[铜川市一体化政务大数据平台暨数据安全底座项目]

建设合同

（项目编码：SXGS-2025-FW017）

项目名称：[铜川市一体化政务大数据平台暨数据安全底座项目]

委托方(甲方)：[铜川市数据中心]

受托方(乙方)：中电信数智科技有限公司

签订地点：铜川市

签订日期：2026 年 1 月 30 日

[铜川市一体化政务大数据平台暨数据安全底座项目]
建设合同

委托方（甲方）：[铜川市数据中心]
地址：[铜川市正阳路 9 号]
法定代表人/负责人：[白永琦]
项目联系人：[杨凡]
电话：[18590985543]

受托方（乙方）：[中电信数智科技有限公司]
地址：[北京市海淀区复兴路 33 号 13 层东塔 13 层 1308 室]
法定代表人/负责人：[陆良军]
项目联系人：[刘珍]
电话：[18991230602]

本合同甲方委托乙方就[铜川市一体化政务大数据平台暨数据安全底座项目]项目（“项目”）进行专项建设，并支付相应的建设报酬。双方经过平等协商，在真实、充分地表达各自意愿的基础上，根据《中华人民共和国民法典》以及相关法律法规的规定，达成如下合同，并由双方共同恪守。

第一条建设内容

1.1 建设目标：[为铜川市搭建全方位的数据安全综合保障体系，实现跨系统、跨部门、跨层级政务数据高质量安全供给，支撑政务数据资源高效应用，充分发挥数据要素乘数效应，同时实现监管单位对辖区网络安全空间的全面掌控与管理]。

1.2 建设内容：[一体化政务大数据平台暨数据安全底座，包括数据服务门户、数据目录系统、数据供需系统、数据交换系统、数据治理系统、数据处理分析系统、数据共享系统、数据开放系统、数据级联系统、数据直达系统 10 个子系统；打造四个场景专题库（具体以甲乙双方商定为准），为场景开发应用做好支撑；数据安全建设依托铜川市政务云资源，基于可信数据空间底座，聚焦数据安全防护能力，为铜川市搭建全方位的数据安全综合保障体系，涵盖数据安全管理体系、数据安全技术体系和数据安全服务体系，实现跨系统、跨部门、跨层级政务数据高质量安全供给，支撑政务数据资源高效应用，充分发挥数据要素乘数效应；网络安全升级优化，梳理网络拓扑，针对网络安全运行态势全面感知，形成防御、检测、响应的完整闭环，监测预警、分析研判、响应处置，联动指挥的多元化服务，为公共数据授权运营做好支撑，实现监管单位对辖区网络安全空间的全面掌控与管理。

1.3 建设方式：[现场建设及远程技术支撑]。

第二条建设时间和地点

2.1 建设地点：[铜川市]。

2.2 建设期限：[建设周期：合同签订之日起 1 年；服务期限：自合同签订之日起 3 年]。

第三条甲方提供的工作条件和协作事项

3.1 提供技术资料：[甲方需协调提供与项目相关的业务、数据及环境对接类技术材料，涵盖业务需求、流程规则、数据样本与字典、现有系统接口文档及接口授权、软硬件配置清单及第三方对接授权文件等]。

3.2 提供工作条件：[甲方需协调提供项目实施所需的软硬件及网络环境，指定专人负责需求确认、方案评审等全流程协作，协调内部资源配合调研、联调等工作，同时授予乙方必要的系统与数据访问、对接权限等，甲方需提供专项人员负责落实完成数据对接相关工作，乙方提供技术支持]。

3.3 其他配合协作事项：[双方协商为准]。

3.4 甲方提供上述技术资料、工作条件和配合协作事项的时间及方式：[双方协商为准]。

第四条合同费用

4.1 本合同费用总额（含税价）：大写人民币[柒佰零伍万元整]，¥[7050000.00]。

服务部分大写人民币[陆佰贰拾贰万柒仟玖佰元整]，¥[6227900]：其中价款为大写人民币[伍佰捌拾柒万伍仟叁佰柒拾柒元叁角陆分]，¥[5875377.36]，增值税款为大写人民币[叁拾伍万贰仟伍佰贰拾贰元陆角肆分]，¥[352522.64]；

