广西壮族自治区政府采购合同

项目名称：信息安全服务

合同编号：12N66971303720261801

采购单位（甲方）：广西壮族自治区人力资源和社会保障信息中心

供 应 商（乙方）：中国—东盟信息港股份有限公司

签订合同地点：广西南宁

签订合同时间：2026年6月26日

《广西壮族自治区政府采购合同》
文本

合同编号：12N669713037202618O1

采购人（甲方）广西壮族自治区人力资源和社会保障信息中心

采购计划号_____

供 应 商（乙方）中国—东盟信息港股份有限公司

招 标 编 号_____

签 订 地 点 南宁市

签 订 时 间 2026年6月26日

本合同为中小企业预留合同：（否）。

根据《中华人民共和国政府采购法》《中华人民共和国政府采购法实施条例》《中华人民共和国民法典》等法律、法规规定，按照招标文件（采购文件）规定条款和乙方投标承诺，甲乙双方签订本合同。

第一条 合同标的

1、服务项目

乙方接受甲方委托，承担《信息安全服务》项目实施及服务工作，并为甲方提供技术服务，以满足甲方对本合同项目服务需求及要求。

2、项目服务所应实现的目标及技术要求以招标文件、投标文件承诺以及本合同约定为准。

序号	名称	服务内容	数 量	单位	单价（元）	总价（元）
1	信息安全服务	详见信息安全及设备运维服务公开招标文件第二章采购需求中标项二	1	1	1,837,800.00	1,837,800.00
详见开标一览表						
人民币合计金额（大写）：壹佰捌拾叁万柒仟捌佰元整（¥1,837,800.00）						

3、合同合计金额包括乙方为完成本项目服务需求及要求所需的全部费用。本项目合同价为总价包干，即完成本服务项目所有工作所需求的合同价格，包括但不限于服务的价格、人员经费、必要的设备、网络专线、平台管理、运维、短信服务、保险和各项税金、运输、装卸、安装、调试、培训、技术支持、售后服务、2026年12月11日至2026年12月31日延续服务等项目实施过程中可预见和不可预见的一切费用。招标文件另有约定的从其约定。乙方承诺不再因本项目向甲方收取其他任何费用。

4、因政府采购预算工作滞后性等原因，如乙方不是该项目原服务供应商，乙方须与原服务供应商结清2026年度已实际产生但甲方未支付的服务费用，该费用亦已包含在合同的合计金额中。

第二条　质量保证

乙方提供的技术服务（含软硬件设施）必须与招标文件、本合同约定及甲方要求相一致。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、乙方应保证独立完成合同约定义务，其所提供服务在甲方使用时不会侵犯任何第三方的专利权、商标权、著作权、工业设计权或其他权利，且所有权、处分权等没有受到任何限制；如合同履行过程中，乙方使用了自有或他人的专利、商标权、工业设计权、著作权等知识产权，所涉及的费用由乙方自行承担；如因乙方原因引起上述有关事项的争议及赔偿等，由乙方承担一切赔偿责任，与甲方无关。

2、乙方应按招标文件规定的时间向甲方提供服务的有关技术资料。

3、乙方保证所交付的货物、服务成果的所有权完全属于乙方且无任何抵押、质押、查封等产权瑕疵。 如乙方所交付货物、服务成果有产权瑕疵的，视为乙方违约，按照本合同第十条第6款约定处理。

4、本合同签订前已存在的知识产权归原拥有方所有，根据本合同新开发出来的技术成果知识产权归甲方所有，包括但不限于系统源代码、技术文档、数据资料等。

5、双方确定，甲方有权利用乙方按照本合同约定提供的服务成果、技术成果【含全部阶段性成果和最终成果，进行后续改进、创作等。由此产生的具有实质性或创造性技术进步特征的新的技术成果及其权利归属，全部由甲方享有。具体相关利益的分配办法如下：甲方100%。

6、本合同技术成果享有的上报奖项、荣誉等权利归甲方所有。

7、未经甲方书面同意，乙方不得将本合同项下技术成果转让、复制或采取其他方式透露给合同以外的任何第三方。

第四条　交付和验收

1、服务期：截止至2026年12月10日。

2、服务地点：采购人指定地点。

3、乙方提供不符合招标文件、本合同约定或甲方要求的服务成果，甲方有权拒绝接受，并要求乙方在规定的期限内进行整改。

4、乙方应对提交的服务成果作出全面检查和整理，并列出清单，作为甲方验收和使用的技术条件依据，清单应随提交的服务成果交给甲方。

5、乙方应按要求提交服务成果材料：详见乙方投标文件，如有缺失应及时补齐，否则视为逾期交付。

6、乙方在指定地点提交服务成果后，甲方应在七个工作日内进行验收，验收合格后由甲乙双方签署验收单并加盖甲方公章，甲乙双方各执一份。

7、甲方对验收有异议的，在验收后五个工作日内以书面形式向乙方提出，乙方应自收到甲方书面异议后 5个工作日内予以解决，逾期未解决的，视为逾期交付，按照本合同第十条第 4 款约定处理。

第五条　服务、质量保证期

乙方应按照国家有关法律法规以及招标文件和本合同所附的《服务承诺》，为甲方提供技术服务。

第六条 甲乙双方的权利义务

（一）甲方的权利义务

1、有权随时向乙方了解项目服务进度，并要求乙方提供项目服务相关资料。

2、有权按照合同约定或有关法律法规、政府管理的相关职能规定，对本项目进行监督和检查，有权要求乙方按监督检查情况制定相应措施并加以整改。

3、有权在乙方履行项目过程中出现损害或可能损害公共利益、公共安全情形时，终止本项目合同。

4、若乙方人员不按本合同履行其职责，甲方有权要求乙方更换不称职、不符合要求的工作人员。

5、甲方发现乙方或其工作人员有违反合同或法律行为的，有权予以制止并做出合理处置。

6、及时向乙方提供完成项目服务工作相关所需的文件、资料。

7、甲方有权要求乙方全面履行合同。甲方不接受部分履行，如本合同项下部分成果未能按时交付则视为整体延误。

8、如乙方所提供的服务成果不符合招标文件、本合同约定及甲方要求，甲方有权要求乙方重新执行相应的工作服务，由此产生的全部费用由乙方自行承担，同时，甲方的付款时间相应顺延。

（二）乙方的权利义务

1、乙方应按时按质按量向甲方提供本项目服务，根据甲方需求，定期向甲方汇报项目服务进度。交付甲方的服务成果需满足甲方需求，如出现质量问题，由乙方承担全部责任，并采取相应补救措施且不收取任何费用。

2、乙方未按本合同约定开具和送达增值税发票的，应按甲方要求采取重新开具发票等补救措施。乙方违反国家法律、法规、规章、政策等规定开具和提供发票的，乙方应自行承担相应法律责任。乙方提供的增值税发票没有通过税务部门认证，造成甲方不能抵扣的，乙方应承担相应的违约责任。

3、乙方在本合同签订后应立即组织项目组成员，并向甲方提交项目实施人员一览表，成员按各岗位职责分工负责相应的工作，在合同服务期间，如乙方需更换项目组成员的应提前书面告知甲方并征得甲方同意，且更换后的人员资质、从业经验须符合甲方要求。同时确保

提供服务过程中的人员、财产的安全，乙方服务过程中造成的人员或财产的损失、损害责任，全部由乙方承担。在接到甲方更换不称职、不符合要求的工作人员通知时，乙方应及时配合甲方更换调配符合要求的工作人员，保证项目的顺利进行。

4、未经甲方书面许可，乙方不得擅自转让或者分包本合同服务内容给任何第三方；在合同履行过程中，乙方将提供必要的配合及协调。

5、乙方在参与投标、服务过程中的所有行为必须符合法律法规、国家政策规定，如发现乙方存在违法违规行为的，甲方有权制止并单方终止本合同。

6、自觉接受甲方对本项目履行情况的监督与检查，对甲方指出的问题作出合理解释并及时纠正，纠正、完善服务成果所产生的全部费用由乙方自行承担。

7、乙方应严格遵守保密义务，未经甲方书面同意，乙方不得将在提供服务过程中所获悉的甲方的国家秘密、商业秘密、业务信息、系统数据资料、个人信息等保密信息、资料等以任何形式向任何与本合同无关的第三方披露、泄露、出售、交易、复制和使用。乙方应当加强项目服务人员保密管理及教育，与项目服务人员签订相关保密协议，并严格履行保密承诺。

8、服务期间，乙方应当妥善保管及维护甲方的设备设施，不得毁损。

9、乙方应妥善保管甲方提交给乙方的数据、资料、信息等。本合同终止时，乙方应在5日内将甲方提交给乙方用于本合同项下服务相关的数据、资料、信息等完整归还甲方。如有缺漏遗失的，乙方应承担相应的违约责任。

10、合同终止后，如甲方根据业务需要向乙方调取有关系统数据、资料、信息或进行系统数据资料迁移、改造的，乙方仍应积极配合及协助甲方提供所需数据、资料、信息，在技术上提供支持和保障。

11、乙方指派的服务人员在甲方值守期间，应当遵守甲方的有关管理规定。

12、乙方应按投标文件要求的响应时间提供维护服务，逾期提供的，甲方有权要求乙方承担相应的违约责任，如甲方因实际需求已委托第三方处理的，乙方应承担由此产生的全部费用。

13、应甲方需求对甲方人员开展与本项目相关的培训服务。

14、乙方负责服务期内因政策调整、业务需求导致的系统变更和升级改造， 并保障系统正常运行，业务正常经办。

15、如乙方不是该项目原服务供应商，乙方承诺与原服务供应商签订有关协议，按原服务供应商与甲方签订的协议标准，结清原服务供应商2026年度已实际产生但甲方未支付的服务费用。

16、项目服务期满后，乙方应根据延续服务承诺将服务延续至2026年12月31日，延续期服务标准应与招标文件、本合同约定和甲方要求一致，因合同金额已包含2026年12月11日至2026年12月31日延续服务期的费用，甲方无需向乙方支付额外服务费用。

17、如项目服务期限届满，项目因政府财政部门预算等原因未能重新组织招投标的，而乙方继续履行服务的，乙方同意继续按招标文件、投标文件、服务承诺及本协议约定履行。项目重新确定新供应商后，乙方与新供应商按本协议标准结算已经履行期间的有关服务费用。

18、乙方必须保证独立完成本合同约定的服务成果，同时须保证服务过程中不侵犯第三方知识产权或其他相关权利，如因乙方原因引起争议及赔偿等事项的，由乙方承担一切赔偿责任，与甲方无关，但因甲方内容原因导致的纠纷除外。

19、乙方应自行对其参与本项目的人员进行管理，乙方与其人员发生的劳资纠纷或因履行本合同过程中的伤亡、责任或导致他人遭受人身、财产损失的，由乙方自行承担赔偿责任。

20、乙方应确保其在进行本合同项下的活动应合法合规以及在授权范围内进行，否则因此产生的全部责任由乙方自行承担。

21、乙方人员应严谨、正确、客观地开展工作，作出的与本项目相关的服务成果及反馈材料等应当保证其合法性、真实性、客观性。

22、乙方在服务过程中，不得向甲方或任何第三方索取、收受本合同约定以外的酬金或其他财物。

23、乙方及其工作人员必须坚持正确的政治方向引导舆论，促进甲方形象提升和开展工作。不得出现因任何违法违规行为或不利于甲方订立合同的目标实现或有损于甲方订立合同目标的行为。

24、完成甲方交办的其他与本项目有关服务事宜。

第七条　付款方式

1、在合同履行期间，甲方要求终止或解除合同，乙方已开始提供服务，经甲方验收合格的，甲方根据乙方已实际提供的服务给予适当的补偿。

2、资金性质：财政资金　。

3、付款方式：详见商务条款中的付款方式。

4、履约保证金：无要求。

5、乙方应在甲方每次付款前向甲方开具等额、合法有效的税务发票。

6、本合同所有的款项甲方以转账方式转入乙方在本合同签署页的指定账户，在甲方每次付款或退付保证金前，若乙方的开户名称、开户银行、账号有变动的，应提前书面形式通知甲方，否则由此产生的后果由乙方自行承担。

第八条　税费

本合同执行中相关的一切税费均由乙方负担。

第九条　质量保证及售后服务

1、乙方应按招标文件规定的服务内容、技术要求、质量标准向甲方提供无瑕疵的服务成果。乙方对 提交的最终服务成果质量负责。

2. 成果提交后，如有修改，乙方应在规定时间按要求完成修改工作，甲方不另行支付额外费用。

第十条　违约责任

1、乙方不能按约定向甲方交付合法有效的发票的，甲方有权顺延付款时间，且不承担任何逾期付款违约责任。

2、乙方擅自转让或分包本合同服务内容的，甲方有权解除合同，不予支付合同款项，已经支付的有权要求乙方返还，并要求乙方按合同总金额的20%向甲方支付违约金。

3、乙方擅自解除合同或如因乙方原因造成不能履行本项目服务的，应向甲方支付合同总金额20%的违约金，同时甲方有权不予支付合同款项，已经支付的有权要求乙方返还。

4、乙方未按招标文件、合同约定或甲方要求的期限提交服务成果的，乙方应向甲方支付合同总金额0.3‰/天的违约金，逾期交付超过30天的，甲方有权解除合同，并要求乙方向甲方支付合同总金额10%的违约金。

5、乙方未按本合同约定、招标文件中规定的服务承诺或甲方要求提供服务的，甲方有权拒绝接受，每发生一次，乙方应按甲方要求负责整改并按本合同总金额1%向甲方支付违约金。乙方拒不整改或整改两次后仍不符合甲方要求的，甲方有权解除合同，同时乙方应按照合同总金额的10%向甲方支付违约金。

6、乙方提供的货物或服务成果如有产权瑕疵或侵犯了第三方合法权益而引发的任何纠纷或诉讼，均由乙方负责交涉并承担全部责任，造成甲方损失或涉诉（包括但不限于甲方对第三人承担的赔偿费、诉讼费、律师费、保全费、鉴定费、调查费、公证费、诉讼财产保全责任保险费等）的，甲方有权向乙方追偿，并要求乙方支付合同总金额的10%作为违约金。

