文图形化配置软件等方式进行配置和管理； 14、支持能效以太网EEE节能环保； 15、配置：2块千兆单模光模块，1根3M万兆堆叠线缆，3年维保服务。	台	2

4	乡镇接入交换机	1、交换容量不低于330Gbps，包转发率不低于120Mpps； 2、提供不少于24个千兆电口，4个千兆光口； 3、支持统一用户管理功能，支持802.1X/MAC/Portal等多种认证方式； 4、支持4K VLAN，支持Voice VLAN、支持端口VLAN、协议VLAN、IP子网VLAN； 5、支持静态路由、RIP、OSPF、RIPng、OSPFv3； 6、支持MAC表项不少于16K，IPv4路由表不少于4K，IPv6路由表不少于1K； 7、支持防ARP攻击、DOS攻击、ICMP防攻击、CPU保护； 8、支持G.8032（ERPS）标准以太环网协议，故障倒换收敛时间小于50ms； 9、支持堆叠，主机堆叠数不小于9台； 10、支持IPv6、支持IPv4/IPv6双栈； 11、支持基于第二层、第三层和第四层的ACL、支持双向ACL； 12、支持SNMP v1/v2/v3、Telnet、RMON、SSHv2，支持通过命令行、Web、中文图形化配置软件等方式进行配置和管理； 13、支持能效以太网EEE节能环保； 14、配置：3年维保服务。	台	70
5	出口防火墙	产品参数： ≤2U设备，≥双电源，≥16个10/100/1000M自适应千兆电接口，≥2个千兆SFP接口及≥4个SPF+万兆接口；≥64G SSD硬盘；网络吞吐：≥14G，开通IPS、防病毒、应用识别及URL功能及3年特征库升级授权，开通3年威胁情报升级授权，提供原厂3年硬件质保。 其余要求： 1,▲支持不少于8种的负载均衡算法，包括但不限于最小抖动、最小延迟、最小丢包率、轮询、加权轮询等；（需要提供界面截图并加盖生产厂商公章） 2,支持对HTTP/SMTP/POP3/FTP/IMAP等协议进行病毒防御,病毒特征库规模超过1200万；	台	2

		3，内置动态黑名单功能，可与入侵防护、WEB 应用防护、防暴力破解功能实现联动封锁；支持静态和动态黑名单命中统计和监控； 4，支持黑名单多种类型导入，如通过文件上传增量添加黑名单、支持页面复制粘贴方式添加黑名单、支持 API 接口下发黑名单； 5，支持超过 100 类、2000 万的 URL 地址分类库，用户可根据网站类别对自身网络的 WEB 应用实施全面化管控，杜绝非法、违规网站的访问行为； 6，支持链路和四层通道嵌套的流量控制功能，可基于上下行区域、地址、地理对象、用户/用户组、服务/服务组、应用/应用组和时间等配置带宽策略； 7，支持 TCP BBR 加速功能； 8，支持将来源为云端的威胁情报对 IP 的威胁类型、威胁值进行动态监测，且支持用户将 IP、文件哈希、邮箱、证书指纹等互联网访问信息发送至威胁情报云进行实时情报查询。 9，威胁情报类型包括可疑行为（垃圾邮件、网络爬虫、挖矿、主机扫描）、攻击威胁（网银大盗、爆破攻击、DDoS 攻击、漏洞利用、Web 漏洞攻击）、恶意站点（欺诈、赌博、钓鱼）、恶意软件（黑客工具、宏病毒、勒索软件、远控木马、网络蠕虫）、攻击组织（APT 组织、僵尸网络 C2、IoT 攻击 C2）、失陷主机（僵尸主机、IoT 失陷主机）等 10，支持独立的入侵防护规则特征库，特征总数在 7000 条以上，能对常见漏洞进行安全防护； 11，支持集中对所有安全策略进行命中频率分析，辅助用户快速完成策略次序的调整，从而达到优化处理性能的目的；		
6	上网行为	产品参数 ≤2U 设备，≥4 个 SFP+万兆口，≥12 个 GE 千兆电口，≥12 个 SFP 千兆光口，双电源，存储容量≥2T。适用于≥2G 带宽接入网络。SSL VPN 最大并发用户数≥3000，开通 3 年特征库升级授权，提供原厂 3 年硬件质保。 其余要求： 1，支持静态路由、策略路由、动态路由、ISP 路由；策略路由支持七元组策略；动态路由支持 RIP、OSPF 等；ISP 路由支持运营商地址自定义 2，支持 IPV6 网络，可对 IPV6 网络进行审计、流量控制。	台	1

		3，支持 4G 网络，并支持接口优先级配置，当监测到主线路出现问题时，能够根据优先级主动切换到 4G 网络，保障网络正常运行。 4，支持 HTTPS 解密功能，支持页面及命令行配置解密策略，包括入接口、源地址对象、目的地址对象、https 对象、域名排除等。支持针对 HTTPS 网站、HTTPS 搜索记录、HTTPS 邮箱等内容进行审计；HTTPS 邮箱支持审计主题、内容、附件等；支持 HTTPS 域名库，预定义域名以及自定义域名； 5，支持基于 P2P 行为和迅雷行为的应用智能识别技术。 6，支持针对应用特征的安全策略配置，应用总数不少于 7300+，其中移动应用总数不少于 2000+，规则总数 12000+。 7，▲支持 HTTP、SOCKS4/SOCKS5 两种代理方式，支持配置代理端口，支持基于原地址和目的地址设置代理策略。（需要提供界面截图并加盖生产厂商公章.） 8，支持多种压缩文件的病毒查杀。压缩默认支持 5 层，最大 20 层。 9，支持 WEB Portal 认证功能，支持本地认证、Radius 认证、LDAP 认证 和 LDAP 用户同步，支持对接 IMC、SAM 等常见 AAA 服务器，支持配置强制重新认证间隔，支持配置认证通过后重定向 URL，要求本机自身支持短信认证功能。 10，提供智能策略分析功能，支持策略命中分析、策略冗余分析、策略冲突检查，并可在 WEB 界面显示检测结果；支持实时和周期性对所有安全策略进行分析。 11，提供威胁情报功能，支持全网威胁情报的搜索查询，可供攻击溯源，预知风险;支持威胁情报订阅，及时对突发威胁进行防护建议;支持 20 余种威胁分类，包括 C&C、僵木蠕、勒索、钓鱼、垃圾邮件等		
7	网络安全准入设备	产品参数： ≤2U 设备，≥1 个 Console 口，≥6 个 10/100/1000M 自适应电口，≥2 个千兆 SFP 接口，≥2 个万兆 SFP+接口，≥2 个网络接口扩展槽位，冗余电源；整机最大吞吐量≥12Gbps，最大支持管理≥2000 个终端设备，本期配置≥500 个终端准入授权。提供原厂 3 年硬件质保。 其余要求： 1，产品支持多系统功能，即同时存在系统 A、系统 B 和备份系统，可在管理员界面直接配置启动顺序，且配置文件支持导出。	台	1

		2，支持在 IPv4 和 IPv6 双栈环境下的终端准入控制。 3，支持对网络攻击行为，如抗地址欺骗攻击、抗 Smurf 攻击、抗 LAND 攻击、抗 Winnuke 攻击、抗 Queso 扫描、抗 SYN/FIN 扫描、抗 NULL 扫描、抗圣诞树攻击、抗 FIN 扫描，支持对攻击行为的发现和告警。 4，▲支持多种准入控制技术，至少支持 802.1X、EVG、DHCP、ARP 准入、SNMP 准入、视频准入、portal 认证、端口镜像、策略路由、透明网桥等技术，并且支持至少四种以上准入技术的同时启用，如同时启用 802.1x、DHCP、端口镜像、策略路由等策略。（提供界面截图并加盖生产厂商公章）. 5，支持入网终端能够在安检结束后重定向到指定 Portal 页面，重定向页面支持 HTTP 协议、HTTPS 协议，并且可自定义端口的 WEB 服务。 6，支持准入 IP/MAC 黑白名单管理功能，处于黑名单表中的 IP 和 MAC 会被准入设备判定为非法设备，处于白名单表中的 IP 和 MAC 会被准入设备信任。 7，支持网络资产自动采集功能，并能够自动分类网络中的接入设备，如交换路由设备、PC 设备、服务器、IP 电话、网络打印机等，同时能够及时发现网络中出现的新设备，对外来终端的接入行为进行告警。 8，支持 IP 地址网络视图管理，可以通过图形化查看全网的在线 IP 地址、空闲 IP 地址、已分配 IP 地址、可用 IP 地址、离线 IP 地址等 IP 地址的使用状态，并可根据使用情况实现子网统计展示。 9，支持周期性进行设备指纹采集，采集信息包括 IP，MAC,操作系统，计算机名，工作组，web 服务，DHCP option，物理识别码等多维度信息；可自定义指纹检测的例外配置，对选定范围内得设备不进行检查；并支持设备指纹自动锁定功能。 10，▲支持扫描并生成全网拓扑图，图形化展现交换机各接口状态（up、down、trunk、单/多 MAC 等）；支持 3D 机柜图展示，可以清晰了解每个机柜当前的状态。（提供界面截图并加盖生产厂商公章）. 11，支持发现内网私接 hub、非网管交换机等，能够及时产生告警并阻断接入设备入网；支持 Hub 下多个终端需分别认证才能入网。 12，支持在线用户管理，可以在线查看用户状态及其所连接的网络设备信息，如此用户接入的登录名称、登录设备 IP、设备类型、认证方式、在线时长等，对非法用户可以执行发强制下线操作。		