设备部分大写人民币[捌拾贰万贰仟壹佰元整]，¥[822100.00]：其中价款为大写人民币[柒拾贰万柒仟伍佰贰拾贰元壹角贰分]，¥[727522.12]，增值税款为大写人民币[玖万肆仟伍佰柒拾柒元捌角捌分]，¥[94577.88]元。

4.2 合同总费用由甲方按照以下方式向乙方支付：

甲方分期向乙方支付本合同费用：

[4.2.1 合同签订，硬件设备到货甲方、监理方、乙方三方验收合格，维保和硬件设备全部调试到位，符合招标文件约定，甲方收到以下资料 10 个工作日内，支付合同总金额的 30.00%，即人民币 2115000.00 元；

①到货证明文件复印件一份。

②乙方开具的相应金额的、符合国家规定的增值税普通发票。

4.2.2 乙方按照合同约定完成所有内容：包括软件开发及安装、调试，经甲方初步验收合格（验收标准详见本合同第八条约定）。试运行三个月内等保、密评、第三方软件测试检测问题全部整改到位，终验合格。甲方收到以下资料 10 个工作日内支付合同总金额的 40.00%，即人民币 2820000.00 元；

①终验报告复印件一份。

②乙方开具的相应金额的、符合国家规定的增值税普通发票。

4.2.3 竣工验收合格后，甲方收到以下资料 10 个工作日内，支付合同总金

额的30.00%，即2115000.00元

①竣工验收报告复印件一份。

②乙方开具的相应金额的、符合国家规定的增值税普通发票。

③交付报告

每次付款前，乙方应当首先提供与本次付款金额相等的合法税票。否则，采购人的付款义务不发生，且不得因此延误合同的正常履行。遇有财政拨款迟延到位的，付款时间在约定基础上自动调整为财政拨款到位后10个工作日内支付。]

4.3 甲乙双方银行账户信息和纳税人信息

甲方信息如下：

开户行：[工行长虹路支行]

户名：[铜川市数据中心]

账号：[2602012409200209154]

统一社会信用代码：[12610200MB24282707]

地址：[铜川市正阳路9号]

电话：[0919-3183601]

乙方信息如下：

开户银行：[广发银行股份有限公司北京太阳宫支行]

开户名称：[中电信数智科技有限公司]

账号：[955088024410900013O]

统一社会信用代码：[91110000710928807K]

地址：[北京市海淀区复兴路33号13层东塔13层1308室]

电话：[010-58552665]

第五条保密

5.1 未经对方书面许可，任何一方不得向第三方提供或者披露因本合同的签订和履行而得知的与对方业务有关的资料和信息，法律、法规、规章或监管要求另有规定或本合同另有约定的除外。乙方向其关联公司提供或披露与甲方业务有关的资料和信息的，不受此限。

5.2 本保密条款在服务期限内及服务终止后二年之内持续有效。

第六条 本合同的变更应当由双方协商一致，并以书面形式确定。但有下列情形之一的，一方可以向另一方提出变更合同权利与义务的书面请求，另一方应当在收到书面请求后15个工作日内予以答复：

（1）因国家法律法规、行业标准调整导致合同履行需变更的；

（2）因项目建设需求发生合理变化，且变更内容不显著增加对方义务或降低合同目的实现程度的；

（3）其他不可抗力或双方认可的合理情形。

变更内容生效后，双方应按变更后的约定履行合同，涉及费用调整的，应同步明确调整方式。

第七条包装运输及发货

7.1所有合同设备应当进行坚固包装使其适用于长途空运等多种方式运输及反复装卸和操作。乙方应当根据货物特点和要求采取保护措施使其免受雨水、潮湿、锈蚀、震荡、撞击和其他的损坏，以使其在正常装卸和操作条件下能够安全无损坏地抵达现场。

