合 同 书

项目名称：国家税务总局青岛市税务局
2026年网络安全服务项目

包　　号：/

合同编号：HYHAQDFGS2026-0011

甲　　方：国家税务总局青岛市税务局

乙　　方：青岛中数智慧科技有限公司

日　　期：2026 年 6 月 6 日

合同条款前附表

序号	内容		
1	合同名称		国家税务总局青岛市税务局2026年网络安全服务项目
2	合同编号		HYHAQDFGS2026-0011
3	合同类型		服务类合同
4	定价方式		公开招标
5	甲方名称		国家税务总局青岛市税务局
	甲方地址		青岛市市南区延安三路236号
	甲方相关部门	甲方采购部门	国家税务总局青岛市税务局财务管理处（装备和采购处）
		联系人	刘晓庆
		联系电话	0532-83931235
		甲方需求部门	国家税务总局青岛市税务局信息中心
		联系人	赵宇鑫
		联系电话	0532-83931282
6	乙方名称		青岛中数智慧科技有限公司
	乙方企业性质		☐ 中型企业 ☑ 小型企业 ☐ 微型企业 ☐ 监狱企业 ☐ 残疾人福利性单位 ☐ 其他
	乙方地址		青岛市崂山区海尔路182号出版大厦3号楼1802-B4
	乙方联系人		刘致宏
	联系电话		0532-66063025
	乙方开户行		
	乙方银行账号		
7	合同金额		人民币贰佰陆拾壹万陆仟捌佰元整（¥2616800.00）。
8	服务内容		本合同服务内容为：本项目乙方采取驻场服务的方式为甲方提供网络安全技术支持服务，并提供软硬件产品维保服务。 1.采购不少于5人1年驻场技术支持服务：主要提供对总局安全管理平台等系统的运维服务、常态化安全运营服务，及时监测、分析、处

<table>
<tr><td>序号</td><td colspan="3">内　　容</td></tr>
<tr><td></td><td></td><td colspan="2">置安全事件，妥善应对安全威胁和告警，并开展基础的技术保障工作。
提供对青岛市税务局网络安全系统的运维服务，及时监测、分析、处置安全事件，妥善应对安全威胁和告警，并开展基础的技术保障工作。
驻场技术支持信息如下：
<table>
<tr><td>序号</td><td>驻场技术支持</td><td>计划运维期限</td><td>人员数量</td></tr>
<tr><td>1</td><td>总局安管平台驻场运维服务</td><td>2026.6.6-
2027.6.5</td><td>1名</td></tr>
<tr><td>2</td><td>驻场运维服务</td><td>2026.6.6-
2027.6.5</td><td>4名（不低于中级，高级至少2名）</td></tr>
</table>
提供对青岛市税务局网络安全系统的运维服务，及时监测、分析、处置安全事件，妥善应对安全威胁和告警，并开展基础的技术保障工作。
相关产品信息如下：
<table>
<tr><td>序号</td><td>相关系统</td><td>品牌</td><td>设备数量</td></tr>
<tr><td>1</td><td>泰合SOC（安全管理平台）</td><td>启明星辰</td><td>1台</td></tr>
<tr><td>2</td><td>360终端安全管理软件</td><td>360</td><td>1套</td></tr>
<tr><td>3</td><td>iNode内网端点准入系统</td><td>新华三</td><td>4台</td></tr>
<tr><td>4</td><td>总局安全管理平台</td><td>360、国富瑞</td><td>1套</td></tr>
<tr><td>5</td><td>天融信态势感知平台</td><td>天融信</td><td>1套</td></tr>
</table>
2.采购网络安全技术支持服务：内网资产梳理服务、服务器安全加固服务、终端安全管理运维服务、iNode巡检维护及应急保障服务、泰合SOC（网络安全管理平台）运维服务、互联网应用系统云安全监测服务、互联网资产测绘及发现服务、互联网终端安全加固服务、网络和数据安全检查技术支撑服务、互联网众测服务、敏感信息筛查服务、漏洞扫描服务、渗透测试服务、配置核查服务、弱口令筛查服务、系统上</td></tr>
</table>

序号	内　　容	
		线前检测服务、移动 APP 安全检测服务、应用程序编程接口安全检测服务、软件全生命周期安全管理咨询服务、总局安管平台深化应用服务、应急演练及应急处置服务、网络安全意识提升服务、供应链合规管理服务、日志审计服务、Web 动态应用保护系统扩容授权服务等。 3. 采购 1 年软硬件产品维保服务：用于保障以往网络安全项目已采购的 iNode 内网端点准入系统、天融信僵尸网络木马和蠕虫监测与处置系统和天融信 Web 应用安全防护系统的正常使用和持续升级。
9	合同付款	本项目服务期满经验收合格，根据验收结果和对乙方服务的评定结果，甲方收到乙方提供的合格发票后，10 个工作日内据实向乙方支付。
10	履约保证金及返还	☑本项目不要求提供履约保证金。 □本项目要求提供履约保证金。履约保证金为合同总金额的　　%，即人民币　　元整（¥　　），乙方应在合同签订之日起 30 日内提交甲方。提交方式为银行电汇、金融机构或担保机构出具的保函。在合同履行期满，扣除应扣除的款项（如有）且双方无争议后，无息返还。 办理返还履约保证金时，乙方应提供履约保证金返还申请（格式另附）、合同或合同关键页复印件、合同约定的其他资料。涉及验收的，应同时提交甲方需求部门出具的项目终验意见或质量保证期（服务期）满验收意见。 满足履约保证金返还条件的，甲方在收到返还相关信息等合同约定资料后，进行核实。对核实结果无异议的，自完成核实之日起 30 日内，以　　方式返还履约保证金或退回保函。
11	合同履行期限	自合同签订之日起至合同全部权利义务履行完毕之日止
12	服务期限	2026 年 6 月 6 日至 2027 年 6 月 5 日。
13	合同履约地点	合同约定地点或甲方指定地点

一 合 同

国家税务总局青岛市税务局（以下简称“甲方”）通过公开招标方式采购，确定青岛中数智慧科技有限公司（以下简称“乙方”）为《国家税务总局青岛市税务局2026年网络安全服务项目》中标（成交）供应商。甲乙双方同意按照该项目招标（采购）文件约定的内容，签署《国家税务总局青岛市税务局2026年网络安全服务项目合同书》（合同编号：HYHAQDFGS2026-0011，以下简称“合同”）。

