合 同 书

项目名称：国家税务总局河南省税务局2024年网络安全防控及重保服务项目

合同编号：HA2023-DLJC-C0109-B00

甲　　方：国家税务总局河南省税务局

乙　　方：北京天融信网络安全技术有限公司

日　　期：2024年1月

合同条款前附表

序号	内容		
1	合同名称		国家税务总局河南省税务局2024年网络安全防控及重保服务项目合同书
2	合同编号		HA2023-DLJC-C0109-B00
3	合同类型		技术合同
4	定价方式		固定总价
5	项目类别		☑信息化项目　　□非信息化项目
6	甲方名称		国家税务总局河南省税务局
	甲方地址		郑州市金水区熊儿河路85号
	甲方相关部门	甲方采购部门	国家税务总局河南省税务局财务管理处
		联系人	管斐
		联系电话	0371-81906701
		甲方实施部门	国家税务总局河南省税务局信息中心
		联系人	王龙标
		联系电话	0371-81906251
7	乙方名称		北京天融信网络安全技术有限公司
	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		北京市海淀区上地东路1号院3号楼四层
	乙方联系人		申亚峰
	联系电话		13373933336
	传真		010-82776666
	开户银行名称		北京银行中关村科技园区支行
	银行账号		01090879400120105013118
8	合同金额		人民币伍拾柒万元整（¥570000.00）。
9	服务内容		发现并消除或减少河南税务网络安全风险，保障全省税务网络和数据安全。在特定时间段开展网络应急响应准备和安全保障工作，及时发现并处置网络安全隐患，避免出现黑客攻击入侵、篡改事件、感染勒索病毒等安全事件。
10	合同付款		分两次付款： 第一次：合同履行半年并初验合格后30日内支付合同金

		额的 50%； 第二次：合同到期并终验合格后 30 日内支付合同金额的 50%。
11	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 3%，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，应同时提交甲方实施部门出具的项目终验意见或质量保障期（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，以电汇方式返还履约保证金或退回保函。
12	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。
13	服务期	合同签订后一年内
14	合同履约地点	合同约定地点或甲方指定地点

合　同

国家税务总局河南省税务局（以下简称“甲方”）通过 竞争性磋商 采购方式，确定北京天融信网络安全技术有限公司（以下简称“乙方”）为“国家税务总局河南省税务局2024年网络安全防控及重保服务项目”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《国家税务总局河南省税务局2024年网络安全防控及重保服务项目合同书》（合同编号：HA2023-DLJC-C0109-B00，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）合同通用条款；

（2）报价表（总报价表和分项报价表）；

（3）采购文件（另附）；

（4）响应文件（另附）。

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

本项目合同金额为人民币伍拾柒万元整（¥570000.00）。

4. 合同付款

同前附表10。

5. 合同签订及生效

本合同一式肆份，甲方执叁份，乙方执壹份，经甲乙双方法定代表人或其授权代表签字盖章后生效。合同的附件是本合同不可分割的部分，与本合同具有同等法律效力。

甲方：国家税务总局河南省税务局

盖章：

签署人：

日期：2024年 1月 22日

乙方：北京天融信网络安全技术有限公司

盖章：

签署人：

日期：2024年 1月 22日

合 同 通 用 条 款

1. 定义

本合同下列术语应解释为：

1.1“甲方”是指国家税务总局河南省税务局。

1.1.1“甲方采购部门”见“合同条款前附表”第6项“甲方采购部门”。

1.1.2“甲方实施部门”见“合同条款前附表”第6项“甲方实施部门”。

1.2“乙方”见“合同条款前附表”第7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协议，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9项“服务内容”。

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，乙方应负全责并在限期内尽快处理解决，由此造成的损失和相关费用由乙方承担，甲方保留解除合同及索赔的权利。

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，应在限期内尽快提出解决方案。

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，由此产生的费用和甲方的损失全部由乙方负责。

3.5 除合同条款另行规定外，伴随服务的费用已全部含在合同总金额中，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。如果甲方在使用乙方货物或货物的任何一部分过程中，