8	网络安全准入设备	产品参数： ≤2U 设备，≥1 个 Console 口，≥6 个 10/100/1000M 自适应电口，≥4 个千兆 SFP 接口，≥2 个网络接口扩展槽位，冗余电源；整机最大吞吐量≥28Gbps，最大支持管理≥5000 个终端设备，本期配置≥2000 个终端准入授权。提供原厂 3 年硬件质保。 其余要求： 1，产品支持多系统功能，即同时存在系统 A、系统 B 和备份系统，可在管理员界面直接配置启动顺序，且配置文件支持导出。 2，支持在 IPv4 和 IPv6 双栈环境下的终端准入控制。 3，支持对网络攻击行为，如抗地址欺骗攻击、抗 Smurf 攻击、抗 LAND 攻击、抗 Winnuke 攻击、抗 Queso 扫描、抗 SYN/FIN 扫描、抗 NULL 扫描、抗圣诞树攻击、抗 FIN 扫描，支持对攻击行为的发现和告警。 4，支持多种准入控制技术，至少支持 802.1X、EVG、DHCP、ARP 准入、SNMP 准入、视频准入、portal 认证、端口镜像、策略路由、透明网桥等技术，并且支持至少四种以上准入技术的同时启用，如同时启用 802.1x、DHCP、端口镜像、策略路由等策略。 5，支持入网终端能够在安检结束后重定向到指定 Portal 页面，重定向页面支持 HTTP 协议、HTTPS 协议，并且可自定义端口的 WEB 服务。 6，支持准入 IP/MAC 黑白名单管理功能，处于黑名单表中的 IP 和 MAC 会被准入设备判定为非法设备，处于白名单表中的 IP 和 MAC 会被准入设备信任。 7，支持网络资产自动采集功能，并能够自动分类网络中的接入设备，如交换路由设备、PC 设备、服务器、IP 电话、网络打印机等，同时能够及时发现网络中出现的新设备，对外来终端的接入行为进行告警。 8，支持 IP 地址网络视图管理，可以通过图形化查看全网的在线 IP 地址、空闲 IP 地址、已分配 IP 地址、可用 IP 地址、离线 IP 地址等 IP 地址的使用状态，并可根据使用情况实现子网统计展示。 9，支持周期性进行设备指纹采集，采集信息包括 IP，MAC,操作系统，计算机名，工作组，web 服务，DHCP option，物理识别码等多维度信息；可自定义指纹检测的例外配置，对选定范围内得设备不进行检查；并支持设备指纹自动锁定功能。	台	1

		10，支持扫描并生成全网拓扑图，图形化展现交换机各接口状态（up、down、trunk、单/多 MAC 等）；支持 3D 机柜图展示，可以清晰了解每个机柜当前的状态。 11，支持发现内网私接 hub、非网管交换机等，能够及时产生告警并阻断接入设备入网；支持 Hub 下多个终端需分别认证才能入网。 12，支持在线用户管理，可以在线查看用户状态及其所连接的网络设备信息，如此用户接入的登录名称、登录设备 IP、设备类型、认证方式、在线时长等，对非法用户可以执行发强制下线操作。		
9	终端安全管理系统	产品参数： 软件系统介质包（含包装盒，光盘，标签等），C/S 架构，本期配置≥40 个通用版本客户端基础点位授权（授权可部署在 Windows\Linux\国产化类别操作系统并实现灵活调整），包括资产管理、运维管理、病毒查杀、外设管理、非法外联监控、网络管理、终端响应、日志管理等基础功能。提供 3 年通用客户端升级授权、规则库升级授权及病毒库升级授权。 其余要求： 1，支持客户端离线打包安装、命令行安装、下载器安装、Portal 引导安装。 2，▲支持通过资产大屏展示终端总数、行为基线告警数 TOP5、资产类型统计、操作系统 TOP5、告警类型 TOP5、终端告警等级统计、漏洞终端 TOP5、最新告警、全网健康分数、风险级别（低危、中危、高危）等维度进行分块呈现。（提供界面截图并加盖生产厂商公章）. 3，支持通过定时任务对局域网内的服务器进行扫描，支持 ARP、Ping、Nmap 三种扫描方式；通过 Nmap 方式能够获取服务器相关信息，包括 MAC 地址、设备类型、未知主机 IP、操作系统、发现方式、首次发现时间等。 4，支持对单个终端风险信息进行清点，包括：漏洞数量及得分、基线违规数量及得分、病毒威胁事件数量及得分、异常行为事件数量及得分、运行状态威胁事件数量及得分、威胁情报事件数量及得分、入侵攻击事件数量及得分；支持单终端视角的综合风险评分以及待处置事件提醒。 5，支持应用商店功能，管理员可以上传需要的软件或脚本至管理端应用商店，方便客户端下载和使用。 6，支持商店下载流量控制，防止过程中对网络带宽的影响。	套	1

		7，支持操作系统弱口令检查，支持对存在弱口令的终端进行弹窗提示。支持开启或关闭弱口令密码展示。 8，支持审计终端的网络访问信息，内容至少包含：本地 IP、本地端口、远端 IP、远端端口、网络接连方向、协议、进程 PID、进程名称、进程路径、进程 MD5。 9，支持审计终端的命令信息，内容至少包括：命令行参数、命令行类型。 10，支持审计终端打印的操作，可以对共享、网络打印机、本地打印进行控制或审计，内容包括打印机名称、文档名称、份数、页数、打印结果和发生时间 11，检测到告警时，可以自动提取告警中的特征，依据预置的处置策略，自动对该终端或全网进行响应处置，提高响应时效。 12，支持终端本地敏感文件密级标识，各敏感文件以不同颜色标识标准不同等级敏感文件，对终端内存储敏感文件起到明显的警示作用 13，支持终端屏幕水印，水印内容支持文字水印、图片水印或点阵水印。 14，支持端口扫描行为检测，并支持设置 IP 白名单对安全设备进行放行，支持自动封禁远端扫描 IP。 15，支持通过自学习的方式，建立资产行为基线模型，包括网络连入/连出模型、端口监听模型、进程行为模型、登录行为模型、DNS 访问模型。 16，支持检测系统命令是否被篡改。		
10	运维审计	产品参数： ≤1U 机架，≥6 个千兆电口，≥2 个万兆光口，≥2 个千兆光口，≥1 个 Console 管理口，存储容量≥4TB，单电源，带液晶面板，≥2 个扩展槽。支持≥600 路字符会话或≥200 路图形会话并发。本期配置≥50 个资源授权，提供原厂 3 年硬件质保。 其余要求： 1，系统内置系统管理员、审计管理员、安全管理员三种角色，系统管理员可针对不同用户指定不同的管理权限，可设定用户（组）和资源（组）的管理范围；支持管理员帐号设置双因认证、IP/MAC 限制，提升帐号安全性。 2，支持用户密码策略包括：最小密码长度（强制最小 8 位）、密码复杂度（小写字母，大写字母，数字，特殊字符）、不允许密码与用户一致设置，不允许密码与用户逆序，密码周期（过期前提醒）、	台	1

		历史密码对比。 3，支持限定配置中可指定用户通过指定的应用发布服务器对资源进行访问。 4，支持僵尸、幽灵、孤儿帐号稽核功能，并可以导出异常账号稽核情况报告，方便管理员统计异常账号情况。 5，支持 Oracle、Postgresql、Sybase、MySQL、SQL server、MSSQL、DM8、DB2、informix、KingBase、Sybase、Teradata、Oracle 数据库下行返回行数记录 6，支持 Oracle、Postgresql、Sybase、MySQL、MSSQL、DM8、DB2、informix、KingBase、Teradata 数据库下行返回行数记录，当超过设定的返回行数时可进行告警或阻断。 7，支持通过应用发布实现字符协议和文件传输协议的命令级审计和图形审计的双重审计效果，命令级审计便于重现真实的完整操作命令，图形审计便于直观的查看到真实的操作行为，并支持通过搜索操作语句或执行结果中关键字定位审计回放。 8，支持对剪贴板拷贝文件记录文件名、拷贝文本进行字符记录，并支持通过搜索字符信息关键字定位审计回放 9，审计查询关键字和结果显示支持多种编码 (UTF-8,Big5,EUC-JP,EUC-KR,GB2312,GB18030,ISO-8859-2,KOI8-R,KS_C_5601_1987,Shift_JIS,Window-874)，由审计管理员自主选择。 10，支持密码找回：支持用户忘记登录密码时，可通过邮件、短信方式获取验证码，验证通过后重置登录密码。 11，支持国产化终端（银河麒麟/统信）调用本地工具运维，无需安装单独的客户端工具。		
11	日志审计	产品参数： ≤1U 标准机架式，双电源，≥6 个千兆电口、≥2 个千兆光口（含光模块），≥1 个扩展槽位，≥2 个 USB 接口，硬盘容量≥32G minisata+6T SATA，日志处理性能（平均）≥2500EPS，本期配置≥50 个审计对象授权，提供原厂 3 年硬件质保。 其余要求： 1，支持定制任务进行日志数据采集扩展，包括文本格式、目录下文本和数据库格式日志采集，支持编辑正则表达式和 SQL 语句进行日志采集，支持设置自定义任务时间。	台	1

		2，支持对主流安全设备、网络设备、服务器、终端、数据库、中间件、大数据组件、应用系统等设备系统进行日志采集，包括交换机和路由器、虚拟化及云计算平台、蜜罐系统、终端管理系统、防火墙、VPN、防病毒网关、入侵检测系统、入侵防御系统、WAF、内容过滤网关、负载均衡设备、数据库设备、Windows/Linux 操作系统、隔离交换设备等设备组件系统。 3，支持与 Kafka、HDFS、ES、MongoDB 大数据存储组件对接进行日志数据采集。 4，支持对国内主流国产化数据库进行日志数据采集，包括武汉达梦、人大金仓、南大通用、神州通用等；支持动态表名模式进行数据库采集，能按照时间或者数字的规则动态每天递增采集日志表。 5，支持自定义过滤条件进行自动化日志过滤，排除繁杂无用的日志，支持一键清除过滤条件；支持自定义日志合并规则，支持一键清除合并规则。 6，支持对范式化字段进行枚举，范式化字段至少包括事件接收时间、用户名称、源地址、源端口、操作、目的地址、目的端口、对象、结果、持续时间、响应、归并条目、事件名称、事件内容摘要、事件分类、等级、原始等级、原始类型、产生时间、网络协议、网络应用协议、设备地址、设备名称、设备类型、程序名称、原始消息、厂商、产品、解析关联等 65 个字段，字段名称支持自定义。 7，支持扩展备用字段使用，可灵活进行特殊字段的标记解析；自定义扩展规范化事件字段并对扩展字段进行重定义； 8，支持在线编辑解析文件，支持基于标准化后的字段自动生成解析文件，同时支持必配事件字段查看和常用事件字段属性在线调整编辑解析规则；实现范式化文件最优化； 9，▲为保证查询数据及时更新，查询页面需支持最近 5 分钟、15 分钟、30 分钟、1 小时、6 小时、12 小时、1 天、7 天、30 天、不刷新等不同间隔的刷新时间设定。(提供界面截图并加盖生产厂商公章)。 10，支持日志加密压缩传输，支持加密压缩方式转发，加密方式支持 SM4 国密算法，支持定时转发。		