7、服务期间，因乙方原因造成的数据、资料、信息丢失、设备损坏等，甲方有权要求乙方支付合同总金额的10%作为违约金。

8、乙方逾期归还甲方及履行本合同义务有关的数据、资料、信息等的，每逾期一日，按合同总金额的3‰支付违约金，直至按甲方要求归还为止。

9、乙方在合同终止后不配合甲方调取有关系统数据、资料、信息的，甲方有权要求乙方支付合同总金额的30%作为违约金，本条款不因为本合同履行终止、解除或者无效而解除。

10、乙方未按合同约定及甲方要求对系统进行变更或升级改造的，甲方有权解除合同，并要求乙方按照合同总金额的20%支付违约金。

11、乙方未在本合同约定或甲方要求的时间内响应或解决甲方所遇到的技术问题，甲方有权另行委托他人进行处理，甲方处理问题所需一切费用由乙方承担，如甲方先行垫付的，有权向乙方追偿，并有权要求乙方按照合同总金额的10%支付违约金。

12、乙方为甲方服务期间，乙方与其具体履约工作人员的劳资纠纷或因本项目工作所发生的乙方人员事故及责任或导致他人遭受人身、财产损失的均由乙方承担，甲方概不负责，如造成甲方损失或涉诉（包括但不限于甲方对第三人承担的赔偿费、诉讼费、律师费、保全费、鉴定费、调查费、公证费、诉讼财产保全责任保险费等）的，甲方有权向乙方追偿，并要求乙方支付合同总金额的10%作为违约金。

13、如乙方操作不当对甲方业务造成影响的，甲方有权单方解除合同、收回全部合同款项并要求乙方支付合同总金额的15%作为违约金，如因此给甲方造成其他损失的，甲方有权向乙方追偿。

14、乙方在参与投标、服务过程中存在违法违规行为的，甲方有权制止并单方终止本合同，如给甲方造成损失的，甲方有权向乙方追偿，不予支付合同款项并要求乙方支付合同总金额的20%作为违约金。

15、因乙方任何违法违规行为或不利于甲方订立合同的目标实现或有损于甲方订立合同目标的，甲方有权解除合同，索回已支付的全部款项，要求乙方支付合同总金额的20%作为违约金，如还有其他损失的，甲方还有权向乙方追偿。

16、乙方提交的服务或服务成果存在违背客观性、真实性、合法性情形的，甲方有权解除本合同，索回已支付的全部款项，并要求乙方支付合同总金额10%的违约金。

17、乙方擅自更换工作人员未书面征得甲方同意或更换后的人员资质、从业经验不符合甲方要求的，甲方有权要求乙方支付合同总金额的10%作为违约金。乙方应当在甲方要求的期限内整改，逾期整改甲方有权解除合同并要求乙方支付合同总金额的10%作为违约金。

18、乙方未按甲方要求更换不称职、不符合要求的工作人员的，每逾期一日，乙方应向甲方支付合同总金额0.3‰的违约金，逾期超过30天的，甲方有权解除合同，并要求乙方向甲方支付合同总金额10%的违约金。

19、乙方违反延续服务承诺，应向甲方支付合同总金额的20%作为违约金。

20、乙方存在其他违反招标文件、本合同约定情形的，除本合同另有约定外，甲方有权要求乙方支付合同总金额的5%作为违约金。

21、如乙方未按招标文件或本协议约定与原服务供应商签订有关协议或结清2026年度已实际产生但甲方未支付的服务费用，由此造成甲方向原服务供应商支付有关服务费用的，乙方应在收到甲方的退款通知之日起3日内将原服务供应商的有关服务费用退还给甲方，并向甲方支付合同总金额10%的违约金。

22、无论因何种原因导致合同解除，在违约方承担违约责任后（违约解除情况适用），双方按（实际 租赁/服务期限÷合同约定租赁/服务期限×对应合同金额）标准据实结算合同费用，乙方多收取的合同费用应在合同解除之日起5 日内返还，逾期返还的，按0.1%/天支付资金占用费。

23、合同约定的违约金不足以弥补甲方全部损失的，乙方除支付合同约定的违约金外，还应承担全部赔偿责任。因乙方违约造成的甲方损失或应向甲方支付的违约金、赔偿金，甲方有权直接从未付款中扣除，不足部分，甲方还有权向乙方追偿。

24、因乙方违约，造成的甲方支出的争议处理费用（包括但不限于诉讼费、律师费、保全费、鉴定费、评估费、诉讼财产保全责任保险费、调查费、公证费、公告费、差旅费、交通食宿费等）由乙方承担。

第十一条　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不能履行合同，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，应立即通知对方，并寄送有关权威机构出具的证明。

3、不可抗力事件延续30天以上，双方应通过友好协商，确定是否继续履行合同。

第十二条　合同争议解决

1、因履行本合同引起的或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，任何一方可向甲方所在地有管辖权的人民法院提起诉讼。

2、诉讼期间，本合同继续履行。

第十三条　合同生效及其它

1、合同经双方法定代表人或委托代理人签字并加盖单位公章后生效。

2、合同执行中涉及采购资金和采购内容修改或补充的，须经财政部门审批，并签书面补充协议报财政 部门备案，而后双方就此签署补充协议确定。

3、本合同未尽事宜，双方协商并签署补充协议确定。

4、双方确认的送达地址详见合同签署页，合同履行过程中需送达的协议、法律文书（包括但不限于起 诉状、应诉通知、传票、裁定书、判决书、律师函等）文件资料一经寄送至送达地址即视为送达。各方的 联系方式和送达地址需要变更时，应当自变更之日起三个工作日内以书面形式通知对方；未通知的，若对 方邮寄送达的，与本合同相关的文件资料包括法律文书邮寄至送达地址即视为送达。

第十四条　合同的变更、终止与转让

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、中止或终止。

第十五条　附件为合同有效组成部分，与合同效力同等。本合同附件如下：

1、招标文件；

2、乙方提供的投标文件；

3、中标通知书；

4、其他约定附件。

第十六条　合同文件的优先顺序

组成合同的各项文件应互相解释，互为说明。解释合同文件的优先顺序如下：

1、本采购合同；

2、中标通知书；

3、乙方提供的投标文件；

4、招标文件；

5、其他合同文件。

上述各项合同文件包括合同当事人就该项合同文件所作出的补充和修改，属于同一类内容的文件，应以最新签署的为准。

在合同订立及履行过程中形成的与合同有关的文件均构成合同文件组成部分，并根据其性质确定优先 解释顺序。

第十七条 本合同一式陆份，具有同等法律效力，财政部门（政府采购监管部门）、采购代理机构各持壹 份，甲乙双方各持贰份。

本合同自签订之日起二个工作日内，甲方或采购代理机构应当将合同在广西政府采购网合同公示。

（以下无正文，为合同签署页）

甲方（章） 广西壮族自治区人力资源和社会保障信息中心 2026年 6 月 26 日	乙方（章） 中国—东盟信息港股份有限公司 2026年 6 月 26 日
单位地址：南宁市民族大道 60 号劳动保障大厦	单位地址：南宁市良庆区秋月路 18 号
法定代表人或者委托代理人：	法定代表人或者委托代理人：
电话：0771-2237922	电话：
电子邮箱：—	电子邮箱：
开户银行：建设银行南宁新华支行	开户银行：中国建设银行股份有限公司南宁青山路支行
账号：4500 1604 6850 5010 5253	账号：45050160455600000042
邮政编码：530000	邮政编码：

合同附件：
1、中标通知书

中标通知书

中国-东盟信息港股份有限公司:

经评定，编号为GXZC2026-G3-001425-GXDY采购文件中的信息安全及设备运维服务-分标2，确定你公司中标，中标价格为1837800元。

自此通知书发出之日起25天内，与采购人签订政府采购合同。合同签订前，需按本项目采购文件和你公司投标文件等约定拟定合同文本(合同格式见采购文件)，报我机构项目联系人确认。

采购人联系人：林圣钧

电话：0771-2237922

代理机构联系人：黄清霞

电话：0771-5084767

邮箱：/

广西德元工程项目管理有限责任公司

2026年06月22日

2、开标一览表

2. 开标一览表

开标一览表

项目名称：信息安全及设备运维服务　　项目编号：GXZC2026-G3-001425-GXDY

投标人名称：中国一东盟信息港股份有限公司　　标项：标项二

序号	标的的名称	数量及单位①	单价（元/年）②	总价（元）③=①×②	备注
1	信息安全服务	1项	1837800	1837800	无
合计金额大写：人民币 壹佰捌拾叁万柒仟捌佰元整 （￥1837800）					

注：

1. 投标人的开标一览表必须加盖投标人电子签章并由法定代表人或者委托代理人签字或者盖章或者电子签名，**否则其投标作无效标处理。**

2. 报价一经涂改，应在涂改处加盖投标人公章或者加盖电子签章或者由法定代表人或者委托代理人签字（或者盖章或者电子签名），**否则其投标作无效标处理。**

3. 如有多分标，按分标分别提供开标一览表。

法定代表人或者委托代理人（签字或者盖章或者电子签名）：

投标人名称（电子签章）：中国一东盟信息港股份有限公司

日期：2026年6月17日

3、采购需求

说明：

1.为落实政府采购政策需满足的要求

（1）本招标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.“实质性要求”是指招标文件中已经指明不满足则投标无效的条款，或者不能负偏离的条款，或者采购需求中带“▲”的条款。**本项目凡标注“▲”的条款或要求不响应或不满足的，投标文件即作无效投标处理。**

3.采购需求中出现的品牌、型号或者生产厂家仅起参考作用，不属于指定品牌、型号或者生产厂家的情形。投标人可参照或者选用其他相当的品牌、型号或者生产厂家替代。

4.投标人必须自行为其投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。

5..**本项目采购需求表中如有要求提供文件材料或承诺书的，请在《技术要求偏离表》或《商务要求偏离表》中应答时，注明相关文件材料或承诺书放置的页码。**

6.本项目所属行业：标项一、二、三均为软件和信息技术服务业。

标项二：

一、项目要求及技术需求			
项号	采购内容	数量	项目要求及技术需求
1	信息安全服务	1项	**一、渗透测试服务** 1.服务概述：对广西人社云承载的应用系统采用黑白盒方式实施渗透测试，尽最大程度找出网站架构、页面漏洞、系统漏洞、应用漏洞等各种风险漏洞问题。对找出的问题进行充分验证，给出有针对性的整改加固方案，配合实施整改。 ▲2.服务要求：安全服务商渗透测试团队采用人工黑白盒的方式对人社云上的应用系统进行安全测试，测试内容包括系统层安全渗透测试、WEB中间件安全渗透测试、WEB应用渗透测试等方面，主要测试方法包括：信息收集、远程溢出、口令猜测、本地溢出、WEB脚本测试等，测试内容包括但不限于如下内容： （1）WEB安全：SQL注入、XSS、CSRF、文件上传、远程代码执行等； （2）业务逻辑安全：用户名枚举、用户密码枚举、平行越权、垂直越权等；

			（3）中间件安全：中间件配置缺陷、中间件弱口令、Weblogic 反序列化命令执行、文件解析代码执行等 （4）服务器安全：域传送漏洞、Redis 未授权访问、MangoDB 未授权访问等。 服务商需具备资深的漏洞挖掘能力，能有效的发现人社应用系统存在的安全风险漏洞，在 CVE 漏洞库与 CNVD 国家信息安全漏洞共享平台报送过相关的安全漏洞。 ▲3.服务范围：广西人社厅范围内所辖信息系统，包括但不限于广西“数智人社”信息系统，以人社云承载的应用系统为重点测试对象。 ▲4.服务频次：项目服务期限内根据实际需求提供渗透测试服务。 5.交付成果：测试完成后输出《应用系统渗透测试报告》《应用系统渗透测试复测报告》 **二、应急响应服务** 1.服务概述：为广西人社厅提供网络安全事件应急响应服务，针对人社云上可能发生的网络安全事件提供应急响应处置、事件原因分析、可疑漏洞验证等专业技术服务支撑，帮助人社云提升安全事件分析能力、响应处置能力，从根本上提高安全事件处置和安全保障水平。 ▲2.服务要求： 应急响应范围：包括网络或系统中的计算机或网络设备系统的硬件、软件、数据因非法攻击或病毒入侵等安全原因而遭到破坏、更改、泄漏造成系统不能正常运行，或已经发现的有可能造成上述现象的安全隐患。包括以下情况，都属于安全事件。 (1) 非授权访问，通过入侵的方式进入到未被授权访问的网络中，而导致数据信息泄漏； (2) 信息泄密，数据在传输中因数据被截取、篡改、分析等而造成信息的泄漏； (3) 拒绝服务，正常用户不能正常访问服务器提供的相关服务； (4) 在系统日志中发现非法登录者； (5) 发现网络大面积爆发计算机病毒感染； (6) 发现有人在不断强行尝试登录系统； (7) 系统中出现不明的新用户账号； (8) 管理员收到来自其它站点系统管理员的警告信，指出系统可能被威胁； (9) 文件的访问权限被修改；

