“广西政府采购云平台”合同编号：12N4985009762025802

采购合同

合同名称：广西工业领域网络安全信息公共服务平台

项目编号：GXZC2025-C3-000848-GXZL

采购单位（甲方）：广西工业职业技术学院

供 应 商（乙方）：广西塔易信息技术有限公司

合同目录

一、广西壮族自治区政府采购合同

合同编号：12N4985009762025802

采购计划号：广西政采[2025]6673号

项目名称编号：GXZC2025-C3-000848-GXZL

采购单位（甲方）：广西工业职业技术学院

供 应 商（乙方）：广西塔易信息技术有限公司

签 订 时 间：2025年5月28日

签 订 地 点：甲方指定地点

根据《中华人民共和国政府采购法》、《中华人民共和国民法典》等法律、法规规定，按照磋商文件规定条款和乙方响应文件及其承诺，甲乙双方签订本合同。

第一条 合同标的

1、项目一览表

序号	标的名称	服务内容	数量	单位	单价（元）	总价（元）
1	工业领域网络安全信息公共 服务平台	详见磋商文件《第二章 采购需求》相关内容	1	套	716100.00	716100.00
2	万兆超融合交换机		2	台	19200.00	38400.00
3	服务器密码机系统		1	台	75144.00	75144.00
4	IPSEC/SSLVP N 综合安全网关系统		1	台	75318.00	75318.00
5	签名验签服务器系统		1	台	97464.00	97464.00
6	协同签名系统		1	台	142104.00	142104.00
7	智能密码钥匙		10	个	27.90	279.00
8	国密数字证书		120	点	980.00	117600.00
9	二级等保测评		1	项	46500.00	46500.00
10	软件测试		1	项	9300.00	9300.00
11	代码审计		1	项	46500.00	46500.00
12	二级密评测评		1	项	46500.00	46500.00

13	渗透测试		1	项	46500.00	46500.00
14	系统集成服务		1	项	116250.00	116250.00
15	平台运营服务		1	项	560000.00	560000.00
16	人员培训服务		1	项	9300.00	9300.00
17	防火墙		1	台	121972.00	121972.00
人民币合计金额（大写）：贰佰贰拾陆万伍仟贰佰叁拾壹元整（¥2,265,231.00）						

2、合同合计金额包括但不限于满足本次竞标全部采购需求所应提供的服务，以及伴随的货物和服务的价格；包含包含但不限于培训、技术支持、售后服务费、测试、保险费和各项税金等完成本项目所产生的全部费用（采购需求另有约定的，从其约定）。

第二条　质量保证

1、乙方所提供的服务及服务内容必须与响应文件承诺相一致，有国家强制性标准的，还必须符合国家强制性标准的规定。没有国家强制性标准但有其他强制性标准的，必须符合其他强制性标准的规定。

第三条　权利保证

1、乙方应保证所提供服务在使用时不会侵犯任何第三方的专利权、商标权、工业设计权等知识产权及其他合法权利，且所有权、处分权等没有受到任何限制。

2、没有甲方事先书面同意，乙方不得将由甲方提供的有关合同或者任何合同条文、规格、计划、图纸、样品或者资料提供给与履行本合同无关的任何其他人。即使向履行本合同有关的人员提供，也应注意保密并限于履行合同的必需范围。乙方的保密义务持续有效，不因为本合同履行终止、解除或者无效而解除。

第四条　交付和验收

1、交付时间：自合同签订之日起60个日历日内验收合格并交付使用，交付地点：广西南宁市采购人指定地点。

2、乙方应按响应文件的承诺向甲方提供相应的服务，并提供所服务内容的相关技术资料。

3、乙方提供不符合响应文件和本合同规定的服务成果，甲方有权拒绝接受。

4、乙方完成服务后应及时书面通知甲方进行验收，甲方应在收到通知后七个工作日内进行验收，逾期不开始验收的，乙方可视同验收合格。验收合格后由甲乙双方签署验收单并加盖采购人公章，甲乙双方各执一份。

5、甲乙双方应按照《广西壮族自治区政府采购项目履约验收管理办法》、双方合同、响应文件验收。

6、甲方在初步验收或者最终验收过程中如发现乙方提供的服务成果不满足响应文件及本合同规定的，可暂缓向乙方付款，直到乙方及时完善并提交相应的服务成果且经甲方验收合格后，方可办理付款。

7、甲方验收时以书面形式提出异议的，乙方应自收到甲方书面异议后五个工作日内及时予以解决，

否则甲方有权不出具服务验收合格单。

第五条 售后服务及培训

1、乙方应按照国家有关法律法规和本合同所附的《售后服务承诺》要求为甲方提供相应的售后服务。

2、甲方应提供必要测试条件（如场地、电源、水源等）。

3、乙方负责甲方有关人员的培训。培训时间、地点：按甲方要求组织 。

第六条 付款方式

1、项目合同、担保措施生效以及具备实施条件后 10 个工作日内，甲方通过银行转账的方式向乙方支付合同总金额的 30%预付款；乙方实施完成本项目，并通过甲方审核验收，在通过验收后的 10 个工作日内，支付合同总金额的 70%。

2、甲方付款前，乙方应向甲方开具等额有效的增值税发票，甲方未收到合格有效发票的，有权不予支付相应款项直至乙方提供合格发票，并不承担延迟付款责任。发票认证通过是付款的必要前提之一。

3、付款方式：银行转账。

第七条 履约保证金

1、履约保证金金额：成交金额的 2%收取（乙方为小型企业）。

2、履约保证金递交方式：银行转账、支票、汇票、本票或者金融、保险机构出具的保函等非现金形式。

3、履约保证金递交时间：签订合同前 5 个工作日内由乙方转入甲方指定保证金账户。

4、履约保证金退还：履约完成并验收合格后无质量问题，乙方提供《政府采购项目履约保证金退付意见书》及《政府采购项目合同验收报告》，向甲方提出书面申请退还，甲方在收到申请后 5 个工作日内办理履约保证金退还手续（无息退还）。

保证金指定账户：

开户名：广西工业职业技术学院

开户行：广西北部湾银行南宁市衡阳路支行

账　号：1702012200017200

第八条 税费

本合同执行中相关的一切税费均由乙方负担，合同另有约定的除外。

第九条 违约责任

1、除不可抗力原因外，乙方没有按照合同规定的时间提供服务或提供服务质量不合格的，甲方可要求乙方支付违约金。每推迟一天按合同金额的万分之四支付违约金，该违约金累计不超过合同金额的 20%。

2、乙方提供的服务如侵犯了第三方合法权益而引发的任何纠纷或者诉讼，均由乙方负责交涉并承担全部责任。乙方保证其所提供的商品或服务不侵犯任何第三方的合法权益，如有违反，由乙方负责处理并承担全部责任。

3、甲方延期付款的，每天向乙方偿付延期款额万分之四违约金，但违约金累计不得超过延期款额 20%。

4、甲乙双方有其它违约行为的，由违约方向守约方方支付合同总金额的 20%，合同总金额的 20%不足以赔偿经济损失的按实际赔偿。违约方应向守约方承担实现合同权益而支出的诉讼费、财产保全费、诉讼财产保全责任保险费、律师费、鉴定费、调查费、差旅费等一切费用。

第十条　不可抗力事件处理

1、在合同有效期内，任何一方因不可抗力事件导致合同不能履行，则合同履行期可延长，其延长期与不可抗力影响期相同。

2、不可抗力事件发生后，甲乙双方有义务立即通知对方，并寄送有关权威机构出具的证明。

3、不可抗力事件延续一百二十天以上，双方应通过友好协商，确定是否继续履行合同。

第十一条　合同争议解决

1、因服务质量问题发生争议的，应邀请国家认可的质量检测机构进行鉴定。服务符合标准的，鉴定费由甲方承担；服务不符合标准的，鉴定费由乙方承担。

2、因履行本合同引起的或者与本合同有关的争议，甲乙双方应首先通过友好协商解决，如果协商不能解决，可向甲方所在地有管辖权人民法院提起诉讼。

3、诉讼期间，本合同继续履行。

第十二条　合同生效及其它

1、合同经双方法定代表人或者授权代表签字并加盖单位公章后生效（委托代理人签字的需后附授权委托书，格式自拟）。

2、合同执行中涉及采购资金和采购内容修改或者补充的，须经财政部门审批，并签书面补充协议报财政部门备案，方可作为主合同不可分割的一部分。

3、本合同未尽事宜，遵照《中华人民共和国民法典》有关条文执行。

第十三条　合同的变更、终止与转让

1、除《中华人民共和国政府采购法》第五十条规定的情形外，本合同一经签订，甲乙双方不得擅自变更、中止或者终止。

2、乙方不得擅自转让其应履行的合同义务。

第十四条　签订本合同依据

1.磋商文件

2.乙方响应文件

3.成交通知书

4.其他约定附件

上述合同文件互相补充和解释。如果合同文件之间存在矛盾或者不一致之处，以上述文件的排列顺序在先者为准。

第十五条 本合同一式七份，具有同等法律效力，财政部门（政府采购监管部门）、采购代理机构各一份，甲方三份，乙方二份（可根据需要另增加）。

本合同甲乙双方签字盖章后生效，自签订之日起七个工作日内，甲方应当将合同副本报同级财政部门备案。

本合同自签订之日起2个工作日内，甲方应当将采购合同在广西壮族自治区财政厅指定的媒体上公告。

甲方（章）广西工业职业技术学院 2025年5月28日	乙方（章）广西塔易信息技术有限公司 2025年5月28日
单位地址：南宁市西乡塘区秀灵路37号	单位地址：中国（广西）自由贸易试验区南宁片区凯旋路13号五象新区总部休闲公园9号楼
法定代表人：	法定代表人：
委托代理人：	委托代理人：
电话：	电话：0771-3360667
电子邮箱：	电子邮箱：
开户银行：	开户银行：中国建设银行股份有限公司广西自贸试验区南宁片区五象支行
纳税人识别号或统一社会信用代码：	纳税人识别号或统一社会信用代码：91450103MA5L7G0P1X
账号：	账号：45050160500100000389
邮政编码：	邮政编码：530020

二、合同附件

成交通知书

广西工业领域网络安全信息公共服务平台（GXZC2025-C3-000848-GXZL）

成交通知书

广西塔易信息技术有限公司：

广西众联工程项目管理有限公司受广西工业职业技术学院的委托，就广西工业领域网络安全信息公共服务平台（GXZC2025-C3-000848-GXZL）采用竞争性磋商方式进行采购。经采购人确认，贵单位为本项目的成交供应商，具体内容如下：

成交总金额（元）：贰佰贰拾陆万伍仟贰佰叁拾壹元整（¥2,265,231.00）

交付时间：自合同签订之日起60个日历日内验收合格并交付使用。

请贵单位接此通知书后25日内尽快与采购人签订合同，并按竞争性磋商文件要求和响应文件的承诺履行合同。

特此通知！

代理机构（盖章）：广西众联工程项目管理有限公司

日期：2025年5月13日

采购需求

说明：

1.为落实政府采购政策需满足的要求

（1）本竞争性磋商采购文件所称中小企业必须符合《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）的规定。

（2）服务项目中包含货物的，根据《财政部 发展改革委 生态环境部 市场监管总局关于调整优化节能产品、环境标志产品政府采购执行机制的通知》（财库〔2019〕9号）和《关于印发节能产品政府采购品目清单的通知》（财库〔2019〕19号）的规定，采购需求中的产品属于节能产品政府采购品目清单内标注“★”的，供应商必须在响应文件中提供所竞标产品的节能产品认证证书复印件（加盖供应商电子公章），否则响应文件作无效处理。如本项目包含的配套货物属于品目清单内非标注“★”的产品时，应优先采购，具体详见“第四章 评审程序和评定成交的标准”。

（3）服务项目中伴随的货物包含列入《网络关键设备和网络安全专用产品目录》的网络安全专用产品，应当按照《信息安全技术 网络安全专用产品安全技术要求》等相关国家标准的强制性要求，提供具备资格的机构安全认证合格或者安全检测证明材料（加盖供应商电子公章），否则响应文件作无效处理。

2.“实质性要求”是指采购需求中带“▲”的条款或者明确不能负偏离的条款或者已经指明不满足按响应文件作无效处理的条款。

3.供应商必须自行为其竞标产品侵犯他人的知识产权或者专利成果的行为承担相应法律责任。

4.本项目采购标的对应的中小企业划分标准所属行业：软件和信息技术服务业。

服务需求一览表				
标段			i	
技术条款	序号	标的名称	数量及单位	技术要求
	1	工业领域网络安全信息公共服务平台	1套	一、平台门户 此模块提供导航信息、信息资讯、法律法规和标准信息展示、用户登录注册等内容。 二、功能模块 （一）漏洞管理 1、漏洞收集 此模块主要负责收集、整理各类工业互联网漏洞信息。其功能包括：漏洞信息实时采集、存储、分析以及定期公布。其中，漏洞信息应包括产品型号、漏洞编号、漏洞等级、漏洞描述等信息，并为使用单位提供下载和查阅。

				2、漏洞上报 此模块主要为使用单位和技术支撑单位将发现的工业互联网漏洞信息上报至本平台，给使用单位和技术支撑单位提供上报通道。其中，漏洞信息应包括产品型号、漏洞编号、漏洞等级、漏洞描述等信息。 3、漏洞验证核实 此模块为收集和上报的漏洞验证核实的流程管理，在人工技术核实确认漏洞可利用后推送到风险信息通报模块。 （二）风险信息通报预警 1、漏洞发布预警和通报 最新漏洞发布，信息发布在线上服务平台首页，提醒用户关注最新的漏洞。 漏洞信息库及查询。与国家工业信息安全漏洞库（CICSVD）实现对接，预置 PLC、数控机床、工业机器人等相关产品漏洞不少于 5000 条。 漏洞通报全生命周期管理。建立“省-市-区县-企”四级线上风险通报工作机制，支撑常态化开展风险预警通报下发、威胁情报信息共享，实现对工业控制系统的重大漏洞、风险等及时向有关行业、地区和工业企业进行线上和短信定点推送的功能，并支持显示信息处理进程，支撑地方主管部门对漏洞整改进度进行全过程跟踪和监督。 2、咨询服务 提供漏洞情况、漏洞修复的技术咨询服务电话。留下技术支撑单位的联系信息，有需求单位来电自行联系。 （三）资产测绘和安全检测 实现面向广西壮族自治区境内全量 IP 的资产测绘，可监测不少于 100 种品牌工业控制系统，至少包括力控、亚控、中控、西门子、施耐德等品牌，覆盖 SCADA、工业实时数据库、PLC 等设备类型，将核查结果从区域、厂商、端口、漏洞等维度进行统计、关联，实时展示联网资产安全态势，监测维度包括 IP 地址、端口号、所属公司、设备类型、协议、设备厂商、运营商等不少于 7 个维度。 （四）安全自查数据报送

				使用单位通过分配账户将年度自查数据填报到系统中，采用数据传输和存储加密技术，报送接口可根据情况设定开启和关闭时间，并提供年度、区域、行业、安全等级等关键字自查数据统计功能。 （五）资源池服务对接 提供企业信息发布功能，可发布资源池服务商企业信息，发布企业需求信息。 （六）公共服务 此模块可为使用单位提供各类公共服务申请功能，如安全检测评估、政策补贴、安全认证、技术支持等。使用单位可以在线提交申请，平台审核通过后将为其提供相应的服务支持。同时，该模块还应包括一个公示区，公布已申请成功的企业名单和相关信息。 （七）在线应急响应服务 对于发生的安全事件，平台提供及时的应急响应服务咨询服务，协助使用单位进行事件处置，降低安全风险。提供网络安全应急响应国家标准、方案模块，可供用户下载。 （八）在线学习模块 在线学习模块。以精品课程、微视频为主的自主学习平台。提升企业网络安全意识和能力。 （九）短信平台 能将风险信息通过短信推送到使用单位相关人员手机中，及时提醒使用单位处理风险信息。 （十）系统基础模块 1、用户管理 自治区、市、县三级用户管理，预计5万用户量。 2、日志模块 账户操作过程日志记录。 3、企业用户基础数据库 国产化基础数据库适配。 （十一）系统对接 ▲1、系统必须实现与国家工业信息安全漏洞库的对接，可获取漏洞信息至少从漏洞名称、所属类型、CVE编号、危害等级、影响行业、漏洞描述、影响产品名称等不少于7个维度进行描述，面向工

				业控制器、数控机床、工业机器人等不少于3种工控设备收录漏洞不少于5000条。如涉及相关二次开发费用，由供应商自行承担[在响应文件中提供承诺函（承诺函需包含本项内容要求）并加盖供应商公章]。 ▲2、系统必须实现与国家工业信息安全态势感知平台的数据对接。如涉及相关二次开发费用，由供应商自行承担[在响应文件中提供承诺函（承诺函需包含本项内容要求）并加盖供应商公章]。
	2	万兆超融合交换机	2台	1、设备性能：交换容量≥2.4Tbps，转发性能≥720Mpps； 2、设备配置：提供万兆SFP+光口≥24个，支持模块化可插拔电源槽位≥2个，本次提供可插拔交流电源模块≥2个；单台8个万兆光模块。
	3	服务器密码机系统	1台	1、2U机架式结构，系统配置≥1个管理口，≥1个HA口，≥4个千兆电口，≥4个SFP插槽，≥32G内存，≥4TB企业级硬盘,冗余电源,≥2个扩展槽位，冗余电源。 2、SM2算法密钥最大生成速率≥5000对/秒，SM2算法最大签名速率≥8000次/秒，SM2算法最大验签速率≥4000次/秒，SM3算法最大校验吞吐率≥1300Mbps，SM4算法最大加解密吞吐率≥2100Mbps； ▲3、产品须为国家密码管理局认证合格的密码产品，而非加密软件密码模块。 4、通过数字签名可以保证信息传输的完整性、对发送者进行源认证以及防抵赖支持用户自行修改单点登录的账户信息。 5、支持三层密钥结构：管理密钥、用户密钥/设备密钥/密钥加密密钥、会话密钥； 6、具备四路随机噪声源，采用由国家密码管理局批准使用的物理噪声源发生器芯片生成随机数； 7、符合GM/T 0018-2023《密码设备应用接口规范》标准，支持WINDOWS、LINUX系统平台，提供JAVA、C语言的接口，具备高兼容性； 8、支持白名单IP授权登录管理页面，业务通信支持国际和国密协议； 9、支持多操作系统Linux、Windows；支持API接口描述，包括