12	政务外网防火墙	产品参数： ≤2U 设备，≥双电源，≥16 个 10/100/1000M 自适应千兆电接口，≥2 个千兆 SFP 接口及≥4 个 SPF+万兆接口；≥64G SSD 硬盘；网络吞吐：≥14G，开通 IPS、防病毒、应用识别及 URL 功能及 3 年特征库升级授权，开通 3 年威胁情报升级授权，提供原厂 3 年硬件质保。 其余要求： 1,支持不少于 8 种的负载均衡算法，包括但不限于最小抖动、最小延迟、最小丢包率、轮询、加权轮询等； 2,支持对 HTTP/SMTP/POP3/FTP/IMAP 等协议进行病毒防御,病毒特征库规模超过 1200 万； 3，内置动态黑名单功能，可与入侵防护、WEB 应用防护、防暴力破解功能实现联动封锁；支持静态和动态黑名单命中统计和监控； 4，支持黑名单多种类型导入，如通过文件上传增量添加黑名单、支持页面复制粘贴方式添加黑名单、支持 API 接口下发黑名单； 5，支持超过 100 类、2000 万的 URL 地址分类库，用户可根据网站类别对自身网络的 WEB 应用实施全面化管控，杜绝非法、违规网站的访问行为 6，支持链路和四层通道嵌套的流量控制功能，可基于上下行区域、地址、地理对象、用户/用户组、服务/服务组、应用/应用组和时间等配置带宽策略； 7，支持 TCP BBR 加速功能； 8，支持将来源为云端的威胁情报对 IP 的威胁类型、威胁值进行动态监测，且支持用户将 IP、文件哈希、邮箱、证书指纹等互联网访问信息发送至威胁情报云进行实时情报查询。 9，威胁情报类型包括可疑行为（垃圾邮件、网络爬虫、挖矿、主机扫描）、攻击威胁（网银大盗、爆破攻击、DDoS 攻击、漏洞利用、Web 漏洞攻击）、恶意站点（欺诈、赌博、钓鱼）、恶意软件（黑客工具、宏病毒、勒索软件、远控木马、网络蠕虫）、攻击组织（APT 组织、僵尸网络 C2、IoT 攻击 C2）、失陷主机（僵尸主机、IoT 失陷主机）等 10，支持独立的入侵防护规则特征库，特征总数在 7000 条以上，能对常见漏洞进行安全防护； 11，支持集中对所有安全策略进行命中频率分析，辅助用户快速完成策略次序的调整，从而达到优化处理性能的目的；	台	2

13	入侵防御	产品参数： ≤1U 设备,≥1 个 Console 口,1 个管理口,≥1 个 HA 口,≥4 个具备 BYPASS 功能的 10/100/1000Base-T 接口，≥4 个千兆光口，≥2 个扩展插槽，≥2 个 USB 口，单电源，吞吐量≥25G，开通 3 年入侵防御特征库升级授权，开通防病毒功能及 3 年病毒库升级授权，提供原厂 3 年硬件质保。 其余要求： 1，支持 HTML 解码、URL 解码、base64 解码、Unicode 解码、十六进制转换、CHR 解码、UTF-7 解码，支持解析 7 层以上混合编解码能力，可实现对多层编码攻击的检测，支持格式文本解析 JSON 解析、xml 解析。 2，规则详情应包含描述信息、CNNVD、CNVD、CVE、影响系统、影响服务、影响应用、事件处理流程、事件性质判定、默认状态、信息泄漏、攻击阶段、默认动作、攻击结果、精确度 3，支持 HTTP 请求和响应缓存的双向检测功能，根据双向流量检测攻击，输出研判详情结果包含威胁级别，攻击阶段，攻击结果，标识状态及处置状态等内容，提供 HTTP 请求信息/响应信息。 4，支持 SQL 注入防护和 XSS 攻击防护，检测点至少支持 URL、Cookie、Reference、Form、User-Agent、X-Forwarded-For，内置 AI 检测模型，利用机器学习和统计分析技术对 SQL 注入报文进行建模和分析，检测和识别 SQL 注入行为。 5，具有多种防 web 扫描能力，防止攻击者通过扫描发现 Web 网站中的缺陷从而发起精确攻击，至少包括如下能力：防爬虫、防止 CGI 和漏洞扫描等，并支持阻断扫描行为和并记录日志，系统支持设置至少 4 个级别的扫描容忍度/扫描敏感度，方便安全管理者采用不同安全级别的行为控制。 6，系统应支持 WEB 过滤，对 web 内容，传输文件名称、传输文件内容过滤，应支持邮件过滤，对邮件标题、邮件正文、附件名称、附件内容过滤，阻断并支持邮件提醒 7，系统应内置硬件 BYPASS，支持手动切换，并支持过载保护功能，通过 CPU 和内存阈值实现过载保护的开启，提供不同的阈值计算方式（最高值/平均值、时间区间等），切换应支持二层回退和三层回退。 8，系统应内置智能分析能力，具备阻断的活动专项分析和综合威胁告警分析，其中阻断的活动应包括阻断的威胁、阻断的文件和阻断的 IP 专项分析。 9，系统应支持攻击日志展示自动聚合，聚合条件包含源、目的 IP+威胁名称、目的 IP+威胁名称、	台	2

		威胁名称，系统应支持攻击源目地址归属地显示，日志信息应包含威胁级别、攻击阶段、攻击结果、标识状态、处置状态展示，应支持存储攻击日志网络负载，其中 WEB 攻击应支持存储 HTTP 头 10，▲产品具备 iPv6 Ready Logo 证书（提供证书扫描件并加盖生产厂商公章）。		
14	流量监测探针	产品参数： ≤2U 上架设备，≥1 个 Console 口，≥6 个 10/100/1000 Base-T 接口，≥2 个 USB 口，≥4 个千兆光接口插槽，支持≥2 个扩展插槽，冗电，≥2T 硬盘，网络吞吐≥3G，开通 3 年特征规则库升级授权，开通 3 年威胁情报升级授权，提供原厂 3 年硬件质保。 其余要求： 1，支持发现网络中存在的可疑通信如：Webshell 请求、XSS 攻击、SQL 注入、僵木蠕等恶意攻击程序。 2，支持通过 web 页面导入 pcap 包离线回放检测能力，单个导入回放的数据包最大支持 1G，支持批量导入或选择文件夹导入，最多支持导入 100 个数据包。 3，支持自定义规则，可结合用户业务进行深度检测，自定义内容包括源 IP、源端口、目的 IP、目的端口、协议、事件威胁等级、主机状态、事件类型、攻击阶段、攻击结果、攻击手段；支持关联规则分析，进行双向检测规则编写。 4，支持提供最近 24 小时/7 天/15 天内接入流量网络中发生的整体安全态势，包括对网络内风险资产进行统计分析、对攻击、受害攻击进行聚合分析输出 TOP10，并可对告警攻击 TOP5 进行排序便于客户直观了解脆弱点。 5，支持病毒检测分析场景，展示病毒文件名称、病毒名称、协议类型，传播时间等内容，可以对病毒日志文件进行下载。 6，▲系统具备专有的挖矿分析场景:基于特征库和威胁情报检测挖矿主机，对挖矿主机进行不同阶段的展示，至少包括连接矿池阶段、获取挖矿任务阶段、控制命令通信阶段、挖矿成功阶段，形成挖矿链可视跟踪。对网络中的挖矿主机活跃程度，挖矿币种有直观的图形化展示。（提供界面截图并加盖生产厂商公章）。 7，支持通过扫描方式发现资产的类型，包括终端、视频设备、办公设备、网络设备、服务器、安全设备、工控设备等。	台	1

		8，支持通过扫描实现对资产精准识别，粒度包含设备类型，操作系统类型（如 Windows，linux 等），MAC 地址，IP 地址，端口服务等资产信息。 9，支持通过页面，对告警前后存储报文数量进行配置，最多支持存储和下载告警前 3 个会话和后 100 个数据包。 10，支持 IPV4/IPV6 双栈管理，支持页面配置 DNS、路由操作。支持对设备各接口和设备整体流量统计能力，以折线图形式呈现 11，支持设备 CPU、内存、磁盘、运行时间展示，可以手动配置 CPU、内存和磁盘资源使用的预警范围，超过配置阈值，进行页面告警。 12，支持对设备存储空间进行清理，手动选择清理时间范围，可以设置数据保存时长，配置磁盘自动清理阈值百分比。		
15	政务边界墙 1	本期项目利旧使用现网的华为 USG6655E 防火墙设备,此次仅购买该设备配套的 3 年原厂硬件维保(含 3 年威胁防护升级），不涉及设备硬件采购。	台	1
16	政务边界墙 2	本期项目利旧使用现网的华为 USG6655E 防火墙设备,此次仅购买该设备配套的 3 年原厂硬件维保(含 3 年威胁防护升级），不涉及设备硬件采购。	台	1
17	云边界墙 1	本期项目利旧使用现网的华为 USG6655E 防火墙设备,此次仅购买该设备配套的 3 年原厂硬件维保(含 3 年威胁防护升级），不涉及设备硬件采购。	台	1
18	云边界墙 2	本期项目利旧使用现网的华为 USG6655E 防火墙设备,此次仅购买该设备配套的 3 年原厂硬件维保(含 3 年威胁防护升级），不涉及设备硬件采购。	台	1

五、运维及安全服务人员要求

投标方需为本项目配置驻场运维服务团队及远程技术支持团队，其中驻场运维服务团队需含有运维主管 1 名、网络工程师 1 名、运维工程师 6 名、信息安全工程师 3 名；投标方的远程技术支持团队入不驻场)中需有如下角色：资深网络工程师 1 名、云平台工程师 1 名、数据库工程师 1 名、机房监控管理工程师 1 名、流程管理工程师 1 名、存储工程师 1 名、资深系统工程师 1 名等。驻场运维服务团队及远程技术支持团队人员数量及角色必须按照对应要求配置。

5.1 项目服务人员数量要求

根据服务需求，投标方需配置 11 名项目服务人员为本项目提供驻场运维服务。

以下为驻场运维服务人员数量及职责简介：

●运维主管 1 名，负责运维体系建设、运维团队日常管理、协调服务提供单位远程资源提供运维服务；

●网络工程师 1 名，负责澄迈县电子政务外网核心级和汇聚级交换路由设备、各乡镇、委办局等接入交换机等网络系统的日常运维、监控及安全设备运维服务；

●运维工程师 6 名，负责为澄迈县电子政务外网相应系统提供运维服务，包括系统软硬件日常运维、数据库运维、系统监控及巡检等工作。

●信息安全工程师 3 名，负责对澄迈政务外网信息安全保障管理进行服务。针对系统面临的日常风险，安全驻点服务主要以人员驻场为主，对日常安全问题以及故障事件能快速的响应处理，保障澄迈政务外网信息系统安全、稳定运行。针对重要信息系统、阶段性安全检查，对重要业务突发的重要安全事件、故障问题进行响应、定位、分析、协调、处理，迅速响应分析、统一协调、有效处理来保障重要业务系统的正常运行。