第三方提出货物侵犯其专利权、工业设计权、使用权等知识产权的，乙方应当修正以避免侵权。如果甲方在使用乙方货物或货物的任何一部分过程中，第三方指控侵犯其专利权、工业设计权、使用权等知识产权的，乙方应自费为甲方答辩，并支付法院最终判决的甲方应支付第三方的一切费用、赔偿甲方由此遭受的损失。

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，包括但不限于对由此给对方造成的经济损失进行赔偿。

6. 项目管理

6.1 乙方应按照甲方项目整编归档内容、整理标准质量、移交时间等档案管理要求，

对项目相关文件进行收集、整理、归档并移交。

6.2 乙方应按甲方要求，配合做好政务信息系统安全检查、评测、审计、工程监理等监督管理工作及系统间数据交互和衔接工作，如实、完整提供政务信息系统建设、运营、维护和政务数据安全管理相关情况，不得拒绝、隐匿、瞒报。

7. 履约验收

7.1 甲方实施部门应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，对乙方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。

7.2 具体履约验收要求及验收方案详见招标（采购）文件。

8. 履约保证金

8.1 需提交履约保证金的项目，乙方应按照“合同条款前附表”第 11 项“履约保证金及返还”提交履约保证金。

8.2 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。

8.3 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。

8.4 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，并应按合同约定支付违约金、赔偿金等。

8.5 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 11 项“履约保证金及返还”。

9. 履约延误

9.1 乙方应按照本合同的规定提供服务。

9.2 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，延误累计超过30日的，甲方有权解除合同，并要求乙方承担合同总价款30%的违约金。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。

9.3 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违约金。

9.4 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违约金之外，乙方延误工期，将按合同规定被收取误期违约金。

9.5 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。乙方可要求甲方按照合同订立时1年期贷款市场报价利率支付逾期利息。特殊原因逾期返还的，双方协商解决。

10 违约责任

10.1 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。

10.2 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9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。

10.3 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。

10.4 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，甲方有权从应付乙方的合同款项中扣除索赔金额。

10.5 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。

10.6 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，自甲方通报之日起三年内，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。

10.7 信息化服务商聘用离职税务人员的风险控制

10.7.1 信息化服务商是指为税务总局、各省（自治区、直辖市和计划单列市）税务局提供信息化项目承建、运维、咨询、监理服务或参加相关采购活动的单位或个人。

10.7.2 乙方应建立防止违法违规聘用离职税务人员的风险控制制度。如乙方未建立上述风险控制制度，甲方有权要求乙方限期纠正。

10.7.3 本合同履行期间，乙方不得聘用 3 年内离职的原从事过税收信息化及相关信息系统业务条线的税务人员。原从事过，是指离职前 3 年内从事过税收信息化工作及相关信息系统业务条线工作。如果乙方有前述违约行为，甲方有权要求乙方承担下列违约责任：

10.7.3.1 要求乙方限期改正并从应付款项中扣除合同总金额的百分之一（1%）作为违约金；

10.7.3.2 自甲方通报之日起三年内，所聘税务人员原单位及下属单位可以拒绝乙方参与信息化项目政府采购活动。

10.8 乙方在本合同履行期间存在“围猎”甲方税务人员行为的（指以获取不正当利益为目的，采取馈赠礼品礼金、邀请娱乐旅游消费、提供便利条件等非正常交往手段“围猎”相关税务人员及亲属），自甲方认定或通报之日起三年内，甲方可以拒绝乙方参与其政府采购活动。

10.9 甲方发票电子化改革领导小组办公室认定乙方在本合同履行期间存在失信行为的，自甲方发票电子化改革领导小组办公室做出认定并通报之日起三年内，税务系统各单位可以拒绝乙方参与信息化项目政府采购活动。

10.10 对于本协议未约定的、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；对本协议与招标（采购）文件（技术部分）约定不同的违约处理条款，以本协议约定为准。

10.11 乙方应按照甲方关于税务信息化供应链安全管理的相关要求，配合供应链安全管理工作，重视和加强网络安全工作、认真履行网络安全责任和义务。

11. 不可抗力及其他

11.1 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。

11.2 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、疫情等。

11.3 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。

11.4 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。

12. 争端的解决

12.1 因本合同产生的纠纷，甲、乙双方可以协商解决，协商不成的，任何一方可以向甲方所在地的人民法院提起诉讼。

13. 违约解除合同

13.1 若出现如下情况，甲方有权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。甲方因主张乙方违约责任及赔偿损失而支付的诉讼费、保全费、担保费、律师费、差旅费等由乙方承担。