				接口类别、接口实例，根据所选择的具体接口，显示该接口函数的名称、参数以及示例 demo； ▲10、支持国密算法 SM2/SM3/SM4；支持算法模式：ECB、CBC、CFB、OFB；支持杂凑算法：MD4、MD5、SHA1、SHA2（在响应文件中提供【支持国密算法 SM2/SM3/SM4】功能截图证明材料复印件并加盖供应商公章）； 11、支持 SM2 和 RSA 的数字信封转换；支持会话密钥生成、导入、导出、协商及销毁； 12、支持基于兑成算法的 MAC 消息鉴别码产生及验证； ▲13、支持密钥的全生命周期管理：密钥的生成、存储、使用、备份、恢复、删除、销毁等功能（在响应文件中提供【上述 7 种】功能截图证明材料复印件并加盖供应商公章）； 14、支持配置管理日志、系统日志、业务日志审计，支持按日志类型、时间、级别、关键词等分类查询； 15、具备系统密码服务的自监控能力，服务器密码机系统运行过程中进行自检测，系统运行异常将停止服务，并且上报服务状态，用户可以实时查看密码服务状态；
	4	IPSEC/SSLVPN 综合安全网关系统	1 台	1、系统≥2U，≥10 个千兆电口，冗余电源，≥2 个扩展槽位，国密 IPSEC VPN 最大吞吐率≥600Mbps 国密 IPSEC VPN 最大隧道数≥4000 条，国密 SSL VPN 最大吞吐率≥200Mbps，国密 SSL VPN 最大建议并发用户数≥1600；默认含≥200 个 SSL VPN 的客户端并发许可； 2、产品为 VPN 硬件设备，而非防火墙\UTM 类设备集成的 VPN 模块； 3、支持基于用户、用户组、用户角色进行授权，实现用户可访问资源、可信接入和客户端杀毒策略； 4、支持动态地址转换和静态地址转换，支持多对一、一对多和一对一等多种方式的地址转换； 5、支持双向 NAT； ▲6、支持静态用户名口令、数字证书、短信、硬件特征码绑定、图形码方式；支持两种或两种以上组合认证方式（在响应文件中提供【支持两种或两种以上组合认证方式】功能截图证明材料复印件并加盖供应商公章）；

				7、支持用户名口令认证防暴力破解，支持使用邮件、短信方式密码找回，支持对用户口令复杂度和有效性设置； 8、支持内置 CA，可以对证书进行生成、签发、废弃操作；支持国际、国密算法证书；支持 DER/PEM/PKCS12 等多种证书编码；支持导入多个第三方 CA 根证书和 CRL 列表，可以对不同的 CA 用户证书进行身份认证； ▲9、支持可信接入功能，能够对接入主机的信息进行检查，包括域名、杀毒软件、安装的程序、运行的服务等；支持可信接入分级授权（在响应文件中提供【支持可信接入功能和支持可信接入分级授权】功能截图证明材料复印件并加盖供应商公章）； 10、支持基于源/目的 IP 地址、MAC 地址、端口和协议、时间、用户、角色的访问控制；支持基于状态检测的动态包过滤；支持隧道内的访问控制； 11、支持 Windows、iOS、Android、Linux、Mac 客户端接入方式； ▲12、支持 AES、DES、3DES、RC4、MD5、SHA1、RSA 等多种算法；支持国密数字证书认证（在响应文件中提供【上述 7 种算法】功能截图证明材料复印件并加盖供应商公章）； ▲13、支持 DES、3DES、AES、MD5、SHA1、DH GROUP1/2/5、RSA 1024/2048 等加密算法；支持国家商密专用的 SM1、SM2、SM3、SM4 算法； 14、支持设备的运行状态、设备资源状态、并发用户数、客户端类型分布、IPSEC 隧道状态、用户流量、安全事件、中国任意省市区县（港澳台除外）的接入用户数监控，并通过图表展示。
	5	签名验签服务器系统	1 台	1、系统≥2U，配置≥1 个管理口，≥1 个 HA 口，≥4 个千兆电口，≥4 个 SFP 插槽，≥32G 内存，≥4TB 企业级硬盘，冗余电源，≥2 个扩展槽位。SM2 算法密钥最大生成速率≥5000 对/秒，SM2 算法最大签名速率≥8000 次/秒，SM2 算法最大验签速率≥4000 次/秒，SM3 算法最大校验吞吐率≥1300Mbps，SM4 算法最大加解密吞吐率≥2100Mbps，SM2 算法制作数字信封最大速率≥4000 次/秒，SM2 算法拆解数字信封最大速率≥3000 次/秒；≥3 年硬件维保； 2、实现基于数字证书的身份认证，支持不同 CA 的证书验证，

				提供 CRL/OCSP 等多种方式的证书有效性验证。 3、提供 PKCS1/ PKCS7 attach/PKCS7 detach/XML Sign 等多种格式的数字签名和数字签名验证功能(PKCS1 签名支持记录签名日志功能)。 4、对数据进行加密传输，只有指定的信封接收者可以解密数据。 5、对文件提供数字签名和数字签名验证功能。 6、提供 CRL/OCSP 等多种方式的证书有效性验证。 7、可同时配置多条证书链，验证不同 CA 系统签发的数字证书。 8、提供证书解析功能，获取证书中的任意主题信息以及扩展项信息。 9、可实现对客户端证书的存储，管理员可以通过页面进行证书导入和查找，业务系统可以通过接口获取已存储的证书。 10、可以自动更新黑名单，采用动态更新方式，无需重启服务。 11、支持服务端负载均衡功能，来解决不能对外提供大数据量服务的问题，即多台机器负载时，多台机器能够同时对外提供一样的服务来处理大数据量。
	6	协同签名系统	1台	1、系统≥2U，配置≥1 个管理口，≥1 个 HA 口，≥4 个千兆电口，≥4 个 SFP 插槽，冗余电源，≥2 个扩展槽位，分量签名性能≥3500 次/秒；验签性能≥8000 次/秒；并发用户数≥3500；最大用户数≥7000； 2、服务端机架式硬件密码设备；客户端 SDK 或 APP 形态。 3、支持 SM2 公钥密码算法。支持 SM4 等对称密码算法。支持 SM3 摘要算法。 4、支持密钥安全存储，除公钥外不允许密钥以明文形式输出。提供密钥生成、密钥存储、密钥备份、密钥恢复等密钥管理功能。 5、具备密钥自毁功能，当未经授权对设备进行开盖时，触发密钥自毁功能；也可通过外置物理装置销毁密钥。 6、管理员需使用证书登录管理界面，保证配置管理安全。具备终端设备访问控制功能，支持对移动端许可进行分配、注销、查询，通过白名单实现对应用服务器的访问授权认证。 ▲7、支持密码卡-实模式，开机启动系统镜像的完整性检验（在响应文件中提供【支持密码卡-实模式】功能截图证明材料复印件并加盖供应商公章）。

				▲8、支持国密 SSH、国密 FTP（在响应文件中提供【支持国密 SSH、国密 FTP】功能截图证明材料复印件并加盖供应商公章）。 9、提供产生随机数功能，所有随机数采用国家密码管理局批准的硬件物理噪声源生成真随机数。 10、提供对称密钥加解密功能。消息鉴别码产生和验证功能。提供非对称密钥数字签名产生和验证功能。提供非对称密钥加解密功能。提供协同密码运算服务。 11、提供 C/C++接口和 Java 接口。支持 Linux、Windows 等系统。
	7	智能密码钥匙	10 个	1、支持国产化环境，包括国产操作系统（统信 UOS、麒麟系统等）和国产处理器（龙芯、飞腾、兆芯、鲲鹏、海光、麒麟等）； 2、硬件内置算法：SM1、SM2、SM3、SM4、RSA（1024/2048）、SHA-1、SHA-256、SHA-384、SHA-512、DES、3DES、AES 128/192/256； 3、符合国家密码管理局提出的 GM/T 0027《智能密码钥匙技术规范》； 4、兼容性：支持 X.509 v3 标准证书格式，支持多浏览器，支持多协议 HID、UMS、SCSI、CCID； 5、抗抵赖：使用内部私钥对数据进行签名操作，满足国家密码管理局和 PKI 规范要求，设备内的私钥无法被外部获取，确保签名数据无法被抵赖。 6、数据存储年限：至少 10 年； 7、擦写次数：室温下 Flash 擦写次数量最少为 10 万次； 8、工作电压：5V±5%； 9、工作电流：≤30mA。
	8	国密数字证书	120 点	采用国家认可的第三方 CA 机构证书，提供国密证书签发和管理服务，应用于个人用户标识真实身份。每张数字证书 3 年有效期，证书有效期起始时间从验收通过日起计算。
	9	二级等保测评	1 项	▲1、总的要求： 依据《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）对工业领域网络安全信息公共服务平台开展网络安全等级保护测评工作，并出具网络安全等级保护测评报告。 ▲2、标准依据： 《计算机信息系统安全保护等级划分准则》（GB 17859-1999）

				《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019） 《信息安全技术 网络安全等级保护测评要求》（GB/T 28448-2019） 《信息安全技术 网络安全等级保护测评过程指南》（GB/T 28449-2018） 《信息安全技术 网络安全等级保护安全设计技术要求》（GB/T 25070-2019） 《信息安全技术 网络安全等级保护测试评估技术指南》（GB/T 36627-2018） ▲3、测评内容： （1）安全通用要求： 安全通用要求测评内容应包括安全技术和安全管理两大类，其中技术类应包括对安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心五个方面的测评，安全管理类测评应包括对安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理五个方面的测评。 （2）安全扩展要求： 根据现场情况，保护对象可能涉及的安全扩展要求包括：移动互联，包括对安全物理环境、安全区域边界、安全计算环境、安全建设管理、安全运维管理等的测评。 4、测评方法： 在测评实施过程中，应采用访谈、检查和测试、渗透测试等测评方法进行，并与国家相关规范及标准的要求相符。 ▲5、服务成果： 测评完成后，出具符合《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）相关技术标准要求、国家网络安全等级保护管理部门规范要求且公安机关认可的网络安全等级保护测评报告。在项目整体验收时提供报告原件核查。 ▲6、提供本项服务的测评机构具备公安部第三研究所颁发的《网络安全等级测评与检测评估机构服务认证证书》。
	10	软件测试	1项	1、测试计划：定义测试的目标、范围、方法、资源需求、时间

				表和风险。 2、需求分析：确保测试团队理解软件的需求，并基于这些需求制定测试计划。 3、测试设计：设计测试用例和测试场景，以覆盖所有的软件功能和用户故事。 4、测试用例开发：编写详细的测试用例，包括输入数据、预期结果和测试步骤。 5、测试环境搭建：准备所需的硬件、软件、网络和其他资源，以模拟真实的运行环境。 6、单元测试：针对软件的最小可测试部分（通常是单个函数或模块）进行测试。 7、集成测试：测试多个软件模块或组件如何协同工作。 8、系统测试：测试完整的、集成的软件系统，以确保它满足所有需求。 9、验收测试：通常由客户或最终用户执行，以确认软件是否满足他们的业务需求。 10、性能测试：评估软件在不同负载下的性能，包括响应时间、吞吐量和资源使用情况。 11、安全测试：确保软件能够抵御外部威胁和攻击。 12、可用性测试：评估软件的用户界面和用户体验。 13、兼容性测试：确保软件能够在不同的硬件、软件、浏览器和操作系统上运行。 14、回归测试：在软件变更后重新执行测试，以确保新代码没有引入新的错误。 15、自动化测试：使用自动化工具来执行测试用例，提高测试效率和覆盖率。 16、测试报告：记录测试活动的结果，包括发现的缺陷、测试覆盖率和测试结论。
	11	代码审计	1项	检查源代码中的安全缺陷，检查程序源代码是否存在安全隐患，或者有编码不规范的地方，通过自动化工具或者人工审查的方式，对程序源代码逐条进行检查和分析，发现这些源代码缺陷引发的安全漏洞，并提供代码修订措施和建议，提供《系统代码审计报告》，

				报告的内容包含但不限于：项目概述、标准依据、项目范围，概要信息；源代码信息，威胁等级、代码分类，以及代码缺陷的详细信息，修复建议等信息。
	12	二级密评测评	1项	（一）总体要求 依据《中华人民共和国密码法》《信息安全技术 信息系统密码应用基本要求》（GB/T39786-2021）要求和系统自身的安全需求分析，对工业领域网络安全信息公共服务平台进行商用密码应用安全性评估，为重要网络和信息系统的密码安全提供科学评价，逐步规范网络运营者的密码使用和管理行为。 （二）技术标准 《信息安全技术 信息系统密码应用基本要求》（GB/T39786-2021） 《信息系统密码应用测评要求（试行）》 《商用密码应用安全性评估测评过程指南（试行）》 《商用密码应用安全性评估测评作业指导书（试行）》 （三）服务内容 1、商用密码应用方案评估 依据中国密码学会密评联委会发布的《商用密码应用安全性评估报告模板》（2023版）对工业领域网络安全信息公共服务平台商用密码应用方案开展评估工作，并出具《密码应用方案评估报告》。方案评估要点： （1）文档结构是否完整 （2）系统基本情况是否梳理充分 （3）密码应用需求是否清晰明确 （4）密码应用技术框架中密码协议、防护机制、密钥管理、密码应用子系统设计是否合理，能否满足安全需求和保障要求 （5）密码产品应用和部署设计是否合理、正确 （6）安全管理方案是否覆盖密码安全相关人员、制度、实施、应急等内容 （7）实施保障方案中实施计划是否科学、合理，组织管理方法和保障是否合理有效 2、商用密码应用安全性评估

				依据《信息安全技术 信息系统密码应用基本要求》（GB/T39786-2021）等技术标准对工业领域网络安全信息公共服务平台进行商用密码应用安全性评估工作，并出具符合要求的《商用密码应用安全性评估报告》。 （1）实施方式 1）系统测评：及时发现系统脆弱性，识别变化的风险，了解系统安全状况，对照密码应用方案对系统开展测评。根据被测评对象的实际情况、所属行业及系统使用的密码产品情况，选择并确定测评依据。在系统真实环境下进行测评，以测评密码保障是否安全有效，密码使用是否合规、正确、有效。并通过测评发现系统存在的安全隐患和风险，提出可行性完善建议。 2）密码技术应用测评：物理安全密码测评、网络安全密码测评、主机安全密码测评、应用安全密码测评、数据安全及备份恢复密码测评。测评验证不同安全等级信息系统的商用密码应用是否达到具有相应安全等级的安全保护能力，是否满足相应安全等级的保护要求。 3）密钥管理测评：检测信息系统密钥管理各环节，包括对密钥的生成、存储、分发、导入、导出、使用、备份、恢复、归档与销毁等环节进行管理和策略制定的全过程是否符合要求。 4）安全管理测评：对制度、人员、实施和应急等四个方面安全管理的测评，并协助完善商用密码应用安全性管理制度，协助完善密码相关系统运维管理制度。 （2）评估成果 出具针对被评估系统编制密码应用安全性评估报告，报告按照国家密码管理局要求包含的内容编制或参考模板编制。报告中应协助被评估单位认清风险，查找漏洞，找出差距，提出有针对性的加强完善密码安全管理和防护建议，并出具商用密码应用安全性评估报告；在项目整体验收时提供报告原件核查。 ▲（四）提供本项服务的测评机构须为国家密码管理局公告（第49号）“商用密码检测机构（商用密码应用安全性评估业务）目录”内的机构。
	13	渗透测试	1项	针对工业领域网络安全信息公共服务平台进行渗透测试，模拟

				黑客攻击的方式，对目标系统的安全性进行全面、深入的评估。通过人工结合工具测试发现更多 WEB 层面上扫描器无法发现的漏洞（如：逻辑漏洞），帮助客户在遭到恶意攻击前将风险降到最低。并根据渗透测试结果出具渗透测试报告。输出《渗透测试报告》，报告的内容包含但不限于：测试目的、范围、依据、工具、主要漏洞信息、具体的操作步骤描述、安全修复建议等。
	14	系统集成服务	1 项	▲1、工作内容：完成工业领域网络安全信息公共服务平台的等保备案定级系统的整改实施服务（信息安全等级保护：二级 2.0 标准）。 2、等级保护网络调试服务：基于单位网络设备（交换机、路由器等）现状，对标信息安全等级保护 2.0 二级标准以及风险评估报告或测评报告进行整改，提交对应整改技术服务方案，整改范围包括但不限于拓扑结构的整改、设备物理位置的整改、设备配置数据的整改、设备版本的整改等。整改完成后实现所有网络设备均无高危漏洞，并达到通过此次信息安全等级保护 2.0 二级测评的要求。 3、等级保护安全调试服务：基于本单位安全设备（防火墙、入侵防御、上网行为管理、杀毒软件，堡垒机、日志审计、数据库审计等设备）现状，对标信息安全等级保护 2.0 二级标准以及风险评估报告或测评报告进行整改，整改范围包括但不限于拓扑结构的整改、设备物理位置的整改、设备配置数据的整改、设备版本的整改等。整改完成后实现所有安全设备均无高危漏洞，并达到通过此次信息安全等级保护 2.0 二级测评的身份鉴别、访问控制、入侵防御、恶意代码防御、日志审计、资源管理、保密性管理等要求。 4、等级保护业务系统调试服务：基于本单位业务系统现状，对标信息安全等级保护 2.0 二级标准以及漏洞扫描报告进行整改，提交对应整改技术服务方案，整改范围包括但不限于操作系统配置优化、操作系统安全补丁安装，操作系统权限优化等。整改完成后实现本单位此次等级保护测评的目标系统均无高危漏洞，并达到通过此次信息安全等级保护 2.0 二级测评的身份鉴别、访问控制、入侵防御、恶意代码防御、日志审计、资源管理、保密性管理等要求。 ▲5、等级保护管理体系整改：对标信息安全等级保护 2.0 二级标准建立网络安全等级保护管理体系，在信息安全管理制度、安全

				管理机构、人员安全管理、系统建设管理、系统管理等方面指导并协助单位建立健全符合相应等级要求的安全管理制度。提交《信息安全等级保护管理制度包》，以达到通过此次信息安全等级保护 2.0 二级测评的要求。 ▲6、协助测评服务：等保测评期间协助开展等保测评工作，协助完成工业领域网络安全信息公共服务平台的等保备案及等级认定工作。 7、应急支撑：在提供等级保护整改服务期间，提供整改相关工作引起的业务异常并需要协助排查故障时 30 分钟内做出响应，2 小时内到达现场协助处理。
	15	平台运营服务	1 项	1、含三年广西工业互联网安全信息公共服务平台运营服务。 2、包含三年国家工业信息安全漏洞库（漏洞名称、所属类型、CVE 编号、危害等级、影响行业、漏洞描述、影响产品，面向工业控制器、数控机床、工业机器人等不少于 10 种工控设备收录漏洞不少于 5000 条）的升级授权。 3、提供三年的平台运维升级服务，为平台提供全面的技术支持和持续的系统优化，以确保平台始终保持平稳运行，充分发挥其功能。服务方式为远程技术支持与现场派驻相结合，成交供应商应拟派具备与运营服务工作相匹配的专业技术人员进行驻场服务；同时能配备有经验丰富且专业的专家团队进行远程技术支持，专家团队必要时能及时到达现场处理问题。运营服务包含平台运营所需的人力成本，提供至少 2 人现场驻场运维服务，工作时间以采购人工作时间为准。驻场人员主要负责信息管理和平台运营日常工作，包括日常信息系统维护管理、漏洞验证、完成发布通报、统计和分类、对服务商发布的企业信息统一审核发布和定期更新、收集资源池服务商企业联系方式、收集提供一些应急演练的方案模版、案例呈现和服务商资源池对接等，具体工作内容如下： （1）信息管理：含日常信息系统的维护管理，负责平台内容的发布，确保信息及时、准确。对平台数据进行统计和分析，对发布内容进行分类管理； （2）漏洞管理：漏洞的定期收集、管理、验证、更新、发布，通告，确保漏洞通告的及时性，验证漏洞的严重性和可利用性，根