1. 合同文件

本合同所附下列文件是构成本合同不可分割的部分：

（1）合同条款前附表；合同通用条款；附件

（2）报价表（总报价表和分项报价表）；

（3）招标（采购）文件；

（4）投标（响应）文件。

2. 合同范围和条件

本合同的范围和条件应与上述合同文件的规定相一致。

3. 合同金额

本合同金额为人民币贰佰陆拾壹万陆仟捌佰元整（¥2616800.00）。本合同项下所有服务的全部人工费、交通费、管理费、税费及其他不可预见的费用等均已包含于合同价中，甲方不再另行支付其他任何费用。

4. 付款条件

本项目服务期满经验收合格，根据验收结果和对乙方服务的评定结果，甲方收到乙方提供的合格发票后，10个工作日内据实向乙方支付。

在服务过程中若乙方出现服务成果未满足甲方要求，出现违反合同约定或服务评定扣除项或造成损失或违约的，则甲方在付款时按照合同对应约定扣除相应金额。

办理付款时，乙方应提供发票、付款申请（格式另附）、合同或合同关键页复印件、合同约定的其他资料。涉及验收的，应同时提交甲方需求部门出具的验收意见。若乙方不能按照甲方要求提供上述发票等资料或提供的资料不适用，则甲方有权拒绝付款且不承担任何违约责任。

5. 合同签订及生效

本合同一式陆份，由甲乙双方法定代表人或被授权人签字并盖章后生效。

乙方由法定代表人签订合同的，应提供法定代表人身份证复印件；乙方由被授权人签订合同的，应提供授权委托书和法定代表人及被授权人身份证复印件。

甲方：国家税务总局青岛市税务局

签字：

签字或印章：

日期：2026年6月6日

乙方：青岛中数智慧科技有限公司

签字：

签字或印章：

日期：2026年6月6日

二 合同通用条款

1. 定义

本合同下列术语应解释为：

1.1“甲方”是指国家税务总局青岛市税务局。

1.1.1“甲方采购部门”见“合同条款前附表”第5项“甲方采购部门”。

1.1.2“甲方需求部门”见“合同条款前附表”第5项“甲方需求部门”。

1.2“乙方”见“合同条款前附表”第6项“乙方名称”。

1.3 “合同”系指甲乙双方签订的、合同格式中载明的甲乙双方所达成的合同，包括所有的附件、附录和上述文件所提到的构成合同的所有文件。

1.4 “天”除非特别指出，“天”均为自然天。

2. 标准

2.1 乙方为甲方交付或提供的服务应符合招标（采购）文件所述的标准，如果没有提及适用标准，则应符合相应的国家标准。这些标准必须是有关机构发布的最新版本的标准。

2.2 除非技术要求中另有规定，计量单位均采用中华人民共和国法定计量单位。

3. 服务

3.1 本项目的“服务”见“合同条款前附表”第8项“服务内容”及“附件”。

3.2 乙方应保证所提供的服务符合合同规定的技术要求。如不符时，乙方应负全责并尽快处理解决，由此造成的损失和相关费用由乙方负责，甲方保留终止合同及索赔的权利。

3.3 乙方应保证通过执行合同中全部方案后，可以取得本合同约定的结果，达到本合同约定的预期目标。对任何情况下出现的问题，应尽快提出解决方案。

3.4 如果乙方提供的服务和解决方案不符合甲方要求，或在规定的时间内没有弥补缺陷，甲方有权采取一切必要的补救措施，由此产生的费用全部由乙方负责。

3.5 除合同条款另行规定外，伴随服务的费用应含在合同价中，不单独进行支付。

4. 知识产权

4.1 乙方应保证所提供的服务免受第三方提出侵犯其知识产权（专利权、商标权、软件著作权、版权等）的起诉。

4.2 甲方对项目实施过程中所产生的所有成果（包括发明、发现、可运行系统、源代码及相关技术资料、文档等）享有永久使用权、复制权和修改权，其专利申请权、专利权、软件著作权、技术秘密的所有权、使用权、转让权等知识产权归甲方所有。

4.3 乙方不得利用本项目实施过程中所产生的成果（包括发明、发现、可运行系统、源代码及相关技术资料、文档等），另行自行开发本合同业务范围内供纳税人缴费人使用的软件或产品，不得利用开发便利变相收费或搭车收费。

5. 保密条款

5.1 甲乙双方应对在本合同签订或履行过程中所接触的对方信息，包括但不限于知识产权、技术资料、技术诀窍、内部管理及其他相关信息，负有保密义务。

5.2 乙方在使用甲方为乙方及其工作人员提供的数据、程序、用户名、口令、资料及甲方相关的业务和技术文档，包括税收政策、方案设计细节、程序文件、数据结构，以及相关业务系统的软硬件、文档、测试和测试产生的数据时，应遵循以下规定：

（1） 应以审慎态度避免泄漏、公开或传播甲方的信息；

（2） 在开发过程中对数据的处理方式应事先得到甲方的许可；

（3） 未经甲方书面许可，不得对有关信息进行修改、补充、复制；

（4） 未经甲方书面许可，不得将信息以任何方式（如E-mail）携带出甲方场所；

（5） 未经甲方书面许可，不得将信息透露给任何其他人；

（6） 严禁在提交的软件产品中设置远程维护接口和后门程序；

（7） 不得进行系统软硬件设备的远程维护；

（8） 甲方以书面形式提出的其他保密措施。

5.3 保密期限不受合同有效期的限制，在合同有效期结束后，信息接受方仍应承担保密义务，直至该等信息成为公开信息。

5.4 甲乙双方如出现泄密行为，泄密方应承担相关的法律责任，包括但是不限于对由此给对方造成的经济损失进行赔偿。

6. 履约验收要求

6.1 甲方需求部门严格按照采购合同开展履约验收。验收时，应当按照本合同约定的技术、服务和安全标准，对供应商各项义务履行情况进行验收确认。未约定相关标准的，应当按照国家强制性规定、政策要求、安全标准和行业有关标准进行验收确认。验收结束后，应当出具验收意见，列明合同事项、验收标准及验收情况，由全体验收人员签字。

6.2 具体履约验收要求详见招标（采购）文件。

7. 履约保证金

7.1 需提交履约保证金的项目，乙方应按照“合同条款前附表”第 10 项“履约保证金及返还”提交履约保证金。

7.2 履约保证金的金额可用于补偿甲方因乙方不能完成其合同义务而蒙受的损失。

7.3 如乙方未能按时支付合同约定的违约金、赔偿金、其他应付款项等的，甲方有权按照本合同的约定从履约保证金中扣除上述款项。乙方应在甲方扣除履约保证金后 15 天内，及时补充扣除部分金额。若逾期补充的，每日应按应补充金额的万分之五（0.05%）支付甲方违约金。