投标方需配置至少 7 名远程技术专家为本项目提供远程技术支持服务，投标方的远程技术支持团队需有如下角色：资深网络工程师、云平台工程师、数据库工程师、机房监控管理工程师、流程管理工程

师、存储工程师、资深系统工程师。

以下为远程技术支持团队的人员数量及职责简介：

●资深网络工程师 1 名：负责为本项目提供远程网络专家支持，负责本项目的电子政务外网络规划及故障处置等；

●云平台工程师 1 名：负责为避迈县电子政务外网提供云平台专家咨询及远程支持服务；

●数据库工程顺 1 名：负责为澄迈县电子政务外网提供数据库专家支持，负责电子政务外网数据库的升级管理及故障管理等；

●机房监控管理工程师 1 名：负责为澄迈县电子政务外网机房环境提供远程技术咨询及故障处置工作等；

●流程管理工程师 1 名：负责为澄迈县营商环境建设局提供 IT 服务流程规划及 IT 服务流程咨询服务；

●存储工程师 1 名：负责为澄迈县电子政务外网数据存储设备提供规划及远程技术支持服务等；

●资深系统工程师 1 名:负责为澄迈县电子政务外网及其项目范围人内的应用系统提供远程技术支持服务；

5.2 驻场运维服务团队能力要求

●运维主管能力要求

投标方负责运维主管工作的工程师应熟悉 IT 基础技术架构及基础设施环境；熟悉基于 ITIL 的 ITSM 服务管理理念,熟悉 IT 服务管理体系，具有 ITSS 服务项目经理认证资质,精通数据中心机房的运维管理技术及流程，有管理大中型数据中心的工作经历和经验；具备良好的团队精神、团队建设技巧、人员辅导技巧及方法；具备问题分析能力、能够进行相关总结报告、分析文档报告、案设计等文档编写能力；能够对 IT 服务管理工作进行规划和实施;能够利用 IT 新技术指导运维管理工作，掌握 IT 发展的趋势并随时跟踪新技术的发展趋势。

●网络工程师能力要求

投标方负责核心级及汇聚级交换路由设备运维的网络工程师应具备丰富的网络维护经验，有从事大型集团骨干网、广域网规划与运

维的经历;能够依据厂家提供的维护标准流程开展相应的运维工作,具备很强的分析和处理问题的能力;对网络安全产品有深入了解和使用经验，精通防火墙/VPN 技术。精通华为、H3C、Cisco 等相关网络设备的安装、调试与维护;

●运维工程师能力要求

投标方负责系统运维的工程师具备大中型数据中心服务器/存储/虚拟化平台的维护经验；熟悉 WINDOWS、Linux 操作系统，VMware 及相关应用；熟悉备份、容灾、双机、SAN 等相关存储备份技术；熟悉存储虚拟化、主机虚拟化等技术，对存储、备份领域或对存储容灾领域有较深的理解。

●信息安全工程师能力要求

投标方负责安全运维的工程师应具备网络、信息安全等相关专业知识。具备对突发事件进行应急处置的能力。具备专业技术能力可对网络安全事件分析并定位问题原因,熟练掌握各类网络安全产品使用与运维（IPS、终端管控、威胁感知、流量分析、行为审计、堡垒机、安全网关等)。可根据客户总体安全防护体系调优安全策略，减少误报提高防护能力。具备编写网络安全应急预案的能力并组织各类安全应急演练。熟练使用各类安全工具（nessus、burp suite、 Kali、cobaltsreike 等)，能够对客户系统进行风险评估、或基线检查。根据所发现的问题给出修复指导或加固指导建议。具备 3 年及以上网络安全相关工作经验。

5.3 远程技术支持团队能力要求

●资深网络工程师能力要求

投标方需具备大型企业或政府单位网络运维及规划能力,精通网络技术及各种网络设备、安全设备等的安装调试及维护，极强的网络故障排除能力。当项目驻场服务团队网络工程师遇到无法解决的故障及问题时，需对项目驻场服务团队提供技术支持，以确保澄迈县政务外网正常稳定运行。

●云平台工程师能力要求

投标方需具备云平台管理经验，熟悉 kvm, qemu, libvirt 等虚拟化技术的使用及故障排查,熟悉 Openstack/Ceph 等虚拟化相关环

境的运维，熟悉Linux系统运维及管理。

●数据库工程师能力要求

投标方本地技术团队数据库工程师需具备大型企业及政府单位数据库管理经验，应具备丰富的大中型数据库的维护经验；熟悉SQL SERVER、ORACLE、MY SQL等数据库基本概念、原理、方法和技术；具备数据库系统安装、配置及数据库管理与维护的基本技能;掌握数据库性能优化的基本方法；能设计并优化数据库建设方案，制定数据库备份和恢复策略及工作流程与规范。

●机房监控管理工程师能力要求

投标方的机房监控管理工程师需具备型企业及政府数据中心管理经验，且具备大型数据中心机房值班经验；熟悉IT基础技术架构及基础设施环境；具备机房机位管理、服务器软硬件基本维护及对机房环境、消防、安保等日常监控的能力;熟悉数据中心机房的运维管理流程并严格遵循数据中心机房各项管理规定和值班计划,满足机房日常运营需求。

●流程管理工程师要求

投标方的流程管理工程师应具备大型企业及政府IT服务流程管理及设计经验,熟悉ITIL、ITSS流程管理规范,实施过大型企业ITSSS ITIL流程管理体系，具备丰富的流程管理经验。能为政府单位设计出符合行业特点的流程管理体系。

●存储工程师能力要求

投标方的存储管理工程师应具备有型企业及政府的存储管理相关工作经验,熟悉市面上主流的存储品牌产品,拥有丰富的存储规划及存储故障处置等工作经验，具备为政府单位提供存储设计、存储运维管理等能力。

●资探系统工程师能力要求

投标方的资探系统工程师应具备大型企业及政府的应用系统运维管理工作经验，熟悉windows、Linux等主流操作系统的运维管理；熟悉服务器相关技术，熟悉中间件相关技术，具有丰富的服务器及应用系统故障排除经验。

投标方需提供资深专家组远程支持团队的工程师名单(含社保)及简介。

5.4 其他要求

●投标方的运维工作人员应严格遵守澄迈县电子政务外网各项规章制度和管理规定，严格遵守信息安全保密制度，运维人员必须与项目建设单位签署相关保密协议。

●投标方应提供维护项目组成员的名单、简介和维护工作的职责分工。

●投标方投入本项目的所有工程师在项目建设单位的驻场办公时必须遵循项目建设单位的规章制度。

●投标方应对投入本项目的所有工程师进行信息安全相关培训，增强安全意识和提高安全技能，在运维过程中确保采购人的信息系统安全。

●投标方不得违反国家相关劳动法律法规，否则所引起的全部后果由服务提供单位负责。

●投标方投入本项目的所有工程师必须服从项目建设单位的统一管理，项目建设单位有权要求服务提供单位更换人员，如投标方要主动更换人员需经项目建设单位同意。

●投标方服务团队必须每月提供工作报告，对月度服务质量情况进行总结及通报。

六、服务方式

6.1 电话支持服务

投标方需提供全年7*24小时不间断的电话支持服务，对网络系统及应用系统的维护及时进行响应，提供的IT服务支持电话语言要求必须符合政府部门的相关标准。提供服务呼叫(包括服务电话、邮件、平台等)的接收、记录、分类和优先级排序;协调二线服务工程师解决上升的突发事件;提供电话完成服务回访工作，并对回访工作进行录单跟踪处理。

6.2 现场支持服务

投标方需提供 5*8 小时现场支持服务,现场响应时间<1 小时，如遇紧急突发事件或重大的安全事件，现场响应时间< 30 分钟。根据故障级别及响应要求，分派工程师现场处理服务请求或故障排查,以及应用系统的版本变更、配置更改等技术支持工作。

6.3 例行巡检服务

投标方需提供每个月 1 次的系统例行检查服务,根据系统运行状况提供例检报告,参与每个月的服务回顾会议,并对例检发现的问题进行跟踪处理，确保各项设备服务的正常稳定运行，可以运维月报的形式体现。

6.4 远程维护服务

投标方可根据故障情况提供远程直接维护服务,针对性服务方式,可以避免由交通等原因造成的服务响应不及时,同时可以提供相应的故障远程排查服务以及相关系统的变更、配置管理支持等,在远程接入条件满足下，连通时间为 15 分钟内。

七、人员培训要求

投标方需要派具有实践经验的培训教师为操作人员针对相关网络及安全设备、安全策略、安全管理及网络运维服务等内容进行现场集中培训,使招标人能够熟悉网络安全及网络运维服务的机制和原理。

八、运营要求

1．投标人遵循“政府指导规范，企业投资建设，政府购买服务”的建设营运机制，由售卖人通过招投标获取售卖服务的许可，政府购买服务，自主经营，自负盈亏。以此降低政府投资风险、技术风险、管理风险和运维风险；

2．投标人提供业务规范指导，进行准入、事前、事中及事后监管；

3．投标人提供包括资源建设的指导规范及运营活动的指导规范等的支持；

4．投标人分三年提供服务。

九、项目成果

9.1 在项目服务实施过程中，投标人应按照项目服务的技术管理、服务质量保障、项目实施管理以及其它需求提供全面详尽的工作报表，包括服务量、变更相关报表及服务 KPI 考核数据报表等，以确保服务提供的完整性，并依照进度计划和里程碑成果向招标方分阶段按时提交。投标方的阶段成果应该包含(但不仅限于)下表所列：

序号	工作阶段	各阶段提交成果
1	前期阶段	《项目服务解决方案》
2	项目启动	《服务提供人员清单及相关技能》
3	移交阶段(如有)	《服务移交方案》
4	正式服务阶段	《服务月报\季报》、《故障分析报告》等
5	服务期满阶段	《服务总结报告》