			（10）因安全漏洞导致的系统问题； （11）其它的入侵行为。 3.服务范围：人社厅本单位范围内的网络安全事件 ▲4、服务频次：应急响应服务为按需服务。 5、交付成果：《安全事件应急响应报告》。 **三、网络攻防服务** ▲1.协同防护组织分工服务：安全服务商根据业界最佳防守实践，为人社厅制定实战攻防演练的安全防护组织，建立综合协同防御组织体系，合理利用人社厅本单位、第三方运维人员、专业安全厂商的技术力量，建立各有关工作组落实系统防御工作。 ▲2.协助安全防护工作方案制定：安全服务商应根据人社厅的网络安全现状，协同人社厅共同编制实战攻防演练工作方案，保证项目实施过程的有序进行。 ▲3.演练前全自查与加固：在正式演练工作开始前，对人社厅系统开展安全自评估工作，查找潜在的安全风险及漏洞，收缩攻击面，降低被攻击风险。 3.1 互联网侧资产暴露面梳理：通过现场调研访谈，同时结合资深攻防专家的安全技能，采取多种方式、多个维度探测业主单位面向互联网暴露的资产信息，形成互联网资产信息表，并对散布互联网上的本单位相关信息进行汇总清理，降低源自互联网侧的攻击路径及风险。 3.2 安全设备梳理：协助人社厅梳理盘点本单位内部的安全设备情况，明确各安全设备的功能及部署位置，整理出安全设备清单；协助设备管理人员对安全设备的策略部署、安全配置等情况进行清查完善，以加强网络安全防护能力。 3.3 安全防护情况评估：根据演练防护需要，对本单位的整体网络安全防护情况进行梳理评估，内容包括但不限于网络架构、主机系统、业务系统、日志审计、数据备份等内容，识别存在的高风险点和事项，积极协助运维管理人员做好弱点加固和风险处置工作，提高本单位的攻击防护能力。 3.4 应用渗透测试评估：在实战攻防演练开始前，对人社厅的重点业务应用系统，特别是面向互联网侧提供服务的业务系统开展专项的渗透测试评估工作，及时检测、发现可能存在的安全漏洞和风险，以协助运维人员快速修复，避免在演练期间被攻击队利用。 ▲4.攻防演练防守服务：服务期内共提供不少于 2 个月专人安全值守服务，服务期间需对发生的网络安全事件及时响应并处

			置，运维广西人社厅各类网络安全设备，及时调整设备策略，如有需要，则进行 7*24 值守服务。按需提供实战攻防演练防守服务。 5.防演练期间为人社厅提供 2 名攻防实战专家，作为演练活动中的防守队伍，主导对本单位的安全防守工作，演练期间实时监测攻击行为，对确认的攻击行为进行处置响应，积极防护本单位业务系统，演练期间根据每日防护情况负责撰写每日演练总结报告；提供不少于 2 个月的安全值守服务。 ▲6.服务范围：监管单位举办的实战攻防演练活动，提供不少于 2 个月的现场值守防护服务。 7.服务频次：项目服务期内按需提供实战攻防演练防守服务。 8.交付成果：输出《防守工作方案》、《安全监测日报》、《防守工作总结》等。 **四、终端威胁防御系统** 1.基于预防、防御、检测、响应的一体化安全体系，赋予广西人社厅终端威胁防御能力，提供服务器版客户端 2000 点和办公电脑客户端版 1000 点授权；采用基因识别、虚拟沙盒、微隔离等技术，精准识别各种已知威胁和未知威胁，帮助单位快速检测、响应终端安全问题，全面提升终端安全防护能力。 2.客户端至少支持 Windows 7、Windows 8、Windows 10、Windows 11 等 32 位/64 位终端操作系统，支持 Windows server 2003、Windows server2008、Windows server 2012、Windows server 2016、Windows server 2019 等 32 位/64 位服务器操作系统。支持飞腾、龙芯、鲲鹏、兆芯等硬件平台和银河麒麟、中标麒麟、中科方德、统信等桌面操作系统。 3.支持部门架构的导入，包含部门规则、部门与 IP 规则、LDAP 规则导入，并可根据 IP 规则一键整理。 4.支持文件分发功能，通过管理中心对终端进行统一的文件分发。 5.支持定制安全防护策略：包括病毒防御（病毒查杀、文件实时监控、恶意行为监控、U 盘保护、下载保护、邮件监控、白名单）；系统防御（浏览器保护、软件安装拦截、系统加固）；网络防御（黑客入侵拦截、IP 协议控制、恶意网站拦截、IP 黑名单）；合规管控（文档检测、文档跟踪、USB 存储、设备监控、进程监控、软件监控、服务监控、账号监控、外联监控）；其他设置（心跳配置、管理员配置、升级配置、补丁配置、弹窗配置、通信管理中心）； 6.支持终端防卸载、防脱离功能，管理员能够统一设置防卸载

			密码，防止终端用户随意脱离保护。 7.支持对终端内部文件进行全盘扫描、快速扫描，自定义扫描三种扫描能力，同时支持错峰扫描。 8.支持开启勒索诱捕功能，设置诱饵文件并实时监控，当勒索病毒对该文件进行加密操作时进行拦截。 9.支持对浏览器主页进行锁定保护，对篡改浏览器设置的恶意行为进行有效防御。 10.支持系统加固，从系统文件保护、病毒免疫、进程保护、注册表保护、危险动作拦截、执行防护等多个维度对系统进行防护。 11.支持动态认证，配置动态认证策略可以在用户本地以及远程登录系统时进行口令认证。 12.支持进程监控，可定义进程黑、白名单， 白名单指定进程可设置自保护、启动退出报警，黑名单中的进程可自动中止。 13.支持管理中心访问控制，包含 WEB 访问控制定制超时时间、登录重试次数等。 **五、驻场安全运维服务** 1.服务概述：提供驻场网络安全运维工程师 2 名，驻场工程师须通过采购人面试确认，主要工作为提供日常安全维护服务。5×8 小时对重要业务系统运行进行实时值守监控，及时发现信息安全风险或者信息安全事件并及时处理；若遇到重大信息安全事件，中标供应商需负责加派具备重大事件处理能力与经验的专业高级工程师进行现场服务。 ▲2.服务要求：驻场对内外网系统进行 5×8 小时不间断监控。对值班期间出现的可疑情况和网络攻击行为，需及时报告采购人。得到采购人授权后，与采购人相关人员一起进行事件处理，事后提供事件处理报告。 3.交付成果：输出《XXX 系统监测报告》、《XXX 系统维保报告》等。 **六、安全培训服务** 1.服务概述：每年针对专题培训和安全专业课程培训的培训至少各安排 1 次通过现有视频会议系统，进行行业信息安全培训，培训时长至少半天，培训时间由采购人指定。 2.专题培训：从加强信息安全能力角度和原则出发，对相关安全技术人员进行针对性的技术、意识专题培训，通过实际案例演示，提高安全技术人员实战经验和能力。 3.安全专业课程培训：从安全基础知识起，系统、全面地引导技术人员学习信息安全理论，掌握安全攻防技能。培训内容包

			括信息安全技术、信息安全管理、信息安全工程、信息安全体系和模型，以及信息安全标准和法律法规。 **七、安全监测和运维服务** 1.安全监测和运维服务包含态势感知安全分析服务和内外网流量监测服务两项内容，包含服务平台和内、外网监测探针使用服务，服务平台与监测探针支持联动运营，以满足服务需求。 2.服务平台硬件配置要求提供国产化 CPU，规格 2U，CPU≥2 颗 2.6GHz（32C），内存≥8*32GB DDR4 3200，系统盘≥2*240GB SATA SSD，数据盘≥12 个* 机械硬盘 8T，标配盘位数≥12，冗余电源，接口≥4 千兆电口+4 万兆光口。内网流量威胁检测探针要求提供国产化 CPU 配套探针性能：网络层吞吐量≥10Gbps，应用层吞吐量≥3.4Gbps。外网流量威胁检测探针要求提供国产化 CPU 配套探针性能：网络层吞吐量≥3Gbps，应用层吞吐量≥1.2Gbps。 3.支持挖矿专项检测页面，帮助更好的应对日益严峻的挖矿风险，避免数据窃取和监管通报，支持基于规则的本地挖矿检测和基于主动探测技术的云端挖矿检测，以实现挖矿病毒的全面检测，支持挖矿实时检测播报本地和云端的挖矿检测分析结果，支持基于攻击阶段展示挖矿主机数量，便于掌握各阶段挖矿主机分布情况，支持以列表的形式展示挖矿事件，包括最近发生时间、威胁描述、威胁定性、挖矿阶段、威胁等级、受害者 IP、攻击次数、威胁情报等信息； 4.支持威胁定性引擎以分析告警的上下文关联、时序关系、历史告警发生的频率规律性，结合威胁情报与安全专家经验对当前的安全告警进行目的性确认，从而确认安全告警的优先级顺序，支持基于人工渗透、程序自动化、业务相关风险、其它 4 个维度对告警进行分类，帮助安全人员快速定位高危告警并及时处置； 5.支持安全态势的可视化呈现，帮助客户更直观的看清风险、看懂威胁，产品内置（非自定义）综合态势大屏、分支安全态势、安全事件态势、全球网络攻击态势、资产态势、重大活动网络安全指挥调度大屏、设备运行态势、外联风险监控态势等不少于 15 块大屏展示界面证明；支持大屏轮播及自定义大屏顺序设置和轮播间隔设置，方便客户结合自身业务需求进行个性化设置； 6. 支持 PPT 格式导出摘要报告，报告内容包括：网络安全整体解读、网络安全风险详情、告警及事件响应盘点，用户可直接通过导出的 PPT 报告进行工作汇报，高效体现工作价值；

			7.支持可扩展通过网络侧（N）与终端侧（E）关联聚合，可以实现进程级取证，失陷主机定位更精准，并以可视化图谱直观清晰地展示出完整的攻击链，帮助用户快速找到症结，大幅提升事件检测、溯源取证、闭环处置效果； 8.为实现安全事件的快速闭环处置，要求支持与防火墙、行为管理、超融合、应用交付、网络控制器、端点安全管理系统等自有设备进行联动，实现效果包含联动封锁、访问控制、上网提醒、冻结账号、一键查杀等，并可联动超融合进行关机、挂起等； 9.支持可视化的形式展示威胁的影响面，通过大数据分析和关联检索技术，可清晰直观看清失陷主机对其他主机的影响，评估受损情况，方便客户快速处置。支持通过首页搜索框输入 IP/域名/URL/端口/通信对进行搜索，支持入口点溯源功能，分析出首次失陷、疑似入口点、首次遭受攻击等信息，帮助管理人员快速找到攻击入口点； 10.支持实体行为分析功能，通过对这些对象进行持续的行为分析和行为画像构建，识别服务器异常，包括 DGA 解析请求、外联 C&C 服务器、异常协议利用、下载可疑文件、异常横向访问等； 11. 支持勒索专项检测页面，帮助组织更好的应对日益严峻的勒索风险，支持对勒索的安全告警进行统一展示和管理，支持以勒索病毒的感染途径/方式为维度进行分类，包括勒索常用端口、勒索常用漏洞、RDP 爆破、感染勒索病毒、黑客勒索攻击、勒索 C&C 通信等维度，支持展示受害资产以及受害资产攻击数 TOP5，支持以列表的形式展示勒索事件，包括最近发生时间、威胁描述、威胁定性、勒索风险、威胁等级、受害者 IP、攻击次数等信息； 12.支持 5 种类型日志传输模式，包含标准模式、精简模式、高级模式、局域网模式、自定义模式，适应不同应用场景需求。 13、支持基于 IP 和域名的旁路阻断，能够在实时镜像的流量中发现恶意 IP 并实现实时阻断，支持 24 小时/7 天/最近 30 天/永久或者自定义时间阻断威胁。 14.支持标准端口运行非标准协议，非标准端口运行标准协议的异常流量检测，端口类型包括 3389、53、80/8080、21、69、443、25、110、143、22 等。 15.支持 HTTP 未知站点下载可执行文件、浏览最近 30 天注册域名、浏览恶意动态域名、访问随机算法生成域名、暴力破解攻击、反弹连接、IRC 通信等僵尸网络行为检测。

			16.具备报文检测引擎,可实现 IP 碎片重组、TCP 流重组、应用层协议识别与解析等；具备多种的入侵攻击模式或恶意 UR 监测模式，可完成模式匹配并生成事件，可提取 URL 记录和域名记录。 17.支持 Database 漏洞攻击、DNS 漏洞攻击、FTP 漏洞攻击、Mail 漏洞攻击、Network Device、Scan 漏洞攻击、System 漏洞攻击、Telnet 漏洞攻击、Tftp 漏洞攻击、Web 漏洞攻击等服务漏洞攻击检测。 18.支持责任人管理功能，可对资产进行全生命周期管理，包括自动识别资产、入库审核、离线资产识别、自动识别资产退库、手动导入资产退库、自定义资产名称等。针对自动识别资产退库功能，可设置全局退库时间，数据更新时间。支持主机资产分级管理，责任人管理； 19.支持实体行为分析功能，通过对这些对象进行持续的行为分析和行为画像构建，识别服务器异常，包括 DGA 解析请求、外联 C&C 服务器、异常协议利用、下载可疑文件、异常横向访问等； 20.服务平台及配套探针具备服务期内规则库更新授权和能力，并支持与防火墙、终端安全产品进行联动封锁。 21.安全监测和运营服务交付成果：《分析与处置报告》、《安全运营报告》、《安全通告》等。 **八、防火墙服务** 1.网络层吞吐量≥160G，应用层吞吐量≥100G，防病毒吞吐量≥20G，IPS 吞吐量≥22G，IPS+AV 吞吐量≥13G，并发连接数≥3000 万，HTTP 新建连接数≥75 万，IPSec VPN 最大接入数≥15000，IPSec VPN 吞吐量≥5G。开启入侵防御、防病毒、云端威胁情报、应用识别和管控、实时漏洞分析识别等功能模块。 2.规格 2U，内存大小≥64G，硬盘容量≥480G SSD+480G SSD，冗余电源，接口≥4 千兆电口+4 千兆光口 SFP+16 万兆光口 SFP+。提供三年软件升级和硬件维保。 3.产品可扩展识别 IT、OT、IoT 混合资产，获取 IP、MAC、操作系统、类型、厂商等信息，终端类型包括但不限于： （1）PC、瘦客户机、手机、平板、交换机、路由器、防火墙、无线控制器、服务器等 IT 资产 （2）摄像头、门禁、打印机、投影仪、VOIP 设备、条形码扫描仪、医学图像打印机、呼吸机、心电图仪、监护仪、放射系