如果因乙方未采取适当的包装或充分的保护措施而造成货物的损坏或丢失，乙方负责维修、更换、补充受损或丢失的设备并送达乙方现场。

7.2本合同项下货物全部由乙方负责运输。

7.3 乙方应当按照合同及附件的规定将合同设备交货至甲方现场，发货清单列于附件一。

7.4 发货同时，乙方应当向甲方或甲方指定的第三方提交两份到货证明原件。甲方或甲方指定的第三方代表根据到货证明核对到货的箱数，在两份到货证明原件上签字并将其中的一份原件退还给乙方。甲方或甲方指定的第三方代表在发/到货证明原件上签字仅具有证明甲方在某一日期所收到的设备箱数以及箱体表面是否严重破损的作用。甲方或甲方指定的第三方在合同设备运抵本合同指定的甲方现场后按工程实施进度依据合同规定和乙方提交的发/到货证明对有关的设备、材料、软件和技术资料进行查验。

7.5 所有设备应当成套装运，设备的特殊安装工具、材料和易磨损部件应当与相关设备一同发出，并由乙方负责对其进行适当的包装并采取足以保护其安全的措施。

7.6 本合同设备的所有权和货物风险按照中国法律的规定转移至甲方。

第八条验收

8.1 乙方完成建设工作的形式：[现场建设及远程技术支撑]。

8.2 建设工作成果的验收方法：[乙方完成项目建设内容并向甲方提出验收申请，甲方接到验收申请单 10 日内组织项目验收，若收到验收申请单超过 20 日未组织验收，则视为验收合格，若存在客观不可抗力因素，甲方提起书面告知，双方商定验收时间。（此项不包含竣工验收）]

8.3 验收的时间和地点：[由甲方确定]。

8.4 验收标准：

8.4.1 初验标准

乙方按照合同约定完成所有内容，包括但不仅限于软件开发、安装、调试，经甲方初步验收合格。

乙方应负责推动并完成省级一体化政务平台的数据接入工作，以及 2026 年度内甲方各部门新建业务系统的前期对接工作，但相关系统等数据接入与对接工作的实现，应以相关应用平台或业务系统具备可行的数据接口、开放必要的技术支持权限且不违反其自身运营规则或相关法律法规为前提。后期，为各单位新建系统提供接口指南，并配合做好接口对接。

乙方承诺，在满足前述前提条件的情况下，将以专业、勤勉的态度积极推动

各项对接工作，不得无故拖延或推诿。对于具备对接条件的系统，乙方应制定并执行可行的对接方案，保障数据对接工作的顺利完成与稳定运行。

若在对接过程中，乙方发现系统因技术限制、权限未开放或其他非乙方原因导致暂时无法满足对接条件，应立即书面通知甲方并说明情况，由双方协商后续处理方案，以确保项目整体进度与双方合法权益。

因不可抗力、或非因任一方过错导致的对接迟延或失败，应根据实际情况由双方友好协商解决，或依据合同其他约定处理。

8.4.2 终验标准

项目运行三个月内，等保、密评、第三方软件测试检测问题全部整改到位，由甲方组织最终验收。

8.4.3 到货验收

甲方应在收到产品后 7 个工作日内组织验货，验货工作由甲方、监理方、乙方共同进行，验收内容包括以下几个方面：

（1）检查货物是否与合同相符；

（2）检查货物封装是否合格，附件是否齐全；

（3）检查货物外观是否全新、完好、规格型号或者内部组件是否符合标准；

（4）检查系统软件和应用系统的相关功能和性能是否满足要求。

8.5 验收结论形成：依据合同要求，综合实施情况以及服务效果，做出验收结论，并形成验收报告。验收报告需明确服务内容的完成情况、服务质量是否达标、服务过程中存在的问题及改进措施等内容，由验收人员签字确认并加盖甲方公章。

8.6 验收不合格处理

到货验收过程中发现不合格产品的，甲方应及时通过电话、传真、信件等方式向乙方提出异议。乙方应在接到异议之日起 5 个工作日内，与甲方协商一致选择以下的一种或多种方式解决异议：

（1）上门修复、调试；

（2）更换同类型合格新产品。

若终验不合格，甲方应在验收结束后 5 个工作日内通知乙方，明确整改要求和期限（最长不超过 15 个工作日），乙方完成整改后应重新提交验收申请，甲方应在收到申请后 15 日内组织二次验收；二次验收仍不合格的，按本合同第十一条违约责任相关约定处理。