7.4 乙方不履行合同、或者履行合同义务不符合约定使得合同目的不能实现，履约保证金不予退还，给甲方造成的损失超过履约保证金数额的，还应当对超过部分予以赔偿。

7.5 履约保证金在合同履行期满后，扣除相应款项（如有）且双方无争议后，凭返还申请等资料一次性无息返还，详见“合同条款前附表”第 10 项“履约保证金及返还”。

8. 履约延误

8.1 乙方应按照本合同的规定提供服务。

8.2 如乙方迟延履行合同义务，甲方将从应付合同金额中扣除误期违约金，每延误一天误期违约金按合同总金额的万分之三（0.03%）计收。乙方支付的误期违约金不足以弥补甲方损失的，应继续承担赔偿责任。本合同约定的损失，包括但不限于：直接损失、调查取证费、诉讼费、律师费等。

8.3 在履行合同过程中，如果乙方可能遇到妨碍按时提供服务的情况时，应

及时以书面形式将拖延的事实，可能拖延的期限和理由通知甲方。甲方在收到乙方通知后，应尽快对情况进行评估，并确定是否酌情延长工期以及是否收取误期赔偿费。

8.4 除不可抗力和根据合同规定延期取得甲方同意而不收取误期赔偿费之外，乙方延误工期，将按合同规定被收取误期赔偿费。

8.5 逾期退还履约保证金的违约责任。满足履约保证金返还条件的，甲方在收到返还相关信息等合同约定资料后，进行核实。对核实结果无异议的，应当自完成核实之日起30日内返还履约保证金。无特殊原因逾期退还履约保证金的，乙方可要求甲方按银行同期活期存款利率支付逾期利息。特殊原因逾期返还的，双方协商解决。

9. 违约责任

9.1 除本合同另有约定外，乙方不履行合同义务或者履行合同义务不符合合同约定的，按每违反一次从应付款项中扣除合同总金额的百分之一（1%）作为违约金；此外，应当承担继续履行、采取补救措施或者赔偿损失等违约责任。乙方支付的上述违约金、赔偿金等不足以弥补甲方损失的，应继续承担赔偿责任。本合同约定的损失，包括但不限于：直接损失、调查取证费、诉讼费、律师费等。

9.2 乙方没有按照时限要求提供服务，且在甲方指定的延长期限内没有采取补救措施，甲方有权自行采取其他方式进行补救，乙方除按合同第8条约定向甲方支付误期违约金外，另外甲方所发生的一切费用和甲方损失，甲方有权从应付的乙方的合同款项中扣除，不足扣除的乙方应另行支付。

9.3 除应支付甲方违约金等外，甲方有权根据合同或有关部门出具的检验证书向乙方提出索赔。

9.4 如果乙方对差异负有责任而甲方提出索赔，乙方同意按照下列方式解决索赔事宜：

如果在甲方发出索赔通知后5个工作日内，乙方未作书面答复，上述索赔应视为已被乙方接受。如乙方未能在甲方发出索赔通知后5个工作日内或甲方同意的延长期限内着手解决索赔事宜，甲方有权从乙方的合同款项中扣除索赔金额。

9.5 乙方利用本项目实施过程中所产生的成果（包括发明、发现、可运行系统、源代码及相关技术资料、文档等），另行自行开发本合同业务范围内供纳税人

缴费人使用的软件或产品，或利用为税务机关提供信息化服务的便利，向纳税人缴费人搭车收费或变相收费的，或有其他失信行为的，纳入国家税务总局失信名单。

对于影响恶劣的严重违法失信行为，推送财政部纳入政府采购严重违法失信行为记录名单。

9.6 如果乙方在本项目实施过程中发生违反网络安全规定行为造成不良后果的，自甲方做出认定之日起三年内，税务系统各单位可以拒绝乙方参与税务系统政府采购活动。

不良后果指造成数据失窃或丢失、敏感信息泄露、主要业务系统瘫痪等网络安全事件。

9.7乙方在本项目实施过程中发生违反网络安全规定行为，造成数据失窃或丢失，敏感信息泄露，主要业务系统瘫痪等不良后果的，自甲方或甲方主管机关做出认定之日起三年内，税务系统各单位可以拒绝乙方参加税务系统政府采购活动。

9.8乙方利用在本项目为税务机关提供信息化货物和服务的便利，向纳税人缴费人搭车收费或变相收费的，或另行开发合同业务需求范围内，供纳税人、缴费人使用的软件等其他失信行为的，纳入国家税务总局失信名单。对于影响恶劣的严重违法失信行为，推送财政部纳入政府采购严重违法失信行为记录名单。

9.9乙方应建立防止违法违规聘用离职税务人员风险控制制度，如乙方未建立上述风险防控制度，甲方有权要求乙方限期改正。对出现违法违规聘用离职税务人员行为将采取限期更正、要求支付违约金、解除合同、3年内限制参加所聘原单位及下属单位信息化政府采购活动等。

9.10服务商（乙方）不得以获取不正当利益为目的，采取馈赠礼品礼金、邀请娱乐旅游服务、提供便利条件等非正当手段交往相关税务人员及亲属。

9.11服务商（乙方）须严格按照国家税务总局青岛市税务局相关要求落实供应链安全管理各项规定，包括按照国家相关法律法规开展的安全审查、安全评估、渗透测试等，落实情况作为项目验收的检查内容。

服务商（乙方）对供应链安全管理责任落实不到位，造成安全事件或产生不良影响的，甲方按照法律法规及合同约定进行处理。

9.12服务商（乙方）供应清单内的产品需具备销售许可并满足国家认可的网络安全规范和认证要求；服务商（乙方）需签订《税务信息化供应链安全承诺书》；服务商（乙方）需配合甲方落实供应链安全管理的要求，落实情况将作为项目验收的检查内容。如合同期间服务商（乙方）因违反甲方供应链安全管理要求造成甲方被总局通报批评或绩效考核扣分的，甲方有权根据事件程度，按次扣除合同金额的5%-20%。