			统等 IoT 资产 4.产品支持云威胁情报网关技术，通过全球超过 30+pop 节点，实现对威胁流量就近进行实时检测&拦截，实现失陷外联实时阻断，支持云端未知威胁主动探测技术，实现 5min 内未知威胁情报全网设备下发。 5.产品支持对压缩病毒文件进行检测和拦截，压缩层数支持 15 层及以上； 6.产品支持用户账号全生命周期保护功能，包括用户账号多余入口检测、用户账号弱口令检测、用户账号暴力破解检测、失陷账号检测，防止因账号被暴力破解导致的非法提权情况发生； 7.产品可扩展主动诱捕功能，通过伪装业务诱捕内外网的攻击行为，并联合云蜜罐获取黑客指纹信息，并自动封锁高危 IP； 8.产品支持策略生命周期管理功能，支持对安全策略修改的时间、变更类型进行统一管理，便于策略的运维与管理。 **（九）IPS 服务** .网络层吞吐量≥160G，应用层吞吐量≥100G，防病毒吞吐量≥20G，IPS 吞吐量≥22G，IPS+AV 吞吐量≥13G，并发连接数≥3000 万，HTTP 新建连接数≥75 万，IPSec VPN 最大接入数≥15000，IPSec VPN 吞吐量≥5G。开启入侵防御、应用识别和管控、实时漏洞分析识别等功能模块。 2.规格 2U，内存大小≥64G，硬盘容量≥480G SSD+480G SSD，冗余电源，接口≥4 千兆电口+4 千兆光口 SFP+16 万兆光口 SFP+。提供三年软件升级和硬件维保。 3.产品内置不低于 16000 种漏洞规则，同时支持在控制台界面通过漏洞 ID、漏洞名称、危险等级、漏洞 CVE 标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义 IPS 规则。 4.产品可扩展云威胁情报网关技术，通过全球超过 30+pop 节点，实现对威胁流量就近进行实时检测&拦截，实现失陷外联实时阻断，支持云端未知威胁主动探测技术，实现 5min 内未知威胁情报全网设备下发。 5.产品支持僵尸主机检测功能，产品内置僵尸网络特征库超过 128 万种，可识别主机的异常外联行为。 6.产品支持用户账号全生命周期保护功能，包括用户账号多余入口检测、用户账号弱口令检测、用户账号暴力破解检测、失陷账号检测，防止因账号被暴力破解导致的非法提权情况发生； 7.产品可扩展主动诱捕功能，通过伪装业务诱捕内外网的攻击

			行为，并联合云蜜罐获取黑客指纹信息，并自动封锁高危 IP； 8.产品支持策略生命周期管理功能，支持对安全策略修改的时间、变更类型进行统一管理，便于策略的运维与管理。 **（十）新系统上线评估服务** 1.服务内容：对人社厅新上线系统、重大版本变动后的业务系统进行上线前的安全评估，以发现新上线业务系统可能存在风险，防止系统带病上线。新系统上线安全评估内容主要包括安全漏洞扫描、安全配置核查、人工渗透测试等三部分内容： 2.安全漏洞扫描：利用漏洞扫描设备对涉及系统的主机操作系统、数据库、应用中间件等进行漏洞检测，以发现已暴露的安全风险漏洞，并出具漏洞扫描检测报告，提供整改建议。 3.安全配置核查：依据安全通用基线标准与等级保护要求，对涉及信息系统的主机操作系统、应用中间件、数据库等进行安全基线检查，并出具安全基线核查报告与整改建议。使业务系统的安全基线处于较高标准之上。 4.人工渗透测试：模拟入侵者对系统 WEB 应用进行攻击测试，在对现有信息系统不造成任何损害的前提下，从攻击者的角度来对主机系统的安全程度进行安全性评估。根据业务实际部署情况，可通过“黑盒”或“白盒”方式进行测试，测试方法不限于信息收集、端口扫描、远程溢出、口令猜测、本地溢出、客户端攻击、中间人攻击、web 脚本渗透等，出具渗透测试与整改建议报告。 ▲5.服务范围：广西人社厅范围内所辖信息系统，包括但不限于广西“数智人社”信息系统，以人社云承载的应用系统为重点测试对象。 6.服务频率：服务期内按实际需要开展。 7.服务交付物：《新系统上线安全评估报告》。 **（十一）数据安全风险评估服务** 1.通过业务系统基本情况梳理，分析业务流程、业务依赖关系、系统交互过程、数据流转情况等业务系统基本信息，提炼业务场景特性，归纳数据全生命周期处理情况，为全面识别数据安全风险提供依据。服务次数：1 次，输出《业务数据处理活动建模》。 2.数据安全风险评估方案设计：通过现场调研和技术评估相结合的方式设计数据安全风险评估方案、方法和流程，对单位数据运行现状开展全面风险评估，了解数据管理相关控制的存在性及有效性，评估分析数据安全整体面上和点上的安全风险，最终形成一致的风险计算规则，为招标人构建持续的风险评估

			机制。服务次数：1 次，输出《数据安全风险评估指南》。 ▲3. 数据安全风险评估实施：对业务及数据应用过程中的安全风险进行分析及评估，确定主要的数据安全风险。服务次数：1 次，输出《业务系统数据安全风险评估报告》 4. 服务范围： 本次数据安全评估服务范围，对象为 1 个重要核心业务系统。

▲二、商务要求表

服务期及地点	1. 服务期：截止至 2026 年 12 月 10 日。 2. 地点：采购人指定地点。
付款条件	1. 采购人分三次向中标供应商支付合同款；第一次付款：自签订合同后 10 个工作日内，支付 50%合同款；第二次付款：执行服务进度过半以上采购人向中标供应商支付 40%合同款；第三次付款：中标供应商完成全部服务内容且服务项目经采购人验收合格后的 10 个工作日内，支付 10%的合同款。 2. 中标供应商应在采购人每次付款前向采购人开具等额、合法有效的税务发票。
投标报价	1.本项目报价为总价包干，包括但不限于：服务的价格、人员经费、必要的设备、平台管理、运维、保险和各项税金、运输、装卸、安装、调试、培训、技术支持、售后服务等项目实施过程中可预见和不可预见的一切费用。采购人不再基于本项目服务另行支付其他额外费用。 2.因政府采购预算工作滞后性等原因，如中标供应商不是原服务供应商，中标供应商须与原服务供应商结清 2026 年度已实际产生但采购人未支付的服务费用，该费用已包含在中标供应商的报价中。 3.因财政预算执行时限要求，合同期限设定至 2026 年 12 月 10 日，但供应商需书面承诺服务延续至 2026 年 12 月 31 日（延续期服务标准与招标文件、合同期约定和采购人要求完全一致，纳入合同约束范围）。供应商须在响应文件中提供：书面承诺书。供应商报价要包含免费服务延续期（2026 年 12 月 11 日至 2026 年 12 月 31 日）。 4.对于本文件中未列明，而供应商认为必需的费用也需列入总报价。在合同实施时，采购人将不予支付中标供应商没有列入的项目费用，并认为此项目的费用已包括在总报价中。
服务要求	1. 服务响应时间要求： （1）提供 7×24 小时电话或电子邮件服务，中标供应商接到采购人的通知后立即响应，在≤ 1 小时内做出明确响应和安排，在≤ 2 小时内做出故障诊断报告，如需现场服务的，具有解决故障能力的工程师应在≤ 2 小时 内到达现场解决问题，以保证系统正常运行，并承担一切相关费用； （2）定期回访、走访采购人； （3）服务期内，中标供应商免费上门提供服务，免费提供应用软件升级。

	（4）其余按中标供应商承诺进行。 2.服务的范围包括：系统、设备的正常运行和维护。 3.中标供应商提供的服务应符合国家标准、行业标准、地方标准或者其他标准、 规范。 4.免费安装调试：中标供应商负责本项目所有货物、设备设施、配件的安装，中标供应商整理验收 材料提交采购人验收。 5.技术支持与服务：提供每周 7×24 小时技术响应服务，中标供应商应负责所售产品的售后服务，并提供至少一年的免费原厂保修服务；质保期内货物发生故障，维修或更换配件所需的全部费用由中标供应商承担。
其他要求	1.保密要求：中标供应商在项目实施过程中，必须对本项目所有项目信息以及接 触到的材料予以保密，未经采购人书面许可，中标供应商不得以任何形式向第三方透露本项目的任何内容。 2.中标供应商应按照本次项目要求完成相关服务，如因中标供应商原因造成不能履行本次项目的情况，采购人有权追究中标供应商相应责任。 3.在实施过程中，若由于中标供应商原因造成的数据、资料、信息丢失、设备损坏等，中标供应商须承担相应的责任。 4.中标供应商负责服务期内因政策调整、业务需求导致的系统变更和升级改造，并保障系统正常运行，业务正常经办。 5.采购人在中华人民共和国境内使用中标供应商提供的产品及服务时免受第三方提出的侵犯其专利权或其它知识产权的起诉。如果第三方提出侵权指控，中标供应商应承担由此而引起的一切法律责任和费用。 6.未经采购人书面许可，中标供应商不得擅自转让或分包其应履行的合同义务给任何第三方；在合同履行过程中，中标供应商将提供必要的配合及协调。 7.如中标供应商不是本项目原服务供应商，成交供应商承诺与原服务供应商签订有关协议，按原服务供应商与采购人签订的协议标准，结清原服务供应商 2026 年度已实际产生但采购人未支付的服务费用。 8.项目服务期满后，中标供应商应根据延续服务承诺将服务延续至 2026 年 12 月 31 日，延续期服务标准应与招标文件、本合同约定和采购人要求一致，因报价已明确要求包含 2026 年 12 月 11 日至 2026 年 12 月 31 日延续服务期的费用，采购人无需向中标供应商支付额外服务费用。 9.如项目服务期限届满，项目因政府财政部门预算等原因未能重新组织招投标的，

	而中标供应商继续履行服务的，中标供应商同意继续按招标文件、投标文件、服务承诺及本项目合同约定履行。项目重新确定新供应商后，中标供应商与新供应商按本项目约定的标准结算已经履行期间的有关服务费用。 10. 其他要求详见合同文本条款。 11. 其他未尽事宜需由采购人与中标供应商双方签订补充协议进行约定。
三、投标人的资信要求表	
政策性加分条件	《政府采购促进中小企业发展管理办法》（财库〔2020〕46 号），《关于我区政府采购支持监狱企业发展有关问题的通知》（桂财采[2015]24 号），《三部门联合发布关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141 号），《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）。
其它加分条件	详见评标办法及标准

4、商务要求偏离表和技术要求偏离表

4. 商务要求偏离表

商务要求偏离表

商务要求	招标文件要求	投标人的承诺	偏离说明
服务期及地点	1. 服务期：截止至 2026 年 12 月 10 日。	1. 服务期：截止至 2026 年 12 月 10 日。 我司承诺服务延续至 2027 年 1 月 15 日。	正偏离
	2. 地点：采购人指定地点。	2. 地点：采购人指定地点。	无偏离
付款条件	1. 采购人分三次向中标供应商支付合同款：第一次付款：自签订合同后 10 个工作日内，支付 50%合同款；第二次付款：执行服务进度过半以上采购人向中标供应商支付 40%合同款；第三次付款：中标供应商完成全部服务内容且服务项目经采购人验收合格后的 10 个工作日内，支付 10%的合同款。	1. 采购人分三次向我司支付合同款：第一次付款：自签订合同后 10 个工作日内，支付 50%合同款；第二次付款：执行服务进度过半以上采购人我司支付 40%合同款；第三次付款：我司完成全部服务内容且服务项目经采购人验收合格后的 10 个工作日内，支付 10%的合同款。	无偏离
	2. 中标供应商应在采购人每次付款前向采购人开具等额、合法有效的税务发票。	2. 我司在采购人每次付款前向采购人开具等额、合法有效的税务发票。	无偏离
投标报价	1.本项目报价为总价包干，包括但不限于：服务的价格、人员经费、必要的设备、平台管理、运维、保险和各项税金、运输、装卸、安装、调试、培训、技术支持、售后服务等项目实施过程中可预见和不可预见的一切费用。采购人不再基于本项目服务另行支付其他额外费用。	1.本项目报价为总价包干，包括但不限于：服务的价格、人员经费、必要的设备、平台管理、运维、保险和各项税金、运输、装卸、安装、调试、培训、技术支持、售后服务等项目实施过程中可预见和不可预见的一切费用。采购人不再基于本项目服务另行支付其他额外费用。	无偏离
	2.因政府采购预算工作滞后性等原因，如中标供应商不是原服务供应商，中标供应商须与原服务供应商结清 2026 年度已实际产生但采购人未支付的服务费用，该费用已包含在中标供应商的报价中。	2.因政府采购预算工作滞后性等原因，如中标供应商不是原服务供应商，中标供应商须与原服务供应商结清 2026 年度已实际产生但采购人未支付的服务费用，该费用已包含在中标供应商的报价中。	无偏离
	3.因财政预算执行时限要求，合同期限设定至 2026 年 12 月 10 日，但供应商需书面承诺服务延续至 2026 年 12 月 31 日（延续期服务标准与招标文件、合同期约定和采购人要求完全一致，纳入合同约束范围）。	3.因财政预算执行时限要求，合同期限设定至 2026 年 12 月 10 日，我司已书面承诺服务延续至 **2027 年 1 月 15 日**（延续期服务标准与招标文件、合同期约定和采购人要求完全一致，纳入合同约束范围）。**（详见 P16 页）**	**正偏离**