8.7 项目运维期间乙方提供 1-2 人驻场运维，三年期间数据归集，编目，共享，治理提供 2-3 人驻场。

软件系统发生故障时接到通知后 1 小时内响应，2 小时内到达现场维护。运行维护内容包括：系统故障修复、BUG 修复、定时检修服务和性能优化服务、运行状态检查、异常数据处理等。乙方应提供 7×24 小时的咨询电话，并安排技术人员解答使用中遇到的疑难。

乙方应当按照甲方要求提供服务，并按照双方约定的时间周期定期向甲方汇

报服务工作情况。

在产品安装、调试时，乙方应根据招标文件要求实施。

在质保期内乙方必须为最终用户提供技术服务热线，负责解答用户在设备使用中遇到的问题，并及时提出解决问题的建议和操作方法。当设备发生非人为因素严重故障时，乙方应当及时补充或者更换的设备运抵发生故障的设备所在地，由此产生的一切相关费用由乙方负担。

如因硬件或软件质量问题，乙方应积极根据甲方的要求及时维修，如需更换产品或配件，费用由乙方负担。

第九条侵权处理

9.1 如本合同以外的第三方指控乙方为甲方提供服务或其为甲方提供的服务成果侵犯该方的专利或著作权，乙方自费就上述指控自行或与甲方共同辩护，并支付法院和行政执法机关最终裁定的或经乙方同意的和解中包括的一切费用、损害赔偿金和合理的律师费用，前提条件是甲方：

（1）就指控立即书面通知乙方。

（2）容许乙方在辩护及任何有关的和解谈判中具有控制权，并配合乙方工作。

在满足上述条件的前提下，乙方就侵权指控对甲方承担本条约定的上述义务。

9.2 对因下列任何一项所引起的指控，无论本合同是否有其他约定，乙方均不承担责任：

（1）甲方提供的被并入服务成果之中的任何东西，或乙方遵照甲方或代表甲方的第三方所提供的任何设计、规格或关于实施方法的指示而提供的任何东西。

（2）甲方修改服务成果。

（3）甲方将服务成果与非由乙方提供的任何产品、数据、装置或商业方法一起结合、操作或使用，或为甲方以外的第三方的利益发行、操作或使用服务成果。

第十条个人信息保护和数据安全

为履行本合同，甲方委托乙方处理相关数据和个人信息的，双方同意按照本条约定执行：

10.1 个人信息种类：包括但不限于政务服务过程中涉及的自然人姓名、身份证号、联系方式、住址、业务办理记录等个人信息（具体以甲方提供的合法数据源为准）；乙方处理数据和个人信息的期限为：自合同签订之日起至服务期限届满后30日（仅用于数据备份清理及后续收尾工作）；处理方式为：数据采集、存储、清洗、脱敏、分析、共享传输及本合同约定的其他建设相关操作。

10.2甲方保证，其委托乙方处理个人信息已经向个人信息主体履行了法定告知义务，并取得了其同意。甲方保证，其委托乙方处理的个人信息和数据来源合法合规，不存在违反法律法规、监管要求的情况。

10.3双方均应当严格按照相关法律法规规定，采取措施确保个人信息处理活动符合法律、行政法规的规定，防止未经授权的访问以及个人信息和数据的泄露、篡改、丢失。

10.4乙方有权对甲方提供的个人信息和数据来源合法合规性情况进行检查。对于乙方检查发现甲方个人信息和数据来源违反法律法规、监管要求，或者就其向乙方提供的个人信息未依法向个人履行法定告知义务、未取得个人同意，乙方有权要求甲方在一定期限内整改。如果甲方未按照乙方要求整改或整改未达到乙方的相关要求，乙方有权解除合同，且不承担赔偿责任；由此给乙方造成损失的，甲方应当全额赔偿。

10.5 甲方违反本合同及其附件个人信息保护和数据安全相关条款和相关法律法规、监管要求的，甲方应当承担一切民事、行政和刑事责任，如因此给个人信息主体、乙方或其他人造成任何损失的，甲方应当承担全部责任