9.13如因特殊原因造成本项目下一服务期与本次采购合同期存在时间空档的情况，本次乙方应提供继续该项目服务工作（费用已含在投标报价中），直至新服务合同生效为止。

9.14因国家政策重大调整、系统重大变更或不可抗力等因素，甲方有权根据实际情况调整服务期限及相关合同内容，并按照调整后的实际工作量结算费用，乙方应积极配合，甲方不承担任何责任。

9.15对于本合同未约定的、招标（采购）文件（技术部分）中约定的违约处理条款，按招标（采购）文件（技术部分）相关约定执行；对本合同与招标（采购）文件（技术部分）约定不同的违约处理条款，以本合同约定为准。

10. 不可抗力

10.1 本条所述的“不可抗力”系指双方不可预见、不可避免、不可克服的客观情况，但不包括双方的违约或疏忽。这些事件包括但不限于：战争、严重火灾、洪水、台风、地震等。

10.2 如果乙方因不可抗力而导致合同实施延误或不能履行合同义务，不应承担误期赔偿或终止合同的责任。

10.3 在不可抗力事件发生后，当事方应及时将不可抗力情况通知合同对方，在不可抗力事件结束后3日内以书面形式将不可抗力的情况和原因通知合同对方，并提供相应的证明文件。合同各方应尽可能继续履行合同义务，并积极寻求采取合理的措施履行不受不可抗力影响的其他事项。合同各方应通过友好协商在合理的时间内达成进一步履行的协议。

10.4 如因国家政策变化、技术实施所需的客观环境发生变化、重大技术变化、国家调减预算、乙方在执行合同的过程中发生对履行合同有直接影响的重大事故或变故、甲方工作计划调整及推广使用新应用系统导致本项目相关服务停止等原

因，本合同不能继续全部或部分履行，甲方有权通知乙方解除本合同的全部或部分，双方将按已经实际履行并验收合格的合同内容进行结算。

11. 争端的解决

11.1 甲乙双方应首先通过友好协商解决在执行本合同中所发生的或与本合同有关的一切争端。如从协商开始30天内仍不能解决，可以按合同约定的方式提起仲裁或诉讼。

11.2.1 仲裁应向甲方所在地或青岛市仲裁委员会申请仲裁。

11.2.2 仲裁裁决应为最终裁决，对双方均具有约束力。

11.2.3 仲裁费除仲裁机关另有裁决外应由败诉方负担。

11.2.4 在仲裁期间，除正在进行仲裁部分外，本合同的其它部分应继续执行。

11.3.1 诉讼应向甲方所在地人民法院提起诉讼。

11.3.2 诉讼费除人民法院另有判决外，应由败诉方负担。

11.3.3 在诉讼期间，除正在进行诉讼部分外，本合同的其它部分应继续执行。

12. 违约终止合同

12.1 若出现如下情况，在甲方对乙方违约行为而采取的任何补救措施不受影响的情况下，甲方可向乙方发出书面通知书，提出解除部分或全部合同。自甲方发出书面通知书之日起30日内，乙方应支付甲方合同总金额20%的违约金，并根据合同执行情况返还部分或全部已收取款项。乙方支付的违约金不足以弥补甲方损失的，应继续承担赔偿责任。本合同约定的损失，包括但不限于：直接损失、调查取证费、诉讼费、律师费等。

12.1.1 乙方不履行合同业务或者履行合同义务不符合合同约定；

12.1.2 如果乙方未能在合同规定的期限或甲方同意延长的期限内提供服务；

12.1.3 因乙方人员自身技术能力、经验不足等问题造成甲方发生重大紧急故障，带来重大影响和损失的；

12.1.4 乙方对重大紧急故障没有及时响应，或不能在规定时间内解决处理故障、恢复正常运行的；

12.1.5 不能满足本项目技术需求的管理要求和规范，且经多次整改无明显改进的；

12.1.6 在合同服务期内，同一个应用系统在升级完善、运行维护支持服务过

程中，出现5次经甲乙双方确认的用户投诉的；

12.1.7 乙方利用本项目实施过程中所产生的成果（包括发明、发现、可运行系统、源代码及相关技术资料、文档等），另行自行开发本合同业务范围内供纳税人缴费人使用的软件或产品的，或利用为税务机关提供信息化服务的便利，向纳税人缴费人搭车收费或变相收费的，或有其他失信行为的；

12.1.8 乙方在本项目实施过程中发生违反网络安全规定行为造成不良后果的。

12.1.9 乙方提供的服务侵犯甲方、第三方知识产权等合法权益的；

12.1.10 乙方或乙方人员造成甲方或第三方经济损失而拒不赔偿的；

12.1.11 乙方转让其应履行的合同义务，或未经甲方同意采取分包方式履行合同的；

12.1.12 乙方有其他严重违约行为的。

12.2 如果甲方根据上述第12.1条的规定，终止了全部或部分合同，甲方可以适当的条件和方法购买乙方未能提供的服务，乙方应对甲方购买类似服务所超出的费用负责。同时，乙方应继续执行合同中未终止的部分。

13. 破产终止合同

13.1 如果乙方破产或无清偿能力，甲方可在任何时候以书面形式通知乙方终止合同而不给乙方补偿。

13.2 该终止合同将不损害或影响甲方已经采取或将要采取的任何行动或补救措施的权力。

14. 其他情况的终止合同

14.1 乙方在执行合同的过程中发生重大事故或变故，对履行合同有直接影响的，甲方可以提出终止合同而不给予乙方任何补偿。

14.2 在服务期内，由于甲方工作计划调整，推广使用新应用系统导致本项目相关服务停止的，甲方可以提出终止合同而不给予乙方任何补偿。

15. 合同修改或变更

15.1 合同如有未尽事宜，须经甲乙双方共同协商，做出补充约定，并签订书面补充合同或变更协议。补充合同或变更协议作为本合同的一部分，与本合同具有同等效力。

15.2 除了双方签署书面修改或变更协议，并成为本合同不可分割的一部分的情况之外，本合同的条款不得有任何变化或修改。

15.3 由于甲方项目统一规划等原因导致本项目停止部分服务的，甲方将启动合同变更程序，与乙方协商变更相关合同条款。

16. 转让和分包

16.1 除甲方事先书面同意外，乙方不得部分转让或全部转让其应履行的合同义务。

16.2 未经甲方同意，乙方不得采取分包方式履行合同。经甲方同意分包履行合同的，乙方就采购项目及分包项目向甲方负责，分包供应商就分包项目承担责任。

17. 合同语言

17.1 本合同语言为中文。

17.2 双方交换的与合同有关的信件和其他文件应用合同语言书写。

18. 适用法律

18.1 本合同按照中华人民共和国现行法律进行解释。

18.2 本合同的履行、违约责任和解决争议的方法等适用《中华人民共和国民法典（合同编）》。

19. 税费

19.1 合同服务的所有税费均已包含于合同价中，甲方不再另行支付。

20. 合同生效

20.1 本合同一式陆份，由甲乙双方法定代表人或被授权人签字并盖章后生效。

21. 通知

21.1 双方均保证本合同所载的联系地址真实有效，保证对方或司法机关按该地址邮寄或送达的邮件或物品均能送达本方，若出现拒收、代收、退回等情形，均视为已送达本方。如因争议纠纷诉至法院的，双方确认以本合同所示地址为诉讼文书的有效送达地址。任何一方更改地址应在七日内以书面形式通知对方，否则应自行承担通知不能的不利法律后果。