	供应商须在响应文件中提供：书面承诺书。供应商报价要包含免费服务延续期（2026 年 12 月 11 日至 2026 年 12 月 31 日）。	我司已在响应文件中提供：书面承诺书。我司包含免费服务延续期（2026 年 12 月 11 日至 2027 年 1 月 15 日）。	
	4.对于本文件中未列明，而供应商认为必需的费用也需列入总报价。在合同实施时，采购人将不予支付中标供应商没有列入的项目费用，并认为此项目的费用已包括在总报价中。	4.对于本文件中未列明，而我司认为必需的费用也已列入总报价。在合同实施时，采购人将不予支付我司没有列入的项目费用，并认为此项目的费用已包括在总报价中。	无偏离
服务要求	1.服务响应时间要求：	1.服务响应时间要求：	无偏离
	（1）提供 7×24 小时电话或电子邮件服务，中标供应商接到采购人的通知后立即响应，在≤ 1 小时内做出明确响应和安排，在≤ 2 小时内做出故障诊断报告，如需现场服务的，具有解决故障能力的工程师应在≤ 2 小时 内到达现场解决问题，以保证系统正常运行，并承担一切相关费用；	（1）我司提供 7×24 小时电话或电子邮件服务，我司接到采购人的通知后立即响应，在 15 分钟内做出明确响应和安排，在 2 小时内做出故障诊断报告，如需现场服务的，具有解决故障能力的工程师在 2 小时 内到达现场解决问题，以保证系统正常运行，并承担一切相关费用；	无偏离
	（2）定期回访、走访采购人；	（2）定期回访、走访采购人；	无偏离
	（3）服务期内，中标供应商免费上门提供服务，免费提供应用软件升级。	（3）服务期内，我司免费上门提供服务，免费提供应用软件升级。	无偏离
	（4）其余按中标供应商承诺进行。	（4）其余按我司承诺进行。	无偏离
	2.服务的范围包括：系统、设备的正常运行和维护。	2.服务的范围包括：系统、设备的正常运行和维护。	无偏离
	3.中标供应商提供的服务应符合国家标准、行业标准、地方标准或者其他标准、 规范。	3.我司提供的服务应符合国家标准、行业标准、地方标准或者其他标准、规范。	无偏离
	4.免费安装调试：中标供应商负责本项目所有货物、设备设施、配件的安装，中标供应商整理验收 材料提交采购人验收。	4.免费安装调试：我司负责本项目所有货物、设备设施、配件的安装，我司整理验收材料提交采购人验收。	无偏离
	5.技术支持与服务：提供每周 7×24 小时技术响应服务，中标供应商应负责所售 产品的售后服务，并提供至少一年的免费原厂保修服务；质保期内货物发生故障， 维修或更换配件所需的全部费用由中标供应商承担。	5.技术支持与服务：提供每周 7×24 小时技术响应服务，我司负责所售产品的售后服务，并提供一年的免费原厂保修服务；质保期内货物发生故障，维修或更换配件所需的全部费用由我司承担。	无偏离
其他	1.保密要求：中标供应商在项目实	1.保密要求：我司在项目实施过程	无偏离

要求	施过程中，必须对本项目所有项目信息以及接 触到的材料予以保密，未经采购人书面许可，中标供应商不得以任何形式向第三方透露本项目的任何内容。	中，对本项目所有项目信息以及接触到的材料予以保密，未经采购人书面许可，我司不得以任何形式向第三方透露本项目的任何内容。	
	2. 中标供应商应按照本次项目要求完成相关服务，如因中标供应商原因造成不能履行本次项目的情况，采购人有权追究中标供应商相应责任。	2. 我司按照本次项目要求完成相关服务，如因我司原因造成不能履行本次项目的情况，采购人有权追究我司相应责任。	无偏离
	3. 在实施过程中，若由于中标供应商原因造成的数据、资料、信息丢失、设备损坏等，中标供应商须承担相应的责任。	3. 在实施过程中，若由于我司原因造成的数据、资料、信息丢失、设备损坏等，我司承担相应的责任。	无偏离
	4. 中标供应商负责服务期内因政策调整、业务需求导致的系统变更和升级改造，并保障系统正常运行，业务正常经办。	4. 我司负责服务期内因政策调整、业务需求导致的系统变更和升级改造，并保障系统正常运行，业务正常经办。	无偏离
	5. 采购人在中华人民共和国境内使用中标供应商提供的产品及服务时免受第三方 提出的侵犯其专利权或其它知识产权的起诉。如果第三方提出侵权指控，中标供应商应承担由此而引起的一切法律责任和费用。	5. 采购人在中华人民共和国境内使用我司提供的产品及服务时免受第三方提出的侵犯其专利权或其它知识产权的起诉。如果第三方提出侵权指控，我司承担由此而引起的一切法律责任和费用。	无偏离
	6. 未经采购人书面许可，中标供应商不得擅自转让或分包其应履行的合同义务给任何第三方；在合同履行过程中，中标供应商将提供必要的配合及协调。	6. 未经采购人书面许可，我司不得擅自转让或分包其应履行的合同义务给任何第三方；在合同履行过程中，我司将提供必要的配合及协调。	无偏离
	7. 如中标供应商不是本项目原服务供应商，成交供应商承诺与原服务供应商签订有关协议，按原服务供应商与采购人签订的协议标准，结清原服务供应商 2026 年度已实际产生但采购人未支付的服务费用。	7. 如中标供应商不是本项目原服务供应商，成交供应商承诺与原服务供应商签订有关协议，按原服务供应商与采购人签订的协议标准，结清原服务供应商 2026 年度已实际产生但采购人未支付的服务费用。	无偏离
	8. 项目服务期满后，中标供应商应根据延续服务承诺将服务延续至 2026 年 12 月 31 日，延续期服务标准应与招标文件、本合同约定和采购人要求一致，因报价已明确要求包含 2026 年 12 月 11 日至 2026 年 12 月 31 日延续服务期的费用，采购人无需向中标供应商支付额外服	8. 项目服务期满后，我司根据延续服务承诺将服务延续至 2027 年 1 月 15 日，延续期服务标准应与招标文件、本合同约定和采购人要求一致，因报价已明确要求包含 2026 年 12 月 11 日至 2027 年 1 月 15 日延续服务期的费用，采购人无需向我司支付额外服务费用。	**正偏离**

	务费用。		
	9. 如项目服务期限届满，项目因政府财政部门预算等原因未能重新组织招投标的，而中标供应商继续履行服务的，中标供应商同意继续按招标文件、投标文件、服务承诺及本项目合同约定履行。项目重新确定新供应商后，中标供应商与新供应商按本项目约定的标准结算已经履行期间的有关服务费用。	9. 如项目服务期限届满，项目因政府财政部门预算等原因未能重新组织招投标的，而中标供应商继续履行服务的，中标供应商同意继续按招标文件、投标文件、服务承诺及本项目合同约定履行。项目重新确定新供应商后，中标供应商与新供应商按本项目约定的标准结算已经履行期间的有关服务费用。	无偏离
	10. 其他要求详见合同文本条款。	10. 其他要求详见合同文本条款。	无偏离
	11. 其他未尽事宜需由采购人与中标供应商双方签订补充协议进行约定。	11. 其他未尽事宜需由采购人与我司双方签订补充协议进行约定。	无偏离

注：

1. 说明：应对照招标文件“第二章 采购需求”中的商务要求逐条作明确的投标响应，并作出偏离说明。

2. 投标人应根据自身的承诺，对照招标文件要求在“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**”。

法定代表人或者委托代理人（签字或者盖章或者电子签名）：

投标人名称（电子签章）：中国—东盟信息港股份有限公司

日　　期：2026年6月17日

1. 技术要求偏离表

技术要求偏离表

项号	标的的名称	项目要求及技术需求	项目要求及技术需求	偏离说明
1	信息安全服务	一、渗透测试服务	一、我公司承诺提供以下渗透测试服务	无偏离
		1.服务概述：对广西人社云承载的应用系统采用黑白盒方式实施渗透测试，尽最大程度找出网站架构、页面漏洞、系统漏洞、应用漏洞等各种风险漏洞问题。对找出的问题进行充分验证，给出有针对性的整改加固方案，配合实施整改。	1.我公司承诺满足以下服务概述：对广西人社云承载的应用系统采用黑白盒方式实施渗透测试，尽最大程度找出网站架构、页面漏洞、系统漏洞、应用漏洞等各种风险漏洞问题。对找出的问题进行充分验证，给出有针对性的整改加固方案，配合实施整改。	无偏离
		▲2.服务要求：安全服务商渗透测试团队采用人工黑白盒的方式对人社云上的应用系统进行安全测试，测试内容包括系统层安全渗透测试、WEB 中间件安全渗透测试、WEB 应用渗透测试等方面，主要测试方法包括：信息收集、远程溢出、口令猜测、本地溢出、WEB 脚本测试等，测试内容包括但不限于如下内容：	▲2.我公司承诺满足以下服务要求：安全服务商渗透测试团队采用人工黑白盒的方式对人社云上的应用系统进行安全测试，测试内容包括系统层安全渗透测试、WEB 中间件安全渗透测试、WEB 应用渗透测试等方面，主要测试方法包括：信息收集、远程溢出、口令猜测、本地溢出、WEB 脚本测试等，测试内容包括但不限于如下内容：	无偏离
		（1）WEB 安全：SQL 注入、XSS、CSRF、文件上传、远程代码执行等；	（1）WEB 安全：SQL 注入、XSS、CSRF、文件上传、远程代码执行等；	无偏离
		（2）业务逻辑安全：用户名枚举、用户密码枚举、平行越权、垂直越权等；	（2）业务逻辑安全：用户名枚举、用户密码枚举、平行越权、垂直越权等；	无偏离
		（3）中间件安全：中间件配置缺陷、中间件弱口令、Weblogic 反序列化命令执行、文件解析代码执行等	（3）中间件安全：中间件配置缺陷、中间件弱口令、Weblogic 反序列化命令执行、文件解析代码执行等	无偏离
		（4）服务器安全：域传送漏洞、Redis 未授权访问、MangoDB 未授权访问等。	（4）服务器安全：域传送漏洞、Redis 未授权访问、MangoDB 未授权访问等。	无偏离
		服务商需具备资深的漏洞挖掘能力，能有效的发现人社应用系统	我公司具备资深的漏洞挖掘能力，能有效的发现人社应用系统	无偏离

		存在的安全风险漏洞，在 CVE 漏洞库与 CNVD 国家信息安全漏洞共享平台报送过相关的安全漏洞。	存在的安全风险漏洞，在 CVE 漏洞库与 CNVD 国家信息安全漏洞共享平台报送过相关的安全漏洞。	
		▲3. 服务范围：广西人社厅范围内所辖信息系统，包括但不限于广西“数智人社”信息系统，以人社云承载的应用系统为重点测试对象。	▲3. 我公司承诺满足以下服务范围：广西人社厅范围内所辖信息系统，包括但不限于广西“数智人社”信息系统，以人社云承载的应用系统为重点测试对象。	无偏离
		▲4. 服务频次：项目服务期限内根据实际需求提供渗透测试服务。	▲4. 我公司承诺提供以下服务频次：项目服务期限内根据实际需求提供渗透测试服务。	无偏离
		5. 交付成果：测试完成后输出《应用系统渗透测试报告》《应用系统渗透测试复测报告》	5. 我公司承诺提供以下交付成果：测试完成后输出《应用系统渗透测试报告》《应用系统渗透测试复测报告》	无偏离
		二、应急响应服务	**二、我公司承诺提供以下应急响应服务**	无偏离
		1. 服务概述：为广西人社厅提供网络安全事件应急响应服务，针对人社云上可能发生的网络安全事件提供应急响应处置、事件原因分析、可疑漏洞验证等专业技术服务支撑，帮助人社云提升安全事件分析能力、响应处置能力，从根本上提高安全事件处置和安全保障水平。	1. 我公司承诺满足以下服务概述：为广西人社厅提供网络安全事件应急响应服务，针对人社云上可能发生的网络安全事件提供应急响应处置、事件原因分析、可疑漏洞验证等专业技术服务支撑，帮助人社云提升安全事件分析能力、响应处置能力，从根本上提高安全事件处置和安全保障水平。	无偏离
		▲2. 服务要求：	▲2. 我公司承诺满足以下服务要求：	无偏离
		应急响应范围：包括网络或系统中的计算机或网络设备系统的硬件、软件、数据因非法攻击或病毒入侵等安全原因而遭到破坏、更改、泄漏造成系统不能正常运行，或已经发现的有可能造成上述现象的安全隐患。包括以下情况，都属于安全事件。	我公司承诺满足以下应急响应范围：包括网络或系统中的计算机或网络设备系统的硬件、软件、数据因非法攻击或病毒入侵等安全原因而遭到破坏、更改、泄漏造成系统不能正常运行，或已经发现的有可能造成上述现象的安全隐患。包括以下情况，都属于安全事件。	无偏离
		(1) 非授权访问，通过入侵的方式进入到未被授权访问的网络中，而导致数据信息泄漏；	(1) 非授权访问，通过入侵的方式进入到未被授权访问的网络中，而导致数据信息泄漏；	无偏离
		(2) 信息泄密，数据在传输中因数据被截取、篡改、分析等而造成信息的泄漏；	(2) 信息泄密，数据在传输中因数据被截取、篡改、分析等而造成信息的泄漏；	无偏离