				据漏洞验证结果，提出并实施安全加固措施； （3）信息审核：审核服务商提交的企业信息，确保信息真实、合规，将审核通过的企业信息发布到平台，定期检查并更新企业信息，确保数据的时效性； （4）信息收集：通过多种渠道，定期收集服务商的企业联系方式，收集行业内的应急演练方案模板和案例，将收集到的方案模板进行标准化整理，形成可复用的模板库，提供对外展示； （5）资源池维护：维护服务商资源池，确保资源池信息的完整性和准确性。确保资源池中的信息及时更新； （6）平台监控：对平台进行实时监控，对日常故障及时排查并解决，确保系统稳定运行； （7）平台评估：定期对系统性能，资源使用进行评估，优化并提升响应速度，保障平台持续可用； （8）数据管理：对平台的日志进行定期审查，数据定期备份与还原，确保数据的安全性； （9）更新升级：定期更新系统软件，修复漏洞； （10）应急响应：对运营中发生的安全事件的应急预案，确保安全事件的快速处理。
	16	人员培训服务	1项	包含本项目相关人员不少于5人网络安全技术培训服务1次，培训时长不少于2课时。
	17	防火墙	1台	1、防火墙≥2U，≥1个管理口、≥1个HA口、≥4个千兆电口、≥4个千兆光口（满配千兆多模模块）和≥2个万兆光口（满配万兆多模模块），冗余电源，≥1个扩展槽位。网络层吞吐量(双向)：IPv4≥10000Mbps，IPv6≥10000Mbps 应用层吞吐量(单向)：IPv4≥8000Mbps，IPv6≥8000Mbps ；TCP新建连接速率：IPv4≥90万/秒，IPv6≥90万/秒 TCP并发连接数：IPv4≥1800万，IPv6≥1800万； 2、配置入侵防御特征库、应用识别库、WEB过滤库、快速扫描查杀防病毒库≥3年升级服务许可，≥3年硬件维保； 3、产品由专用的硬件平台、安全操作系统及功能软件构成。设备采用自主知识产权的专用安全操作系统，采用多核多平台并行处理机制； 4、支持RIP、OSPF、BGP4、策略路由，支持根据入接口、源/

				目的 IP 地址、协议、用户、应用、选路算法、探测等多种条件设置策略路由； 5、支持手动和 LACP 链路聚合，可根据源/目的 MAC、源/目的 IP、源/目的端口、五元组、端口轮询等条件提供不少于 8 种链路负载算法； ▲6、支持 DNS Doctoring 功能，能够将来自内部网络的域名解析请求定向到真实内网资源，提高访问效率，同时支持通过配置多条 DNS Doctoring，实现内网资源服务器的负载均衡（在响应文件中提供【支持 DNS Doctoring 功能】功能截图证明材料复印件并加盖供应商公章）； 7、支持一体化安全策略配置，可以通过一条策略实现五元组、源 MAC、源地区、目的地区、域名、应用、服务、时间、长连接、并发会话、WEB 认证、IPS、AV、URL 过滤、WAF、邮件安全、数据过滤、文件过滤、审计等功能配置,简化用户管理； 8、支持 IPv4/IPv6 双栈工作模式，支持 RADVD、ND、RIPng、OSPFv3、BGP4+；支持 IPv6 安全控制策略设置，能针对 IPv6 的目的/源地址、目的/源服务端口、区域、服务、时间、扩展头属性等条件进行安全访问规则的设置； 9、支持在一台物理设备上划分出不少于 128 个相互独立的虚拟系统，可根据连接配额及连接新建速率为每个虚拟系统分配资源，实配不少于 24 个虚拟防火墙授权； ▲10、支持针对 IP、ICMP、TCP、UDP、DNS、HTTP、NTP 等协议进行 DDOS 防护。支持 NTP 流量检测清洗，能对 NTP QUERY FLOOD、NTP REPLY FLOOD 等攻击进行检测并提供基于 NTP 请求限速、NTP 响应限速、源认证、会话认证的防御策略； 11、支持对达梦、人大金仓等数据库应用、P2P、移动应用、迅雷加密流量、向日葵/Teamview 等远程控制软件、Modbus/IEC/OPC 等工控物联网协议进行识别控制，支持自定义应用特征； ▲12、支持独立的入侵防护规则特征库，特征总数在 5000 条或以上，能对常见漏洞进行安全防护，兼容国家信息安全漏洞库（在响应文件中提供【特征总数在 5000 条或以上】功能截图证明材料复印件并加盖供应商公章）；

				13、支持配置文件本地备份和回滚，支持>2 个配置文件备份，支持对访问控制策略、NAT 策略等关键配置进行单独及加密备份和恢复；支持对配置命令及配置文件的操作行为进行审计； 14、支持 CPU 利用率、内存利用率、磁盘利用率、会话数告警及 CPU 利用率、内存利用率、磁盘利用率等硬件资源实时利用率及其历史使用情况追踪； 15、支持对病毒防御、入侵防御、DDOS 攻击等按照威胁类型/攻击主机/受攻击主机三种维度结合威胁等级和时间周期进行统计、排名； 16、支持系统管理员本地认证、外部认证和证书认证，外部认证失败时可转本地认证。支持设置管理员首次登录是否强制修改密码，支持密码强度、有效期设置。
商务条款		▲报价要求		供应商须就本项目采购需求中的所有实施内容作完整报价，总报价包含但不限于培训、技术支持、售后服务费、测试、保险费和各项税金等完成本项目所产生的全部费用。 注：供应商在报价时应考虑各方面因素、各种风险和自己的承受能力，报价中应包含全部内容，成交后采购人不再另行支付额外费用。
		▲合同签订期		自成交通知书发出之日起 25 日内。
		▲交付时间及地点		1、交付时间：自合同签订之日起 60 个日历日内验收合格并交付使用。 2、交付地点：广西南宁市采购人指定地点。
		▲质保期限		按国家有关产品“三包”规定执行“三包”，自最终验收合格并交付使用之日起计算，产品质保期不少于 3 年（“技术条款”另有约定的，从其约定）。若厂家质保期超过此年限的，合同履行过程中按厂家规定执行。
		售后服务要求		除另行特别注明外，售后服务要求如下： 1、成交供应商按采购人指定的地点负责送货上门、安装、调试，负责培训使用人员和维护人员。 ▲2、成交供应商必须提供安装、配线以及软硬件的测试和调整服务。开始安装时应让用户的硬软件和系统集成人员参与安装、检测和排除故障。成交供应商在施工、安装、调试等全过程中接受用户的监

		督。 3、在成交供应商承诺的保修期内，设备保修包换所需要的配件均是原厂原装，不得使用兼容货物。 4、售后服务按厂家承诺执行。超过厂家承诺标准的，按成交供应商提交的售后服务承诺书执行。定期回访以及对软件进行维护；质保期后需提供维修维护服务。 5、成交供应商在质量保证期内应当为采购人提供以下技术支持和服务： 5.1 电话咨询 成交供应商应当为采购人提供技术援助电话，解答采购人在使用中遇到的问题，及时为采购人提出解决问题的建议。 5.2 服务响应时间 质保期内，用户遇到使用或技术问题，电话咨询不能解决的，成交供应商应在 48 小时内到达现场进行处理，到达现场后 24 小时内排除故障，恢复正常使用。未能修复的直接更换，保证采购人正常使用，产生的一切费用由成交供应商承担。 5.3 技术升级 在质保期内，如果成交供应商的产品或服务升级，成交供应商应及时通知采购人，如采购人有相应要求，成交供应商应对采购人购买的产品或服务进行升级。 6、质保期外服务要求 6.1 质量保证期过后，成交供应商应同样无偿提供电话咨询服务，并应承诺提供产品或服务上门维护。 6.2 质量保证期过后，采购人需要继续由原成交供应商提供售后服务的，成交供应商和制造商应以优惠价格提供售后服务。 7、培训要求：安装设备之前，成交供应商须对采购人提供现场培训服务，培训内容包括提供产品或服务的使用和操作；培训服务涉及的相关费用应计算在项目报价内，并使使用人员能独立、熟练操作软件。 8、成交供应商应保证采购人在接受其提供的相关服务时免受第三方提出侵犯其知识产权的起诉，由此引起的知识产权纠纷由成交供应商负责。

		9、确保本项目所有内容不存在意识形态问题。
	▲付款方式	1、项目合同、担保措施生效以及具备实施条件后10个工作日内，采购人通过银行转账的方式向成交供应商支付合同总金额的30%预付款；成交供应商实施完成本项目，并通过采购人审核验收，在通过验收后的10个工作日内，支付合同总金额的70%。 2、采购人付款前，成交供应商应向采购人开具等额有效的增值税发票，采购人未收到合格有效发票的，有权不予支付相应款项直至成交供应商提供合格发票，并不承担延迟付款责任。发票认证通过是付款的必要前提之一。 3、付款方式：银行转账。
	▲履约保证金	1、履约保证金金额：成交金额的5%。（若成交供应商被认定为中小企业的，履约保证金数额将按成交金额的2%收取） 2、履约保证金递交方式：银行转账、支票、汇票、本票或者金融、保险机构出具的保函等非现金形式。 3、履约保证金递交时间：签订合同前5个工作日内由成交供应商转入采购人指定保证金账户。 4、履约保证金退还：履约完成并验收合格后无质量问题，成交供应商提供《政府采购项目履约保证金退付意见书》及《政府采购项目合同验收报告》，向采购人提出书面申请退还，采购人在收到申请后5个工作日内办理履约保证金退还手续（无息退还）。 保证金指定账户： 开户名：广西工业职业技术学院 开户行：广西北部湾银行南宁市衡阳路支行 账　号：1702012200017200
	验收标准及要求	1、验收过程中所产生的一切费用均由成交供应商承担。报价时应考虑相关费用。 2、成交供应商在验收时由采购人对照磋商文件及响应文件承诺的功能目标及技术指标全面核对检验，对所有要求出具的证明文件的原件进行核查，如不符合磋商文件的技术需求及要求以及提供虚假承诺的，按相关规定做退货处理及违约处理，成交供应商承担所有责任和费用，采购人保留进一步追究责任的权利。
	规范标准	采购标的需执行的国家标准、行业标准、地方标准或者其他标准、

		规范。多项标准的，按最新标准或较高标准执行。
	▲进口产品说明	□本表的第项货物所涉及的货物已按规定办妥进口产品采购审核手续，竞标产品可选用进口产品；但如选用进口产品时必须为全套原装进口产品（即通过中国海关报关验放进入中国境内且产自关境外的产品），同时投标人必须负责办理进口产品所有相关手续并承担所有费用。其他货物不接受进口产品参与竞标，否则作无效标处理。 ☑本服务所涉及的货物不接受进口产品（即通过中国海关报关验放进入中国境内且产自关境外的产品）参与竞标，如有进口产品参与竞标的作无效标处理。

附件：

节能产品政府采购品目清单

品目序号	名称			依据的标准
1	A020101计算机设备	★A02010104台式计算机		《微型计算机能效限定值及能效等级》（GB28380）
		★A02010105便携式计算机		《微型计算机能效限定值及能效等级》（GB28380）
		★A02010107平板式微型计算机		《微型计算机能效限定值及能效等级》（GB28380）
2	A020106输入输出设备	A02010601打印设备	A0201060101喷墨打印机	《复印机、打印机和传真机能效限定值及能效等级》（GB21521）
			★A0201060102激光打印机	《复印机、打印机和传真机能效限定值及能效等级》（GB21521）
			★A0201060104针式打印机	《复印机、打印机和传真机能效限定值及能效等级》（GB21521）
		A02010604显示设备	★A0201060401液晶显示器	《计算机显示器能效限定值及能效等级》（GB21520）
		A02010609图形图像输入设备	A0201060901扫描仪	参照《复印机、打印机和传真机能效限定值及能效等级》（GB21521中打印速度为15页/分的针式打印机相关要求
3	A020202投影仪			《投影机能效限定值及能效等级（GB32028）
4	A020204多功能一体机			《复印机、打印机和传真机能效限定值及能效等级》（GB21521）
5	A020519泵	A02051901离心泵		《清水离心泵能效限定值及节能评价值》（GB19762）
6	A020523制冷空调设备	★A02052301制冷压缩机	冷水机组	《冷水机组能效限定值及能效等级》（GB19577），《低环境温度空气源热泵（冷水）机组能效限定值及能效等级》（GB37480）
			水源热泵机组	《水（地）源热泵机组能效限定值及能效等级》（GB30721）

			溴化锂吸收式冷水机组	《溴化锂吸收式冷水机组能效限定值及能效等级》（GB29540）
		★A02052305空调机组	多联式空调（热泵）机组(制冷量>14000W)	《多联式空调（热泵）机组能效限定值及能源效率等级》（GB21454
			单元式空气调节机(制冷量>14000W)	《单元式空气调节机能效限定值及能效等级》（GB19576）《风管送风式空调机组能效限定值及能效等级》（GB37479）
		★A02052309专用制冷、空调设备	机房空调	《单元式空气调节机能效限定值及能效等级》（GB19576）
		A02052399其他制冷空调设备	冷却塔	《机械通风冷却塔第1部分：中小型开式冷却塔》（GB/T7190.1）《机械通风冷却塔第2部分：大型开式冷却塔》（GB/T7190.2
7	A020601电机			《中小型三相异步电动机能效限定值及能效等级》（GB18613）
8	A020602变压器	配电变压器		《三相配电变压器能效限定值及能效等级》（GB20052）
9	★A020609镇流器	管型荧光灯镇流器		《管形荧光灯镇流器能效限定值及能效等级》（GB17896）
10	A020618生活用电器	A0206180101电冰箱		《家用电冰箱耗电量限定值及能效等级》（GB12021.2）
		★A0206180203空调机	房间空气调节器	《转速可控型房间空气调节器能效限定值及能效等级》（GB21455-2013），待2019年修订发布后，按《房间空气调节器能效限定值及能效等级》（GB21455-2019）实施。
			多联式空调（热泵）机组（制冷量≤14000W）	《多联式空调（热泵）机组能效限定值及能源效率等级》（GB2145
			单元式空气调节机	《单元式空气调节机能效限定值及能源效率等级》（GB19576）《风
			(制冷量≤14000W)	管送风式空调机组能效限定值及能效等级》（GB37479）
		A0206180301洗衣机		《电动洗衣机能效水效限定值及等级》（GB12021.4）
		A02061808热水器	★电热水器	《储水式电热水器能效限定值及能效等级》（GB21519）
			燃气热水器	《家用燃气快速热水器和燃气采暖热

				水炉能效限定值及能效等级》（GB20665）
			热泵热水器	《热泵热水机（器）能效限定值及能效等级》（GB29541）
			太阳能热水系统	《家用太阳能热水系统能效限定值及能效等级》（GB26969）
11	A020619照明设备	★普通照明用双端荧光灯		《普通照明用双端荧光灯能效限定值及能效等级》（GB19043）
		LED道路/隧道照明产品		《道路和隧道照明用LED灯具能效限定值及能效等级》（GB37478
		LED筒灯		《室内照明用LED产品能效限定值及能效等级》（GB30255）
		普通照明用非定向自镇流LED灯		《室内照明用LED产品能效限定值及能效等级》（GB30255）
12	★A020910电视设备	A02091001普通电视设备（电视机）		《平板电视能效限定值及能效等级》（GB24850）
13	★A020911视频设备	A02091107视频监控设备	监视器	以射频信号为主要信号输入的监视器应符合《平板电视能效限定值及能效等级》（GB24850），以数字信号为主要信号输入的监视器应符合《计算机显示器能效限定值及能效等级》（GB21520）
14	A031210饮食炊事机械	商用燃气灶具		《商用燃气灶具能效限定值及能效等级》（GB30531）
15	★A060805便器	坐便器		《坐便器水效限定值及水效等级》（GB25502）
		蹲便器		《蹲便器用水效率限定值及用水效率等级》（GB30717）
		小便器		《小便器用水效率限定值及用水效率等级》（GB28377）
16	★A060806水嘴			《水嘴用水效率限定值及用水效率等级》（GB 25501）
17	A060807便器冲洗阀			《便器冲洗阀用水效率限定值及用水效率等级》（GB28379）

18	A060810淋浴器			《淋浴器用水效率限定值及用水效率等级》（GB28378）

注：1. 节能产品认证应依据相关国家标准的最新版本，依据国家标准中二级能效（水效）指标。

2. 以“★”标注的为政府强制采购产品。

响应函

一、响应函

（必须提供，否则响应文件按无效响应处理）

响应函

致：广西工业职业技术学院

我方已仔细阅读了贵方组织的广西工业领域网络安全信息公共服务平台项目（项目编号：GXZC2025-C3-000848-GXZL）的竞争性磋商采购文件的全部内容，签字代表蒙文婷经正式授权并代表供应商广西塔易信息技术有限公司提交响应文件。

据此函，签字人兹宣布：

1.我方愿意以（大写）人民币贰佰贰拾陆万捌仟贰佰叁拾壹元整（¥2268231.00元）的响应总报价，提供本项目竞争性磋商采购文件第二章“采购需求”中相应的采购内容。

2.我方同意自本项目竞争性磋商采购文件采购公告规定的递交响应文件截止时间起遵循本响应函，并承诺在“第三章 供应商须知”规定的响应有效期内不修改、撤销响应文件。

3.我方在此声明，所递交的响应文件及有关资料内容完整、真实和准确。

4.我方承诺符合《中华人民共和国政府采购法》第二十二条规定：

（1）具有独立承担民事责任的能力；

（2）具有良好的商业信誉和健全的财务会计制度；

（3）具有履行合同所必需的设备和专业技术能力；

（4）有依法缴纳税收和社会保障资金的良好记录；

（5）参加政府采购活动前三年内，在经营活动中没有重大违法记录；

（6）法律、行政法规规定的其他条件。

5.我方在此声明，我方在参加本项目的政府采购活动前三年内，在经营活动中没有重大违法记录（重大违法记录是指供应商因违法经营受到刑事处罚或者责令停产停业、吊销许可证或者执照、较大数额罚款等行政处罚），未被列入失信被执行人、重大税收违法失信主体、政府采购严重违法失信行为记录名单，完全符合《中华人民共和国政府采购法》第二十二条规定的供应商资格条件，我方对此声明负全部法律责任。

6. 如本项目采购内容涉及须符合国家强制规定的，我方承诺我方本次竞标均符合国家有关强制规定。

7. 如我方成交，我方承诺在收到成交通知书后，在成交通知书规定的期限内，根据竞争性磋商采购文件、我方的响应文件及有关澄清承诺书的要求按第六章“拟签订的合同文本”与采购人订立书面合同，并按照合同约定承担完成合同的责任和义务。