附件1

投标报价表

1.总报价表

价格单位：人民币　元

序号	内　　容	价格小计
1	1.提供9人1年驻场技术支持服务：主要提供对总局安全管理平台等系统的运维服务、常态化安全运营服务，及时监测、分析、处置安全事件，妥善应对安全威胁和告警，并开展基础的技术保障工作。提供对青岛市税务局网络安全系统的运维服务，及时监测、分析、处置安全事件，妥善应对安全威胁和告警，并开展基础的技术保障工作。 2.提供4人月非驻场技术支持工作量，负责提供重保值守、应急响应等服务，人员资质满足中级岗位要求。	1488000.00
2	网络安全技术支持服务：内网资产梳理服务、服务器安全加固服务、终端安全管理运维服务、iNode巡检维护及应急保障服务、泰合SOC（网络安全管理平台）运维服务、互联网应用系统云安全监测服务、互联网资产测绘及发现服务、互联网终端安全加固服务、网络和数据安全检查技术支撑服务、互联网众测服务、敏感信息筛查服务、漏洞扫描服务、渗透测试服务、配置核查服务、弱口令筛查服务、系统上线前检测服务、移动APP安全检测服务、应用程序编程接口安全检测服务、软件全生命周期安全管理咨询服务、总局安管平台深化应用服务、应急演练及应急处置服务、网络安全意识提升服务、供应链合规管理服务、日志审计服务、Web动态应用保护系统扩容授权服务等。	818800.00
3	1年软硬件产品维保服务：用于保障以往网络安全项目已采购的iNode内网端点准入系统、天融信僵尸网络木马和蠕虫监测与处置系统和天融信Web应用安全防护系统的正常使用和持续升级。	310000.00
报价合计（小写）		2616800

报价合计（大写）	贰佰陆拾壹万陆仟捌佰元整
服务期	2026 年 6 月 6 日至 2027 年 6 月 5 日

特别说明：

1. 本项目总价及分项报价均不接受任何形式的赠送、“零”报价和折扣报价。
2. 本项目执行中所发生的所有费用均计入投标报价中，甲方不再另行支付其他任何费用。
3. 乙方应根据《招标文件-技术部分》相关要求填报。
4. 如报价不一致，按照乙方须知“19. 核价原则”进行修正。

附件2

2.分项报价表

价格单位：人民币　元

序号	项目名称	内容描述	单价	数量	小计（元）	备注
1	驻场技术支持服务（总局安管平台运维服务）	1名高级工程师，驻场服务12个月，服务周期2026.6.6-2027.6.5，主要工作包括对总局安管平台的系统运行监控、服务器基础设施巡检、预警监测与事件处置、故障分析及处理、系统升级、咨询服务、系统对接支持和平台深化应用等。	216000.00	1人	216000.00	单价为12人月费用
2	常态化安全管理运维服务（高级）	3名高级工程师，驻场服务12个月，服务周期2026.6.6-2027.6.5，主要工作包括市局SOC平台运维、应急演练及应急处置、网络安全宣传周服务、网络和数据安全检查技术支撑、日志审计、渗透测试、供应链第三方组件审计等	216000.00	3人	648000.00	单价为12人月费用
3	常态化安全管理运维服务（中级）	5名中级工程师，驻场服务12个月，服务周期2026.6.6-2027.6.5，主要工作包括对甲方资产进行收敛和维护、漏洞扫描、基线核查、敏感信息筛查、弱口令筛查、终端安全管理、iNode巡检维护等。	120000.00	5人	600000.00	单价为12人月费用
5	非驻场技术支持服务	提供4人月非驻场技术支持工作量，负责提供重保值守、应急响应等服务，人员资质满足中级岗位要求。	6000.00	4人月	24000.00	单价为12人月费用

6	网络安全技术支持服务	内网资产梳理服务、服务器安全加固服务、终端安全管理运维服务、iNode 巡检维护及应急保障服务、泰合 SOC（网络安全管理平台）运维服务、互联网应用系统云安全监测服务、互联网资产测绘及发现服务、互联网终端安全加固服务、网络和数据安全检查技术支撑服务、互联网众测服务、敏感信息筛查服务、漏洞扫描服务、渗透测试服务、配置核查服务、弱口令筛查服务、系统上线前检测服务、移动 APP 安全检测服务、应用程序编程接口安全检测服务、软件全生命周期安全管理咨询服务、总局安管平台深化应用服务、应急演练及应急处置服务、网络安全意识提升服务、供应链合规管理服务、日志审计服务、Web 动态应用保护系统扩容授权服务等。服务周期 12 个月，2026.6.6-2027.6.5	818800	1 项	818800.00	单价为 12 个月服务费用
7	iNode 内网端点准入系统维保服务	1 年软硬件产品维保服务：用于保障以往网络安全项目已采购的 iNode 内网端点准入系统的正常使用和持续升级。 新华三 Inode 内网端点准入 4 台，原厂维保一年，2026.6.6-2027.6.5	170000	1 项	170000.00	单价为维保 12 个月费用
8	天融信僵尸网络木马和蠕虫监测与处置系统维保服务	1 年软硬件产品维保服务：用于保障以往网络安全项目已采购的天融信僵尸网络木马和蠕虫监测与处置系统的正常使用和持续升级。 天融信僵尸网络木马和蠕虫监测与处置系统 V3。2 套；天融信僵尸网络木马和蠕虫监测与处置系统维保。2 台；维保一年，2026.6.6-2027.6.5	60000	1 项	60000.00	单价为维保 12 个月费用