		(3) 拒绝服务，正常用户不能正常访问服务器提供的相关服务；	(3) 拒绝服务，正常用户不能正常访问服务器提供的相关服务；	无偏离
		(4) 在系统日志中发现非法登录者；	(4) 在系统日志中发现非法登录者；	无偏离
		(5) 发现网络大面积爆发计算机病毒感染；	(5) 发现网络大面积爆发计算机病毒感染；	无偏离
		(6) 发现有人在不断强行尝试登录系统；	(6) 发现有人在不断强行尝试登录系统；	无偏离
		(7) 系统中出现不明的新用户账号；	(7) 系统中出现不明的新用户账号；	无偏离
		(8) 管理员收到来自其它站点系统管理员的警告信，指出系统可能被威胁；	(8) 管理员收到来自其它站点系统管理员的警告信，指出系统可能被威胁；	无偏离
		(9) 文件的访问权限被修改；	(9) 文件的访问权限被修改；	无偏离
		(10) 因安全漏洞导致的系统问题；	(10) 因安全漏洞导致的系统问题；	无偏离
		(11) 其它的入侵行为。	(11) 其它的入侵行为。	无偏离
		3. 服务范围：人社厅本单位范围内的网络安全事件	3. 我公司承诺满足以下服务范围：人社厅本单位范围内的网络安全事件	无偏离
		▲4、服务频次：应急响应服务为按需服务。	▲4、我公司承诺提供以下服务频次：应急响应服务为按需服务。	无偏离
		5、交付成果：《安全事件应急响应报告》。	5、我公司承诺提供以下交付成果：《安全事件应急响应报告》。	无偏离
		三、网络攻防服务	**三、我公司承诺提供以下网络攻防服务**	无偏离
		▲1. 协同防护组织分工服务：安全服务商根据业界最佳防守实践，为人社厅制定实战攻防演练的安全防护组织，建立综合协同防御组织体系，合理利用人社厅本单位、第三方运维人员、专业安全厂商的技术力量，建立各有关工作组落实系统防御工作。	▲1. 我公司承诺满足以下协同防护组织分工服务：安全服务商根据业界最佳防守实践，为人社厅制定实战攻防演练的安全防护组织，建立综合协同防御组织体系，合理利用人社厅本单位、第三方运维人员、专业安全厂商的技术力量，建立各有关工作组落实系统防御工作。	无偏离
		▲2. 协助安全防护工作方案制定：安全服务商应根据人社厅的网络安全现状，协同人社厅共同编制实战攻防演练工作方案，保证项目实施过程的有序进行。	▲2. 我公司承诺提供以下协助安全防护工作方案制定：安全服务商应根据人社厅的网络安全现状，协同人社厅共同编制实战攻防演练工作方案，保证项目实施过程的有序进行。	无偏离
		▲3. 演练前全自查与加固：在正式演练工作开始前，对人社厅系	▲3. 我公司承诺提供以下演练前全自查与加固：在正式演练工作	无偏离

		统开展安全自评估工作，查找潜在的安全风险及漏洞，收缩攻击面，降低被攻击风险。	开始前，对人社厅系统开展安全自评估工作，查找潜在的安全风险及漏洞，收缩攻击面，降低被攻击风险。	
		3.1 互联网侧资产暴露面梳理：通过现场调研访谈，同时结合资深攻防专家的安全技能，采取多种方式、多个维度探测业主单位面向互联网暴露的资产信息，形成互联网资产信息表，并对散布互联网上的本单位相关信息进行汇总清理，降低源自互联网侧的攻击路径及风险。	3.1 我公司承诺提供以下互联网侧资产暴露面梳理：通过现场调研访谈，同时结合资深攻防专家的安全技能，采取多种方式、多个维度探测业主单位面向互联网暴露的资产信息，形成互联网资产信息表，并对散布互联网上的本单位相关信息进行汇总清理，降低源自互联网侧的攻击路径及风险。	无偏离
		3.2 安全设备梳理：协助人社厅梳理盘点本单位内部的安全设备情况，明确各安全设备的功能及部署位置，整理出安全设备清单；协助设备管理人员对安全设备的策略部署、安全配置等情况进行清查完善，以加强网络安全防护能力。	3.2 我公司承诺提供安全设备梳理：协助人社厅梳理盘点本单位内部的安全设备情况，明确各安全设备的功能及部署位置，整理出安全设备清单；协助设备管理人员对安全设备的策略部署、安全配置等情况进行清查完善，以加强网络安全防护能力。	无偏离
		3.3 安全防护情况评估：根据演练防护需要，对本单位的整体网络安全防护情况进行梳理评估，内容包括但不限于网络架构、主机系统、业务系统、日志审计、数据备份等内容，识别存在的高风险点和事项，积极协助运维管理人员做好弱点加固和风险处置工作，提高本单位的攻击防护能力。	3.3 我公司承诺提供安全防护情况评估：根据演练防护需要，对本单位的整体网络安全防护情况进行梳理评估，内容包括但不限于网络架构、主机系统、业务系统、日志审计、数据备份等内容，识别存在的高风险点和事项，积极协助运维管理人员做好弱点加固和风险处置工作，提高本单位的攻击防护能力。	无偏离
		3.4 应用渗透测试评估：在实战攻防演练开始前，对人社厅的重点业务应用系统，特别是面向互联网侧提供服务的业务系统开展专项的渗透测试评估工作，及时检测、发现可能存在的安全漏洞和风险，以协助运维人员快速修复，避免在演练期间被攻击队利用。	3.4 我公司承诺提供应用渗透测试评估：在实战攻防演练开始前，对人社厅的重点业务应用系统，特别是面向互联网侧提供服务的业务系统开展专项的渗透测试评估工作，及时检测、发现可能存在的安全漏洞和风险，以协助运维人员快速修复，避免在演练期间被攻击队利用。	无偏离
		▲4.攻防演练防守服务：服务期内共提供不少于 2 个月专人安全值守服务，服务期间需对发生的	▲4.我公司承诺提供攻防演练防守服务：服务期内共提供不少于 2 个月专人安全值守服务，服务期	无偏离

		网络安全事件及时响应并处置，运维广西人社厅各类网络安全设备，及时调整设备策略，如有需要，则进行 7*24 值守服务。按需提供实战攻防演练防守服务。	间需对发生的网络安全事件及时响应并处置，运维广西人社厅各类网络安全设备，及时调整设备策略，如有需要，则进行 7*24 值守服务。按需提供实战攻防演练防守服务。	
		5. 防演练期间为人社厅提供 2 名攻防实战专家，作为演练活动中的防守队伍，主导对本单位的安全防守工作，演练期间实时监测攻击行为，对确认的攻击行为进行处置响应，积极防护本单位业务系统，演练期间根据每日防护情况负责撰写每日演练总结报告；提供不少于 2 个月的安全值守服务。	5. 我公司承诺防演练期间为人社厅提供 2 名攻防实战专家，作为演练活动中的防守队伍，主导对本单位的安全防守工作，演练期间实时监测攻击行为，对确认的攻击行为进行处置响应，积极防护本单位业务系统，演练期间根据每日防护情况负责撰写每日演练总结报告；提供不少于 2 个月的安全值守服务。	无偏离
		▲6. 服务范围：监管单位举办的实战攻防演练活动，提供不少于 2 个月的现场值守防护服务。	▲6. 我公司承诺满足以下服务范围：监管单位举办的实战攻防演练活动，提供不少于 2 个月的现场值守防护服务。	无偏离
		7. 服务频次：项目服务期内按需提供实战攻防演练防守服务。	7. 我公司承诺满足以下服务频次：项目服务期内按需提供实战攻防演练防守服务。	无偏离
		8. 交付成果：输出《防守工作方案》、《安全监测日报》、《防守工作总结》等。	8. 我公司承诺提供以下交付成果：输出《防守工作方案》、《安全监测日报》、《防守工作总结》等。	无偏离
		四、终端威胁防御系统	**四、我公司承诺终端威胁防御系统满足以下要求**	无偏离
		1. 基于预防、防御、检测、响应的一体化安全体系，赋予广西人社厅终端威胁防御能力，提供服务器版客户端 2000 点和办公电脑客户端版 1000 点授权；采用基因识别、虚拟沙盒、微隔离等技术，精准识别各种已知威胁和未知威胁，帮助单位快速检测、响应终端安全问题，全面提升终端安全防护能力。	1. 基于预防、防御、检测、响应的一体化安全体系，赋予广西人社厅终端威胁防御能力，提供服务器版客户端 2000 点和办公电脑客户端版 1000 点授权；采用基因识别、虚拟沙盒、微隔离等技术，精准识别各种已知威胁和未知威胁，帮助单位快速检测、响应终端安全问题，全面提升终端安全防护能力。	无偏离
		2. 客户端至少支持 Windows 7、Windows 8、Windows 10、Windows 11 等 32 位/64 位终端操作系统，支持 Windows server 2003、Windows server2008、Windows	2. 客户端支持 Windows 7、Windows 8、Windows 10、Windows 11 等 32 位/64 位终端操作系统，支持 Windows server 2003、Windows server2008、Windows	无偏离

		server 2012、Windows server 2016、Windows server 2019 等 32 位/64 位服务器操作系统。支持飞腾、龙芯、鲲鹏、兆芯等硬件平台和银河麒麟、中标麒麟、中科方德、统信等桌面操作系统。	server 2012、Windows server 2016、Windows server 2019 等 32 位/64 位服务器操作系统。支持飞腾、龙芯、鲲鹏、兆芯等硬件平台和银河麒麟、中标麒麟、中科方德、统信等桌面操作系统。	
		3.支持部门架构的导入，包含部门规则、部门与 IP 规则、LDAP 规则导入，并可根据 IP 规则一键整理。	3.支持部门架构的导入，包含部门规则、部门与 IP 规则、LDAP 规则导入，并可根据 IP 规则一键整理。	无偏离
		4.支持文件分发功能，通过管理中心对终端进行统一的文件分发。	4.支持文件分发功能，通过管理中心对终端进行统一的文件分发。	无偏离
		5.支持定制安全防护策略：包括病毒防御（病毒查杀、文件实时监控、恶意行为监控、U 盘保护、下载保护、邮件监控、白名单）；系统防御（浏览器保护、软件安装拦截、系统加固）；网络防御（黑客入侵拦截、IP 协议控制、恶意网站拦截、IP 黑名单）；合规管控（文档检测、文档跟踪、USB 存储、设备监控、进程监控、软件监控、服务监控、账号监控、外联监控）；其他设置（心跳配置、管理员配置、升级配置、补丁配置、弹窗配置、通信管理中心）；	5.支持定制安全防护策略：包括病毒防御（病毒查杀、文件实时监控、恶意行为监控、U 盘保护、下载保护、邮件监控、白名单）；系统防御（浏览器保护、软件安装拦截、系统加固）；网络防御（黑客入侵拦截、IP 协议控制、恶意网站拦截、IP 黑名单）；合规管控（文档检测、文档跟踪、USB 存储、设备监控、进程监控、软件监控、服务监控、账号监控、外联监控）；其他设置（心跳配置、管理员配置、升级配置、补丁配置、弹窗配置、通信管理中心）；	无偏离
		6.支持终端防卸载、防脱离功能，管理员能够统一设置防卸载密码，防止终端用户随意脱离保护。	6.支持终端防卸载、防脱离功能，管理员能够统一设置防卸载密码，防止终端用户随意脱离保护。	无偏离
		7.支持对终端内部文件进行全盘扫描、快速扫描，自定义扫描三种扫描能力，同时支持错峰扫描。	7.支持对终端内部文件进行全盘扫描、快速扫描，自定义扫描三种扫描能力，同时支持错峰扫描。	无偏离
		8.支持开启勒索诱捕功能，设置诱饵文件并实时监控，当勒索病毒对该文件进行加密操作时进行拦截。	8.支持开启勒索诱捕功能，设置诱饵文件并实时监控，当勒索病毒对该文件进行加密操作时进行拦截。	无偏离
		9.支持对浏览器主页进行锁定保护，对篡改浏览器设置的恶意行为进行有效防御。	9.支持对浏览器主页进行锁定保护，对篡改浏览器设置的恶意行为进行有效防御。	无偏离
		10.支持系统加固，从系统文件保护、病毒免疫、进程保护、注册表保护、危险动作拦截、执行防	10.支持系统加固，从系统文件保护、病毒免疫、进程保护、注册表保护、危险动作拦截、执行防	无偏离

		护等多个维度对系统进行防护。	护等多个维度对系统进行防护。	
		11. 支持动态认证，配置动态认证策略可以在用户本地以及远程登录系统时进行口令认证。	11. 支持动态认证，配置动态认证策略可以在用户本地以及远程登录系统时进行口令认证。	无偏离
		12. 支持进程监控，可定义进程黑、白名单， 白名单指定进程可设置自保护、启动退出报警，黑名单中的进程可自动中止。	12. 支持进程监控，可定义进程黑、白名单， 白名单指定进程可设置自保护、启动退出报警，黑名单中的进程可自动中止。	无偏离
		13. 支持管理中心访问控制，包含 WEB 访问控制定制超时时间、登录重试次数等。	13. 支持管理中心访问控制，包含 WEB 访问控制定制超时时间、登录重试次数等。	无偏离
		五、驻场安全运维服务	**五、我公司承诺提供以下驻场安全运维服务**	无偏离
		1. 服务概述：提供驻场网络安全运维工程师 2 名，驻场工程师通过采购人面试确认，主要工作为提供日常安全维护服务。5×8 小时对重要业务系统运行进行实时值守监控，及时发现信息安全风险或者信息安全事件并及时处理；若遇到重大信息安全事件，中标供应商需负责加派具备重大事件处理能力与经验的专业高级工程师进行现场服务。	1. 我公司承诺满足以下服务概述：提供驻场网络安全运维工程师 2 名，驻场工程师通过采购人面试确认，主要工作为提供日常安全维护服务。5×8 小时对重要业务系统运行进行实时值守监控，及时发现信息安全风险或者信息安全事件并及时处理；若遇到重大信息安全事件，我司负责加派具备重大事件处理能力与经验的专业高级工程师进行现场服务。	无偏离
		▲2. 服务要求：驻场对内外网系统进行 5×8 小时不间断监控。对值班期间出现的可疑情况和网络攻击行为，需及时报告采购人。得到采购人授权后，与采购人相关人员一起进行事件处理，事后提供事件处理报告。	▲2. 我公司承诺满足以下服务要求：驻场对内外网系统进行 5×8 小时不间断监控。对值班期间出现的可疑情况和网络攻击行为，并及时报告采购人。得到采购人授权后，与采购人相关人员一起进行事件处理，事后提供事件处理报告。	无偏离
		3. 交付成果：输出《XXX 系统监测报告》、《XXX 系统维保报告》等。	3. 我公司承诺提供以下交付成果：输出《XXX 系统监测报告》、《XXX 系统维保报告》等。	无偏离
		六、安全培训服务	**六、我公司承诺提供以下安全培训服务**	无偏离
		1. 服务概述：每年针对专题培训和安全专业课程培训的培训至少各安排 1 次通过现有视频会议系统，进行行业信息安全培训，培训时长至少半天，培训时间由采购人指定。	1. 我公司承诺满足以下服务概述：每年针对专题培训和安全专业课程培训的培训至少各安排 1 次通过现有视频会议系统，进行行业信息安全培训，培训时长至少半天，培训时间由采购人指定。	无偏离