9.2 投标人必须根据所投项目的技术参数、资质资料编写投标文件。在中标结果公示期间，采购人有权对中标候选人所投的资质证书、公司场地等进行核查，如发与其投标文件中的描述不一，采购人将报政府管理部门严肃处理。

9.3 如在项目实施过程中投标人不按投标文件或合同内容要求执行，无法满足项目服务标准要求、降低服务质量标准等行为，采购人有权终止合同，并报政府采购管理部门严肃处理。

9.4 验收方法及标准：按本招标文件、中标人响应文件及国家、地方和行业的相关政策、法规及规定实施。安全标准：符合国家、地方及行业的相关政策、法规及规定要求。

9.5 项目的实质性要求：按本招标文件要求实施。

9.6 合同的实质性条款：采购人与中标人的名称和住所、标的、数量、质量、价款或者报酬、履行期限及地点和方式、验收要求、违约责任、解决争议的方法等内容。

十、其他事项

（一）合同履行期限（服务期）、服务地点及验收要求

1、合同履行期限（服务期）：自合同签订之日起提供 3 年相关服务；

2、服务地点：采购人指定地点；

3、验收要求：按照国家有关标准及招、投标文件的技术要求等进行验收。

（二）特殊说明

本项目预算为人民币 10744100.00 元，为保证服务质量，投标人不能低于成本价恶意报价，如中标人的报价过低，明显不符合市场价格,则采购人有权要求中标人提供预算金额的 10%作为履约保证金，同时预付款比例调整为 0%。如中标人在实施过程中偷工减量、不按工期完成项目，则采购人有权终止合同，没收履约保证金，并报主管部门严肃处理。

采购需求B包

一、总体要求

本期项目租赁运营商共计70条100M电子政务外网区网络专线，使澄迈县各政府部门及乡镇政府100多家单位采用数字电路接入方式连接澄迈县政务云，线路租赁规格需求清单如下：

序号	名称	规格要求	数量（条）	租赁期限（年）	备注
1	电子政务外网区网络租赁费	上下行带宽100M数字电路专线	70	3	

二、线路安装地点

电子政务外网区网络是由澄迈县各政府部门及乡镇政府单位多点数字电路专线单点汇聚到电子政务外网核心机房，各政府部门及乡镇政府线路租赁安装地点清单如下：

序号	安装地点	数量（条）
1	老城镇人民政府	1
2	永发镇人民政府	1
3	瑞溪镇人民政府	1
4	加乐镇人民政府	1
5	文儒镇人民政府	1
6	中兴镇人民政府	1
7	福山镇人民政府	1
8	桥头镇人民政府	1
9	大丰镇人民政府	1
10	金江镇人民政府	1
11	仁兴镇人民政府	1
12	金安筹备组	1
13	福山咖啡风情镇管理委员会	1
14	老城科技新城管理委员会	1
15	澄迈县委办公楼	1

16	澄迈县政府办公楼	1
17	澄迈县文化馆、双创指挥部	1
18	澄迈县总工会	1
19	中共澄迈县委政法委员会、澄迈县信访局	1
20	澄迈县卫生健康委员会	1
21	澄迈县财政局、发改委、住建局、审计局	1
22	澄迈县民政局	1
23	澄迈县旅文局	1
24	澄迈县乡村振兴局、综合执法局、团县委	1
25	澄迈县生态环境局、资规局	1
26	澄迈县农业农村局	1
27	澄迈县老干局	1
28	澄迈县工商业联合会	1
29	澄迈县司法局	1
30	澄迈县残联	1
31	澄迈县水务局	1
32	澄迈县税务局（金马办公点）	1
33	澄迈县税务局（文化北办公点）	1
34	澄迈县教育局	1
35	澄迈县人社局	1
36	澄迈县侨联	1
37	澄迈县林业局	1
38	澄迈县交通运输局	1
39	澄迈县澄迈中学	1
40	澄迈县工信科局、商务局、医保局、促投中心	1
41	澄迈县编制委员会（县科协）	1
42	澄迈县图书馆	1
43	澄迈县地震中心	1
44	澄迈县营商环境建设局（政务中心）	1

45	澄迈县热作中心	1
46	澄迈县疾病预防控制中心	1
47	澄迈县中医院	1
48	澄迈县妇幼保健院	1
49	澄迈县应急局	1
50	澄迈县委党校	1
51	澄迈县供销社	1
52	澄迈县农业技术服务中心	1
53	澄迈县党史研究中心	1
54	澄迈县农业机械服务中心	1
55	澄迈县房管局	1
56	澄迈县粮食中心	1
57	澄迈县机关事务管理局	1
58	爱国卫生运动服务中心	1
59	澄迈县市场监督管理局	1
60	澄迈县红十字会	1
61	澄迈县皮肤性病防治所	1
62	国家统计调查大队（政府办门）	1
63	澄迈县畜牧局、二轻中心	1
64	澄迈城市建设投资有限公司、城乡建设与旅游发展有限	1
65	澄迈县劳动执法大队（澄迈就业驿站大楼）	1
66	澄迈县纪委办公楼	1
67	澄迈县纪委太平办事点	1
68	澄迈县质量监督管理所、澄迈县乡村振兴投资发展有限公司	1
69	澄迈县交警大队（金马办公点）	1
70	澄迈县公安局	1

三、技术要求

1、线路技术要求：

电路质量标准：

（1）电路通路可用率达到99.9%。

（2）电路验收指标为：比特率误码率小于10^{-7}。

2、交付工期要求：自合同签订之日起35个自然日内完成线路实施并交付使用。

3、平均无故障时间：网络线路故障发生后应立即响应。需要现场处理的，在道路畅通无拥塞的情况下，应在1小时内响应故障并到达故障现场。业务中断4个小时内线路恢复百分比为95%。

采购需求C包

一、总体要求

为了保障澄迈县电子政务外网的可用性,本期项目租赁运营商共计70条50M数字电路专线组建独立办公互联网区网络，与电子政务外网区网络安全隔离，满足澄迈县各政府部门及乡镇政府100多家单位互联网安全接入需求,此标包为其中35条50M数字电路专线租赁服务，线路租赁规格需求清单如下：

序号	名称	规格要求	数量（条）	租赁期限（年）	备注
1	互联网区专线租赁服务	上下行带宽50M数字电路专线	35	3	

二、线路安装地点

互联网区网络是由澄迈县各政府部门及乡镇政府单位多点数字电路专线单点汇聚到电子政务外网核心机房,各政府部门及乡镇政府线路租赁安装地点清单如下：

序号	安装地点	数量（条）
1	老城镇人民政府	1
2	瑞溪镇人民政府	1
3	文儒镇人民政府	1
4	大丰镇人民政府	1
5	金江镇人民政府	1
6	仁兴镇人民政府	1
7	金安筹备组	1
8	福山咖啡风情镇管理委员会	1
9	老城科技新城管理委员会	1
10	澄迈县委办公楼	1
11	澄迈县政府办公楼	1
12	澄迈县文化馆、双创指挥部	1
13	中共澄迈县委政法委员会、澄迈县信访局	1
14	澄迈县卫生健康委员会	1
15	澄迈县财政局、发改委、住建局、审计局	1

16	澄迈县旅文局	1
17	澄迈县生态环境局、资规局	1
18	澄迈县残联	1
19	澄迈县税务局（金马办公点）	1
20	澄迈县税务局（文化北办公点）	1
21	澄迈县人社局	1
22	澄迈县侨联	1
23	澄迈县图书馆	1
24	澄迈县妇幼保健院	1
25	澄迈县应急局	1
26	澄迈县委党校	1
27	澄迈县党史研究中心	1
28	澄迈县机关事务管理局	1
29	爱国卫生运动服务中心	1
30	澄迈县皮肤性病防治所	1
31	国家统计调查大队（政府办门）	1
32	澄迈城市建设投资有限公司、城乡建设与旅游发展有限	1
33	澄迈县劳动执法大队（澄迈就业驿站大楼）	1
34	澄迈县纪委办公楼	1
35	澄迈县纪委太平办事点	1

三、技术要求

1、线路技术要求：

电路质量标准：

（1）电路通路可用率达到99.9%。

（2）电路验收指标为：比特率误码率小于10^{-7}。

2、交付工期要求：自合同签订之日起35个自然日内完成线路实施并交付使用。

3、平均无故障时间：网络线路故障发生后应立即响应。需要现场处理的，在道路畅通无拥塞的情况下，应在 1 小时内响应故障并到达故障现场业务中断 4 个小时内线路恢复百分比为 95%。

采购需求D包

一、总体要求

为了保障澄迈县电子政务外网的可用性,本期项目租赁运营商共计70条50M数字电路专线组建独立办公互联网区网络，与电子政务外网区网络安全隔离，满足澄迈县各政府部门及乡镇政府100多家单位互联网安全接入需求,此标包为其中35条50M数字电路专线租赁服务，线路租赁规格需求清单如下：

序号	名称	规格要求	数量（条）	租赁期限（年）	备注
1	互联网区专线租赁服务	上下行带宽50M数字电路专线	35	3	

二、线路安装地点

互联网区网络是由澄迈县各政府部门及乡镇政府单位多点数字电路专线单点汇聚到电子政务外网核心机房,各政府部门及乡镇政府线路租赁安装地点清单如下：

序号	安装地点	数量（条）
1	永发镇人民政府	1
2	加乐镇人民政府	1
3	中兴镇人民政府	1
4	福山镇人民政府	1
5	桥头镇人民政府	1
6	澄迈县总工会	1
7	澄迈县民政局	1
8	澄迈县乡村振兴局、综合执法局、团县委	1
9	澄迈县农业农村局	1
10	澄迈县老干局	1
11	澄迈县工商业联合会	1
12	澄迈县司法局	1
13	澄迈县水务局	1
14	澄迈县教育局	1
15	澄迈县林业局	1

16	澄迈县交通运输局	1
17	澄迈县澄迈中学	1
18	澄迈县工信科局、商务局、医保局、促投中心	1
19	澄迈县编制委员会（县科协）	1
20	澄迈县地震中心	1
21	澄迈县营商环境建设局（政务中心）	1
22	澄迈县热作中心	1
23	澄迈县疾病预防控制中心	1
24	澄迈县中医院	1
25	澄迈县供销社	1
26	澄迈县农业技术服务中心	1
27	澄迈县农业机械服务中心	1
28	澄迈县房管局	1
29	澄迈县粮食中心	1
30	澄迈县市场监督管理局	1
31	澄迈县红十字会	1
32	澄迈县畜牧局、二轻中心	1
33	澄迈县质量监督管理所、澄迈县乡村振兴投资发展有限公司	1
34	澄迈县交警大队（金马办公点）	1
35	澄迈县公安局	1