8. 我方已详细审核竞争性磋商文件，我方知道必须放弃提出含糊不清或误解问题的权利。

9. 我方承诺满足竞争性磋商文件第六章“拟签订的合同文本”的条款，承担完成合同的责任和义务。

10. 我方同意应贵方要求提供与本竞标有关的任何数据或资料。若贵方需要，我方愿意提供我方作出的一切承诺的证明材料。

11. 我方完全理解贵方不一定接受响应报价最低的供应商为成交供应商的行为。

12. 我方将严格遵守《中华人民共和国政府采购法》第七十七条的规定，即供应商有下列情形之一的，处以采购金额千分之五以上千分之十以下的罚款，列入不良行为记录名单，在一至三年内禁止参加政府采购活动，有违法所得的，并处没收违法所得，情节严重的，由工商行政管理机关吊销营业执照；构成犯罪的，依法追究刑事责任：

（1）提供虚假材料谋取中标、成交的；

（2）采取不正当手段诋毁、排挤其他供应商的；

（3）与采购人、其他供应商或者采购代理机构恶意串通的；

（4）向采购人、采购代理机构行贿或者提供其他不正当利益的；

（5）在采购过程中与采购人进行协商谈判的；

（6）拒绝有关部门监督检查或提供虚假情况的。

13. 以上事项如有虚假或者隐瞒，我方愿意承担一切后果，并不再寻求任何旨在减轻或者免除法律责任的辩解。

14. 与本磋商有关的一切正式往来信函请寄：

地址：中国（广西）自由贸易试验区南宁片区凯旋路13号五象新区总部休闲公园9号楼

电话：0771-3360667

传真：0771-3360667

邮政编码：530020

开户名称：广西塔易信息技术有限公司

开户银行：中国建设银行股份有限公司广西自贸试验区南宁片区五象支行

银行账号：45050160500100000389

特此承诺。

供应商名称（电子签章）：广西塔易信息技术有限公司

日期：2025年05月08日

响应报价表

二、响应报价表

（必须提供，否则响应文件按无效响应处理）

项目名称：广西工业领域网络安全信息公共服务平台

项目编号：GXZC2025-C3-000848-GXZL

供应商名称：广西塔易信息技术有限公司

序号	标的名称	技术要求	数量及单位①	单价(元)②	单项合价（元）③=①×②	备注
1	工业领域网络安全信息公共服务平台	详见偏离表	1 套	716100.00	716100.00	塔易技术 塔易漏洞管理平台
2	万兆超融合交换机	详见偏离表	2 台	19200.00	38400.00	华为 S6730S-S24X6Q
3	服务器密码机系统	详见偏离表	1 台	75144.00	75144.00	北京天融信 TopCSP
4	IPSEC/SSLVPN 综合安全网关系统	详见偏离表	1 台	75318.00	75318.00	北京天融信 TopVPN6000
5	签名验签服务器系统	详见偏离表	1 台	97464.00	97464.00	北京天融信 TopSVS
6	协同签名系统	详见偏离表	1 台	142104.00	142104.00	渔翁信息 XT/V1.0
7	智能密码钥匙	详见偏离表	10 个	27.90	279.00	北京世纪龙脉 mToken
8	国密数字证书	详见偏离表	120 点	980.00	117600.00	广西 CA gxca
9	二级等保测评	详见偏离表	1 项	46500.00	46500.00	广西电子信息和网络安全测评研究院 定制服务
10	软件测试	详见偏离表	1 项	9300.00	9300.00	塔易技术 定制服务
11	代码审计	详见偏离表	1 项	46500.00	46500.00	塔易技术 定制服务
12	二级密评测评	详见偏离表	1 项	46500.00	46500.00	广西电子信息和网络安全测评研究院 定制服务

13	渗透测试	详见偏离表	1 项	46500.00	46500.00	塔易技术 定制服务
14	系统集成服务	详见偏离表	1 项	116250.00	116250.00	塔易技术 定制服务
15	平台运营服务	详见偏离表	1 项	563000.00	563000.00	塔易技术 定制服务
16	人员培训服务	详见偏离表	1 项	9300.00	9300.00	塔易技术 定制服务
17	防火墙	详见偏离表	1 台	121972.00	121972.00	北京天融信 NGFW4000-UF
报价合计（包含税费等所有费用）：（大写）人民币 贰佰贰拾陆万捌仟贰佰叁拾壹元整（¥ 2268231.00 元）						
无 分标（此处有分标时填写具体分标号，无分标时填写"无"）						
交付时间：自合同签订之日起 60 个日历日内验收合格并交付使用。						

注：

1、供应商需按本表格式填写，不得自行更改，也不得留空，如有多分标，按分标分别提供响应报价表。

2、如为联合体响应的，"供应商名称"处必须列明联合体各方名称，并标注联合体牵头人名称，且盖章处须加盖联合体牵头人公章，**否则其响应作无效响应处理。**

3、以上表格要求细分项目及报价，**否则其响应作无效响应处理。**

4、特别提示：采购机构将对项目名称和项目编号，成交供应商名称、地址和成交金额，主要成交标的的名称、服务范围、服务要求、服务时间、服务标准等予以公示。

供应商名称（电子签章）：广西塔易信息技术有限公司

日期：2025 年 05 月 08 日

最后报价表

投标报价明细表

投标人全称（公章）：广西[illegible]信息技术有限公司

项目编号及名称：广西[illegible]（[illegible]）

供应商名称	报价(总价：元)	交付时间	备注
广西[illegible]信息技术有限公司	2260231	自合同签订之日起60个日历日内完成合同并交付使用。	无

最终报价表

项目名称：广西工业领域网络安全信息公共服务平台

项目编号：GXZC2025-[illegible]-000848-GXZL

供应商名称：广西塔易[illegible]技术有限公司

序号	标的名称	技术要求	数量及单位①	单价(元)②	单项合价（元）③=①×②	备注
1	工业领域网络安全信息公共服务平台	详见偏离表	1 套	716100.00	716100.00	塔易技术 塔易漏洞管理平台
2	万兆超融合交换机	详见偏离表	2 台	19200.00	38400.00	华为 S6730S-S24X6Q
3	服务器密码机系统	详见偏离表	1 台	75144.00	75144.00	北京天融信 TopCSP
4	IPSEC/SSL VPN 综合安全网关系统	详见偏离表	1 台	75318.00	75318.00	北京天融信 TopVPN6000
5	签名验签服务器系统	详见偏离表	1 台	97464.00	97464.00	北京天融信 TopSVS
6	协同签名系统	详见偏离表	1 台	142104.00	142104.00	渔翁信息 XT/V1.0
7	智能密码钥匙	详见偏离表	10 个	27.90	279.00	北京世纪龙脉 mToken
8	国密数字证书	详见偏离表	120 点	980.00	117600.00	广西 CA gxca
9	二级等保测评	详见偏离表	1 项	46500.00	46500.00	广西电子信息和网络安全测评研究院 定制服务
10	软件测试	详见偏离表	1 项	9300.00	9300.00	塔易技术 定制服务
11	代码审计	详见偏离表	1 项	46500.00	46500.00	塔易技术 定制服务
12	二级密评测评	详见偏离表	1 项	46500.00	46500.00	广西电子信息和网络安全测评研究院 定制服务
13	渗透测试	详见偏离表	1 项	46500.00	46500.00	塔易技术 定制服务

14	系统集成服务	详见偏离表	1 项	116250.00	116250.00	塔易技术 定制服务
15	平台运营服务	详见偏离表	1 项	560000.00	560000.00	塔易技术 定制服务
16	人员培训服务	详见偏离表	1 项	9300.00	9300.00	塔易技术 定制服务
17	防火墙	详见偏离表	1 台	121972.00	121972.00	北京天融信 NGFW4000-UF
报价合计（包含税费等所有费用）：（大写）人民币 贰佰贰拾陆万伍仟贰佰叁拾壹元整（¥ 2265231.00 元）						
无 分标（此处有分标时填写具体分标号，无分标时填写"无"）						
交付时间：自合同签订之日起60个日历日内验收合格并交付使用。						

供应商名称（电子签章）：广西塔易信息技术有限公司

日期：2025年 05 月 08 日

九、技术条款偏离表

（必须提供，否则响应文件按无效响应处理）

技术条款偏离表

(注：按采购需求具体条款修改)

所竞分标： 无

序号	竞争性磋商采购文件需求			响应文件承诺			偏离说明
	标的名称	数量及单位	技术要求	标的名称	数量及单位	技术要求	
1	工业领域网络安全信息公共服务平台	1套	一、平台门户	工业领域网络安全信息公共服务平台	1套	**满足** 一、平台门户	无偏离
			此模块提供导航信息、信息资讯、法律法规和标准信息展示、用户登录注册等内容。			**满足** 此模块提供导航信息、信息资讯、法律法规和标准信息展示、用户登录注册等内容。	无偏离
			二、功能模块			**满足** 二、功能模块	无偏离
			（一）漏洞管理			**满足** （一）漏洞管理	无偏离
			1、漏洞收集			**满足** 1、漏洞收集	无偏离
			此模块主要负责收集、整理各类工业互联网漏洞信息。其功能包括：漏洞信息实时采集、存储、分析以及定期公布。其中，漏			**满足** 此模块主要负责收集、整理各类工业互联网漏洞信息。其功能包括：漏洞信息实时采集、存储、分析以及定期公布。其中，漏洞信	无偏离

技术条款偏离表

			洞信息应包括产品型号、漏洞编号、漏洞等级、漏洞描述等信息，并为使用单位提供下载和查阅。			息应包括产品型号、漏洞编号、漏洞等级、漏洞描述等信息，并为使用单位提供下载和查阅。	
			2、漏洞上报			**满足** 2、漏洞上报	无偏离
			此模块主要为使用单位和技术支撑单位将发现的工业互联网漏洞信息上报至本平台，给使用单位和技术支撑单位提供上报通道。其中，漏洞信息应包括产品型号、漏洞编号、漏洞等级、漏洞描述等信息。			**满足** 此模块主要为使用单位和技术支撑单位将发现的工业互联网漏洞信息上报至本平台，给使用单位和技术支撑单位提供上报通道。其中，漏洞信息应包括产品型号、漏洞编号、漏洞等级、漏洞描述等信息。	无偏离
			3、漏洞验证核实			**满足** 3、漏洞验证核实	无偏离
			此模块为收集和上报的漏洞验证核实的流程管理，在人工技术核实确认漏洞可利用后推送到风险信息通报模块。			**满足** 此模块为收集和上报的漏洞验证核实的流程管理，在人工技术核实确认漏洞可利用后推送到风险信息通报模块。	无偏离
			（二）风险信息通报预警			**满足** （二）风险信息通报预警	无偏离
			1、漏洞发布预警和通报			**满足** 1、漏洞发布预警和通报	无偏离
			最新漏洞发布，信息发布在线上服务平台首页，提醒用户关注最新的漏洞。			**满足** 最新漏洞发布，信息发布在线上服务平台首页，提醒用户关注最新的漏洞。	无偏离
			漏洞信息库及查询。与国家工业信息安全漏洞库（CICSVD）实现对接，预置 PLC、数控机床、工业机器人等相关产品漏洞不少于 5000 条。			**满足** 漏洞信息库及查询。与国家工业信息安全漏洞库（CICSVD）实现对接，预置 PLC、数控机床、工业机器人等相关产品漏洞 5000 条。	无偏离
			漏洞通报全生命周期管理。建立“省-市-区县-企”四级线上风险通报工作机制，支撑常态化开展风险预警通报下发、威胁情报信息共享，实现对工业控制系统的重大漏洞、风			**满足** 漏洞通报全生命周期管理。建立“省-市-区县-企”四级线上风险通报工作机制，支撑常态化开展风险预警通报下发、威胁情报信息共享，实现对工业控制系统的重大漏洞、风险等	无偏离

			路等及时向有关行业、地区和工业企业进行线上和短信定点推送的功能，并支持显示信息处理进程，支撑地方主管部门对漏洞整改进度进行全过程跟踪和监督。			及时向有关行业、地区和工业企业进行线上和短信定点推送的功能，并支持显示信息处理进程，支撑地方主管部门对漏洞整改进度进行全过程跟踪和监督。	
			2、咨询服务			**满足** 2、咨询服务	无偏离
			提供漏洞情况、漏洞修复的技术咨询服务电话。留下技术支撑单位的联系信息，有需求单位来电自行联系。			**满足** 提供漏洞情况、漏洞修复的技术咨询服务电话。留下技术支撑单位的联系信息，有需求单位来电自行联系。	无偏离
			（三）资产测绘和安全检测			**满足** （三）资产测绘和安全检测	无偏离
			实现面向广西壮族自治区境内全量IP的资产测绘，可监测不少于100种品牌工业控制系统，至少包括力控、亚控、中控、西门子、施耐德等品牌，覆盖SCADA、工业实时数据库、PLC等设备类型，将核查结果从区域、厂商、端口、漏洞等维度进行统计、关联，实时展示联网资产安全态势，监测维度包括IP地址、端口号、所属公司、设备类型、协议、设备厂商、运营商等不少于7个维度。			**满足** 实现面向广西壮族自治区境内全量IP的资产测绘，可监测100种品牌工业控制系统，包括力控、亚控、中控、西门子、施耐德等品牌，覆盖SCADA、工业实时数据库、PLC等设备类型，将核查结果从区域、厂商、端口、漏洞等维度进行统计、关联，实时展示联网资产安全态势，监测维度包括IP地址、端口号、所属公司、设备类型、协议、设备厂商、运营商等7个维度。	无偏离
			（四）安全自查数据报送			**满足** （四）安全自查数据报送	无偏离
			使用单位通过分配账户将年度自查数据填报到系统中，采用数据传输和存储加密技术，报送接口可根据情况设定开启和关闭时间，并提供年度、区域、行业、安全等级等关键字自查数据统计功能。			**满足** 使用单位通过分配账户将年度自查数据填报到系统中，采用数据传输和存储加密技术，报送接口可根据情况设定开启和关闭时间，并提供年度、区域、行业、安全等级等关键字自查数据统计功能。	无偏离
			（五）资源池服务对接			**满足** （五）资源池服务对接	无偏离

			提供企业信息发布功能，可发布资源池服务商企业信息，发布企业需求信息。			**满足** 提供企业信息发布功能，可发布资源池服务商企业信息，发布企业需求信息。	无偏离
			（六）公共服务			**满足** （六）公共服务	无偏离
			此模块可为使用单位提供各类公共服务申请功能，如安全检测评估、政策补贴、安全认证、技术支持等。使用单位可以在线提交申请，平台审核通过后将为其提供相应的服务支持。同时，该模块还应包括一个公示区，公布已申请成功的企业名单和相关信息。			**满足** 此模块可为使用单位提供各类公共服务申请功能，如安全检测评估、政策补贴、安全认证、技术支持等。使用单位可以在线提交申请，平台审核通过后将为其提供相应的服务支持。同时，该模块还应包括一个公示区，公布已申请成功的企业名单和相关信息。	无偏离
			（七）在线应急响应服务			**满足** （七）在线应急响应服务	无偏离
			对于发生的安全事件，平台提供及时的应急响应服务咨询服务，协助使用单位进行事件处置，降低安全风险。提供网络安全应急响应国家标准、方案模块，可供用户下载。			**满足** 对于发生的安全事件，平台提供及时的应急响应服务咨询服务，协助使用单位进行事件处置，降低安全风险。提供网络安全应急响应国家标准、方案模块，可供用户下载。	无偏离
			（八）在线学习模块			**满足** （八）在线学习模块	无偏离
			在线学习模块。以精品课程、微视频为主的自主学习平台。提升企业网络安全意识和能力。			**满足** 在线学习模块。以精品课程、微视频为主的自主学习平台。提升企业网络安全意识和能力。	无偏离
			（九）短信平台			**满足** （九）短信平台	无偏离
			能将风险信息通过短信推送到使用单位相关人员手机中，及时提醒使用单位处理风险信息。			**满足** 能将风险信息通过短信推送到使用单位相关人员手机中，及时提醒使用单位处理风险信息。	无偏离
			（十）系统基础模块			**满足** （十）系统基础模块	无偏离
			1、用户管理			**满足** 1、用户管理	无偏离
			自治区、市、县三级用户管理，预计5			**满足** 自治区、市、县三级用户管理，预计5	无偏离

			万用户量。			万用户量。	
			2、日志模块			**满足** 2、日志模块	无偏离
			账户操作过程日志记录。			**满足** 账户操作过程日志记录。	无偏离
			3、企业用户基础数据库			**满足** 3、企业用户基础数据库	无偏离
			国产化基础数据库适配。			**满足** 国产化基础数据库适配。	无偏离
			（十一）系统对接			**满足** （十一）系统对接	无偏离
			▲1、系统必须实现与国家工业信息安全漏洞库的对接，可获取漏洞信息至少从漏洞名称、所属类型、CVE 编号、危害等级、影响行业、漏洞描述、影响产品名称等不少于 7 个维度进行描述，面向工业控制器、数控机床、工业机器人等不少于 3 种工控设备收录漏洞不少于 5000 条。如涉及相关二次开发费用，由供应商自行承担[在响应文件中提供承诺函（承诺函需包含本项内容要求）并加盖供应商公章]。			**满足** ▲1、系统实现与国家工业信息安全漏洞库的对接，可获取漏洞信息从漏洞名称、所属类型、CVE 编号、危害等级、影响行业、漏洞描述、影响产品名称等 7 个维度进行描述，面向工业控制器、数控机床、工业机器人等 3 种工控设备收录漏洞 5000 条。如涉及相关二次开发费用，由我司自行承担[在响应文件中提供承诺函（承诺函包含本项内容要求）并加盖公章]。	无偏离
			▲2、系统必须实现与国家工业信息安全态势感知平台的数据对接。如涉及相关二次开发费用，由供应商自行承担[在响应文件中提供承诺函（承诺函需包含本项内容要求）并加盖供应商公章]。			**满足** ▲2、系统实现与国家工业信息安全态势感知平台的数据对接。如涉及相关二次开发费用，由我司自行承担[在响应文件中提供承诺函（承诺函包含本项内容要求）并加盖公章]。	无偏离
2	万兆超融合交换机	2 台	1、设备性能：交换容量≥2.4Tbps，转发性能≥720Mpps；	万兆超融合交换机	2 台	**满足** 1、设备性能：交换容量 2.4Tbps，转发性能 720Mpps；	无偏离
			2、设备配置：提供万兆 SFP+光口≥24 个，支持模块化可插拔电源槽位≥2 个，本次			**满足** 2、设备配置：提供万兆 SFP+光口 24 个，支持模块化可插拔电源槽位 2 个，本次	无偏离