		2.专题培训：从加强信息安全能力角度和原则出发，对相关安全技术人员进行针对性的技术、意识专题培训，通过实际案例演示，提高安全技术人员实战经验和能力。	2.我公司承诺提供以下专题培训：从加强信息安全能力角度和原则出发，对相关安全技术人员进行针对性的技术、意识专题培训，通过实际案例演示，提高安全技术人员实战经验和能力。	无偏离
		3.安全专业课程培训：从安全基础知识起，系统、全面地引导技术人员学习信息安全理论，掌握安全攻防技能。培训内容包括信息安全技术、信息安全管理、信息安全工程、信息安全体系和模型，以及信息安全标准和法律法规。	3.我公司承诺提供以下安全专业课程培训：从安全基础知识起，系统、全面地引导技术人员学习信息安全理论，掌握安全攻防技能。培训内容包括信息安全技术、信息安全管理、信息安全工程、信息安全体系和模型，以及信息安全标准和法律法规。	无偏离
		七、安全监测和运维服务	**七、我公司承诺提供以下安全监测和运维服务**	无偏离
		1.安全监测和运维服务包含态势感知安全分析服务和内外网流量监测服务两项内容，包含服务平台和内、外网监测探针使用服务，服务平台与监测探针支持联动运营，以满足服务需求。	1.安全监测和运维服务包含态势感知安全分析服务和内外网流量监测服务两项内容，包含服务平台和内、外网监测探针使用服务，服务平台与监测探针支持联动运营，以满足服务需求。	无偏离
		2.服务平台硬件配置要求提供国产化 CPU，规格 2U，CPU≥2 颗 2.6GHz（32C），内存≥8*32GB DDR4 3200，系统盘≥2*240GB SATA SSD，数据盘≥12 个* 机械硬盘 8T，标配盘位数≥12，冗余电源，接口≥4 千兆电口+4 万兆光口。内网流量威胁检测探针要求提供国产化 CPU 配套探针性能：网络层吞吐量≥10Gbps，应用层吞吐量≥3.4Gbps。外网流量威胁检测探针要求提供国产化 CPU 配套探针性能：网络层吞吐量≥3Gbps，应用层吞吐量≥1.2Gbps。	2.服务平台硬件配置要求提供国产化 CPU，规格 2U，CPU：2 颗 2.6GHz（32C），内存：8*32GB DDR4 3200，系统盘：2*240GB SATA SSD，数据盘：12 个* 机械硬盘 8T，标配盘位数：12，冗余电源，接口：4 千兆电口+4 万兆光口。内网流量威胁检测探针要求提供国产化 CPU 配套探针性能：网络层吞吐量：10Gbps，应用层吞吐量：3.4Gbps。外网流量威胁检测探针要求提供国产化 CPU 配套探针性能：网络层吞吐量：3Gbps，应用层吞吐量：1.2Gbps。	无偏离
		3.支持挖矿专项检测页面，帮助更好的应对日益严峻的挖矿风险，避免数据窃取和监管通报，支持基于规则的本地挖矿检测和基于主动探测技术的云端挖矿检测，以实现挖矿病毒的全面检测，支持挖矿实时检测播报本地和云端	3.支持挖矿专项检测页面，帮助更好的应对日益严峻的挖矿风险，避免数据窃取和监管通报，支持基于规则的本地挖矿检测和基于主动探测技术的云端挖矿检测，以实现挖矿病毒的全面检测，支持挖矿实时检测播报本地和云端	无偏离

		的挖矿检测分析结果，支持基于攻击阶段展示挖矿主机数量，便于掌握各阶段挖矿主机分布情况，支持以列表的形式展示挖矿事件，包括最近发生时间、威胁描述、威胁定性、挖矿阶段、威胁等级、受害者 IP、攻击次数、威胁情报等信息；	的挖矿检测分析结果，支持基于攻击阶段展示挖矿主机数量，便于掌握各阶段挖矿主机分布情况，支持以列表的形式展示挖矿事件，包括最近发生时间、威胁描述、威胁定性、挖矿阶段、威胁等级、受害者 IP、攻击次数、威胁情报等信息；	
		4.支持威胁定性引擎以分析告警的上下文关联、时序关系、历史告警发生的频率规律性，结合威胁情报与安全专家经验对当前的安全告警进行目的性确认，从而确认安全告警的优先级顺序，支持基于人工渗透、程序自动化、业务相关风险、其它 4 个维度对告警进行分类，帮助安全人员快速定位高危告警并及时处置；	4.支持威胁定性引擎以分析告警的上下文关联、时序关系、历史告警发生的频率规律性，结合威胁情报与安全专家经验对当前的安全告警进行目的性确认，从而确认安全告警的优先级顺序，支持基于人工渗透、程序自动化、业务相关风险、其它 4 个维度对告警进行分类，帮助安全人员快速定位高危告警并及时处置；	无偏离
		5.支持安全态势的可视化呈现，帮助客户更直观的看清风险、看懂威胁，产品内置（非自定义）综合态势大屏、分支安全态势、安全事件态势、全球网络攻击态势、资产态势、重大活动网络安全指挥调度大屏、设备运行态势、外联风险监控态势等不少于 15 块大屏展示界面证明；支持大屏轮播及自定义大屏顺序设置和轮播间隔设置，方便客户结合自身业务需求进行个性化设置；	5.支持安全态势的可视化呈现，帮助客户更直观的看清风险、看懂威胁，产品内置（非自定义）综合态势大屏、分支安全态势、安全事件态势、全球网络攻击态势、资产态势、重大活动网络安全指挥调度大屏、设备运行态势、外联风险监控态势等不少于 15 块大屏展示界面证明（详见 P1364-1372 页）；支持大屏轮播及自定义大屏顺序设置和轮播间隔设置，方便客户结合自身业务需求进行个性化设置；	无偏离
		6. 支持 PPT 格式导出摘要报告，报告内容包括：网络安全整体解读、网络安全风险详情、告警及事件响应盘点，用户可直接通过导出的 PPT 报告进行工作汇报，高效体现工作价值；	6. 支持 PPT 格式导出摘要报告，报告内容包括：网络安全整体解读、网络安全风险详情、告警及事件响应盘点，用户可直接通过导出的 PPT 报告进行工作汇报，高效体现工作价值；	无偏离
		7.支持可扩展通过网络侧（N）与终端侧（E）关联聚合，可以实现进程级取证，失陷主机定位更精准，并以可视化图谱直观清晰地展示出完整的攻击链，帮助用户快速找到症结，大幅提升事件检测、溯源取证、闭环处置效果；	7.支持可扩展通过网络侧（N）与终端侧（E）关联聚合，可以实现进程级取证，失陷主机定位更精准，并以可视化图谱直观清晰地展示出完整的攻击链，帮助用户快速找到症结，大幅提升事件检测、溯源取证、闭环处置效果；	无偏离

		8.为实现安全事件的快速闭环处置，要求支持与防火墙、行为管理、超融合、应用交付、网络控制器、端点安全管理系统等自有设备进行联动，实现效果包含联动封锁、访问控制、上网提醒、冻结账号、一键查杀等，并可联动超融合进行关机、挂起等；	8.为实现安全事件的快速闭环处置，要求支持与防火墙、行为管理、超融合、应用交付、网络控制器、端点安全管理系统等自有设备进行联动，实现效果包含联动封锁、访问控制、上网提醒、冻结账号、一键查杀等，并可联动超融合进行关机、挂起等；	无偏离
		9.支持可视化的形式展示威胁的影响面，通过大数据分析和关联检索技术，可清晰直观看清失陷主机对其他主机的影响，评估受损情况，方便客户快速处置。支持通过首页搜索框输入IP/域名/URL/端口/通信对进行搜索，支持入口点溯源功能，分析出首次失陷、疑似入口点、首次遭受攻击等信息，帮助管理人员快速找到攻击入口点；	9.支持可视化的形式展示威胁的影响面，通过大数据分析和关联检索技术，可清晰直观看清失陷主机对其他主机的影响，评估受损情况，方便客户快速处置。支持通过首页搜索框输入IP/域名/URL/端口/通信对进行搜索，支持入口点溯源功能，分析出首次失陷、疑似入口点、首次遭受攻击等信息，帮助管理人员快速找到攻击入口点；	无偏离
		10.支持实体行为分析功能，通过对这些对象进行持续的行为分析和行为画像构建，识别服务器异常，包括DGA解析请求、外联C&C服务器、异常协议利用、下载可疑文件、异常横向访问等；	10.支持实体行为分析功能，通过对这些对象进行持续的行为分析和行为画像构建，识别服务器异常，包括DGA解析请求、外联C&C服务器、异常协议利用、下载可疑文件、异常横向访问等；	无偏离
		11. 支持勒索专项检测页面，帮助组织更好的应对日益严峻的勒索风险，支持对勒索的安全告警进行统一展示和管理，支持以勒索病毒的感染途径/方式为维度进行分类，包括勒索常用端口、勒索常用漏洞、RDP爆破、感染勒索病毒、黑客勒索攻击、勒索C&C通信等维度，支持展示受害资产以及受害资产攻击数TOP5，支持以列表的形式展示勒索事件，包括最近发生时间、威胁描述、威胁定性、勒索风险、威胁等级、受害者IP、攻击次数等信息；	11. 支持勒索专项检测页面，帮助组织更好的应对日益严峻的勒索风险，支持对勒索的安全告警进行统一展示和管理，支持以勒索病毒的感染途径/方式为维度进行分类，包括勒索常用端口、勒索常用漏洞、RDP爆破、感染勒索病毒、黑客勒索攻击、勒索C&C通信等维度，支持展示受害资产以及受害资产攻击数TOP5，支持以列表的形式展示勒索事件，包括最近发生时间、威胁描述、威胁定性、勒索风险、威胁等级、受害者IP、攻击次数等信息；	无偏离
		12.支持5种类型日志传输模式，包含标准模式、精简模式、高级模式、局域网模式、自定义模式，适应不同应用场景需求。	12.支持5种类型日志传输模式，包含标准模式、精简模式、高级模式、局域网模式、自定义模式，适应不同应用场景需求。	无偏离

		13、支持基于 IP 和域名的旁路阻断，能够在实时镜像的流量中发现恶意 IP 并实现实时阻断，支持 24 小时/7 天/最近 30 天/永久或者自定义时间阻断威胁。	13、支持基于 IP 和域名的旁路阻断，能够在实时镜像的流量中发现恶意 IP 并实现实时阻断，支持 24 小时/7 天/最近 30 天/永久或者自定义时间阻断威胁。	无偏离
		14.支持标准端口运行非标准协议，非标准端口运行标准协议的异常流量检测，端口类型包括 3389、53、80/8080、21、69、443、25、110、143、22 等。	14.支持标准端口运行非标准协议，非标准端口运行标准协议的异常流量检测，端口类型包括 3389、53、80/8080、21、69、443、25、110、143、22 等。	无偏离
		15.支持 HTTP 未知站点下载可执行文件、浏览最近 30 天注册域名、浏览恶意动态域名、访问随机算法生成域名、暴力破解攻击、反弹连接、IRC 通信等僵尸网络行为检测。	15.支持 HTTP 未知站点下载可执行文件、浏览最近 30 天注册域名、浏览恶意动态域名、访问随机算法生成域名、暴力破解攻击、反弹连接、IRC 通信等僵尸网络行为检测。	无偏离
		16.具备报文检测引擎,可实现 IP 碎片重组、TCP 流重组、应用层协议识别与解析等；具备多种的入侵攻击模式或恶意 UR 监测模式，可完成模式匹配并生成事件，可提取 URL 记录和域名记录。	16.具备报文检测引擎,可实现 IP 碎片重组、TCP 流重组、应用层协议识别与解析等；具备多种的入侵攻击模式或恶意 UR 监测模式，可完成模式匹配并生成事件，可提取 URL 记录和域名记录。	无偏离
		17. 支持 Database 漏洞攻击、DNS 漏洞攻击、FTP 漏洞攻击、Mail 漏洞攻击、Network Device、Scan 漏洞攻击、System 漏洞攻击、Telnet 漏洞攻击、Tftp 漏洞攻击、Web 漏洞攻击等服务漏洞攻击检测。	17. 支持 Database 漏洞攻击、DNS 漏洞攻击、FTP 漏洞攻击、Mail 漏洞攻击、Network Device、Scan 漏洞攻击、System 漏洞攻击、Telnet 漏洞攻击、Tftp 漏洞攻击、Web 漏洞攻击等服务漏洞攻击检测。	无偏离
		18. 支持责任人管理功能，可对资产进行全生命周期管理，包括自动识别资产、入库审核、离线资产识别、自动识别资产退库、手动导入资产退库、自定义资产名称等。针对自动识别资产退库功能，可设置全局退库时间，数据更新时间。支持主机资产分级管理，责任人管理；	18. 支持责任人管理功能，可对资产进行全生命周期管理，包括自动识别资产、入库审核、离线资产识别、自动识别资产退库、手动导入资产退库、自定义资产名称等。针对自动识别资产退库功能，可设置全局退库时间，数据更新时间。支持主机资产分级管理，责任人管理；	无偏离
		19. 支持实体行为分析功能，通过对这些对象进行持续的行为分析和行为画像构建，识别服务器异常，包括 DGA 解析请求、外联 C&C 服务器、异常协议利用、下载可疑文件、异常横向访问等；	19. 支持实体行为分析功能，通过对这些对象进行持续的行为分析和行为画像构建，识别服务器异常，包括 DGA 解析请求、外联 C&C 服务器、异常协议利用、下载可疑文件、异常横向访问等；	无偏离