三、技术要求

1、线路技术要求：

电路质量标准：

（1）电路通路可用率达到99.9%。

（2）电路验收指标为：比特率误码率小于10^{-7}。

2、交付工期要求：自合同签订之日起35个自然日内完成线路实施并交付使用。

3、平均无故障时间：网络线路故障发生后应立即响应。需要现场处理的，

在道路畅通无拥塞的情况下，应在 1 小时内响应故障并到达故障现场。业务中断 4 个小时内线路恢复百分比为 95%。

采购需求E包

一、项目名称

购买澄迈县政务外网服务项目。

二、监理内容

本包监理范围为本招标文件购买澄迈县政务外网服务项目内容的监理。

三、监理服务周期

本项目监理服务周期自签订合同之日起，至建设项目完成竣工验收。

四、监理技术要求

4.1 监理范围

重点对项目建设过程中设备/材料的采购、设备安装调试、系统集成、软件开发及应用技术培训、试运行、测试、验收等全过程进行监督管理，从硬件监理、软件监理、系统集成监理等三个方面梳理该项目建设的工程监理应如何通过切实有效方式、方法、手段达到建设方所要求的深度、广度，最终实现工程监理的目标。实现对质量、进度、经费、变更的控制及合同管理和文档管理。当工程质量或工期出现问题或严重偏离计划时，应及时指出，并提出对策建议，同时督促承建单位尽快采取措施。

4.2 监理目标控制方案

以工程建设合同、监理委托合同、国家（GB/T19668.1-19668.6《信息化工程监理规范》、信息产业部信部信[2002]570号《信息系统工程监理暂行规定》）及有关法规、技术规范与标准、项目建设单位需求为依据，通过专业的控制手段，协助建设单位全面地进行技术

咨询和技术监督，对工程全过程进行监督、管理、指导、评价，并采取相应的组织措施、技术措施、经济措施和合同措施，确保建设行为合法、合理、科学、经济，使建设进度、投资、质量达到建设合同规定的目标。

1)、监理质量目标控制

监理质量目标控制是监理技术服务的核心所在，也是监理单位综合实力的最好反映，所以做好监理质量目标控制方案，确保本项目建设质量能达到建设单位要求的质量目标。

确保本项目建设质量达到工程合同中规定的功能、技术参数等目标。

确保工程建设中的设备和各个节点满足相关国家（GB/T19668.1-19668.6《信息化工程监理规范》、信息产业部信部信[2002]570号《信息系统工程监理暂行规定》）、地方或行业质量标准和技术标准，按照承建合同要求进行基于总体方案的细化设计、开发、安装、调试和运行；系统集成和软件开发过程涉及用户需求调研分析、概要设计、详细设计、系统实现、系统测试和系统运行等比较复杂、制约因素多的工作内容，应该成为质量控制的重点；深化设计方案的确定、开发平台选定，也要进行充分论证。

要求监理在整个工程实施过程中做好对工程质量的事前控制，事中监督和事后评估，以确保工程质量合格。

投标人应针对本项目建设中软硬件设备采购、设备安装调试、系统集成、软件开发、工程培训等提出工程监理的质量控制原则、方法、措施、工作流程和目标。

2)、监理进度目标控制

确保本项目按合同规定的工期完工。

依据合同所约定的工期目标，在确保质量和安全的原则下，采用动态的控制方法，对进度进行主动控制，确保项目按规定的工期完工。

通过对本项目概要设计的分析、研究，提出针对本项目建设的、有代表性的信息工程监理进度控制的主要原则、方法、内容、措施、工作流程和目标。

3)、监理投资目标控制

协助用户控制本项目建设总投资在项目预算及审计范围内，减少项目建设中的额外开支。

以项目建设方和承建单位实际签订的合同金额为准，确保项目费用控制在合同规定的范围内。

在项目建设中，合理减少项目变更，保护建设单位的经济利益。

4.3 工程监理重点难点分析

投标人应根据本项目建设的特点，从实际出发分析本项目监理工作的重点、难点，并根据分析的结果制定相应的监理工作规划、对策和策略，以便日后有针对性的开展建设工程的监理服务工作。

（一）项目组织及总体技术方案的质量控制

1、协助审查项目建设方的投标书、合同及实施方案；

2、在技术上、经济上、性能上和风险上进行分析和评估，为采购人提供建议；

3、协助审查项目建设方提交的组织实施方案和项目计划等相关文档；

4、协助审查项目建设方的工程质量保证计划及质量控制体系；

5、参与制定项目质量控制的关键节点及关键路径。

（二）项目质量控制

1、组织措施：建立质量管理系统，完善职责分工及有关质量监督制度，落实质量控制责任。

2、系统集成质量控制

审核系统总集成方案；

对采购的硬件设备及网络环境的综合质量进行检验、测试和验收；

参与制定系统验收大纲；

对设备安装、调试进行验收；

对系统进行总体验收。

3、人员培训的质量控制

协助审查并确认培训计划，审定培训大纲；

监督审查建设方实施其培训计划，并征求采购人的意见反馈；

监督审查考核工作，评估培训效果；

协助审核并确认培训总结报告。

4、文档、资料的质量控制

监督审查建设方提供的设备型号、数量、到货时间以及设备的技术资料、系统集成和软件安装在实施过程中所有相关文件的标准性和规范化，在各项目验收时，应监督项目建设方提交符合规定的成套资料，包括印刷本和电子版。

对监理项目实施过程中的文档进行标准化、规范化管理，在监理项目验收时，应提交符合规定的监理项目的成套资料，包括印刷本和电子版。

（三）进度协调控制

1、组织措施：建立进度控制协调制度，落实进度控制责任。

2、编制项目控制进度计划：编制项目总进度计划和网络图。按各子系统实际情况进行编制，包括系统建设开工、设备的采购、设备

的安装调试、软件的编制、试运行等各方面内容，做到既要保证各子系统、各阶段目标的顺利实现，又要保证项目间、阶段间的衔接、统一和协调。

3、审查各子系统建设方编制的工作进度计划：分析系统建设进度计划是否能满足合同工期及系统建设总进度计划的要求，特别要对照上阶段计划工程量完成情况进行审查，对为完成系统建设进度计划所采取的措施是否恰当、设备能否满足要求、管理上有无缺陷进行审查。要根据建设方所能提供的人员及设备性能复核、计算设备能力和人员安排是否满足要求等，分析判断计划是否能落实，审查建设方提出的设备供应计划能否落实。如发现供应计划未落实，应及时报告采购人，要求建设方采取应急措施满足系统建设的需求。

4、系统建设进度的现场检查：随时或定期、全面地对进度计划的执行情况跟踪检查，发现问题及时采取有效措施加以解决。加强系统建设准备工作的检查，在工程项目或部分工序实施前，对情况进行检查，要加强检查设备、人员安排、各项措施的落实情况，确保准备工作符合要求，不影响后续工程的进行。

5、进度计划的分析与调整：要保证建设进度与计划进度一致，经常对计划进度与实际进度进行比较分析，发现实际进度与计划进度不符时，即出现进度偏差时，首先分析原因，分析偏差对后续工作的影响程度，并及时通知建设方采取措施，向建设方提出要求和修改计划的指令。

（四）投资控制

1、组织措施：建立健全项目管理组织，完善职责分工及有关质量项目管理制度，落实投资控制的责任。

2、审查设计图纸和文件，审查建设方的施工组织设计和各项技

术措施，深入了解设计意图，在保证系统建设质量和安全的前提下尽可能优化设计。

3、严格督促建设方按合同实施，严格控制合同外项目的增加，协助采购人严格控制设计变更，制定设计变更增加工作量的报批制度；及时了解系统建设情况，协调好各方矛盾，减少索赔事件的发生。对发生的事件严格按合同及法律条款进行处理，认真进行索赔调解。

（五）合同管理

合同管理是加快系统建设进度、降低系统建设造价、保证系统建设质量的有效途径之一。通过合同管理，可以督促建设方在各个阶段按照合同要求保证设备、人员的配备及投入，保证各阶段目标按合同实施，减少索赔事件，控制系统建设结算等。具体要求如下：

1、以合同为依据，本着“实事求是、公正”的原则，合情合理地处理合同执行过程中的各种争议。

2、分析、跟踪和检查合同执行情况，确保项目建设方按时履约。

3、对合同的工期的延误和延期进行审核确认。

4、对合同变更、索赔等事宜进行审核确认。

5、根据合同约定，审核项目建设方的支付申请。

6、建立合同目录、编码和档案。

7、合同管理坚持标准化、程序化，如设计变更、延期、索赔、计量支付等应规定出固定格式和报表。合同价款的增减要有依据，合同外项目增加要严格审批制度。重大合同管理问题的处理，如大的变更、索赔、复杂的技术问题等，组成专门小组进行研究。不符合实际情况的合同条款及时向采购人报告，尽早处理，以免造成损失。

（六）信息、工程文档管理

在项目管理过程中，为了实现对进度、质量、投资的有效控制，

处理有关合同管理中的各种问题，监理方需要收集各种有用的信息。信息的来源主要包括采购人文件、设计图纸和文件、建设方的文件、建设现场的现场记录（或项目管理日志）、会议记录、验收情况及备忘录等等。其中项目管理日志是进行信息管理的一个最重要的方面。项目管理日志主要包括当天的工作项目和工作内容、投入的人力和设备运行情况、计划的完成情况及进度情况、停工和返工及窝工情况。信息管理主要措施要求如下：

1、制定详细的信息收集、整理、汇总、分析、传递和利用制度，力求信息管理的标准化和制度化。由专人负责系统建设信息的收集、分类、整理储存及传递工作。信息传递以文字为主，统一编号，利用计算机进行管理，力求信息管理的高效、迅速、及时和准确，为系统建设提供及时有用的信息和决策依据。

2、在项目实施过程中做好工程监理日记和工程大事记。

3、做好双方合同、技术建设方案、测试文档、验收报告等各类往来文件的存档。

4、建立必要的会议、例会制度，整理好会议纪要，并监督会议有关事项的执行情况。

5、立足于建设现场，加强动态信息管理，对现场的信息进行详细记录和分析，做到以文字为基础，以数据说明问题。根据收集到的信息与合同进行比较，督促建设方的人员和设备到位，促使承包商按合同完成各项目标，从而实现对进度、质量、投资的控制。