13.1.1 乙方不履行合同义务或者履行合同义务不符合合同约定，累计达2次的；

13.1.2 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；

13.1.3 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；

13.1.4 不能满足本项目技术需求的管理要求和规范，且经2次整改无明显改进的；

13.1.5 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；

13.1.6 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；

13.1.7 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不良后果的；

13.1.8 乙方拒不修复或更换有缺陷的、损坏的货物的；

13.1.9 乙方提供的货物侵犯甲方、第三方知识产权等合法权益的；

13.1.10 乙方提供的货物造成甲方或第三方经济损失而拒不赔偿的；

13.1.11 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；

13.1.12 乙方对政务信息系统建设、运营、维护项目的主体和关键部分采取转包、分包方式履行合同的；

13.1.13 乙方不配合政务信息系统安全检查、评测、审计、工程监理及系统间数据交互和衔接等工作，不如实、完整提供政务信息系统建设、运营、维护和政务数据安全管理相关情况的；

13.1.14 乙方违反协议10.7.2的规定，且未按甲方要求在限期内改正或者拒不改正的；

13.1.15 乙方违反协议10.7.3的规定，且未按甲方要求在限期内改正或拒不改正或拒不支付违约金的；

13.1.16 乙方在本合同履行过程中存在“围猎”税务人员行为的。

13.1.17 乙方有其他严重违约行为的。

13.2 如果甲方根据上述第13.1条的规定，解除了全部或部分合同，甲方可以适当的条件和方法购买乙方未能提供的货物及服务，乙方应对甲方购买类似货物及服务所超出的费用负责。同时，乙方应继续执行合同中未解除的部分。

14. 破产终止合同

14.1 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。

14.2 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利。

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，甲方将与乙方协商处理。

16. 转让和分包

16.1 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。

16.3 乙方不得对政务信息系统建设、运营、维护项目的主体和关键部分采取分包方式履行合同。

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 乙方应依法缴纳的合同货物及服务相关税费，均已包含于合同总金额中，甲方不再另行支付。

20. 合同生效

20.1 本合同由甲、乙双方盖章后生效。

附件 1 ：技术需求

（一）服务内容

序号	指标项目	重要性	具体要求
1	网络安全防控	★	提供2人5*8驻场运维服务，梳理网络拓扑和现有防护措施，分析重要系统的可能攻击路径和存在的防护短板，协助加强纵深防御能力，对风险排查工作发现的安全隐患提供建议，输出方案，协助优化防护策略，最大程度防范安全事件的发生。
			对堡垒机、VPN 等集权设备进行风险排查。对在互联网上的暴露源中的敏感信息进行搜索发现并及时报告。
			根据省局授权和需求，在网络内部对指定系统或地址段进行渗透性测试，提前发现系统潜在的各种高危漏洞和安全威胁。
			排查非必要的互联网出口以及非必要的服务器上网。排查是否有接入到内网的无线网络，是否存在私建热点以及不安全接入等安全问题。
			对省局指定网段进行资产探查，防止出现僵尸资产。
		▲	对数据库、操作系统、中间件和应用系统的安全漏洞进行检测和研判，识别出可被利用的漏洞。
			协助对应用系统、操作系统、数据库、中间件、网络设备、安全设备的用户账户、管理员账户、系统账户等开展默认口令和弱口令检查。
		▲	制定安全检查标准和系统基线配置标准，协助对操作系统、中间件、数据库、网络设备、安全设备等的配置进行核查。
			通过人工或工具产品检测相关主机系统上的恶意文件和网络行为，判断主机是否失陷并做处置。
			梳理全网软硬件安全系统的版本信息、补丁信息、检测和防护规则库版本信息等，确保核心业务系统的安全防护设备的软、硬件补丁、系统版本、规则库版本持续更新。
			对省局指定的4个重要信息系统开展风险评估，对在运行和维护工作中的网络安全风险进行深入剖析和全面评价，提供整改措施和整改建议，以提高应用系统安全防护能力，保障应用系统安全运行。
2	重要时期网络安全保障	★	协助单位完成重保启动会议，落实和完成各阶段工作任务。编写重保工作计划表，并明确各阶段任务分工及时间安排。服务方在重保期提供不少于6名重保安全工程师，要求必须有攻防演习工作经验，进行7*24小时值守工作。