第十一条违约责任

11.1 双方确定，任何一方未履行或未完全履行本合同项下的义务，均构成违约。违约方应当赔偿因违约给对方造成的一切损失。

11.2 甲方未能按照本合同约定支付相关费用的，每逾期[1]日，甲方应当按照全国银行间同业拆借中心公布的同期一年期贷款市场报价利率向乙方支付违约金。甲方逾期付费累计达[30]日的，乙方有权终止本合同并不承担任何责任，并要求甲方承担乙方因追讨欠费支出的各项费用（包括但不限于律师费、诉讼费、保全费、财产保全担保费等）。

11.3 乙方未能按本合同约定按期提供建设的，每逾期[1]日，甲方应当按照全国银行间同业拆借中心公布的同期一年期贷款市场报价利率向乙方支付违约金。如违约金数额累计达到合同总费用的[20]%时，甲方有权终止本合同。

11.4 乙方对因本合同项下行为而导致的甲方或第三方可得利益损失、商业信誉损失、数据丢失或损坏以及间接损失或后果性经济损失等其他损失承担责任。甲方数据属甲方所有，甲方应当负责数据备份，乙方对甲方数据的丢失或损坏承担责任。

11.5 甲方承诺遵守国家相关法律法规，不进行危害网络安全的活动，若乙方发现甲方有危害网络安全的事项等活动，乙方有权停止技术支持，并解除本合同不负违约责任。若造成损失的，乙方使用合同款项进行处理，不足以处理损失的，乙方有权另行追究甲方违约责任。

11.6 本合同履行过程中，如乙方发生以下任一情形的，甲方有权视情节严重程度采取中止或终止履行合同、解除合同等措施并不承担违约责任。如该情形导致第三方向乙方提出法律或行政程序，乙方应当负责解决。如该情形给甲方造成损失的，乙方应当全额赔偿：

（1）被行政机关纳入“严重违法失信”名单；

（2）被人民法院纳入“失信被执行人”名单；

（3）被甲方（含甲方上级单位）纳入违规失信合作商名单；

（4）如存在网络和信息安全违法、违规行为的，包括但不限于因网络和信息安全问题承担刑事责任或受到行政处罚，被列入各级公安机关的涉通讯信息诈骗违法犯罪高危自然人或法人名单、电信业务经营不良名单、失信名单等；

（5）其他相关法律法规规定或有权机关认定的违法失信情形，以及可能导致合同履行风险或侵甲方合法权益或声誉的违规失信情形。

第十二条所有权和知识产权

12.1 乙方保证甲方在使用成交货物（服务）时，不侵犯任何第三方知识产权。如因乙方提供的原生软件产品（非二次开发部分）引发知识产权纠纷，由乙方承担全部责任（包括但不限于赔偿损失、维权费用）。

12.2 本项目软件产品的原生知识产权（包括源代码、基础功能模块等）归原权利人所有，甲方享有合法使用权；项目二次开发成果（包括针对本项目定制的功能模块、代码修改、适配开发成果等）的知识产权归甲方所有，乙方享有在不侵犯甲方知识产权前提下的技术成果推广权，但不得直接用于其他同类项目。