			提供可插拔交流电源模块≥2 个；单台 8 个万兆光模块。			提供可插拔交流电源模块 2 个；单台 8 个万兆光模块。	
3	服务器密码机系统	1 台	1、2U 机架式结构，系统配置≥1 个管理口，≥1 个 HA 口，≥4 个千兆电口，≥4 个 SFP 插槽，≥32G 内存，≥4TB 企业级硬盘,冗余电源,≥2 个扩展槽位，冗余电源。	服务器密码机系统	1 台	**满足** 1、2U 机架式结构，系统配置 1 个管理口，1 个 HA 口， 4 个千兆电口， 4 个 SFP 插槽， 32G 内存， 4TB 企业级硬盘,冗余电源,2 个扩展槽位，冗余电源。	无偏离
			2、SM2 算法密钥最大生成速率≥5000 对/秒，SM2 算法最大签名速率≥8000 次/秒，SM2 算法最大验签速率≥4000 次/秒，SM3 算法最大校验吞吐率≥1300Mbps，SM4 算法最大加解密吞吐率≥2100Mbps；			**满足** 2、SM2 算法密钥最大生成速率 5000 对/秒，SM2 算法最大签名速率 8000 次/秒，SM2 算法最大验签速率 4000 次/秒，SM3 算法最大校验吞吐率 1300Mbps，SM4 算法最大加解密吞吐率 2100Mbps；	无偏离
			▲3、产品须为国家密码管理局认证合格的密码产品，而非加密软件密码模块。			**满足** ▲3、产品为国家密码管理局认证合格的密码产品，而非加密软件密码模块。	无偏离
			4、通过数字签名可以保证信息传输的完整性、对发送者进行源认证以及防抵赖支持用户自行修改单点登录的账户信息。			**满足** 4、通过数字签名可以保证信息传输的完整性、对发送者进行源认证以及防抵赖支持用户自行修改单点登录的账户信息。	无偏离
			5、支持三层密钥结构：管理密钥、用户密钥/设备密钥/密钥加密密钥、会话密钥；			**满足** 5、支持三层密钥结构：管理密钥、用户密钥/设备密钥/密钥加密密钥、会话密钥；	无偏离
			6、具备四路随机噪声源，采用由国家密码管理局批准使用的物理噪声源发生器芯片生成随机数；			**满足** 6、具备四路随机噪声源，采用由国家密码管理局批准使用的物理噪声源发生器芯片生成随机数；	无偏离
			7、符合 GM/T 0018-2023《密码设备应用接口规范》标准，支持 WINDOWS、LINUX 系统平台，提供 JAVA、C 语言的接口，具备高兼容性；			**满足** 7、符合 GM/T 0018-2023《密码设备应用接口规范》标准，支持 WINDOWS、LINUX 系统平台，提供 JAVA、C 语言的接口，具备高兼容性；	无偏离

			8、支持白名单 IP 授权登录管理页面，业务通信支持国际和国密协议；			**满足** 8、支持白名单 IP 授权登录管理页面，业务通信支持国际和国密协议；	无偏离
			9、支持多操作系统 Linux、Windows；支持 API 接口描述，包括接口类别、接口实例，根据所选择的具体接口，显示该接口函数的名称、参数以及示例 demo；			**满足** 9、支持多操作系统 Linux、Windows；支持 API 接口描述，包括接口类别、接口实例，根据所选择的具体接口，显示该接口函数的名称、参数以及示例 demo；	无偏离
			▲10、支持国密算法 SM2/SM3/SM4；支持算法模式：ECB、CBC、CFB、OFB；支持杂凑算法：MD4、MD5、SHA1、SHA2（在响应文件中提供【支持国密算法 SM2/SM3/SM4】功能截图证明材料复印件并加盖供应商公章）；			**满足** ▲10、支持国密算法 SM2/SM3/SM4；支持算法模式：ECB、CBC、CFB、OFB；支持杂凑算法：MD4、MD5、SHA1、SHA2（在响应文件中提供【支持国密算法 SM2/SM3/SM4】功能截图证明材料复印件并加盖公章）；	无偏离
			11、支持 SM2 和 RSA 的数字信封转换；支持会话密钥生成、导入、导出、协商及销毁；			**满足** 11、支持 SM2 和 RSA 的数字信封转换；支持会话密钥生成、导入、导出、协商及销毁；	无偏离
			12、支持基于兑成算法的 MAC 消息鉴别码产生及验证；			**满足** 12、支持基于兑成算法的 MAC 消息鉴别码产生及验证；	无偏离
			▲13、支持密钥的全生命周期管理：密钥的生成、存储、使用、备份、恢复、删除、销毁等功能（在响应文件中提供【上述 7 种】功能截图证明材料复印件并加盖供应商公章）；			**满足** ▲13、支持密钥的全生命周期管理：密钥的生成、存储、使用、备份、恢复、删除、销毁等功能（在响应文件中提供【上述 7 种】功能截图证明材料复印件并加盖公章）；	无偏离
			14、支持配置管理日志、系统日志、业务日志审计，支持按日志类型、时间、级别、关键词等分类查询；			**满足** 14、支持配置管理日志、系统日志、业务日志审计，支持按日志类型、时间、级别、关键词等分类查询；	无偏离

			15、具备系统密码服务的自监控能力，服务器密码机系统运行过程中进行自检测，系统运行异常将停止服务，并且上报服务状态，用户可以实时查看密码服务状态；			**满足** 15、具备系统密码服务的自监控能力，服务器密码机系统运行过程中进行自检测，系统运行异常将停止服务，并且上报服务状态，用户可以实时查看密码服务状态；	无偏离
4	IPSEC/SSL VPN 综合安全网关系统	1 台	1、系统≥2U≥10 个千兆电口,冗余电源≥2 个扩展槽位,国密 IPSEC VPN 最大吞吐率≥600Mbps 国密 IPSEC VPN 最大隧道数≥4000 条，国密 SSL VPN 最大吞吐率≥200Mbps,国密 SSL VPN 最大建议并发用户数≥1600；默认含≥200 个 SSL VPN 的客户端并发许可；	IPSEC/SSL VPN 综合安全网关系统	1 台	**满足** 1、系统=2U，10 个千兆电口,冗余电源,2 个扩展槽位,国密 IPSEC VPN 最大吞吐率 600Mbps 国密 IPSEC VPN 最大隧道数 4000 条，国密 SSL VPN 最大吞吐率 200Mbps，国密 SSL VPN 最大建议并发用户数 1600；默认含 200 个 SSL VPN 的客户端并发许可；	无偏离
			2、产品为 VPN 硬件设备，而非防火墙\UTM 类设备集成的 VPN 模块；			**满足** 2、产品为 VPN 硬件设备，而非防火墙\UTM 类设备集成的 VPN 模块；	无偏离
			3、支持基于用户、用户组、用户角色进行授权，实现用户可访问资源、可信接入和客户端杀毒策略；			**满足** 3、支持基于用户、用户组、用户角色进行授权，实现用户可访问资源、可信接入和客户端杀毒策略；	无偏离
			4、支持动态地址转换和静态地址转换，支持多对一、一对多和一对一等多种方式的地址转换；			**满足** 4、支持动态地址转换和静态地址转换，支持多对一、一对多和一对一等多种方式的地址转换；	无偏离
			5、支持双向 NAT；			**满足** 5、支持双向 NAT；	无偏离
			▲6、支持静态用户名口令、数字证书、短信、硬件特征码绑定、图形码方式；支持两种或两种以上组合认证方式（在响应文件中提供【支持两种或两种以上组合认证方式】功能截图证明材料复印件并加盖供应商公			**满足** ▲6、支持静态用户名口令、数字证书、短信、硬件特征码绑定、图形码方式；支持两种以上组合认证方式（在响应文件中提供【支持两种或两种以上组合认证方式】功能截图证明材料复印件并加盖公章）；	无偏离

			章）；				
			7、支持用户名口令认证防暴力破解，支持使用邮件、短信方式密码找回，支持对用户口令复杂度和有效性设置；			**满足** 7、支持用户名口令认证防暴力破解，支持使用邮件、短信方式密码找回，支持对用户口令复杂度和有效性设置；	无偏离
			8、支持内置 CA，可以对证书进行生成、签发、废弃操作；支持国际、国密算法证书；支持 DER/PEM/PKCS12 等多种证书编码；支持导入多个第三方 CA 根证书和 CRL 列表，可以对不同的 CA 用户证书进行身份认证；			**满足** 8、支持内置 CA，可以对证书进行生成、签发、废弃操作；支持国际、国密算法证书；支持 DER/PEM/PKCS12 等多种证书编码；支持导入多个第三方 CA 根证书和 CRL 列表，可以对不同的 CA 用户证书进行身份认证；	无偏离
			▲9、支持可信接入功能，能够对接入主机的信息进行检查，包括域名、杀毒软件、安装的程序、运行的服务等；支持可信接入分级授权（在响应文件中提供【支持可信接入功能和支持可信接入分级授权】功能截图证明材料复印件并加盖供应商公章）；			**满足** ▲9、支持可信接入功能，能够对接入主机的信息进行检查，包括域名、杀毒软件、安装的程序、运行的服务等；支持可信接入分级授权（在响应文件中提供【支持可信接入功能和支持可信接入分级授权】功能截图证明材料复印件并加盖公章）；	无偏离
			10、支持基于源/目的 IP 地址、MAC 地址、端口和协议、时间、用户、角色的访问控制；支持基于状态检测的动态包过滤；支持隧道内的访问控制；			**满足** 10、支持基于源/目的 IP 地址、MAC 地址、端口和协议、时间、用户、角色的访问控制；支持基于状态检测的动态包过滤；支持隧道内的访问控制；	无偏离
			11、支持 Windows、iOS、Android、Linux、Mac 客户端接入方式；			**满足** 11、支持 Windows、iOS、Android、Linux、Mac 客户端接入方式；	无偏离
			▲12、支持 AES、DES、3DES、RC4、MD5、SHA1、RSA 等多种算法；支持国密数字证书认证（在响应文件中提供【上述 7 种算法】功能截图证明材料复印件并加盖供应			**满足** ▲12、支持 AES、DES、3DES、RC4、MD5、SHA1、RSA 等多种算法；支持国密数字证书认证（在响应文件中提供【上述 7 种算法】功能截图证明材料复印件并加盖公章）；	无偏离

			商公章）；				
			▲13、支持 DES、3DES、AES、MD5、SHA1、DH GROUP1/2/5、RSA 1024/2048 等加密算法；支持国家商密专用的 SM1、SM2、SM3、SM4 算法；			**满足** ▲13、支持 DES、3DES、AES、MD5、SHA1、DH GROUP1/2/5、RSA 1024/2048 等加密算法；支持国家商密专用的 SM1、SM2、SM3、SM4 算法；	无偏离
			14、支持设备的运行状态、设备资源状态、并发用户数、客户端类型分布、IPSEC 隧道状态、用户流量、安全事件、中国任意省市区县（港澳台除外）的接入用户数监控，并通过图表展示。			**满足** 14、支持设备的运行状态、设备资源状态、并发用户数、客户端类型分布、IPSEC 隧道状态、用户流量、安全事件、中国任意省市区县（港澳台除外）的接入用户数监控，并通过图表展示。	无偏离
5	签名验签服务器系统	1 台	1、系统≥2U，配置≥1 个管理口，≥1 个 HA 口，≥4 个千兆电口，≥4 个 SFP 插槽，≥32G 内存，≥4TB 企业级硬盘，冗余电源，≥2 个扩展槽位。SM2 算法密钥最大生成速率≥5000 对/秒，SM2 算法最大签名速率≥8000 次/秒，SM2 算法最大验签速率≥4000 次/秒，SM3 算法最大校验吞吐率≥1300Mbps，SM4 算法最大加解密吞吐率≥2100Mbps，SM2 算法制作数字信封最大速率≥4000 次/秒，SM2 算法拆解数字信封最大速率≥3000 次/秒；≥3 年硬件维保；	签名验签服务器系统	1 台	**满足** 1、系统=2U，配置 1 个管理口，1 个 HA 口，4 个千兆电口，4 个 SFP 插槽，32G 内存，4TB 企业级硬盘，冗余电源，2 个扩展槽位。SM2 算法密钥最大生成速率 5000 对/秒，SM2 算法最大签名速率 8000 次/秒，SM2 算法最大验签速率 4000 次/秒，SM3 算法最大校验吞吐率 1300Mbps，SM4 算法最大加解密吞吐率 2100Mbps，SM2 算法制作数字信封最大速率 4000 次/秒，SM2 算法拆解数字信封最大速率 3000 次/秒；3 年硬件维保；	无偏离
			2、实现基于数字证书的身份认证，支持不同 CA 的证书验证，提供 CRL/OCSP 等多种方式的证书有效性验证。			**满足** 2、实现基于数字证书的身份认证，支持不同 CA 的证书验证，提供 CRL/OCSP 等多种方式的证书有效性验证。	无偏离
			3、提供 PKCS1/ PKCS7 attach/PKCS7 detach/XML Sign 等多种格式的数字签名和数			**满足** 3、提供 PKCS1/ PKCS7 attach/PKCS7 detach/XML Sign 等多种格式的数字签名和数	无偏离

			字签名验证功能(PKCS1 签名支持记录签名日志功能)。			字签名验证功能(PKCS1 签名支持记录签名日志功能)。	
			4、对数据进行加密传输，只有指定的信封接收者可以解密数据。			**满足** 4、对数据进行加密传输，只有指定的信封接收者可以解密数据。	无偏离
			5、对文件提供数字签名和数字签名验证功能。			**满足** 5、对文件提供数字签名和数字签名验证功能。	无偏离
			6、提供 CRL/OCSP 等多种方式的证书有效性验证。			**满足** 6、提供 CRL/OCSP 等多种方式的证书有效性验证。	无偏离
			7、可同时配置多条证书链，验证不同 CA 系统签发的数字证书。			**满足** 7、可同时配置多条证书链，验证不同 CA 系统签发的数字证书。	无偏离
			8、提供证书解析功能，获取证书中的任意主题信息以及扩展项信息。			**满足** 8、提供证书解析功能，获取证书中的任意主题信息以及扩展项信息。	无偏离
			9、可实现对客户端证书的存储，管理员可以通过页面进行证书导入和查找，业务系统可以通过接口获取已存储的证书。			**满足** 9、可实现对客户端证书的存储，管理员可以通过页面进行证书导入和查找，业务系统可以通过接口获取已存储的证书。	无偏离
			10、可以自动更新黑名单，采用动态更新方式，无需重启服务。			**满足** 10、可以自动更新黑名单，采用动态更新方式，无需重启服务。	无偏离
			11、支持服务端负载均衡功能，来解决不能对外提供大数据量服务的问题，即多台机器负载时，多台机器能够同时对外提供一样的服务来处理大数据量。			**满足** 11、支持服务端负载均衡功能，来解决不能对外提供大数据量服务的问题，即多台机器负载时，多台机器能够同时对外提供一样的服务来处理大数据量。	无偏离
6	协同签名系统	1台	1、系统≥2U,配置≥1 个管理口，≥1 个 HA 口，≥4 个千兆电口，4 个 SFP 插槽,冗余电源,≥2 个扩展槽位,分量签名性能≥3500 次/秒；验签性能≥8000 次/秒；并发用户数≥3500；最	协同签名系统	1台	**满足** 1、系统=2U,配置 1 个管理口，1 个 HA 口，4 个千兆电口，4 个 SFP 插槽,冗余电源，2 个扩展槽位,分量签名性能 3500 次/秒；验签性能 8000 次/秒；并发用户数 3500；最大用	无偏离

			大用户数≥7000；			户数 7000；	
			2、服务端机架式硬件密码设备；客户端 SDK 或 APP 形态。			**满足** 2、服务端机架式硬件密码设备；客户端 SDK 或 APP 形态。	无偏离
			3、支持 SM2 公钥密码算法，支持 SM4 等对称密码算法，支持 SM3 摘要算法。			**满足** 3、支持 SM2 公钥密码算法，支持 SM4 等对称密码算法，支持 SM3 摘要算法。	无偏离
			4、支持密钥安全存储，除公钥外不允许密钥以明文形式输出，提供密钥生成、密钥存储、密钥备份、密钥恢复等密钥管理功能。			**满足** 4、支持密钥安全存储，除公钥外不允许密钥以明文形式输出，提供密钥生成、密钥存储、密钥备份、密钥恢复等密钥管理功能。	无偏离
			5、具备密钥自毁功能，当未经授权对设备进行开盖时，触发密钥自毁功能；也可通过外置物理装置销毁密钥。			**满足** 5、具备密钥自毁功能，当未经授权对设备进行开盖时，触发密钥自毁功能；也可通过外置物理装置销毁密钥。	无偏离
			6、管理员需使用证书登录管理界面，保证配置管理安全，具备终端设备访问控制功能，支持对移动端许可进行分配、注销、查询，通过白名单实现对应用服务器的访问授权认证。			**满足** 6、管理员需使用证书登录管理界面，保证配置管理安全，具备终端设备访问控制功能，支持对移动端许可进行分配、注销、查询，通过白名单实现对应用服务器的访问授权认证。	无偏离
			▲7、支持密码卡-实模式，开机启动系统镜像的完整性检验（在响应文件中提供【支持密码卡-实模式】功能截图证明材料复印件并加盖供应商公章）。			**满足** ▲7、支持密码卡-实模式，开机启动系统镜像的完整性检验（在响应文件中提供【支持密码卡-实模式】功能截图证明材料复印件并加盖公章）。	无偏离
			▲8、支持国密 SSH、国密 FTP（在响应文件中提供【支持国密 SSH、国密 FTP】功能截图证明材料复印件并加盖供应商公章）。			**满足** ▲8、支持国密 SSH、国密 FTP（在响应文件中提供【支持国密 SSH、国密 FTP】功能截图证明材料复印件并加盖公章）。	无偏离
			9、提供产生随机数功能，所有随机数采用国家密码管理局批准的硬件物理噪声源生			**满足** 9、提供产生随机数功能，所有随机数采用国家密码管理局批准的硬件物理噪声源生	无偏离

			成真随机数。			成真随机数。	
			10、提供对称密钥加解密功能。消息鉴别码产生和验证功能。提供非对称密钥数字签名产生和验证功能。提供非对称密钥加解密功能。提供协同密码运算服务。			**满足** 10、提供对称密钥加解密功能。消息鉴别码产生和验证功能。提供非对称密钥数字签名产生和验证功能。提供非对称密钥加解密功能。提供协同密码运算服务。	无偏离
			11、提供 C/C++接口和 Java 接口。支持 Linux、Windows 等系统。			**满足** 11、提供 C/C++接口和 Java 接口。支持 Linux、Windows 等系统。	无偏离
7	智能密码钥匙	10 个	1、支持国产化环境，包括国产操作系统（统信 UOS、麒麟系统等）和国产处理器（龙芯、飞腾、兆芯、鲲鹏、海光、麒麟等）；	智能密码钥匙	10 个	**满足** 1、支持国产化环境，包括国产操作系统（统信 UOS、麒麟系统等）和国产处理器（龙芯、飞腾、兆芯、鲲鹏、海光、麒麟等）；	无偏离
			2、硬件内置算法：SM1、SM2、SM3、SM4、RSA（1024/2048）、SHA-1、SHA-256、SHA-384、SHA-512、DES、3DES、AES 128/192/256；			**满足** 2、硬件内置算法：SM1、SM2、SM3、SM4、RSA（1024/2048）、SHA-1、SHA-256、SHA-384、SHA-512、DES、3DES、AES 128/192/256；	无偏离
			3、符合国家密码管理局提出的 GM/T 0027《智能密码钥匙技术规范》；			**满足** 3、符合国家密码管理局提出的 GM/T 0027《智能密码钥匙技术规范》；	无偏离
			4、兼容性：支持 X.509 v3 标准证书格式，支持多浏览器，支持多协议 HID、UMS、SCSI、CCID；			**满足** 4、兼容性：支持 X.509 v3 标准证书格式，支持多浏览器，支持多协议 HID、UMS、SCSI、CCID；	无偏离
			5、抗抵赖：使用内部私钥对数据进行签名操作，**满足**国家密码管理局和 PKI 规范要求，设备内的私钥无法被外部获取，确保签名数据无法被抵赖。			**满足** 5、抗抵赖：使用内部私钥对数据进行签名操作，满足国家密码管理局和 PKI 规范要求，设备内的私钥无法被外部获取，确保签名数据无法被抵赖。	无偏离
			6、数据存储年限：至少 10 年；			**满足** 6、数据存储年限： 10 年；	无偏离
			7、擦写次数：室温下 Flash 擦写次数量			满足 7、擦写次数：室温下 Flash 擦写次数量	无偏离