		▲	对监控上报的报警日志和可疑日志进行分析确认和安全事件确认，对各安全系统发现的事件进行分析，对攻击样本进行分析，对攻击相关系统、设备的日志进行分析研判。对于态势感知以及防火墙等安全日志中成功攻击事件进行验证和确认。研判分析发现的安全事件进行主动应急响应和快速处置，包括封堵IP、断网、快速打补丁以及删除恶意文件等工作，确保快速抑制安全事件，防止攻击方的进一步横向渗透行为，防止更多系统被入侵。
			进行模拟演练，按照应急预案及其标准工作程序，讨论紧急情况时应采取的行动，提升参演人员解决问题的能力，以及应急组织相互协作和职责划分的问题。按照正常重保值守方式，组织监控组、封堵组、分析研判组、综合协调组等提前进行演练。对演练中发现的问题进行分析研判和策略优化，确保在正式开始时候能快速有效识别攻击。
			根据省局网络情况，增添部署相关监测设备，基于全流量分析技术、蜜罐诱捕技术等，进行全网威胁可视化与智能分析预警，持续排除误判，强化检测有效性和易用性。
			安全漏洞预警，针对重保期间爆发的高危0day、热点漏洞进行预警和内部通告，形成重保预警。收集、分析和确认不同来源攻击事件（攻击事件涉及的IP地址、攻击方式，攻击行为和相关威胁情报等）并整理后进行威胁情报共享。
		▲	实时对安全设备状态、日志和事件进行监测，对系统失陷情况进行监测，对重保目标系统、堡垒机、等重要系统和设备进行安全监测，一旦发现异常及时预警。
		▲	对入侵的网络安全攻击成功事件进行深度分析，并对攻击方法、攻击方式、攻击路径进行深度分析，查找定位被入侵根因以及后门程序，并且撰写应急溯源报告。
			结合省局业务系统进行高仿真、高交互蜜罐部署以及精心构造诱捕插件。通过蜜罐对攻击者进行捕获并且依据反制插件反攻，获得攻击者主机相关信息和权限，定位到攻击团队和个人。
			梳理重保过程中黑客攻击和防护手段，分析防护能力、安全制度、防护流程及方案的缺陷，商讨可落地的整改建议。根据重保过程的产出和复盘结果，编写重保总结报告。
3	服务工具	★	供应商应作出以下服务工具提供承诺： 1、提供硬件流量探针1台，支持对网络原始通讯数据进行全流量完整保存，可用于溯源分析。产品网络吞吐量不小于10Gbps，存储容量不小于48T，内存不小于128G。为防止敏感数据信息泄露，服务期结束后相关软硬件不再返还。 2、提供软件版本漏洞扫描工具，分别在互联网区、外联网区、内网区部署,不限制扫描IP数量。 3、在重保时期，根据工作需要提供态势感知、蜜罐等工

			具使用服务。 4、提供自动化溯源反制工具，支撑溯源反制、攻击测试、报表、知识库、统计分析，工具支持信息侦测、资产测绘、攻击验证及攻击反制功能，支持调用威胁情报，攻击测试支持通过URI自定义选择POC或EXP进行攻击测试。
		▲	提供应用API接口监测系统，对网络中的API接口风险进行监测，快速对数据泄露事件进行风险预警。