12.3 乙方保证对其提供的合同产品及二次开发成果拥有合法权利，无任何权利瑕疵（包括但不限于无抵押、质押、查封等限制），不妨碍甲方对产品的使用和所有权行使。

12.4 本合同硬件资产的所有权归甲方所有，具体资产明细详见附件清单。

12.5 甲方如需将二次开发成果进行后续商业化应用或对外授权，应提前书面告知乙方，乙方应提供必要的技术支持（另行约定费用的除外）。

第十三条双方确定，在本合同有效期内，甲方指定[杨凡]为甲方项目联系人，乙方指定[刘珍]为乙方项目联系人。

一方变更项目联系人的，应当及时以书面形式通知另一方。未及时通知并影响本合同履行或造成损失的，应当承担相应的责任。

第十四条双方确定，出现下列情形之一，致使本合同的履行成为不必要或不可能的，可以解除本合同：

14.1 发生不可抗力，且受影响方在不可抗力发生后 30 日内通知对方，双方协商后仍无法继续履行合同的；

14.2 一方严重违约，经另一方书面催告后 15 日内仍未整改，导致合同目的无法实现的；

14.3 乙方被吊销营业执照、宣告破产或进入清算程序，无法继续履行合同义务的；

14.4 因国家政策调整导致项目停建、缓建，且超过 90 日仍无法恢复建设的；

14.5 双方协商一致书面同意解除的。

合同解除后，已完成的合格工作成果对应的费用按合同约定结算，未完成部分停止履行，违约方应赔偿对方因此造成的损失。

第十五条法律适用和争议解决

15.1 本合同适用中华人民共和国法律。

15.2 所有因本合同引起的或与本合同有关的任何争议通过双方友好协商解

决。如果双方不能通过友好协商解决争议，则任何一方均可向项目所在地有管辖权的人民法院起诉。

15.3 诉讼进行过程中，双方继续履行本合同未涉诉讼的其他部分。

第十六条不可抗力及免责

16.1 如由于战争、骚乱、恐怖主义、灾害、国家法律法规或规章变动、网络安全、网络无法覆盖、停电、通信线路被人为破坏、黑客攻击、计算机病毒侵入或发作、突发事件等，导致甲乙双方或一方不能履行或不能完全履行本合同项下有关义务时，受影响方不承担违约责任，但应当尽快书面通知对方。在影响消除后的合理时间内，一方或双方应当继续履行合同。如因此导致合同不能或者没有必要继续履行的，本合同可由一方解除。

16.2 如乙方根据政府管理部门要求暂停或终止提供相应服务，乙方不承担任何责任。

第十七条合同生效和其他

17.1 本合同纸质文本一式四份，甲乙双方各执二份，自双方签字盖章之日起生效；若使用电子印章的，自双方盖章之日起生效。

若乙方加盖电子印章的，以加盖乙方电子印章的本合同电子文档所载内容为准。

17.2 如果本合同的任何条款在任何时候变成不合法、无效或不可强制执行而不从根本上影响本合同的效力时，本合同的其他条款不受影响。

17.3 本合同各条标题仅为提示之用，应当以条文内容确定各方的权利义务。

17.4 未得到对方的书面许可，一方均不得以广告或在公共场合使用或模仿对方的商业名称、商标、图案、服务标志、符号、代码、型号或缩写，任何一方均不得声称对方的商业名称、商标、图案、服务标志、符号、代码、型号或缩写拥有所有权。

17.5 本合同的任何内容不应当被视为或解释为双方之间具有合资、合伙关系。

17.6 本合同替代此前双方所有关于本合同事项的口头或书面的纪要、备忘录、合同和协议等法律文件。

17.7 甲乙双方因履行本合同或与本合同有关的一切通知都应当按照本合同中的地址，以书面信函或者传真或者电子邮件方式进行。其中：

17.7.1 除本合同另有约定外，有关下述任一事项的通知，均应当采用书面信函形式作出，否则，该通知无效，不产生本合同项下的任何通知效力：

（1）与本合同费用及支付事宜有关的通知；

（2）与本合同违约事宜有关的通知；

（3）与本合同终止、解除或变更事宜有关的通知；

（4）与本合同延续/续展有关的通知；

17.7.2 本合同约定的各种通知方式的送达标准如下：

（1）如采用书面信函形式，应当使用挂号信或者具有良好信誉的特快专递

送达，接受方签收挂号信或特快专递的时间（以邮局或快递公司系统记录为准）为通知送达时间；

（2）如采用传真方式，传真到达接收方指定传真系统的时间为通知送达时间；

（3）如采用电子邮件方式，电子邮件到达接收方指定电子邮箱的时间为通知送达时间。

如果因接受方原因（包括但不限于接受方拒收书面信函、接受方传真机关闭或故障、接受方电子邮箱地址不存在或者邮箱已满或者设置拒收等）导致通知发送失败，视为通知已经送达（发送方侧载明的书面信函寄出时间或者传真发送时间或者电子邮件发送时间视为通知送达时间）。

17.7.3 本合同双方通知地址及方式如下：

甲方：[铜川市数据中心]

地址：[铜川市正阳路 9 号]

联系人：[杨凡]

电话：[18590985543]

乙方：[中电信数智科技有限公司]