9	天融信Web应用安全防护系统维保服务	1年软硬件产品维保服务：用于保障以往网络安全项目已采购的天融信Web应用安全防护系统的正常使用和持续升级。天融信Web应用安全防护系统V3维保，2台，维保一年，2026.6.6-2027.6.5	80000	1项	80000	单价为维保12个月费用
合　计					2616800	

特别说明：

1. 乙方应根据招标文件技术部分相关要求填报。
2. 本项目总价及分项报价均不接受任何形式的赠送、“零”报价和折扣报价。
3. 本表中小计=　　数量×单价。
4. 本表“合计”中应等于《开标一览表》中的“投标报价”。

附件3

项目服务内容

序号	服务名称	服务内容	交付成果	服务频次	服务工具
1	总局安管平台运维服务	提供1名中级工程师，驻场服务12个月，主要工作包括对总局安管平台的系统运行监控、服务器基础设施巡检、预警监测与事件处置、故障分析及处理、系统升级、咨询服务、系统对接支持和平台深化应用等。	出勤记录	/	
2	安全运维服务-中级	提供4名中级工程师，驻场服务12个月，主要工作包括对甲方资产进行收敛和维护、漏洞扫描、基线核查、敏感信息筛查、弱口令筛查、终端安全管理、iNode巡检维护等。	出勤记录	/	
3	安全运维服务-高级	提供4名高级工程师，驻场服务12个月，主要工作包括市局SOC平台运维、应急演练及应急处置、网络安全宣传周服务、网络和数据安全检查技术支撑、日志审计、渗透测试、供应链第三方组件审计等。	出勤记录	/	
4	内网资产梳理服务	自备工具软件对甲方内网所有设备及主机等资产进行梳理和收敛。工具功能要求：（1）支持资产扫描，支持针对本任务设置扫描参数，如扫描速率、协议并发数等；（2）系统内置识别规则，能够识别包括交换机、路由器、网络安全产品、服务器设备等；（3）支持分析资产属性变化，包括端口、组件、协议、漏洞、管理信息（负责人、机房、管理单元、地理位置等）；（4）支持对风险及风险主机的处置和维护，支持通过发现时间、风险信息和资产信息对风险事件进行检索；（5）支持通过EXCEL方式导入资产	《内网资产台账》	按需	安恒资产脆弱性扫描与管理平台

		信息，支持从 CMDB 或 ITSM 系统同步资产；（6）支持漏洞全生命周期管理，包括漏洞工单下发、整改、验证、关闭等流程，支持自动复扫规则自定义；（7）支持从资产、扫描任务、漏洞、扫描器等多维度进行综合性分析，支持资产风险分布、业务系统分布、责任人资产分布等维度统计。			
5	服务器安全加固服务	提供不少于 300 点位的主机防护软件加固服务，能够对主机系统漏洞及时发现与修复，监控主机资源使用，监测主机安全基线，形成《安全配置基线检查报告》。工具功能要求:(1)支持主机、虚拟机、容器等多种资产类型的发现与管理;(2)支持漏洞检测与 POC 验证交叉验证，自动关联官方补丁，提升漏洞修复效率；（3）支持不少于 2000+合规基线检查项，主动触发合规基线检测任务；（4）支持反弹 Shell 检测（响应时间不超过 1 秒）、WebShell 检测（响应时间不超过 10 秒）、木马文件识别、恶意命令检测等入侵威胁检测能力；（5）探针 CPU 占用率不超过 2%，内存占用不超过 80MB，无需 Root 权限即可运行；（6）支持容器全生命周期管理，支持通过宿主机探针监测容器安全；（7）支持 Linux、Windows 操作系统，支持 IDC 机房、私有云、混合云等多环境部署。		300 点位	牧云（CloudWalker）主机安全管理平台
6	终端安全管理运维服务	提供终端安全运维服务，按照总局要求对总局统推的 360 终端安全管理平台，以及甲方现有的深信服 EDR 和 DLP 系统进行日常巡检及配合完成系统升级，及时发现处置甲方内外网终端安全软件管理风险。	《360 运维服务报告》	1 年期	

7	iNode巡检维护及应急保障服务	对甲方iNode系统进行日常运维与巡检，处理一般性和较为可控的突发事件。提供iNode原厂维保和应急保障服务。	《iNode系统巡检报告》	1年期	
8	泰合SOC（安全管理平台）运维服务	对平台升级、资产更新、风险监测处置和风险模型构建优化并出具模型成效分析报告。提供原厂维保、使用授权和国产化升级改造服务。		1年期	
9	互联网应用系统云安全监测服务	自备云监测工具或平台，对甲方互联网系统进行7×24h监测，及时上报风险信息，定期出具监测报告。工具功能要求：支持依靠云端资源，实现网站漏洞监测、网页篡改监测、网站挂马监测、网页暗链监测、网站可用性监测、未知资产监测等网络安全服务。	《互联网云监测报告》	1年期	非凡互联网云安全检测
10	互联网资产测绘及发现服务	对甲方互联网资产进行周期性发现及收敛工作并出具测绘报告；定期提供各类高危或重大漏洞预警。工具功能要求：（1）支持通过IP、域名、icon、证书、ICP、关键字等多类资产线索方式周期监测发现企业未知资产；（2）支持自定义各类线索规则组合进行云端资产获取，可自定义线索范围包括但不限于证书、域名、ICP、icon、关键字、IP等；（3）支持仅输入单位名称，对各类线索进行正则组合匹配；（4）支持对单位潜存危险资产进行预警发现；（5）支持资产全生命周期监控和攻击路径全链路刻画；（6）覆盖不少于22个大类、102个小类风险类型，支持近千个已知高危漏洞的POC检	《互联网资产台账》	1年期	云图（CloudAtlas）攻击面管理运营平台