（二）服务要求

序号	指标名称	指标种类	指标内容
1	日常要求	▲	服务提供商安排人员对服务采购方目标系统相关的网络访问路径、关键及未知资产、专项应急预案以及已有的安全监测和防御产品进行梳理。须形成报告，并协助调整服务采购方现有的安全产品策略。
			服务提供商对服务采购方进行网络安全检查、主机安全检查、应用系统安全检查、运维终端安全检查、日志审计检查。须形成报告。
2	重保期间要求	▲	重保前检查整改阶段周期暂定为 1 个月，具体时间以服务采购方通知为准。在此阶段内，服务提供商须向服务采购方提供重保前安全检查和整改计划书。
			服务提供商须向服务采购方提供重保工作所需要用到的安全监测产品和防御产品，建立安全监测防御体系。
			服务提供商对服务采购方进行安全意识培训。针对重保参与人员进行安全意识培训，明确重保工作中应注意的安全事项，提高重保参与人员的安全处置能力，针对攻击中可能用到的手段和应对措施进行培训。
			在重保期间，服务提供商全程参与现场值守、应急响应、安全保障等工作；协助服务采购方完成各类安全事件的检测、分析、响应处置及上报等工作。在服务采购方的系统受到攻击时提供现场应急响应支持，支持内容包括但不限于：快速阻止攻击、攻击溯源取证、事件调查分析、事后安全加固、撰写防护报告等。
3	重保人员要求	▲	重保服务期内安排不少于 6 名有国家级或省级攻防演习工作经验的人员进行现场值班和保障（提供证明材料），7×24 小时轮班值守。
			服务提供商向服务采购方提供重保期间的人员分组安排和 24 小时驻场值守人员排班表，具体时长以实际重保工作的开始和结束日期为准。在重保期间，服务提供商需严格按照排班表进行排班值守。

（三）企业及人员能力要求

序号	指标名称	指标种类	指标内容

1	企业资质要求	▲	投标人应具备信息技术服务标准证书（ITSS）
		▲	投标人应具备质量管理体系认证证书（ISO 9001）、信息技术服务管理体系认证（ISO/IEC 20000）、信息安全管理体系认证（ISO/IEC 27001）
		▲	投标人应具备信息系统安全集成资质、信息系统安全运维服务资质、信息安全风险评估服务资质、国家信息安全测评信息安全服务-安全开发类资质
			投标人应为工业和信息化部移动互联网 APP 产品安全漏洞库技术支撑单位
			投标人应具备为 CNNVD 技术支撑单位
2	企业能力要求	▲	投标人应具备近三年同类项目案例。提供证明材料并加盖公章
3	人员资质要求	▲	投标人需为本项目配备 1 名项目经理，项目经理应具备五年或以上网络安全工作经历，具备人社部门颁发的系统集成项目管理工程师或信息系统项目管理师证书或系统架构设计师。提供证明材料并加盖公章
		▲	驻场人员（2 名）均需具备 CISP 或 CISAW 认证，有 3 年以上国家攻防实战演习经验。 重保值守小组（不少于 6 名）均需具备国家或省级攻防演习经验。 以上需提供证明材料并加盖公章。
		▲	本项目所有人员均须为投标人正式员工，提供近 6 个月以来任意 1 个月的社保证明并加盖公章。
4	人员能力要求	▲	具备网络安全渗透攻击、防御拦截和应急响应工作经验，并且具备良好的安全威胁分析和应急处置能力；
		▲	具备一定的业务分析、问题判断和解决等方面的能力；
			熟悉大型企业信息化建设和网络安全相关流程；具备一定的沟通协调、口头表达及文字写作能力。

（四）项目要求

序号	指标名称	指标种类	指标内容
1	合规要求	★	中标供应商所有服务内容应符合国家有关标准、规范和要求。 中标供应商有义务协助采购人开展相关工作，以符合国家及有关主管部门相关要求。
2	税收信息化项目开发和应用管理工作要求	★	供应商在采购以及后续项目实施过程中，应严格遵守税务总局税收信息化项目开发和应用管理工作要求。对于因失信行为纳入《税务系统信息化服务商失信行为记录名单》的供应商，存在一般失信行为的，由采购人函告服务商；存在严重失信行为的，由采购人约谈服务商主要负责人；对于违反合同约定的，依据合同约定及政府采购有关规定，采购人可采取要求限期改正、在应付合同金额中扣除违约金、解除合同、拒绝参加税务系统政府采购活动等措施；对于存在影响恶劣的严重违法失信行为的，由采购人按规定推送财政部纳入政府采购严重违法失信行为记录名