地址：[北京市海淀区复兴路 33 号 13 层东塔 13 层 1308 室]

联系人：[刘珍]

电话：[18991230602]

上述任何信息发生变更的，变更方应当及时以书面形式通知另一方，未及时通知并影响本合同履行或造成损失的，应当承担相应的责任。

17.8 附件为本合同不可分割的部分。若附件与合同正文有任何冲突，以合同正文为准。

17.9 本合同未尽事宜，根据甲方需求，双方协商确定补充内容。

本合同附件为：

附件一：服务清单

附件二：数据安全及保密协议

附件三：交付内容

补充附页

经友好协商，对本合同条款补充、修改如下，本补充附页为合同正文的一部分，与合同正文冲突时，以本补充附页为准：[无]

（本页无正文）

甲方：[铜川市数据中心]

法定代表人/负责人
或授权代表：

乙方：中电信数智科技有限公司

法定代表人/负责人
或授权代表：

签署日期：[2026]年[1]月[30]日

附件一：服务清单

铜川市一体化政务大数据平台暨数据安全底座项目分项报价表

单位：万元

（一）政务一体化大数据平台

序号	模块名称	品牌	型号	参数要求	数量	单价	合计
1	数据服务门户	中国电信	定制	1.门户覆盖部门、分类及服务方面最全，且提供数据单位最多的政府信息整合和数据共享服务的平台，现政务信息的“网络互通、数据共享、业务协同、服务融合” 2.数据服务门户主要包含通知公告、政策法规、资源目录、事项办理、资源服务、综合统计、个人中心等模块。	1	22	22
2	数据治理系统	中国电信	定制	1.数据采集：主要包含以下功能：数据概览、采集记录、离线任务、实时任务、文件模板、文件上传、消息管理、消息概览、数据模板、主题管理、消费组管理、消息配置。 2.管理中心：分类管理、业务场景、业务标签、资产申请、审批中心、权限审计、类型映射、类目授权 3.数据资产：主要包括资产概览、我的数据、我的接口、资产编目、资产发布、资产目录、资产授权、应用管理等功能 4.数据标准：主要包含数据元素、代码管理、标准文件、命名标准、命名标准报告、函数管理、资源分类、数据分层、组件管理、开发场景、公共字段集合等功能 5.元数据：主要包含元数据分布、数据源管理、元数据采集、数据表管理、回收站、热点表、热点字段表、血缘查询、版本查询、元数据监控、数据操作记录等功能。 6.数据探查：以标准数据元素的配置数据格式校验规则、数据识别规则为基准，通过数据识别技术自动建立数据元素与表字段的关联关系，从而识别出数据元素的探查规则，了解表的现状，快速制定数据检核方案，提供数据质量。	1	30	30

		中国电信	定制	1.数据标识与分类：建立数据库，数据挖掘与基础治理； 2.数据工具模型建立，编写工具脚本，提供规模化数据治理服务；	1	36	36
3	数据处理分析系统	中国电信	定制	1.数据处理：数据处理主要是通过对各类数据资源进行标准化处理和融合处理，从而提升数据价值密度。主要包括清洗记录、数据清洗、数据比对、数据分发等功能。 2.数据质量：面向管理数据，对数据完整性、准确性、一致性、规范性进行分析和管理，并对数据进行跟踪、处理和解决，实现对数据质量的全程管理，提高数据的质量。主要包括综合质量报告、质量检核规则、质量检核任务、质量检核记录、问题数据管理等功能。 3.数据模型：提供体系化、系统化建模及研发的功能，将数据仓库理论以工具化半自动化实现：自顶向下快速构建业务维度、业务过程，并进一步细化开发维度表、事实表、汇总表、应用层，沉淀标准统一的数据资产，便于业务分层数据应用的同时优化计算存储。主要包括指标属性、原子指标、派生指标、复合指标、关系建模、维度建模、指标计算等功能。 4.数据安全：数据安全提供全面的数据安全管理能力，涵盖了数据资产发现、分类分级、加密、脱敏、权限控制以及数据访问监测等多个环节。配套本地化安全服务，帮助客户提高数据风险识别和应对能力，满足合规要求，降低潜在的数据安全威胁。主要包含安全等级、识别规则、脱敏规则、识别函数、敏感数据识别、敏感数据确认、敏感数据配置、用户安全等级、脱敏任务、敏感词库等功能。 5.任务运维：任务运维通过多维度监控、异常任务快速定位与处理、数据上下游溯源与差异定位、服务器资源及任务状态监控、用户权限与日志等基础信息管控，实现了调度任务全生命周期的透明化运维，提升了任务运行的可控性、问题处理效率及系统资源利用合理性数据运维、系统管理	1	35	35
		中国电信	定制	1.利用数据治理的工具从业务系统对接数据、采集元数据、识别数据关系，进行可视化治理分析，形成数据字典的数据模型， 2.从业务流程和数据应用的视角出发，完善包含业务属性、管理属性的数据资产信息，形成数据治理分析资产目录	1	57	57