			最少为 10 万次；			为 10 万次；	
			8、工作电压：5V±5%；			**满足** 8、工作电压：5V±5%；	无偏离
			9、工作电流：≤30mA。			**满足** 9、工作电流：≤30mA。	无偏离
8	国密数字证书	120 点	采用国家认可的第三方 CA 机构证书，提供国密证书签发和管理服务，应用于个人用户标识真实身份。每张数字证书 3 年有效期，证书有效期起始时间从验收通过日起计算。	国密数字证书	120 点	**满足** 采用国家认可的第三方 CA 机构证书，提供国密证书签发和管理服务，应用于个人用户标识真实身份。每张数字证书 3 年有效期，证书有效期起始时间从验收通过日起计算。	无偏离
9	二级等保测评	1 项	▲1、总的要求：	二级等保测评	1 项	**满足** ▲1、总的要求：	无偏离
			依据《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）对工业领域网络安全信息公共服务平台开展网络安全等级保护测评工作，并出具网络安全等级保护测评报告。			**满足** 依据《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）对工业领域网络安全信息公共服务平台开展网络安全等级保护测评工作，并出具网络安全等级保护测评报告。	无偏离
			▲2、标准依据：			**满足** ▲2、标准依据：	无偏离
			《计算机信息系统安全保护等级划分准则》（GB 17859-1999）			**满足** 《计算机信息系统安全保护等级划分准则》（GB 17859-1999）	无偏离
			《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）			**满足**《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）	无偏离
			《信息安全技术 网络安全等级保护测评要求》（GB/T 28448-2019）			**满足**《信息安全技术 网络安全等级保护测评要求》（GB/T 28448-2019）	无偏离
			《信息安全技术 网络安全等级保护测评过程指南》（GB/T 28449-2018）			**满足**《信息安全技术 网络安全等级保护测评过程指南》（GB/T 28449-2018）	无偏离
			《信息安全技术 网络安全等级保护安全设计技术要求》（GB/T 25070-2019）			**满足**《信息安全技术 网络安全等级保护安全设计技术要求》（GB/T 25070-2019）	无偏离

			《信息安全技术 网络安全等级保护测试评估技术指南》（GB/T 36627-2018）			**满足**《信息安全技术 网络安全等级保护测试评估技术指南》（GB/T 36627-2018）	无偏离
			▲3、测评内容：			**满足** ▲3、测评内容：	无偏离
			（1）安全通用要求：			**满足** （1）安全通用要求：	无偏离
			安全通用要求测评内容应包括安全技术和安全管理两大类，其中技术类应包括对安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心五个方面的测评，安全管理类测评应包括对安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理五个方面的测评。			**满足** 安全通用要求测评内容应包括安全技术和安全管理两大类，其中技术类应包括对安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心五个方面的测评，安全管理类测评应包括对安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理五个方面的测评。	无偏离
			（2）安全扩展要求：			**满足** （2）安全扩展要求：	无偏离
			根据现场情况，保护对象可能涉及的安全扩展要求包括：移动互联，包括对安全物理环境、安全区域边界、安全计算环境、安全建设管理、安全运维管理等的测评。			**满足** 根据现场情况，保护对象可能涉及的安全扩展要求包括：移动互联，包括对安全物理环境、安全区域边界、安全计算环境、安全建设管理、安全运维管理等的测评。	无偏离
			4、测评方法：			**满足** 4、测评方法：	无偏离
			在测评实施过程中，应采用访谈、检查和测试、渗透测试等测评方法进行，并与国家相关规范及标准的要求相符。			**满足** 在测评实施过程中，应采用访谈、检查和测试、渗透测试等测评方法进行，并与国家相关规范及标准的要求相符。	无偏离
			▲5、服务成果：			**满足** ▲5、服务成果：	无偏离
			测评完成后，出具符合《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）相关技术标准要求，国家网络安全等级保护管理部门规范要求且公安机关			**满足** 测评完成后，出具符合《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）相关技术标准要求，国家网络安全等级保护管理部门规范要求且公安机关认	无偏离

			认可的网络安全等级保护测评报告。在项目整体验收时提供报告原件核查。			可的网络安全等级保护测评报告。在项目整体验收时提供报告原件核查。	
			▲6、提供本项服务的测评机构具备公安部第三研究所颁发的《网络安全等级测评与检测评估机构服务认证证书》。			**满足** ▲6、提供本项服务的测评机构具备公安部第三研究所颁发的《网络安全等级测评与检测评估机构服务认证证书》。	无偏离
10	软件测试	1项	1、测试计划：定义测试的目标、范围、方法、资源需求、时间表和风险。	软件测试	1项	**满足** 1、测试计划：定义测试的目标、范围、方法、资源需求、时间表和风险。	无偏离
			2、需求分析：确保测试团队理解软件的需求，并基于这些需求制定测试计划。			**满足** 2、需求分析：确保测试团队理解软件的需求，并基于这些需求制定测试计划。	无偏离
			3、测试设计：设计测试用例和测试场景，以覆盖所有的软件功能和用户故事。			**满足** 3、测试设计：设计测试用例和测试场景，以覆盖所有的软件功能和用户故事。	无偏离
			4、测试用例开发：编写详细的测试用例，包括输入数据、预期结果和测试步骤。			**满足** 4、测试用例开发：编写详细的测试用例，包括输入数据、预期结果和测试步骤。	无偏离
			5、测试环境搭建：准备所需的硬件、软件、网络和其他资源，以模拟真实的运行环境。			**满足** 5、测试环境搭建：准备所需的硬件、软件、网络和其他资源，以模拟真实的运行环境。	无偏离
			6、单元测试：针对软件的最小可测试部分（通常是单个函数或模块）进行测试。			**满足** 6、单元测试：针对软件的最小可测试部分（通常是单个函数或模块）进行测试。	无偏离
			7、集成测试：测试多个软件模块或组件如何协同工作。			**满足** 7、集成测试：测试多个软件模块或组件如何协同工作。	无偏离
			8、系统测试：测试完整的、集成的软件系统，以确保它满足所有需求。			**满足** 8、系统测试：测试完整的、集成的软件系统，以确保它满足所有需求。	无偏离
			9、验收测试：通常由客户或最终用户执行，以确认软件是否满足他们的业务需求。			**满足** 9、验收测试：通常由客户或最终用户执行，以确认软件是否满足他们的业务需求。	无偏离
			10、性能测试：评估软件在不同负载下			**满足** 10、性能测试：评估软件在不同负载下	无偏离

			的性能，包括响应时间、吞吐量和资源使用情况。			的性能，包括响应时间、吞吐量和资源使用情况。	
			11、安全测试：确保软件能够抵御外部威胁和攻击。			**满足** 11、安全测试：确保软件能够抵御外部威胁和攻击。	无偏离
			12、可用性测试：评估软件的用户界面和用户体验。			**满足** 12、可用性测试：评估软件的用户界面和用户体验。	无偏离
			13、兼容性测试：确保软件能够在不同的硬件、软件、浏览器和操作系统上运行。			**满足** 13、兼容性测试：确保软件能够在不同的硬件、软件、浏览器和操作系统上运行。	无偏离
			14、回归测试：在软件变更后重新执行测试，以确保新代码没有引入新的错误。			**满足** 14、回归测试：在软件变更后重新执行测试，以确保新代码没有引入新的错误。	无偏离
			15、自动化测试：使用自动化工具来执行测试用例，提高测试效率和覆盖率。			**满足** 15、自动化测试：使用自动化工具来执行测试用例，提高测试效率和覆盖率。	无偏离
			16、测试报告：记录测试活动的结果，包括发现的缺陷、测试覆盖率和测试结论。			**满足** 16、测试报告：记录测试活动的结果，包括发现的缺陷、测试覆盖率和测试结论。	无偏离
11	代码审计	1项	检查源代码中的安全缺陷，检查程序源代码是否存在安全隐患，或者有编码不规范的地方，通过自动化工具或者人工审查的方式，对程序源代码逐条进行检查和分析，发现这些源代码缺陷引发的安全漏洞，并提供代码修订措施和建议，提供《系统代码审计报告》，报告的内容包含但不限于：项目概述、标准依据、项目范围、概要信息；源代码信息，威胁等级、代码分类，以及代码缺陷的详细信息，修复建议等信息。	代码审计	1项	**满足** 检查源代码中的安全缺陷，检查程序源代码是否存在安全隐患，或者有编码不规范的地方，通过自动化工具或者人工审查的方式，对程序源代码逐条进行检查和分析，发现这些源代码缺陷引发的安全漏洞，并提供代码修订措施和建议，提供《系统代码审计报告》，报告的内容包含但不限于：项目概述、标准依据、项目范围、概要信息；源代码信息，威胁等级、代码分类，以及代码缺陷的详细信息，修复建议等信息。	无偏离
12	二级密评测	1项	（一）总体要求	二级密评测	1项	**满足** （一）总体要求	无偏离

	评		依据《中华人民共和国密码法》《信息安全技术 信息系统密码应用基本要求》（GB/T39786-2021）要求和系统自身的安全需求分析，对工业领域网络安全信息公共服务平台进行商用密码应用安全性评估，为重要网络和信息系统的密码安全提供科学评价，逐步规范网络运营者的密码使用和管理行为。	评		**满足** 依据《中华人民共和国密码法》《信息安全技术 信息系统密码应用基本要求》（GB/T39786-2021）要求和系统自身的安全需求分析，对工业领域网络安全信息公共服务平台进行商用密码应用安全性评估，为重要网络和信息系统的密码安全提供科学评价，逐步规范网络运营者的密码使用和管理行为。	无偏离
			（二）技术标准			**满足** （二）技术标准	无偏离
			《信息安全技术 信息系统密码应用基本要求》（GB/T39786-2021）			**满足** 《信息安全技术 信息系统密码应用基本要求》（GB/T39786-2021）	无偏离
			《信息系统密码应用测评要求（试行）》			**满足** 《信息系统密码应用测评要求（试行）》	无偏离
			《商用密码应用安全性评估测评过程指南（试行）》			**满足** 《商用密码应用安全性评估测评过程指南（试行）》	无偏离
			《商用密码应用安全性评估测评作业指导书（试行）》			**满足** 《商用密码应用安全性评估测评作业指导书（试行）》	无偏离
			（三）服务内容			**满足** （三）服务内容	无偏离
			1、商用密码应用方案评估			**满足** 1、商用密码应用方案评估	无偏离
			依据中国密码学会密评联委会发布的《商用密码应用安全性评估报告模板》（2023版）对工业领域网络安全信息公共服务平台商用密码应用方案开展评估工作，并出具《密码应用方案评估报告》。方案评估要点：			**满足** 依据中国密码学会密评联委会发布的《商用密码应用安全性评估报告模板》（2023版）对工业领域网络安全信息公共服务平台商用密码应用方案开展评估工作，并出具《密码应用方案评估报告》。方案评估要点：	无偏离
			（1）文档结构是否完整			**满足** （1）文档结构是否完整	无偏离
			（2）系统基本情况是否梳理充分			**满足** （2）系统基本情况是否梳理充分	无偏离

			（3）密码应用需求是否清晰明确			**满足** （3）密码应用需求是否清晰明确	无偏离
			（4）密码应用技术框架中密码协议、防护机制、密钥管理、密码应用子系统设计是否合理，能否**满足**安全需求和保障要求			**满足** （4）密码应用技术框架中密码协议、防护机制、密钥管理、密码应用子系统设计是否合理，能否满足安全需求和保障要求	无偏离
			（5）密码产品应用和部署设计是否合理、正确			**满足** （5）密码产品应用和部署设计是否合理、正确	无偏离
			（6）安全管理方案是否覆盖密码安全相关人员、制度、实施、应急等内容			**满足** （6）安全管理方案是否覆盖密码安全相关人员、制度、实施、应急等内容	无偏离
			（7）实施保障方案中实施计划是否科学、合理，组织管理方法和保障是否合理有效			**满足** （7）实施保障方案中实施计划是否科学、合理，组织管理方法和保障是否合理有效	无偏离
			2、商用密码应用安全性评估			**满足** 2、商用密码应用安全性评估	无偏离
			依据《信息安全技术 信息系统密码应用基本要求》（GB/T39786-2021）等技术标准对工业领域网络安全信息公共服务平台进行商用密码应用安全性评估工作，并出具符合要求的《商用密码应用安全性评估报告》。			**满足** 依据《信息安全技术 信息系统密码应用基本要求》（GB/T39786-2021）等技术标准对工业领域网络安全信息公共服务平台进行商用密码应用安全性评估工作，并出具符合要求的《商用密码应用安全性评估报告》。	无偏离
			（1）实施方式			**满足** （1）实施方式	无偏离
			1）系统测评：及时发现系统脆弱性，识别变化的风险，了解系统安全状况，对照密码应用方案对系统开展测评。根据被测评对象的实际情况，所属行业及系统使用的密码产品情况，选择并确定测评依据。在系统真实环境下进行测评，以测评密码保障是否安全有效，密码使用是否合规、正确、有效。			**满足** 1）系统测评：及时发现系统脆弱性，识别变化的风险，了解系统安全状况，对照密码应用方案对系统开展测评。根据被测评对象的实际情况，所属行业及系统使用的密码产品情况，选择并确定测评依据。在系统真实环境下进行测评，以测评密码保障是否安全有效，密码使用是否合规、正确、有效。并通过测评发	无偏离

			并通过测评发现系统存在的安全隐患和风险，提出可行性完善建议。			现系统存在的安全隐患和风险，提出可行性完善建议。	
			2）密码技术应用测评：物理安全密码测评、网络安全密码测评、主机安全密码测评、应用安全密码测评、数据安全及备份恢复密码测评。测评验证不同安全等级信息系统的商用密码应用是否达到具有相应安全等级的安全保护能力，是否**满足**相应安全等级的保护要求。			**满足** 2）密码技术应用测评：物理安全密码测评、网络安全密码测评、主机安全密码测评、应用安全密码测评、数据安全及备份恢复密码测评。测评验证不同安全等级信息系统的商用密码应用是否达到具有相应安全等级的安全保护能力，是否满足相应安全等级的保护要求。	无偏离
			3）密钥管理测评：检测信息系统密钥管理各环节，包括对密钥的生成、存储、分发、导入、导出、使用、备份、恢复、归档与销毁等环节进行管理和策略制定的全过程是否符合要求。			**满足** 3）密钥管理测评：检测信息系统密钥管理各环节，包括对密钥的生成、存储、分发、导入、导出、使用、备份、恢复、归档与销毁等环节进行管理和策略制定的全过程是否符合要求。	无偏离
			4）安全管理测评：对制度、人员、实施和应急等四个方面安全管理的测评，并协助完善商用密码应用安全性管理制度，协助完善密码相关系统运维管理制度。			**满足** 4）安全管理测评：对制度、人员、实施和应急等四个方面安全管理的测评，并协助完善商用密码应用安全性管理制度，协助完善密码相关系统运维管理制度。	无偏离
			（2）评估成果			**满足** （2）评估成果	无偏离
			出具针对被评估系统编制密码应用安全性评估报告，报告按照国家密码管理局要求包含的内容编制或参考模板编制。报告中应协助被评估单位认清风险，查找漏洞，找出差距，提出有针对性的加强完善密码安全管理和防护建议，并出具商用密码应用安全性			**满足** 出具针对被评估系统编制密码应用安全性评估报告，报告按照国家密码管理局要求包含的内容编制或参考模板编制。报告中应协助被评估单位认清风险，查找漏洞，找出差距，提出有针对性的加强完善密码安全管理和防护建议，并出具商用密码应用安全性评估报	无偏离

			评估报告。在项目整体验收时提供报告原件核查。			告。在项目整体验收时提供报告原件核查。	
			▲（四）提供本项服务的测评机构须为国家密码管理局公告（第49号）“商用密码检测机构(商用密码应用安全性评估业务)目录”内的机构。			**满足** ▲（四）提供本项服务的测评机构须为国家密码管理局公告（第49号）“商用密码检测机构(商用密码应用安全性评估业务)目录”内的机构。	无偏离
13	渗透测试	1项	针对工业领域网络安全信息公共服务平台进行渗透测试，模拟黑客攻击的方式，对目标系统的安全性进行全面、深入的评估。通过人工结合工具测试发现更多WEB层面上扫描器无法发现的漏洞（如：逻辑漏洞），帮助客户在遭到恶意攻击前将风险降到最低。并根据渗透测试结果出具渗透测试报告。输出《渗透测试报告》，报告的内容包含但不限于：测试目的、范围、依据、工具、主要漏洞信息、具体的操作步骤描述、安全修复建议等。	渗透测试	1项	**满足** 针对工业领域网络安全信息公共服务平台进行渗透测试，模拟黑客攻击的方式，对目标系统的安全性进行全面、深入的评估。通过人工结合工具测试发现更多WEB层面上扫描器无法发现的漏洞（如：逻辑漏洞），帮助客户在遭到恶意攻击前将风险降到最低。并根据渗透测试结果出具渗透测试报告。输出《渗透测试报告》，报告的内容包含但不限于：测试目的、范围、依据、工具、主要漏洞信息、具体的操作步骤描述、安全修复建议等。	无偏离
14	系统集成服务	1项	▲1、工作内容：完成工业领域网络安全信息公共服务平台的等保备案定级系统的整改实施服务（信息安全等级保护：二级2.0标准）。	系统集成服务	1项	**满足** ▲1、工作内容：完成工业领域网络安全信息公共服务平台的等保备案定级系统的整改实施服务（信息安全等级保护：二级2.0标准）。	无偏离
			2、等级保护网络调试服务：基于单位网络设备（交换机、路由器等）现状，对标信息安全等级保护2.0二级标准以及风险评估报告或测评报告进行整改，提交对应整改技			**满足** 2、等级保护网络调试服务：基于单位网络设备（交换机、路由器等）现状，对标信息安全等级保护2.0二级标准以及风险评估报告或测评报告进行整改，提交对应整改技术服务	无偏离