		测；（7）支持通过API接口与其他安全产品、网络设备联动，实现风险自动化处置。			
11	互联网终端安全加固服务	提供不少于500点位的互联网终端安全加固服务，包含杀毒、漏洞管理、资产盘点、端点发现、APT防护、虚拟化管理模块等功能。工具功能要求：（1）控制中心支持Windows Server 2003_SP2及以上版本、中标麒麟、Deepin、SUSE Linux、Red Hat Linux等操作系统，客户端支持Windows XP_SP2及以上版本、Windows Vista、Windows 7/8/10/11等操作系统；（2）支持自定义时间、自定义扫描频率、自定义扫描类型，对终端进行定时查毒，支持自定义查杀病毒后的处理方式；（3）支持文件与目录自定义黑白名单管理，文件被加入白名单则客户端不再查杀，加入黑名单则客户端不可执行此文件；（4）支持按病毒、木马、终端等维度统计全网病毒感染状况；（5）支持漏洞利用防御，对通过文件漏洞的攻击行为进行有效检测与防御；（6）支持文件解压缩病毒查杀，支持对zip、rar、7z等多种格式的压缩文件查杀；（7）支持断网状态下不依赖病毒库特征对未知病毒进行查杀；（8）支持定时修复漏洞功能，支持设置筛选高危漏洞、软件更新、功能性补丁等修复类型；（9）支持智能屏蔽过期补丁、与操作系统不兼容的补丁，支持查看或搜索系统已安装的全部补丁；（10）支持漏洞集中修复、强制修复、自动修复，具备蓝屏修复功能。	《平台使用手册》	500点位	360终端安全管理系统

12	网络和数据安全检查技术支撑服务	自备适应甲方环境的检查工具，每年度协助开展各单位及基层局的网络和数据安全风险检查工作，编写《网络安全检查方案》，检查完成后形成《安全检查报告》。工具功能要求：（1）网络行为自学习支持自动从网络流量中学习用户内网业务系统域名；（2）违规外联监测类型支持监测代理上网、3G/4G/5G 设备、无线网卡、NAT 网关、手机热点上互联网等方式接入互联网的外联行为，同时支持非法外联主机网络信息自动识别，包括 IP、操作系统、MAC、所使用的外网 IP 等；（3）被控反联检测支持对流量内 TCP、UDP、DNS 包中出现与威胁情报（IOC）中存在的风险 IP、域名、URL 的连接请求的检测，并定义相关风险类型；（4）数据审计支持自动探测网段范围内的数据库，从网络流量中自动发现数据库，记录数据库的 IP 地址、端口号、数据库类型等信息，记录触发的规则名称、访问者的信息、受保护的对象信息、审计级别、操作行为；（5）隐私数据合规检查支持至少 3 种隐私保护（如 GDPR、CCPA、ISO 27018）检查，能够自动生成隐私合规性报告，确保数据处理流程符合隐私法规要求。	《网络安全检查方案》、《安全检查报告》	1 次/年	
13	互联网众测服务	对甲方互联网应用系统开展 2 次众测服务：由 30 名具备 3 年以上攻防工作经验的白帽子每半年对甲方互联网应用系统开展渗透测试，共 2 次，每次 15 天，测试内容应包括端口扫描、SQL 注入、XXE 注入、跨站脚本、口令获取、远程命令执行、社会工程、逻辑缺陷、越权漏洞、XSS 漏洞、CSRF 漏洞、SSRF 漏		2 次/年	360 众测

		洞、任意文件操作、Web 脚本及应用测试、中间件漏洞等，只验证漏洞是否存在，不得影响系统运行或获取数据，对服务期间发现的漏洞，及时提供漏洞报告并制定安全加固方案，协助开展安全加固工作和回归测试。			
14	敏感信息筛查服务	定期进行敏感信息筛查，确保公开信息符合隐私保护法规。提供敏感信息筛查工具，每月对甲方外部网站公开信息进行核查，判断是否存在纳税人敏感信息。	《敏感信息筛查记录》	12 次/年	
15	漏洞扫描服务	自备工具软件每季度对主机资产及 WEB 应用进行漏洞扫描，编制漏洞扫描结果表和报告并协助运维进行整改，记录检查结果，形成《安全漏洞扫描报告》。工具功能要求：（1）支持主机扫描、WEB 扫描、基线扫描、数据库扫描及弱口令扫描等扫描类型；（2）支持扫描任务的定时单次执行、立即执行；（3）支持集成多个扫描器的漏洞库，内置来自 CVE、CNNVD 等权威机构发布的完整漏洞库，并定期更新；（4）支持将漏洞信息标记为误报或搁置，支持取消误报、搁置操作；（5）支持通过 EXCEL、XML、CSV 格式导入第三方扫描器扫描报告。	《安全漏洞扫描报告》	12 次/年	明鉴漏洞扫描系统
16	渗透测试服务	自备工具软件每季度对甲方互联网系统进行渗透测试并出具互联网系统渗透测试报告书；每半年对内网系统进行渗透测试，并提交《渗透测试报告》。工具功能要求：（1）支持国际主流 Web 应用类型，支持国内、国外知名 Web 应用程序漏洞扫描；（2）全面支持 Web 2.0，支持各类 JavaScript 脚本解析；（3）全面支持 FLASH 解析；（4）支持 WAP 类及 WMLScript	《渗透测试报告》	互联网:4 次/年 内网：2 次/年	明鉴自动化渗透测试平台

		脚本类应用系统；（5）支持基于HTTPS应用系统的检测，能够自动获取所有必需的要素，对基于SSL传输的内容进行分析；（6）支持所有类型的动态页面；（7）支持HTTP 1.0和1.1标准的Web应用系统。			
17	配置核查服务	自备工具软件每季度对主机、网络设备等进行安全配置核查，检查项包括账户策略、访问控制、日志设置等，编制核查报告，提供整改意见。	《安全配置检查报告》	4次/年	牧云（CloudWalker）主机安全管理平台
18	弱口令筛查服务	自备工具软件对甲方应用系统、终端、服务器、中间件等进行弱口令核查，出具弱口令情况排查报告并协助整改。工具功能要求：（1）端口扫描与自动触发支持在IP端口扫描、URL扫描时，可自动触发POC检测、密码破解、目录扫描等功能；（2）设备自带端口扫描功能，支持批量导入IP地址或设置IP段，同时进行多个服务的弱口令检查。	《弱口令筛查结果》	4次/年	明鉴漏洞扫描系统
19	系统上线前检测服务	对甲方新上线系统进行漏洞扫描、渗透测试、基线核查及合规性审查并提供安全整改指导和复检，直至系统符合上线条件。	《应用系统上线前检测报告》	按需	明鉴信息安全等级保护检查工具箱、明鉴WEB应用弱点扫描器、数据库弱点扫描器、明鉴漏洞扫描系统、明