			单。 **（供应商在响应文件中需提供满足该项要求的服务承诺函，未提供或提供的不符合要求的，投标将被拒绝。）**
3	供应链安全管理要求	★	成交供应商应遵守国家税务总局供应链安全管理相关要求，包括但不限于： 1.人员资格要求 （1）签订承诺书。成交供应商应严格落实国家税务总局网络安全和保密管理要求，承担技术支持人员的网络安全和保密管理责任，按采购人要求签订协议和承诺书。 （2）开展背景审查。成交供应商承担技术支持人员背景审查工作，提供其身份证明、履历、家庭成员及主要社会关系、无犯罪记录证明等材料，并提交采购人进行备案。 （3）设置网络安全负责人（由项目经理兼任）。成交供应商为本项目配备一名网络安全负责人，该负责人具备独立决策能力并保持相对稳定，在项目实施的全过程负责网络安全工作，组织落实各项网络安全要求。 2.日常行为规范要求 （1）工作能力要求。成交供应商负责对技术支持人员进行资格条件、工作胜任力以及网络安全能力评估，对技术支持人员承担的工作进行安全保密风险分析，明确技术支持人员工作范围和边界，重点防范设备和资料失窃、误操作导致的软硬件故障、工作秘密和税费数据等信息泄露、信息系统越权访问和网络攻击等风险。 （2）教育培训要求。成交供应商负责对技术支持人员进行网络和数据安全法律法规、网络安全意识、网络安全管理、网络安全技能、保密意识以及网络安全警示教育等培训，上岗前对其进行考核。 3.违约惩戒措施 成交供应商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，采购人按照《税务系统信息化服务商失信行为记录名单制度（试行）》（税总办征科发〔2022〕1号）要求，组织对成交供应商进行失信行为认定，并采取相应的处置措施。 **（供应商在响应文件中需提供满足该项要求的服务承诺函，未提供或提供的不符合要求的，投标将被拒绝。）**

（五）其他要求

1.服务提供商的服务质量和人员资质、数量、排班周期等必须满足服务采购方的相关要求。

2.服务提供商提供的服务人员及项目负责人在服务期间不得随意调换，如需调换，需经服务采购方书面审核批准。

3.在服务采购方指定的办公地点开展工作。

4.服务人员严格遵守服务采购方安全保密要求，按照服务采购方管理流程开展工作。

9 拟派服务人员情况表

9.1 拟派技术服务人员情况表

序号	姓名	职务	职称或执（从）业资格证明					备注
			证书名称	级别	证号	专业	同类项目工作经验年限	
1	吴谦	项目经理	信息系统项目管理师证书	高级	12101440222	计算机科学与技术	16 年	无
2	张贺勋	驻场人员	CISP	高级	CNITSEC2014CISE01055	计算机科学与技术	22 年	无
3	丁林涛	驻场人员	CISP-PTE	高级	CNITSEC2019CISE[illegible]PTE[illegible]07	计算机[illegible]术	5 年	无
4	赵威	重保值守	CISP	高级	CNITSEC[illegible]9CISE06[illegible]	计算机网络技术	9 年	无
5	景昊阳	重保值守	CISP	高级	CNITSEC2019CISE06752	网络工程	5 年	无
6	王银章	重保值守	CISP	高级	CNITSEC2018CISE03029	网络工程	7 年	无
7	白子	重保	CISP	高级	CNITSEC201	计算机科学与	11 年	无

附件2：技术人员表

	文	值守			3CISE00202	技术		
8	赵晓燕	重保值守	CISP	高级	CNITSEC2019CISE00055	安全工程	6年	无
9	陈香君	重保值守	CISP-PTE	高级	CNITSEC2018CISP-PTE00362	计算机科学与技术	5年	无
10	李铎	重保值守	CISP	高级	CNITSEC2019CISE00476	网络工程	7年	无
11	乐洋	重保值守	CCSK	高级	CCSA8102951688	计算机科学与技术	14年	无

供应商名称：北京天融信网络安全技术有限公司（加盖公章）

法定代表人或其授权代表：（签字或盖章）

日期：2023 年 12 月 21 日