6、建立完整的各项报表制度，规范各种适合本项目的报表。定期将各种报表、信息分类汇总，及时向采购人及有关各方报送。

7、监理项目验收时，应提交符合规定的有关工程的成套资料，包括印刷本和电子版。

（七）日常监理

1.掌握监理范围内涉及的各种技术及相关标准；

2.安排足够的监理人员，按工程需要派驻相应的专业人员进行项目监理，至少保证2名专职信息系统监理工程师在现场，随时为采购人提供服务，总监理工程师必需专职于本项目；

3.制定工程管理的组织机构方案并协助采购人组建相关机构，并提供相关培训；

4.熟悉了解项目的业务需求，协助采购人对项目的目标、范围和功能进行界定，参与并协助项目的设计方案交底审核工作；

5.建立健全科学合理的会议制度，并予以贯彻落实；

6.建立健全科学合理的文档管理制度，制订开发过程中产生的各类文档制作、管理规范，并予以贯彻落实；

7.与采购方一起制定评审机制，在工程实施全过程中随时关注隐患苗头，如发现将会导致工程失败的情况出现时，应及时启动评审机制，组织专家对工程实施情况进行评审，对评审不合格的，应向采购方提出终止合同意见。此外，还应组织定期评审（阶段性评审、里程碑评审、验收评审），对评审结果为优的，提出奖励意见，评审不合格的，则向采购方提出处理意见；

4.4 工程各阶段的监理规划、实施

投标人应对本项目从设计施工到项目竣工验收阶段制定一整套工程监理的工作流程，并叙述各阶段主要监理工作内容。

本项目监理工作主要分为设备/材料采购、施工阶段、验收阶段、质保期阶段等。

⑴、设备/材料采购监理

建设项目由承包单位承担设备/材料采购任务，工程监理单位在设备/材料采购阶段监理工作主要有：

✧ 审核承包单位的设备采购计划和设备采购清单；

✧ 订货进货验证；

✧ 组织到货验收；

✧ 鉴定、设备移交等；

⑵、施工阶段监理

1、开工前的监理

1） 审核施工设计方案：开工前，由监理单位组织实施方案的审核，内容包括设计交底，了解需求、质量要求，依据设计招标文件，审核总体设计方案和有关的技术合同附件，以避免因设计失误造成实施的障碍；

2） 审核实施方案的合法性、合理性、与设计方案的符合性；

3） 审批施工组织设计：对施工单位的实施工作准备情况进行和监督；

4） 审核施工进度计划：对施工单位的施工进度计划进行评估和审查；

5） 审核实施人员：确认施工方提交的实施人员与实际工作人员的一致性，如有变更，则要求叙述其原因；

6） 审核《软件项目开发计划》。

2、施工准备阶段的监理

1） 审批开工申请，确定开工日期；

2） 了解承包商设备订单的定购和运输情况；

3） 了解施工条件准备情况；

4） 了解承建单位实施前期的人员组织、施工设备到位情况；

5） 编制各个子项目监理细则；

6） 签发开工令。

3、施工阶段的监理

1） 审核软件开发各个阶段文件；

2） 协助采购人组织软件开发阶段评审；

3） 材料、硬件设备、系统软件的供货计划的审核；

4） 材料、硬件设备、系统软件的进场、开箱和检验；

5） 促使项目中所使用的产品和服务符合合同及国家相关法律法规和标准；

6） 对施工各个阶段的安装工艺进行检查；

7） 审核项目各个阶段进度计划；

8） 督促、检查承建单位进度执行情况；

9） 审查项目变更，提出监理意见；

10） 审查承建单位阶段款支付申请，提出监理意见；

11） 按周（月、旬）定期报告项目情况；

12） 组织召开项目例会和专项会议。

4、试运行阶段的监理

1） 协助建设方确认项目进入试运行；

2） 监查系统的调试和试运行情况，记录系统试运行数据；

3） 进行试运行期系统检测或测试，做出检测或测试报告；

4） 对试运行期间系统出现的质量问题进行记录，并责成有关单位解决。解决问题后，进行二次监测；

5） 进行试运行时间核算；

6） 协助业主确认试运行通过。

⑶、验收阶段监理

1、验收阶段

1） 对承建单位在试运行阶段出现的问题的整改情况进行监督和复查；

2） 监督检查承建单位作好用户培训工作，检查用户文档；

3） 组织系统初步验收；

4） 审查承建单位提交的竣工文档；

5） 参与项目竣工验收；

6） 竣工资料收集整理齐全并装订，签署验收报告；

7） 审核项目结算；

8） 审查承建单位阶段款支付申请，提出监理意见；

9） 向建设单位提交监理工作总结；

10) 将所有的监理材料汇总，编制监理业务手册，提交采购人；

11) 系统验收完毕进入保修阶段的审核与签发移交证书。

2、项目移交阶段

1） 系统的设计方案、设计图纸和竣工资料的全部移交；

2） 设备、软件、材料等的验收文档核实；

3） 施工文档的移交；

4) 竣工文档的移交；

5) 项目的整体移交。

⑷、质保期阶段监理

监理单位承诺依据委托监理合同约定的工程质量保修期规定的时间、范围和内容开展工作主要有：

1) 定期对项目进行回访，协助解决技术问题；

2) 对项目建设单位提出的质量缺陷进行检查和记录；

3) 对质量缺陷原因进行调查分析并确定责任归属；

4) 检查承建单位质保期履约情况，督促执行；

5) 审查承建单位阶段款支付申请，提出监理意见。

投标人应根据上述监理工作内容（但不局限于上述内容），分别制定详细的监理工作流程，使本项目的监理工作流程化、制度化。

2.6 监理工作要求

1、监理工作制度要求

根据本项目的特色，本项目要求以现场监理为主要方式进行，在施工现场主要监理人员必须具备所从事监理业务的专业技术和类似系统经验，并具有丰富的项目管理经验。监理工作必须由具有相应资质和职称的人员来担任。本次监理项目实行总监理工程师负责制，在整个项目建设期间，必须在建设期间全程常驻至少一名监理工程师在甲方现场。监理公司应建立项目监理小组，负责整个项目的全程监理工作，本项目必须配备不少于 3 名的监理工程师。监理人员的确定和变更，须事先经业主方同意。监理人员必须奉公守法，具有高度的责任心。

2、监理项目组织要求

工程监理组织形式应根据工程项目的特点、工程项目承包模式、业主委托的任务以及监理单位自身情况而确定，结构形式的选择应考虑有利于项目合同管理、有利于目标控控制、有利于决策指挥、有利于信息沟通。

要求投标人在报价方案中要明确工程监理的各项运作，包括监理人员的相关资料、职能分配、监理组织的构成及工作流程、各项监理工作的相关负责人等。

3、监理信息管理要求

投标人应制定有关本项目信息管理流程，规范各方文档并负责整理记录归档业主单位与承建单位来往的文件、合同、协议及会议记录等各种文档，并定期以监理月（周/季）报形式提交业主。包括下列监理工作：

1）做好监理日记及工程大事记；

2）做好合同批复等各类往来文件的批复和存档；

3）做好项目协调会、技术专题会等各项会议纪要；

4）管理好实施期间的各类、各方技术文档；

5）做好项目周报；

6）做好监理建议书、监理通知书存档；

7）阶段性项目总结。

投标人应针对项目特点，制定相应的信息分类表、信息流程图、信息管理表格、信息管理工作流程与措施，同时要求采用先进的项目信息管理软件对项目信息进行综合管理。

4、监理合同管理要求

本项目建设过程中会与承建单位签订各种合同，投标人应该针对项目特点制定合同从草案到签署的管理工作流程与措施，规范合同管

理，并在具体项目合同执行时进行下列监理工作：

1）跟踪检查合同的执行情况，确保承建单位按时履约；

2）对合同工期的延误和延期进行审核确认；

3）对合同变更、索赔等事宜进行审核确认；

4）对合同终止进行审核确认；

5）根据合同约定，审核承建单位提交的支付申请，签发付款凭证。

要求对项目合同进行合理的管理，以完善整个项目建设的过程。

五、监理服务准则

遵照国家 GB/T19668.1-19668.6《信息化工程监理规范》、信息产业部信部信[2002]570 号《信息系统工程监理暂行规定》的规定，以“守法、诚信、公正、科学”的准则执业，维护建设方与承建方的合法权益。具体应做到：

1） 执行有关项目建设的法律、法规、规范、标准和制度，履行监理合同规定的义务和职责。

2） 不收受被监理单位的任何礼金。

3） 不泄漏所监理项目各方认为需要保密的事项。

4） 遵守国家的法律和政府的有关条例、规定和办法等。

5） 坚持公正的立场，独立、公正地处理有关各方的争议。

6） 坚持科学的态度和实事求是的原则。

7） 在坚持按监理合同的规定向建设单位提供技术服务的同时，帮助被监理者完成起担负的建设任务。

8） 不泄漏所监理的项目需保密的事项。

六、监理依据

1）国家 GB/T19668.1-19668.6《信息化工程监理规范》、信息产

业部信部信[2002]570号《信息系统工程监理暂行规定》和海南省有关信息系统项目建设和监理管理规范；

2）建设单位与承建单位签订的承包工程合同

3）建设单位与监理单位签订的委托监理合同

4）本工程招标书、招标过程文件、各中标商的投标书

5）国家有关合同、招投标、政府采购的法律法规

6）部颁、地方政府的信息工程、信息工程监理的管理办法和规定

7）建设工程和信息工程相关的国家、行业标准和规范

8）建设工程和信息工程技术监督、工程验收规范

9）与工程相关的技术资料

10）其他与本项目适用的法律、法规和标准

11）国家、地方及行业相关的技术标准

七、安全保密要求

本项目要求投标人制定一整套工程监理安全保密制度，确定工程保密责任人，同时要求投标人：

1） 按照国家、省、市的有关法规文件规定，要求监理履行保密责任，并与建设单位签订保密协议；

2） 监理单位各级组织严格履行保密职责；

3） 按照公司内部保密规定开展监理工作。

八、监理验收要求

1） 审核监理方应提交的各类监理文档和最终监理总结报告，综合评估监理方在系统开发进度、质量把关、重难点问题解决、项目投资等方面的监理情况。只有文档齐全，系统开发工作中没有出现重大质量事故才予验收。