			术服务方案，整改范围包括但不限于拓扑结构的整改、设备物理位置的整改、设备配置数据的整改、设备版本的整改等。整改完成后实现所有网络设备均无高危漏洞，并达到通过此次信息安全等级保护 2.0 二级测评的要求。			方案，整改范围包括但不限于拓扑结构的整改、设备物理位置的整改、设备配置数据的整改、设备版本的整改等。整改完成后实现所有网络设备均无高危漏洞，并达到通过此次信息安全等级保护 2.0 二级测评的要求。	
			3、等级保护安全调试服务：基于本单位安全设备（防火墙、入侵防御、上网行为管理、杀毒软件、堡垒机、日志审计、数据库审计等设备）现状，对标信息安全等级保护 2.0 二级标准以及风险评估报告或测评报告进行整改，整改范围包括但不限于拓扑结构的整改、设备物理位置的整改、设备配置数据的整改、设备版本的整改等。整改完成后实现所有安全设备均无高危漏洞，并达到通过此次信息安全等级保护 2.0 二级测评的身份鉴别、访问控制、入侵防御、恶意代码防御、日志审计、资源管理、保密性管理等要求。			**满足** 3、等级保护安全调试服务：基于本单位安全设备（防火墙、入侵防御、上网行为管理、杀毒软件、堡垒机、日志审计、数据库审计等设备）现状，对标信息安全等级保护 2.0 二级标准以及风险评估报告或测评报告进行整改，整改范围包括但不限于拓扑结构的整改、设备物理位置的整改、设备配置数据的整改、设备版本的整改等。整改完成后实现所有安全设备均无高危漏洞，并达到通过此次信息安全等级保护 2.0 二级测评的身份鉴别、访问控制、入侵防御、恶意代码防御、日志审计、资源管理、保密性管理等要求。	无偏离
			4、等级保护业务系统调试服务：基于本单位业务系统现状，对标信息安全等级保护 2.0 二级标准以及漏洞扫描报告进行整改，提交对应整改技术服务方案，整改范围包括但不限于操作系统配置优化、操作系统安全补丁安装、操作系统权限优化等。整改完成后			**满足** 4、等级保护业务系统调试服务：基于本单位业务系统现状，对标信息安全等级保护 2.0 二级标准以及漏洞扫描报告进行整改，提交对应整改技术服务方案，整改范围包括但不限于操作系统配置优化、操作系统安全补丁安装、操作系统权限优化等。整改完成后实现本	无偏离

			实现本单位此次等级保护测评的目标系统均无高危漏洞，并达到通过此次信息安全等级保护 2.0 二级测评的身份鉴别、访问控制、入侵防御、恶意代码防御、日志审计、资源管理、保密性管理等要求。			单位此次等级保护测评的目标系统均无高危漏洞，并达到通过此次信息安全等级保护 2.0 二级测评的身份鉴别、访问控制、入侵防御、恶意代码防御、日志审计、资源管理、保密性管理等要求。	
			▲5、等级保护管理体系整改：对标信息安全等级保护 2.0 二级标准建立网络安全等级保护管理体系，在信息安全管理制度、安全管理机构、人员安全管理、系统建设管理、系统管理等方面指导并协助单位建立健全符合相应等级要求的安全管理制度。提交《信息安全等级保护管理制度包》，以达到通过此次信息安全等级保护 2.0 二级测评的要求。			**满足** ▲5、等级保护管理体系整改：对标信息安全等级保护 2.0 二级标准建立网络安全等级保护管理体系，在信息安全管理制度、安全管理机构、人员安全管理、系统建设管理、系统管理等方面指导并协助单位建立健全符合相应等级要求的安全管理制度。提交《信息安全等级保护管理制度包》，以达到通过此次信息安全等级保护 2.0 二级测评的要求。	无偏离
			▲6、协助测评服务：等保测评期间协助开展等保测评工作，协助完成工业领域网络安全信息公共服务平台的等保备案及等级认定工作。			**满足** ▲6、协助测评服务：等保测评期间协助开展等保测评工作，协助完成工业领域网络安全信息公共服务平台的等保备案及等级认定工作。	无偏离
			7、应急支撑：在提供等级保护整改服务期间，提供整改相关工作引起的业务异常并需要协助排查故障时 30 分钟内做出响应，2 小时内到达现场协助处理。			**满足** 7、应急支撑：在提供等级保护整改服务期间，提供整改相关工作引起的业务异常并需要协助排查故障时 30 分钟内做出响应，2 小时内到达现场协助处理。	无偏离
15	平台运营服务	1 项	1、含三年广西工业互联网安全信息公共服务平台运营服务。	平台运营服务	1 项	**满足** 1、含三年广西工业互联网安全信息公共服务平台运营服务。	无偏离
			2、包含三年国家工业信息安全漏洞库（漏洞名称、所属类型、CVE 编号、危害等			**满足** 2、包含三年国家工业信息安全漏洞库（漏洞名称、所属类型、CVE 编号、危害等	无偏离

			级、影响行业、漏洞描述、影响产品，面向工业控制器、数控机床、工业机器人等不少于10种工控设备收录漏洞不少于5000条）的升级授权。			级、影响行业、漏洞描述、影响产品，面向工业控制器、数控机床、工业机器人等10种工控设备收录漏洞5000条）的升级授权。	
			3、提供三年的平台运维升级服务，为平台提供全面的技术支持和持续的系统优化，以确保平台始终保持平稳运行，充分发挥其功能。服务方式为远程技术支持与现场派驻相结合，成交供应商应拟派具备与运营服务工作相匹配的专业技术人员进行驻场服务；同时能配备有经验丰富且专业的专家团队进行远程技术支持，专家团队必要时能及时到达现场处理问题。运营服务包含平台运营所需的人力成本，提供至少2人现场驻场运维服务，工作时间以采购人工作时间为准，驻场人员主要负责信息管理和平台运营日常工作，包括日常信息系统维护管理、漏洞验证、完成发布通报、统计和分类、对服务商发布的企业信息统一审核发布和定期更新、收集资源池服务商企业联系方式、收集提供一些应急演练的方案模版、案例呈现和服务商资源池对接等，具体工作内容如下：			**满足** 3、提供三年的平台运维升级服务，为平台提供全面的技术支持和持续的系统优化，以确保平台始终保持平稳运行，充分发挥其功能。服务方式为远程技术支持与现场派驻相结合，我司派具备与运营服务工作相匹配的专业技术人员进行驻场服务；同时能配备有经验丰富且专业的专家团队进行远程技术支持，专家团队必要时能及时到达现场处理问题。运营服务包含平台运营所需的人力成本，提供2人现场驻场运维服务，工作时间以采购人工作时间为准，驻场人员主要负责信息管理和平台运营日常工作，包括日常信息系统维护管理、漏洞验证、完成发布通报、统计和分类、对服务商发布的企业信息统一审核发布和定期更新、收集资源池服务商企业联系方式、收集提供一些应急演练的方案模版、案例呈现和服务商资源池对接等，具体工作内容如下：	无偏离
			（1）信息管理：含日常信息系统的维护管理，负责平台内容的发布，确保信息及时、准确。对平台数据进行统计和分析，对发布			**满足** （1）信息管理：含日常信息系统的维护管理，负责平台内容的发布，确保信息及时、准确。对平台数据进行统计和分析，对发布内	无偏离

			内容进行分类管理；			容进行分类管理；	
			（2）漏洞管理：漏洞的定期收集、管理、验证、更新、发布，通告，确保漏洞通告的及时性，验证漏洞的严重性和可利用性，根据漏洞验证结果，提出并实施安全加固措施；			**满足** （2）漏洞管理：漏洞的定期收集、管理、验证、更新、发布，通告，确保漏洞通告的及时性，验证漏洞的严重性和可利用性，根据漏洞验证结果，提出并实施安全加固措施；	无偏离
			（3）信息审核：审核服务商提交的企业信息，确保信息真实、合规，将审核通过的企业信息发布到平台，定期检查并更新企业信息，确保数据的时效性；			**满足** （3）信息审核：审核服务商提交的企业信息，确保信息真实、合规，将审核通过的企业信息发布到平台，定期检查并更新企业信息，确保数据的时效性；	无偏离
			（4）信息收集：通过多种渠道，定期收集服务商的企业联系方式，收集行业内的应急演练方案模板和案例，将收集到的方案模板进行标准化整理，形成可复用的模板库，提供对外展示；			**满足** （4）信息收集：通过多种渠道，定期收集服务商的企业联系方式，收集行业内的应急演练方案模板和案例，将收集到的方案模板进行标准化整理，形成可复用的模板库，提供对外展示；	无偏离
			（5）资源池维护：维护服务商资源池，确保资源池信息的完整性和准确性，确保资源池中的信息及时更新；			**满足** （5）资源池维护：维护服务商资源池，确保资源池信息的完整性和准确性。确保资源池中的信息及时更新；	无偏离
			（6）平台监控：对平台进行实时监控，对日常故障及时排查并解决，确保系统稳定运行；			**满足** （6）平台监控：对平台进行实时监控，对日常故障及时排查并解决，确保系统稳定运行；	无偏离
			（7）平台评估：定期对系统性能，资源使用进行评估，优化并提升响应速度，保障平台持续可用；			**满足** （7）平台评估：定期对系统性能，资源使用进行评估，优化并提升响应速度，保障平台持续可用；	无偏离
			（8）数据管理：对平台的日志进行定期审查，数据定期备份与还原，确保数据的安			**满足** （8）数据管理：对平台的日志进行定期审查，数据定期备份与还原，确保数据的安全	无偏离

			全性；			性；	
			（9）更新升级：定期更新系统软件，修复漏洞；			**满足** （9）更新升级：定期更新系统软件，修复漏洞；	无偏离
			（10）应急响应：对运营中发生的安全事件的应急预案，确保安全事件的快速处理。			**满足** （10）应急响应：对运营中发生的安全事件的应急预案，确保安全事件的快速处理。	无偏离
16	人员培训服务	1 项	包含本项目相关人员不少于 5 人网络安全技术培训服务 1 次，培训时长不少于 2 课时。	人员培训服务	1 项	**满足** 包含本项目相关人员不少于 5 人网络安全技术培训服务 1 次，培训时长不少于 2 课时。	无偏离
17	防火墙	1 台	1、防火墙≥2U，≥1 个管理口、≥1 个 HA 口、≥4 个千兆电口、≥4 个千兆光口（满配千兆多模模块）和≥2 个万兆光口（满配万兆多模模块），冗余电源，≥1 个扩展槽位。网络层吞吐量（双向）：IPv4≥10000Mbps，IPv6≥10000Mbps 应用层吞吐量（单向）：IPv4≥8000Mbps，IPv6≥8000Mbps；TCP 新建连接速率：IPv4≥90 万/秒，IPv6≥90 万/秒 TCP 并发连接数：IPv4≥1800 万，IPv6≥1800 万；	防火墙	1 台	**满足** 1、防火墙=2U，1 个管理口，1 个 HA 口、4 个千兆电口、4 个千兆光口（满配千兆多模模块）和 2 个万兆光口（满配万兆多模模块），冗余电源 1 个扩展槽位。网络层吞吐量（双向）：IPv4 10000Mbps，IPv6 10000Mbps 应用层吞吐量（单向）：IPv4 8000Mbps，IPv6 8000Mbps；TCP 新建连接速率：IPv4 90 万/秒，IPv6 90 万/秒 TCP 并发连接数：IPv4 1800 万，IPv6 1800 万；	无偏离
			2、配置入侵防御特征库、应用识别库、WEB 过滤库、快速扫描查杀防病毒库≥3 年升级服务许可，≥3 年硬件维保；			**满足** 2、配置入侵防御特征库、应用识别库、WEB 过滤库、快速扫描查杀防病毒库 3 年升级服务许可，3 年硬件维保；	无偏离
			3、产品由专用的硬件平台、安全操作系统及功能软件构成。设备采用自主知识产权的专用安全操作系统，采用多核多平台并行处理机制；			**满足** 3、产品由专用的硬件平台、安全操作系统及功能软件构成。设备采用自主知识产权的专用安全操作系统，采用多核多平台并行处理机制；	无偏离

			4、支持 RIP、OSPF、BGP4、策略路由，支持根据入接口、源/目的 IP 地址、协议、用户、应用、选路算法、探测等多种条件设置策略路由；			**满足** 4、支持 RIP、OSPF、BGP4、策略路由，支持根据入接口、源/目的 IP 地址、协议、用户、应用、选路算法、探测等多种条件设置策略路由；	无偏离
			5、支持手动和 LACP 链路聚合，可根据源/目的 MAC、源/目的 IP、源/目的端口、五元组、端口轮询等条件提供不少于 8 种链路负载算法；			**满足** 5、支持手动和 LACP 链路聚合，可根据源/目的 MAC、源/目的 IP，源/目的端口，五元组、端口轮询等条件提供 8 种链路负载算法；	无偏离
			▲6、支持 DNS Doctoring 功能，能够将来自内部网络的域名解析请求定向到真实内网资源，提高访问效率，同时支持通过配置多条 DNS Doctoring，实现内网资源服务器的负载均衡（在响应文件中提供【支持 DNS Doctoring 功能】功能截图证明材料复印件并加盖供应商公章）；			**满足** ▲6、支持 DNS Doctoring 功能，能够将来自内部网络的域名解析请求定向到真实内网资源，提高访问效率，同时支持通过配置多条 DNS Doctoring，实现内网资源服务器的负载均衡（在响应文件中提供【支持 DNS Doctoring 功能】功能截图证明材料复印件并加盖公章）；	无偏离
			7、支持一体化安全策略配置，可以通过一条策略实现五元组、源 MAC、源地区、目的地区、域名、应用、服务、时间、长连接、并发会话、WEB 认证、IPS、AV、URL 过滤、WAF、邮件安全、数据过滤、文件过滤、审计等功能配置,简化用户管理；			**满足** 7、支持一体化安全策略配置，可以通过一条策略实现五元组、源 MAC、源地区、目的地区、域名、应用、服务、时间、长连接、并发会话、WEB 认证、IPS、AV、URL 过滤、WAF、邮件安全、数据过滤、文件过滤、审计等功能配置,简化用户管理；	无偏离
			8、支持 IPv4/IPv6 双栈工作模式，支持 RADVD、ND、RIPng、OSPFv3、BGP4+；支持 IPv6 安全控制策略设置，能针对 IPv6 的目的/源地址、目的/源服务端口、区域、服			**满足** 8、支持 IPv4/IPv6 双栈工作模式，支持 RADVD、ND、RIPng、OSPFv3、BGP4+；支持 IPv6 安全控制策略设置，能针对 IPv6 的目的/源地址、目的/源服务端口、区域、服务、	无偏离

			务、时间、扩展头属性等条件进行安全访问规则的设置；			时间、扩展头属性等条件进行安全访问规则的设置；	
			9、支持在一台物理设备上划分出不少于128个相互独立的虚拟系统，可根据连接配额及连接新建速率为每个虚拟系统分配资源，实配不少于24个虚拟防火墙授权；			**满足** 9、支持在一台物理设备上划分出128个相互独立的虚拟系统，可根据连接配额及连接新建速率为每个虚拟系统分配资源，实配24个虚拟防火墙授权；	无偏离
			▲10、支持针对IP、ICMP、TCP、UDP、DNS、HTTP、NTP等协议进行DDOS防护，支持NTP流量检测清洗，能对NTP QUERY FLOOD、NTP REPLY FLOOD等攻击进行检测并提供基于NTP请求限速、NTP响应限速、源认证、会话认证的防御策略；			**满足** ▲10、支持针对IP、ICMP、TCP、UDP、DNS、HTTP、NTP等协议进行DDOS防护，支持NTP流量检测清洗，能对NTP QUERY FLOOD、NTP REPLY FLOOD等攻击进行检测并提供基于NTP请求限速、NTP响应限速、源认证、会话认证的防御策略；	无偏离
			11、支持对达梦、人大金仓等数据库应用、P2P、移动应用、迅雷加密流量、向日葵/Teamview等远程控制软件、Modbus/IEC/OPC等工控物联网协议进行识别控制，支持自定义应用特征；			**满足** 11、支持对达梦、人大金仓等数据库应用、P2P、移动应用、迅雷加密流量、向日葵/Teamview等远程控制软件、Modbus/IEC/OPC等工控物联网协议进行识别控制，支持自定义应用特征；	无偏离
			▲12、支持独立的入侵防护规则特征库，特征总数在5000条或以上，能对常见漏洞进行安全防护，兼容国家信息安全漏洞库（在响应文件中提供【特征总数在5000条或以上】功能截图证明材料复印件并加盖供应商公章）；			**满足** ▲12、支持独立的入侵防护规则特征库，特征总数在5000条或以上，能对常见漏洞进行安全防护，兼容国家信息安全漏洞库（在响应文件中提供【特征总数在5000条或以上】功能截图证明材料复印件并加盖公章）；	无偏离
			13、支持配置文件本地备份和回滚，支持＞2个配置文件备份，支持对访问控制策			**满足** 13、支持配置文件本地备份和回滚，支持＞2个配置文件备份，支持对访问控制策	无偏离

			略、NAT 策略等关键配置进行单独及加密备份和恢复；支持对配置命令及配置文件的操作行为进行审计；			略、NAT 策略等关键配置进行单独及加密备份和恢复；支持对配置命令及配置文件的操作行为进行审计；	
			14、支持 CPU 利用率、内存利用率、磁盘利用率、会话数告警及 CPU 利用率、内存利用率、磁盘利用率等硬件资源实时利用率及其历史使用情况追踪；			**满足** 14、支持 CPU 利用率、内存利用率、磁盘利用率、会话数告警及 CPU 利用率、内存利用率、磁盘利用率等硬件资源实时利用率及其历史使用情况追踪；	无偏离
			15、支持对病毒防御、入侵防御、DDOS 攻击等按照威胁类型/攻击主机/受攻击主机三种维度结合威胁等级和时间周期进行统计、排名；			**满足** 15、支持对病毒防御、入侵防御、DDOS 攻击等按照威胁类型/攻击主机/受攻击主机三种维度结合威胁等级和时间周期进行统计、排名；	无偏离
			16、支持系统管理员本地认证、外部认证和证书认证，外部认证失败时可转本地认证。支持设置管理员首次登录是否强制修改密码，支持密码强度、有效期设置。			**满足** 16、支持系统管理员本地认证、外部认证和证书认证，外部认证失败时可转本地认证。支持设置管理员首次登录是否强制修改密码，支持密码强度、有效期设置。	无偏离

注：

1、应写明竞争性磋商响应文件对技术条款的响应和偏离情况；

2、应对照竞争性磋商文件第二章"服务需求一览表"中技术条款，逐条一一说明所提供货物和服务已对竞争性磋商文件的技术做出了实质性的响应，并申明技术条款的响应和偏离。特别对有具体技术参数要求的，磋商供应商必须提供对应的详细应答。如果仅注明"符合"、"满足"或简单复制竞争性磋商文件要求，将导致磋商被拒绝。