					鉴半动化渗透测试平台
20	移动APP安全检测服务	自备专用工具结合人工方式，按APP发版情况对总局移动APP进行安全及隐私合规检查，深入渗透测试，深度检测系统安全性，提交渗透测试报告并协助整改。	《移动APP安全检查报告》	按需	梆梆应用安全测评平台
21	软件全生命周期安全管理咨询服务	协助甲方提升应用系统全生命周期管理和漏洞全生命周期管理体系建设，完善管理流程，提升管理手段，提供专业咨询服务。		按需	
22	供应链合规管理服务	对甲方供应链厂商使用的软硬件定期核查，梳理供应链产品清单；对供应链厂商引入的第三方组件开展风险评估和漏洞扫描，出具第三方组件清单和安全分析报告。工具功能要求：（1）支持对源代码、二进制文件中的组件进行深层解析，实时监测0day风险；（2）基于机器学习技术，对项目引用到的组件及漏洞进行高效深层分析；（3）采用深层开源依赖分析、高效软件指纹分析、二进制0day风险分析等技术，对软件中使用的开源组件进行快速精确识别；（4）支持开源组件与漏洞自动关联，及时推送影响软件安全的最新开源软件漏洞情报；（5）支持与多类CI/CD工具集成，无感知接入企业现有开发流程，实现开发阶段的风险组件生命周期闭环管理。		2次/年	安恒软件成分分析系统
23	日志审计服务	自备工具软件每季度对甲方应用系统日志、运维操作日志、网络日志等进行审计并出具审计报告。工具功能要求：（1）	《日志审计报告》	4次/年	Allog大数据日志

		具备PB级数据处理能力，日志处理性能不低于 100 万 EPS；（2）支持基于云原生技术的高可用部署和弹性扩容，支持计算和存储动态扩容；（3）支持 Collector（日志接收引擎）、Mapper（日志解析引擎）、分布式实时关联分析引擎、准实时计算数仓、日志采集终端、智能运维平台等组件；（4）支持灵活高效的即席分析、简单丰富的仪表盘、私人定制的报表系统；（5）支持 AI 智能检索、AI 智能翻译、AI 智能分析功能；（6）支持面向用户自定义分析的仪表盘、报表、分析场景的配置能力及专业的查询分析手段。			管理与分析平台
24	Web 动态应用保护系统扩容授权服务	对甲方现有在用 Web 动态应用保护系统进行性能扩容。需扩容采购 1 个 16C 虚拟机许可、支持不低于 10 个应用站点保护授权许可，对国产环境有良好支持。		1 年期	动态 Web 应用防火墙
25	总局安管平台深化应用服务	提供新版总局安管平台建设与升级服务，优化“外防攻击、内防窃数”模型能力。提供高级持续性威胁分析系统及探针，进行流量深度分析、威胁情报与行为分析。提供原厂安全公司的人力技术支持服务。提供全面接入日志、扩容终端审计、优化风险模型等方面技术支持。提供税务安全模型服务，具备日志统一采集与语义化清洗基座的能力、告警智能降噪与误报抑制的能力、构建智能根因分析与处置建议能力、安全知识库与智能问答助手的能力。		按需	360 高级持续性威胁预警系统
26	应急演练	对突发安全事件进行应急响应处理，快速恢复系统运行，降	《应急响	应急演	

	及应急处置服务	低安全事件造成的损失和影响，提供7×24小时应急响应服务，事件响应时间不超过1小时，重大安全事件2小时内应进行现场响应，及时编写并提交《应急响应报告》。协助甲方对应急响应综合预案和各专项预案进行修订或制定；参与完成不少于2次应急演练工作。	应报告》	练：2次/年 应急响应：按需	
27	网络安全意识提升服务	开发并交付定制化的面向税务干部全员年度网络安全培训课程，提供考核试题库及面向税务人员、运维人员等岗位的专项培训模块，并提供相应的培训学习数据统计；开展常态化网络安全教育内容运营，指定时间内开发并交付网络安全知识推文、图解、短视频等数字教育内容，建立并维护税务系统内部网络安全知识库，同时设计一套覆盖主要风险的安全风险提示模板库；组织实施安全意识强化活动，每年至少一次全员社会工程学攻击演练；完成环境氛围物料设计，如电子屏海报、网络安全教育短视频、培训课程讲义等，最终交付物以可验收的实物或数字产品形式提供。	培训课程及讲义、宣传屏保、宣传视频、电子宣传物料等	1次/年	
28	应用程序编程接口安全检测服务	保障甲方API接口安全性，提供内外网API梳理工具，工具具备行为模型创建、安全事件预警、接口鉴权检测、越权漏洞检测、业务逻辑检测、敏感数据检测、配置缺陷检测、API清单导出、API访问频次统计、敏感数据统计、API敏感数据分析、API资产台账更新、API字段标注、扫描误报排除等功能，能够实时不停机进行不少于5Gbps的镜像流量分析，API分析结果存储期限不少于1年。按甲方要求对甲方API资	《API资产清单》、《API风险风险排查报告》	按需	API与应用系统安全审计系统

		产进行梳理，形成动态《API资产清单》,内容包括但不限于协议类型、请求方法、认证方式、数据格式、API用途、所属系统、是否包含敏感数据、历史访问频次、历史访问ip等属性。按甲方要求按月出具《API风险风险排查报告》，针对模型告警、爬虫分析、漏洞情况、僵尸API、恶意扫描等多种问题出具分析报告，提供详细漏洞报告和修复建议。按甲方要求结合甲方实际业务风险完善API安全审计模型，基于行为分析对恶意爬虫、恶意扫描、目录遍历等风险建立风险审计模型。			

附件4

服务团队一览表

序号	姓 名	人员级别	工作年限	认证情况
一、项目负责人				
1	王程程	高级	15 年	注册信息安全管理人员/信息系统项目管理师
二、驻场技术人员				
1	许德磊	高级	13 年	cisp 注册信息安全管理人员
2	高亚娟	高级	7 年	cisp 注册信息安全管理人员
3	岳肖扬	高级	9 年	cisp 注册渗透测试工程师
4	张继康	高级	8 年	cisp 注册渗透测试工程师
5	董天硕	中级	4 年	cisp 注册渗透测试工程师
6	任衍旭	中级	4 年	cisp 注册信息安全工程师
7	孟凡铸	中级	5 年	cisp 注册信息安全工程师
8	王静昆	中级	4 年	cisp 注册信息安全工程师
9	张秀松	中级	4 年	cisp 注册信息安全工程师
三、二线支持人员				
1	刘鹏飞	高级	7 年	cisp 注册信息安全工程师
2	杨济泉	中级	12 年	cisp 注册信息安全工程师
3	张海成	中级	7 年	cisp 注册信息安全工程师
4	曹勇闯	高级	9 年	cisp 注册信息安全工程师