2) 本监理工作的最终验收由委托方组织。

九、其它要求

1.监理总工程师

1) 具有信息系统监理师资格证书；

2) 5 年以上监理或项目管理经验。

2.监理工程师

1) 具有信息系统监理师资格证书资格；

3.项目管理及施工组织

投标人须提供详尽的监理技术方案，包括但不限于施工组织部署、项目管理目标、施工准备、进度控制、质量管理、验收方法等内容。

采购需求 F 包

一、项目概况

1、服务期限：3 年，采购人下达当年测评通知书后 60 日内交付测评报告。

2、交付地点：用户指定地点。

3、交付方式：免费送至用户指定地点。

二、技术要求

1、标包名称

澄迈县政务外网服务项目网络安全等级保护测评服务

2、项目内容

通过委托专业的网络安全等级保护测评服务机构，依据《信息安全技术网络安全等级保护基本要求》等相关文件及标准要求，针对正在运行的信息系统实施信息安全等级保护测评，服务对象如下：

序号	信息系统/服务项目		级别	备注	服务类型
1	澄迈县政务外网平台		三级	S3A3G3	现场服务
3	测评实施过程及结果输出	一、依据《信息安全技术网络安全等级保护基本要求》等有关管理规范和技术标准，对等级保护对象进行安全等级保护测评； 二、测评的内容包括安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理等十个层面进行合规性检查，分析信息系统与安全保护等级要求之间的差距； 三、完成测评工作后，《网络安全等级保护测评报告》，并根据信息系统及安全防护措施的现状提出具有针对性的整改意见。			

3、服务实施

3.1　服务目标

通过信息安全等级保护测评服务，对本单位运行的信息系统开展符合性测评,衡量信息系统的安全保护管理措施和技术防护措施是否符合等级保护基本要求，是否具备了相应的安全保护能力。找出问题，针对性的制定整改措施，推进信息 安全防护体系不断完善。

3.2　服务期限

采购人下达测评通知书后 60 日内交付测评
报告。

4、服务要求

4.1　服务内容

1) 对用户进行等级保护咨询服务，包括等级保护政策/标准咨询、信息系统等级变更咨询、等级保护建设整改咨询等。

2) 对用户的信息系统进行摸底、分析和梳理，提出详细的测评方案及完成系统备案工作。

3) 逐一对信息系统进行安全等级保护测评，测评的内容包括但不限于以下内容：

①安全技术测评：包括安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心等五个方面的安全测评；

②安全管理测评：安全管理机构、安全管理制度、安全管理人员、安全建设管理、安全运维管理等五个方面的安全测评。

4) 完成测评工作后，提出整改方案；最后出具符合要求的测评报告。

4.2　项目成果交付

1）信息系统定级相关文件和报告；

2）信息系统测评报告及整改建议。

4.3　测评服务步骤

信息系统等级保护测评过程需按照《信息系统安全等级保护测评过程指南》开展工作，等级测评过程分为四个基本测评活动：测评准备活动、方案编制活动、现场测评活动、分析及报告编制活动。测评双方之间的沟通与洽谈应贯穿整个等级测评过程。

4.3.1 测评准备活动

测评准备工作包括编制项目启动、信息收集和分析、工具和表单准备。

详细要求见下表：

项目内容	工作内容	成果输出
1.项目启动	1.组建测评项目组	
	2.编制《项目计划书》	
	3.确定测评委托单位应提供的资料	
2.信息收集分析	1.定级报告及整改方案分析	《系统基本情况调研表》
	2.整理调查表单	
	3.发放调查表单给测评委托单位	
	4.协助测评委托单位填写调查表	
	5.收回调查结果	
	6.分析调查结查	
3.工具和表单准备	1.调试测评工具	确定测评工具、形成测评结果记录表
	2.模拟被测系统搭建测评环境	
	3.模拟测评	
	4.准备打印表单	

4.3.2 方案编制活动

方案编制活动包括测评对象确定、测评指标确定、测试工具接入点确定、测评内容确定、测评指导书开发及测评方案编制等六项主要任务。

详细要求见下表：

工作内容	工作详细任务	输出成果

1.测评对象确认	识别被测系统等级 识别被测系统的整体结构 识别被测系统的边界 识别被测系统的网络区域 识别被测系统的重要节点和业务应用 确定测评对象	《测评方案》的测评对象部分
2.测评指标确定	识别被测系统业务信息和系统服务安全保护等级	《测评方案》的测评指标部分
	选择对应等级的 ASG 三类安全要求作为测评指标	
	就高原则调整多个定级对象共用的某些物理安全或管理安全测评指标	
3.工具测试点确定	确定工具测试的测评对象 选择测试路径 确定测试工具的接入点	《测评方案》的测试工具接入点部分
4.测试内容确定	识别每个测评对象对象的测评指标	《测评方案》的单项测评实施和
	识别每个测评对象对应的每个测试指标的测试	
工作内容	**工作详细任务**	**输出成果**
	方法	系统测评实施部分
5.测评指导书开发	从已有的测评指导书中选择与测评对象对应的手册	《测评方案》的测评实施手册部分
	针对没有现成测评指导书的测评对象，开发新的测评指导书	
6. 测评方案编制	描述测评项目基本情况和工作依据	向用户提交《测评方案》
	描述被测系统的整体结构、边界和网络区域	
	描述被测系统的重要节点和业务应用	
	描述测评指标	
	描述测评对象	

	描述测评内容和方法	

4.3.3 现场测评活动

现场测评活动通过与测评委托单位进行沟通和协调，为现场测评的顺利开展打下良好基础，然后依据测评方案实施现场测评工作，将测评方案和测评工具等具体落实到现场测评活动中。现场测评工作应取得分析与报告编制活动所需的、足够的证据和资料。

现场测评活动包括现场测评准备、现场测评和结果记录、结果确认和资料归还三项主要任务。

详细要求见下表：

工作内容	工作详细任务	输出
1.现场测评准备	现场测评授权书签署	向用户确认测评方案
	召开现场测评启动会	
	双方确认测评方案	
	双方确认配合人员、环境等资源	
	确认信息系统已经备份	
	测评方案、结构记录表格等资料更新	
2.现场测评和结果记录	依据测评指导书实施测评	访谈结果：技术安全和管理安全测评的测评结果记录或录音文档审查结果：管理安全测评的测评结果记录 配置检查结果： 技术安全测评的网络、主
	记录测评获取的证据、资料等信息	
	汇总测评记录，如果需要，实施补充测评	
工作内容	**工作详细任务**	**输出**
	召开现场测评结束会	机、应用测评结果记录表格 工具测试结果： 技术安全测评的网络、主机、应用测评结果记
	测评委托单位确认测评过程中获取的证据和资料的正确	

	性，并签字认可	录，工具测试完成后的电子输出记录，备份的测试结果文件
3.结果确认和资料归还	测评人员归还借阅的各种资料	实地察看结果： 技术安全测评的物理安全和管理安全测评结果记录 测评结果确认： 现场核查中发现的问题汇总、证据和证据源记录、被测单位的书面认可文件

4.3.4 报告分析及编制活动

在现场测评工作结束后，应对现场测评获得的测评结果（或称测评证据）进行汇总分析，形成等级测评结论，并编制测评报告。

测评人员在初步判定单元测评结果后，还需进行整体测评，经过整体测评后，有的单元测评结果可能会有所变化，需进一步修订单元测评结果，而后进行风险分析和评价，形成等级测评结论。分析与报告编制活动包括单项测评结果判定、单元测评结果判定、整体测评、风险分析、等级测评结论形成及测评报告编制六项主要任务。

详细要求见下表：

工作内容	工作详细任务	工作依据（模版）
1.单项测评结果判定	分析测评项所对抗威胁的存在情况	等级测评报告的单项测评结果部分
	分析单个测评项是否有多方面的要求内容，依据“优势证据”法选择优势证据，并将优势证据与预期测评结果相比较	
	综合判定单个测评项的测评结果	
2.单元测评	汇总每个测评对象在每个测评单元的	等级测评报告的单项测

结果判定	单项测评结果	评结果汇总分析部分
	判定每个测评对象的单元测评结果	
3.整体测评	分析不符合和部分符合的测评项与其	等级测评报告的系统整
工作内容	**工作详细任务**	**工作依据（模版）**
	他测评项（包括单元内、层面间、区域间）之间的关联关系及对结果的影响情况	体测评分析部分
	分析被测系统整体结构的安全性对结果的影响情况	
4.风险分析	整体测评后的单项测评结果再次汇总	等级测评报告的风险分析部分
	分析部分符合项或不符合项所产生的安全问题被威胁利用的可能性	
	分析威胁利用安全问题后造成的影响程度	
	为被测系统面临的风险进行赋值	
	评价风险分析结果	
5.等级测评结论形成	统计再次汇总后的单项测评结果为部分符合和不符合项的项数	等级测评报告的等级测评结论部分
	形成等级测评结论	
6.测评报告编制	概述测评项目情况	等级测评报告提交用户
	描述被测系统情况	
	描述测评范围和方法	
	描述整体测评情况	
	汇总测评结果	
	描述风险情况	
	给出等级测评结论和整改建议	

4.4　项目相关要求

项目实施过程中，投标人应遵循国家标准、行业标准。在项目实施中投标人须做到：

1）提供完整的系统实施方案和项目实施管理办法；

2）提供详细的项目实施方案和计划进度说明书；

3）项目实施完成后提供可靠的后期技术服务工作；

4）严格按照双方确定的计划进度保质保量完成工作；

5）规范项目实施过程中的文档管理；

6）有较好的保密管理及风险管理。

5.　服务保障

（1）投标人必须确保能建立一支具有一定服务能力的管理团队，至少包含5名具有网络/信息安全等级测评师(高级)的专业人员，并且要求项目负责人具备项目管理、技术咨询和检验检测等相关能力，保障各项服务工作相关岗位的需要。

（2）中标单位在采购人下达评估通知书后 60 日内交付成果和报告。

（3）服务期间提供 7×24 服务响应，技术人员能够在 4 小时之内到达现场，并且现场支持的技术人员具备网络/信息安全等级测评师(高级)证书。

（4）服务期间提供应急保障工作，具备信息安全风险评估能力和信息安全应急处理服务能力，针对应急、攻坚克难等事宜提供保障方案，包括高层支撑和响应时间等。

（5）严守工作秘密。中标服务商必须与采购人签署保密协议，工作人员须与单位签署《保密承诺书》，对知悉的事项及信息予以保密，所有资料、技术文档妥善保管，不得遗失、转借、复印，不得以任何形式向第三方透露。

（6）严格遵循操作规程，承担服务工作质量责任。