		20. 服务平台及配套探针具备服务期内规则库更新授权和能力，并支持与防火墙、终端安全产品进行联动封锁。	20. 服务平台及配套探针具备服务期内规则库更新授权和能力，并支持与防火墙、终端安全产品进行联动封锁。	无偏离
		21. 安全监测和运营服务交付成果：《分析与处置报告》、《安全运营报告》、《安全通告》等。	21. 安全监测和运营服务交付成果：《分析与处置报告》、《安全运营报告》、《安全通告》等。	无偏离
		八、防火墙服务	**八、我公司承诺提供以下防火墙服务**	无偏离
		1. 网络层吞吐量≥160G，应用层吞吐量≥100G，防病毒吞吐量≥20G，IPS 吞吐量≥22G，IPS+AV 吞吐量≥13G，并发连接数≥3000 万，HTTP 新建连接数≥75 万，IPSec VPN 最大接入数≥15000，IPSec VPN 吞吐量≥5G。开启入侵防御、防病毒、云端威胁情报、应用识别和管控、实时漏洞分析识别等功能模块。	1. 网络层吞吐量：160G，应用层吞吐量：100G，防病毒吞吐量：20G，IPS 吞吐量：22G，IPS+AV 吞吐量：13G，并发连接数：3000 万，HTTP 新建连接数：75 万，IPSec VPN 最大接入数：15000，IPSec VPN 吞吐量：5G。开启入侵防御、防病毒、云端威胁情报、应用识别和管控、实时漏洞分析识别等功能模块。	无偏离
		2. 规格 2U，内存大小≥64G，硬盘容量≥480G SSD+480G SSD，冗余电源，接口≥4 千兆电口+4 千兆光口 SFP+16 万兆光口 SFP+。提供三年软件升级和硬件维保。	2. 规格 2U，内存大小：64G，硬盘容量：480G SSD+480G SSD，冗余电源，接口：4 千兆电口+4 千兆光口 SFP+16 万兆光口 SFP+。提供三年软件升级和硬件维保。	无偏离
		3. 产品可扩展识别 IT、OT、IoT 混合资产，获取 IP、MAC、操作系统、类型、厂商等信息，终端类型包括但不限于：	3. 产品可扩展识别 IT、OT、IoT 混合资产，获取 IP、MAC、操作系统、类型、厂商等信息，终端类型包括但不限于：	无偏离
		（1）PC、瘦客户机、手机、平板、交换机、路由器、防火墙、无线控制器、服务器等 IT 资产	（1）PC、瘦客户机、手机、平板、交换机、路由器、防火墙、无线控制器、服务器等 IT 资产	无偏离
		（2）摄像头、门禁、打印机、投影仪、VOIP 设备、条形码扫描仪、医学图像打印机、呼吸机、心电图仪、监护仪、放射系统等 IoT 资产	（2）摄像头、门禁、打印机、投影仪、VOIP 设备、条形码扫描仪、医学图像打印机、呼吸机、心电图仪、监护仪、放射系统等 IoT 资产	无偏离
		4. 产品支持云威胁情报网关技术，通过全球超过 30+pop 节点，实现对威胁流量就近进行实时检测&拦截，实现失陷外联实时阻断，支持云端未知威胁主动探测技术，实现 5min 内未知威胁情报全网设备下发。	4. 产品支持云威胁情报网关技术，通过全球超过 30+pop 节点，实现对威胁流量就近进行实时检测&拦截，实现失陷外联实时阻断，支持云端未知威胁主动探测技术，实现 5min 内未知威胁情报全网设备下发。	无偏离
		5. 产品支持对压缩病毒文件进行	5. 产品支持对压缩病毒文件进行	无偏离

		检测和拦截，压缩层数支持 15 层及以上；	检测和拦截，压缩层数支持 15 层及以上；	
		6.产品支持用户账号全生命周期保护功能，包括用户账号多余入口检测、用户账号弱口令检测、用户账号暴力破解检测、失陷账号检测，防止因账号被暴力破解导致的非法提权情况发生；	6.产品支持用户账号全生命周期保护功能，包括用户账号多余入口检测、用户账号弱口令检测、用户账号暴力破解检测、失陷账号检测，防止因账号被暴力破解导致的非法提权情况发生；	无偏离
		7.产品可扩展主动诱捕功能，通过伪装业务诱捕内外网的攻击行为，并联合云蜜罐获取黑客指纹信息，并自动封锁高危 IP；	7.产品可扩展主动诱捕功能，通过伪装业务诱捕内外网的攻击行为，并联合云蜜罐获取黑客指纹信息，并自动封锁高危 IP；	无偏离
		8.产品支持策略生命周期管理功能，支持对安全策略修改的时间、变更类型进行统一管理，便于策略的运维与管理。	8.产品支持策略生命周期管理功能，支持对安全策略修改的时间、变更类型进行统一管理，便于策略的运维与管理。	无偏离
		（九）IPS 服务	（九）我公司承诺提供以下 IPS 服务	无偏离
		.网络层吞吐量≥160G，应用层吞吐量≥100G，防病毒吞吐量≥20G，IPS 吞吐量≥22G，IPS+AV 吞吐量≥13G，并发连接数≥3000 万，HTTP 新建连接数≥75 万，IPSec VPN 最大接入数≥15000，IPSec VPN 吞吐量≥5G。开启入侵防御、应用识别和管控、实时漏洞分析识别等功能模块。	.网络层吞吐量：160G，应用层吞吐量：100G，防病毒吞吐量：20G，IPS 吞吐量：22G，IPS+AV 吞吐量：13G，并发连接数：3000 万，HTTP 新建连接数：75 万，IPSec VPN 最大接入数：15000，IPSec VPN 吞吐量：5G。开启入侵防御、应用识别和管控、实时漏洞分析识别等功能模块。	无偏离
		2.规格 2U，内存大小≥64G，硬盘容量≥480G SSD+480G SSD，冗余电源，接口≥4 千兆电口+4 千兆光口 SFP+16 万兆光口 SFP+。提供三年软件升级和硬件维保。	2.规格 2U，内存大小：64G，硬盘容量：480G SSD+480G SSD，冗余电源，接口：4 千兆电口+4 千兆光口 SFP+16 万兆光口 SFP+。提供三年软件升级和硬件维保。	无偏离
		3.产品内置不低于 16000 种漏洞规则，同时支持在控制台界面通过漏洞 ID、漏洞名称、危险等级、漏洞 CVE 标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义 IPS 规则。	3.产品内置 16000 种漏洞规则，同时支持在控制台界面通过漏洞 ID、漏洞名称、危险等级、漏洞 CVE 标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义 IPS 规则。	无偏离
		4.产品可扩展云威胁情报网关技术，通过全球超过 30+pop 节点，实现对威胁流量就近进行实时检测&拦截，实现失陷外联实时阻断，支持云端未知威胁主动探测技术，实现 5min 内未知威胁情报	4.产品可扩展云威胁情报网关技术，通过全球超过 30+pop 节点，实现对威胁流量就近进行实时检测&拦截，实现失陷外联实时阻断，支持云端未知威胁主动探测技术，实现 5min 内未知威胁情报	无偏离

		全网设备下发。	全网设备下发。	
		5.产品支持僵尸主机检测功能，产品内置僵尸网络特征库超过128万种，可识别主机的异常外联行为。	5.产品支持僵尸主机检测功能，产品内置僵尸网络特征库超过128万种，可识别主机的异常外联行为。	无偏离
		6.产品支持用户账号全生命周期保护功能，包括用户账号多余入口检测、用户账号弱口令检测、用户账号暴力破解检测、失陷账号检测，防止因账号被暴力破解导致的非法提权情况发生；	6.产品支持用户账号全生命周期保护功能，包括用户账号多余入口检测、用户账号弱口令检测、用户账号暴力破解检测、失陷账号检测，防止因账号被暴力破解导致的非法提权情况发生；	无偏离
		7.产品可扩展主动诱捕功能，通过伪装业务诱捕内外网的攻击行为，并联合云蜜罐获取黑客指纹信息，并自动封锁高危IP；	7.产品可扩展主动诱捕功能，通过伪装业务诱捕内外网的攻击行为，并联合云蜜罐获取黑客指纹信息，并自动封锁高危IP；	无偏离
		8.产品支持策略生命周期管理功能，支持对安全策略修改的时间、变更类型进行统一管理，便于策略的运维与管理。	8.产品支持策略生命周期管理功能，支持对安全策略修改的时间、变更类型进行统一管理，便于策略的运维与管理。	无偏离
		（十）新系统上线评估服务	**（十）我公司承诺提供以下新系统上线评估服务**	无偏离
		1.服务内容：对人社厅新上线系统、重大版本变动后的业务系统进行上线前的安全评估，以发现新上线业务系统可能存在风险，防止系统带病上线。新系统上线安全评估内容主要包括安全漏洞扫描、安全配置核查、人工渗透测试等三部分内容：	1.服务内容：对人社厅新上线系统、重大版本变动后的业务系统进行上线前的安全评估，以发现新上线业务系统可能存在风险，防止系统带病上线。新系统上线安全评估内容主要包括安全漏洞扫描、安全配置核查、人工渗透测试等三部分内容：	无偏离
		2.安全漏洞扫描：利用漏洞扫描设备对涉及系统的主机操作系统、数据库、应用中间件等进行漏洞检测，以发现已暴露的安全风险漏洞，并出具漏洞扫描检测报告，提供整改建议。	2.安全漏洞扫描：利用漏洞扫描设备对涉及系统的主机操作系统、数据库、应用中间件等进行漏洞检测，以发现已暴露的安全风险漏洞，并出具漏洞扫描检测报告，提供整改建议。	无偏离
		3.安全配置核查：依据安全通用基线标准与等级保护要求，对涉及信息系统的主机操作系统、应用中间件、数据库等进行安全基线检查，并出具安全基线核查报告与整改建议。使业务系统的安全基线处于较高标准之上。	3.安全配置核查：依据安全通用基线标准与等级保护要求，对涉及信息系统的主机操作系统、应用中间件、数据库等进行安全基线检查，并出具安全基线核查报告与整改建议。使业务系统的安全基线处于较高标准之上。	无偏离

		4.人工渗透测试：模拟入侵者对系统WEB应用进行攻击测试，在对现有信息系统不造成任何损害的前提下，从攻击者的角度来对主机系统的安全程度进行安全性评估。根据业务实际部署情况，可通过“黑盒”或“白盒”方式进行测试，测试方法不限于信息收集、端口扫描、远程溢出、口令猜测、本地溢出、客户端攻击、中间人攻击、web脚本渗透等，出具渗透测试与整改建议报告。	4.人工渗透测试：模拟入侵者对系统WEB应用进行攻击测试，在对现有信息系统不造成任何损害的前提下，从攻击者的角度来对主机系统的安全程度进行安全性评估。根据业务实际部署情况，可通过“黑盒”或“白盒”方式进行测试，测试方法不限于信息收集、端口扫描、远程溢出、口令猜测、本地溢出、客户端攻击、中间人攻击、web脚本渗透等，出具渗透测试与整改建议报告。	无偏离
		▲5.服务范围：广西人社厅范围内所辖信息系统，包括但不限于广西“数智人社”信息系统，以人社云承载的应用系统为重点测试对象。	▲5.服务范围：广西人社厅范围内所辖信息系统，包括但不限于广西“数智人社”信息系统，以人社云承载的应用系统为重点测试对象。	无偏离
		6.服务频率：服务期内按实际需要开展。	6.服务频率：服务期内按实际需要开展。	无偏离
		7.服务交付物：《新系统上线安全评估报告》。	7.服务交付物：《新系统上线安全评估报告》。	无偏离
		（十一）数据安全风险评估服务	**（十一）我公司承诺提供以下数据安全风险评估服务**	无偏离
		1.通过业务系统基本情况梳理，分析业务流程、业务依赖关系、系统交互过程、数据流转情况等业务系统基本信息，提炼业务场景特性，归纳数据全生命周期处理情况，为全面识别数据安全风险提供依据。服务次数：1次，输出《业务数据处理活动建模》。	1.通过业务系统基本情况梳理，分析业务流程、业务依赖关系、系统交互过程、数据流转情况等业务系统基本信息，提炼业务场景特性，归纳数据全生命周期处理情况，为全面识别数据安全风险提供依据。服务次数：1次，输出《业务数据处理活动建模》。	无偏离
		2.数据安全风险评估方案设计：通过现场调研和技术评估相结合的方式设计数据安全风险评估方案、方法和流程，对单位数据运行现状开展全面风险评估，了解数据管理相关控制的存在性及有效性，评估分析数据安全整体面上和点上的安全风险，最终形成一致的风险计算规则，为招标人构建持续的风险评估机制。服务次数：1次，输出《数据安全风险评估指南》。	2.数据安全风险评估方案设计：通过现场调研和技术评估相结合的方式设计数据安全风险评估方案、方法和流程，对单位数据运行现状开展全面风险评估，了解数据管理相关控制的存在性及有效性，评估分析数据安全整体面上和点上的安全风险，最终形成一致的风险计算规则，为招标人构建持续的风险评估机制。服务次数：1次，输出《数据安全风险评估指南》。	无偏离

		▲3.数据安全风险评估实施：对业务及数据应用过程中的安全风险进行分析及评估，确定主要的数据安全风险。服务次数：1次，输出《业务系统数据安全风险评估报告》	▲3.数据安全风险评估实施：对业务及数据应用过程中的安全风险进行分析及评估，确定主要的数据安全风险。服务次数：1次，输出《业务系统数据安全风险评估报告》	无偏离
		4.服务范围：	4.服务范围：	无偏离
		本次数据安全评估服务范围，对象为1个重要核心业务系统。	本次数据安全评估服务范围，对象为1个重要核心业务系统。	无偏离

注：

1.说明：应对照招标文件“第二章 采购需求”中的技术要求逐条作明确的投标响应，并作出偏离说明。

2.投标人应根据自身的承诺，对照招标文件要求，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**”。

法定代表人或者委托代理人（签字或者盖章或者电子签名）：

投标人名称（电子签章）：中国—东盟信息港股份有限公司

日　　期：2026年6月17日