3、在"偏离说明"中注明"正偏离"、"负偏离"或者"无偏离"。既不属于"正偏离"也不属于"负偏离"即为"无偏离"。

供应商名称（电子签章）：广西[illegible]信息技术有限公司

日期：2023年08月08日

商务条款偏离表

四、商务条款偏离表

（必须提供，否则响应文件按无效响应处理）

商务条款偏离表

采购项目编号：GXZC2025-C3-000848-GXZL

采购项目名称：广西工业领域网络安全信息公共服务平台

分标号（此处有分标时填写具体分标号，无分标时填写"无"）：无

序号	竞争性磋商采购文件的商务条款	响应文件承诺的商务条款	偏离说明
1.▲报价要求	供应商须就本项目采购需求中的所有实施内容作完整报价，总报价包含但不限于培训、技术支持、售后服务费、测试、保险费和各项税金等完成本项目所产生的全部费用。	**我司**就本项目采购需求中的所有实施内容作完整报价，总报价包含但不限于培训、技术支持、售后服务费、测试、保险费和各项税金等完成本项目所产生的全部费用。	无偏离
	注：供应商在报价时应考虑各方面因素、各种风险和自己的承受能力，报价中应包含全部内容，成交后采购人不再另行支付额外费用。	注：**我司**在报价时考虑各方面因素、各种风险和自己的承受能力，报价中包含全部内容，成交后采购人不再另行支付额外费用。	无偏离
2.▲合同签订期	自成交通知书发出之日起25日内。	**我司同意**自成交通知书发出之日起25日内。	无偏离
3.▲交付时间及地点	1、交付时间：自合同签订之日起60个日历日内验收合格并交付使用。	**我司同意** 1、交付时间：自合同签订之日起60个日历日内验收合格并交付使用。	无偏离
	2、交付地点：广西南宁市采购人指定地点。	**我司同意** 2、交付地点：广西南宁市采购人指定地点。	无偏离
4.▲质保期限	按国家有关产品"三包"规定执行"三包"，自最终验收合格并交付使用之日起计算，产品质保期不少于3年（"技术条款"另有约定的，从其约定），若厂家质保期超过此年限的，合同履行过程中按厂家规定执行。	**我司同意** 按国家有关产品"三包"规定执行"三包"，自最终验收合格并交付使用之日起计算，产品质保期3年（"技术条款"另有约定的，从其约定），若厂家质保期超过此年限的，合同履行过程中按厂家规定执行。	无偏离
5.售后服务要求	除另行特别注明外，售后服务要求如下：	**我司同意** 除另行特别注明外，售后服务要求如下：	无偏离

	1、成交供应商按采购人指定的地点负责送货上门、安装，调试，负责培训使用人员和维护人员。	**我司同意** 1、按采购人指定的地点负责送货上门、安装，调试，负责培训使用人员和维护人员。	无偏离
	▲2、成交供应商必须提供安装，配线以及软硬件的测试和调整服务。开始安装时应让用户的硬软件和系统集成人员参与安装、检测和排除故障。成交供应商在施工、安装、调试等全过程中接受用户的监督。	**我司同意** ▲2、提供安装，配线以及软硬件的测试和调整服务。开始安装时应让用户的硬软件和系统集成人员参与安装、检测和排除故障。在施工、安装、调试等全过程中接受用户的监督。	无偏离
	3、在成交供应商承诺的保修期内，设备保修包换所需要的配件均是原厂原装，不得使用兼容货物。	**我司同意** 3、在承诺的保修期内，设备保修包换所需要的配件均是原厂原装，不得使用兼容货物。	无偏离
	4、售后服务按厂家承诺执行。超过厂家承诺标准的，按成交供应商提交的售后服务承诺书执行。定期回访以及对软件进行维护；质保期后需提供维修维护服务。	**我司同意** 4、售后服务按厂家承诺执行。超过厂家承诺标准的，按我司提交的售后服务承诺书执行。定期回访以及对软件进行维护；质保期后需提供维修维护服务。	无偏离
	5、成交供应商在质量保证期内应当为采购人提供以下技术支持和服务：	**我司同意** 5、在质量保证期内应当为采购人提供以下技术支持和服务：	无偏离
	5.1 电话咨询	5.1 电话咨询	无偏离
	成交供应商应当为采购人提供技术援助电话，解答采购人在使用中遇到的问题，及时为采购人提出解决问题的建议。	**我司**为采购人提供技术援助电话，解答采购人在使用中遇到的问题，及时为采购人提出解决问题的建议。	无偏离
	5.2 服务响应时间	5.2 服务响应时间	无偏离
	质保期内，用户遇到使用或技术问题，电话咨询不能解决的，成交供应商应在 48 小时内到达现场进行处理，到达现场后 24 小时内排除故障，恢复正常使用。未能修复的直接更换，保证采购人正常使用，产生的一切费用由成交供应商承担。	**我司同意** 质保期内，用户遇到使用或技术问题，电话咨询不能解决的，在 48 小时内到达现场进行处理，到达现场后 24 小时内排除故障，恢复正常使用。未能修复的直接更换，保证采购人正常使用，产生的一切费用由我司承担。	无偏离
	5.3 技术升级	5.3 技术升级	无偏离
	在质保期内，如果成交供应商的产品或服务升级，成交供应商应及时通知采购人，如采购人有相应要求，成交供应商应对采购人购买的产品或服务进行升级。	**我司同意** 在质保期内，如果**我司**的产品或服务升级，**我司**及时通知采购人，如采购人有相应要求，**我司同意**对采购人购买的产品或服务进行升级。	无偏离

	6、质保期外服务要求	6、质保期外服务要求	无偏离
	6.1 质量保证期过后，成交供应商应同样无偿提供电话咨询服务，并应承诺提供产品或服务上门维护。	**我司同意** 6.1 质量保证期过后，**我司**同样无偿提供电话咨询服务，并应承诺提供产品或服务上门维护。	无偏离
	6.2 质量保证期过后，采购人需要继续由原成交供应商提供售后服务的，成交供应商和制造商应以优惠价格提供售后服务。	**我司同意** 6.2 质量保证期过后，采购人需要继续由**我司**提供售后服务的，**我司同意**和制造商应以优惠价格提供售后服务。	无偏离
	7、培训要求：安装设备之前，成交供应商须对采购人提供现场培训服务，培训内容包括提供产品或服务的使用和操作；培训服务涉及的相关费用应计算在项目报价内，并使使用人员能独立、熟练操作软件。	**我司同意** 7、培训要求：安装设备之前，**我司**对采购人提供现场培训服务，培训内容包括提供产品或服务的使用和操作；培训服务涉及的相关费用应计算在项目报价内，并使使用人员能独立、熟练操作软件。	无偏离
	8、成交供应商应保证采购人在接受其提供的相关服务时免受第三方提出侵犯其知识产权的起诉，由此引起的知识产权纠纷由成交供应商负责。	**我司同意** 8、保证采购人在接受其提供的相关服务时免受第三方提出侵犯其知识产权的起诉，由此引起的知识产权纠纷由我司负责。	无偏离
	9、确保本项目所有内容不存在意识形态问题。	**我司同意** 9、确保本项目所有内容不存在意识形态问题。	无偏离
6.▲付款方式	1、项目合同、担保措施生效以及具备实施条件后 10 个工作日内，采购人通过银行转账的方式向成交供应商支付合同总金额的 30%预付款；成交供应商实施完成本项目，并通过采购人市核验收，在通过验收后的 10 个工作日内，支付合同总金额的 70%。	**我司同意** 1、项目合同、担保措施生效以及具备实施条件后 10 个工作日内，采购人通过银行转账的方式向**我司**支付合同总金额的 30%预付款；**我司**实施完成本项目，并通过采购人市核验收，在通过验收后的 10 个工作日内，支付合同总金额的 70%。	无偏离
	2、采购人付款前，成交供应商应向采购人开具等额有效的增值税发票，采购人未收到合格有效发票的，有权不予支付相应款项直至成交供应商提供合格发票，并不承担延迟付款责任。发票认证通过是付款的必要前提之一。	**我司同意** 2、采购人付款前，**我司**向采购人开具等额有效的增值税发票，采购人未收到合格有效发票的，有权不予支付相应款项直至**我司**提供合格发票，并不承担延迟付款责任。发票认证通过是付款的必要前提之一。	无偏离
	3、付款方式：银行转账。	3、付款方式：银行转账。	无偏离
7.▲履约保证金	1、履约保证金金额：成交金额的 5%。（若成交供应商被认定为中小企业的，履约保证金数额将按成交金额的 2%收取）	**我司同意** 1、履约保证金金额：成交金额的 5%。（若**我司**被认定为中小企业的，履约保证金数额将按成交金额的 2%收取）	无偏离

	2、履约保证金递交方式：银行转账、支票、汇票、本票或者金融、保险机构出具的保函等非现金形式。	**我司同意** 2、履约保证金递交方式：银行转账、支票、汇票、本票或者金融、保险机构出具的保函等非现金形式。	无偏离
	3、履约保证金递交时间：签订合同前5个工作日内由成交供应商转入采购人指定保证金账户。	**我司同意** 3、履约保证金递交时间：签订合同前5个工作日内由我司转入采购人指定保证金账户。	无偏离
	4、履约保证金退还：履约完成并验收合格后无质量问题，成交供应商提供《政府采购项目履约保证金退付意见书》及《政府采购项目合同验收报告》，向采购人提出书面申请退还，采购人在收到申请后5个工作日内办理履约保证金退还手续（无息退还）。	**我司同意** 4、履约保证金退还：履约完成并验收合格后无质量问题，**我司**提供《政府采购项目履约保证金退付意见书》及《政府采购项目合同验收报告》，向采购人提出书面申请退还，采购人在收到申请后5个工作日内办理履约保证金退还手续（无息退还）。	无偏离
	保证金指定账户： 开户名：广西工业职业技术学院 开户行：广西北部湾银行南宁市衡阳路支行 账　号：1702012200017200	保证金指定账户： 开户名：广西工业职业技术学院 开户行：广西北部湾银行南宁市衡阳路支行 账　号：1702012200017200	无偏离
8.验收标准及要求	1、验收过程中所产生的一切费用均由成交供应商承担。报价时应考虑相关费用。	**我司同意** 1、验收过程中所产生的一切费用均由**我司**承担。报价时应考虑相关费用。	无偏离
	2、成交供应商在验收时由采购人对照磋商文件及响应文件承诺的功能目标及技术指标全面核对检验，对所有要求出具的证明文件的原件进行核查，如不符合磋商文件的技术需求及要求以及提供虚假承诺的，按相关规定做退货处理及违约处理，成交供应商承担所有责任和费用，采购人保留进一步追究责任的权利。	**我司同意** 2、在验收时由采购人对照磋商文件及响应文件承诺的功能目标及技术指标全面核对检验，对所有要求出具的证明文件的原件进行核查，如不符合磋商文件的技术需求及要求以及提供虚假承诺的，按相关规定做退货处理及违约处理，**我司**承担所有责任和费用，采购人保留进一步追究责任的权利。	无偏离
9.规范标准	采购标的需执行的国家标准、行业标准、地方标准或者其他标准、规范，多项标准的，按最新标准或较高标准执行。	**我司同意** 采购标的需执行的国家标准、行业标准、地方标准或者其他标准、规范。多项标准的，按最新标准或较高标准执行。	无偏离

10.▲进口产品说明	□本表的第项货物所涉及的货物已按规定办妥进口产品采购审核手续，竞标产品可选用进口产品；但如选用进口产品时必须为全套原装进口产品（即通过中国海关报关验放进入中国境内且产自关境外的产品），同时投标人必须负责办理进口产品所有相关手续并承担所有费用，其他货物不接受进口产品参与竞标，否则作无效标处理。	**我司承诺** □本表的第项货物所涉及的货物已按规定办妥进口产品采购审核手续，竞标产品可选用进口产品；但如选用进口产品时为全套原装进口产品（即通过中国海关报关验放进入中国境内且产自关境外的产品），同时投标人负责办理进口产品所有相关手续并承担所有费用。其他货物不接受进口产品参与竞标，否则作无效标处理。	无偏离
	☑本服务所涉及的货物不接受进口产品（即通过中国海关报关验放进入中国境内且产自关境外的产品）参与竞标，如有进口产品参与竞标的作无效标处理。	**我司承诺** ☑本服务所涉及的货物不接受进口产品（即通过中国海关报关验放进入中国境内且产自关境外的产品）参与竞标，如有进口产品参与竞标的作无效标处理。	无偏离

注：

1、应写明竞争性磋商响应文件对商务条款的响应和偏离情况；

2、应对照竞争性磋商文件第二章"服务需求一览表"中的商务条款，逐条一一说明所提供货物和服务已对竞争性磋商文件的商务做出了实质性的响应，并申明商务条款的响应和偏离情况。特别对有具体商务要求的，磋商供应商必须提供对应的详细应答。如果仅注明"符合"、"满足"或简单复制竞争性磋商文件要求，将导致磋商被拒绝。

3、在"偏离说明"中注明"正偏离"、"负偏离"或者"无偏离"。既不属于"正偏离"也不属于"负偏离"即为"无偏离"。

供应商名称（电子签章）：广西络易信息技术有限公司

日期：2025 年 08 月 08 日

售后服务承诺书

我公司针对售后团队技能与技术的提升建立了培训体系，藉此确保售后团队的技能与技术不断提升，藉此更专业、高效地解决客户的问题，为客户提供更优质的服务。如：

- 每月远程组织职业素养与专业技能培训，提升售后团队技能水平。
- 每月现场开展厂商产品、解决方案培训，加强售后团队对厂商的产品及解决方案的了解程度。
- 每季度现场培训职业素养，提升售后团队专业性与职业素质。

■ **绩效考核**

为激励售后团队更高效地开展工作，我公司制定了一套完善的考核机制来确保售后人员服务的规范性与职业性。

我公司将根据售后团队的绩效考核结果给予相应的奖励与惩罚。

■ **知识库**

一本通

我公司致力于提升售后服务人员的能力，借此整合各产品线信息，包括产品性能、参数详情、安装指南、配置步骤及常见问题解决方案，汇编成《知识一本通》，售后团队可凭借《知识一本通》，迅速掌握各厂商产品的相关知识。

文档管理系统

我公司构建了全面的文档管理系统，助力售后团队在学习《一本通》之余，深入了解公司的规章制度、企业文化及核心价值观。

7、售后服务承诺书

提高产品质量和加强全方位的服务，是我公司一贯的宗旨，在售后服务上特别注重服务质量和维修的技术力量[illegible]，为此公司配备了专业维修技术人员，由公司统一为用户[illegible]等各种售后服务。

公司内设有专门的售后服务[illegible]，服务态度好，从而能够满足我们对客户的产品[illegible]，实现我们对客户的承诺。我公司为本项目顺利实施做出如下承诺。

1、合同签订期：自成交通知书发出之日起 25 日内。

2、交付时间：自合同签订之日起 90 个日历日内[illegible]验收合格并交付使用。

3、交付地点：广西南宁市采购人指定地点。

4、质保期限：按国家有关产品"三包"规定执行"三包"，自最终验收合格并交付使用之日起计算，产品质保期 3 年（"技术条款"另有约定的，从其约定）。若厂家质保期超过此年限的，合同履行过程中按厂家规定执行。

5、按采购人指定的地点免费送货上门、安装、调试，培训使用人员和维护人员。

6、提供安装、配线以及软硬件的测试和调整服务，并确保安装时应让用户的

硬软件和系统集成人员参与安装、检测和排除故障。在施工、安装、调试等全过程中接受用户的监督。

7、在承诺的保修期内，设备保修拉换所需要的配件均是原厂配装，不得使用兼容货物。

8、售后服务按厂家承诺执行，超过厂家承诺标准的，按提交的售后服务承诺书执行。定期回访以及对软件进行维护，质保期后需提供维修维护服务。

9、在质量保证期内为采购人提供以下技术支持和服务：

9.1 电话咨询

为采购人提供技术援助电话，解答采购人在使用中遇到的问题，及时为采购人提出解决问题的建议。

9.2 服务响应时间

质保期内，用户遇到使用或技术问题，电话咨询不能解决的，**在48小时内到达现场进行处理，到达现场后24小时内排除故障**，恢复正常使用。未能修复的应接更换，保证采购人正常使用，产生的一切费用由公司承担。

9.3 技术升级

在质保期内，如果产品或服务升级，应及时通知采购人，如采购人有相应要求，公司对采购人购买的产品或服务进行升级。

10、质保期外服务要求

10.1 质量保证期过后，同样无偿提供电话咨询服务，并承诺提供产品或服务上门维护。

10.2 质量保证期过后，采购人需要继续由成交公司提供售后服务的，成交供应商和制造商以优惠价格提供售后服务。

11、培训要求：安装设备之后，[illegible]提供现场培训服务，培训内容包括提供产品或服务的使用和操作，培训服务产生的相关费用应计算在项目报价内，并使使用人员能够[illegible]。

12、成交供应商保证采购人在使用该货物或其任何一部分时不受第三方提出侵犯其知识产权的起诉，由此引起的知识产权纠纷由成交供应商负责。

13、确保本项目所有内容不存在意识形态问题。

8. 服务响应与故障处理管理流程

8.1. 故障管理流程概述

事件管理通过服务台（7*24小时）邮件和电话以及二线、三线技术支持，迅速排除采购方故障，高效响应用户需求，助力用户快速恢复工作，最大程度降低影响。

规范的事件管理流程可使IT运行维护服务统一进行管理，并确保能够及时响应用户的需求，在服务台与用户之间有唯一而且通畅的服务渠道，服务支持信

中小企业声明函

三、中小企业声明函

中小企业声明函（工程、服务）

本公司（联合体）郑重声明，根据《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）的规定，本公司（联合体）参加 广西工业职业技术学院 的 广西工业领域网络安全信息公共服务平台 采购活动，工程的施工单位全部为符合政策要求的中小企业（或者：服务全部由符合政策要求的中小企业承接）。相关企业（含联合体中的中小企业、签订分包意向协议的中小企业）的具体情况如下：

1. 工业领域网络安全信息公共服务平台、万兆超融合交换机、服务器密码机系统、IPSEC/SSLVPN综合安全网关系统、签名验签服务器系统、协同签名系统、智能密码钥匙、国密数字证书、二级等保测评、软件测试、代码审计、二级密评测评、渗透测试、系统集成服务、平台运营服务、人员培训服务、防火墙，属于 软件和信息技术服务业；承建（承接）企业为 广西塔易信息技术有限公司，从业人员 101 人，营业收入为 840.0679 万元，资产总额为 448.7046 万元，属于 小型企业；

以上企业，不属于大企业的分支机构，不存在控股股东为大企业的情形，也不存在与大企业的负责人为同一人的情形。

本企业对上述声明内容的真实性负责。如有虚假，将依法承担相应责任。

供应商名称（电子签章）：广西塔易信息技术有限公司

日期：2025年08月08日

注：

1. 从业人员、营业收入、资产总额填报上一年度数据，无上一年度数据的新成立企业可不填报。

2. 中小企业划型应按《关于印发中小企业划型标准规定的通知》（工信部联企业〔2011〕300号）规定的划型标准划分。

3. 请根据自己的真实情况出具《中小企业声明函》。依法享受中小企业优惠政策的，采购人或者采购代理机构在公告中标(成交)结果时，同时公告其《中小企业声明函》，接受社会监督。