4	数据目录系统	中国电信	定制	1. 数据目录：数据目录系统是梳理、登记数据资源的核心工具，可汇聚多源数据的基本信息并分类编目，形成结构化数据清单，方便用户快速查找、理解和申请使用数据，同时支撑数据管理与共享，为数据高效流转奠定基础。主要包含数据服务门户资源目录、信息资源目录等功能。 2.资源图谱：政务数据资源图谱，是一张由政务数据资源要素相互连接而成的关系网络，是基于图的数据结构，由节点和边（节点间的相互关系）组成。政务数据资源图谱从不同维度对政务数据进行结构化关联和可视化描述，是对政务数据资源背后复杂逻辑关系的梳理和展示。主要包含资源图谱确定流程、数据图谱等功能。	1	20	20

5	数据供需系统	中国电信	定制	1.任务中心：任务中心是对清单系统内所有应走审核流程的一个统一管理界面，界面以概览页面形式展示，包括我申请的、我审核的、待认领的等一键式查看方式，同时可直观查看审核概况、待办事项数量、审核流转位置查看、已办结事项数量、待审批数量、已审批、已申请等数量展示。 2.清单交办是针对管理部门对上级派发下来的任务进行统一分配和分发所预留的功能，方便管理进行统一的线上管理，避免了过去只能线下交互的方式，能快速整理并分发任务到各级部门，实现工作效率有效提升。主要包含清单派发、实施情况、清单公示等功能。 3.责任清单：明确本单位可以向其他单位共享的数据责任清单，具体可细分为数源责任和共享责任，数源责任即本单位按照行政职能采集，作为公共数据资源的权威来源。主要包含责任清单编制、责任清单认领、责任清单关联目录、责任清单转负面清单、清单下线、清单变更等功能。 4.需求清单：对各部门需求清单需求事进行管理，对相同的需求申请可由提供方将数据的授权权限给予管理部门用户，进行整体授权并进行一键批复，授权通过后，授权信息自动备案至提供方部门。主要包含清单编制、需求清单变更、需求清单撤销、需求合并等功能。 5.负面清单：各部门对法律、法规、规章明确规定不能共享的数据、列入到负面清单中，形成负面清单。主要包括负面清单编制、负面清单转责任清单、负面清单变更、负面清单删除、清单暂办等功能。 6.知识库管理：清单知识库维护对国家、及地方有关标准发文、法律依据、条文等进行及时管理，确保清单来源有依据、清单修改有判定，不同角色用户都有权利进行知识库文件维护。主要包含知识搜索、知识中心、文档新建等功能。 7.系统接口对接：主要包含共享交换平台接口对接、共享网站接口对接等功能。	1	12	12

6	数据共享系统	中国电信	定制	1.分类管理：把各类行业的分类信息进行分组，每个分组内单独管理自有的分类信息和编码规则信息。 2.数据资产：通过我的应用支撑用户应用与数据资产的关联使用，资产编目实现数据资产的清晰梳理与分类，资产发布推动数据资产的共享流通，类目授权保障数据资产访问的合规性。主要包括我的应用、资产编目、资产发布、类目授权等功能。 3.元数据管理：元数据管理涵盖数据源管理、元数据采集、数据表管理、回收站及数据分层等子项，通过对数据源、元数据、数据表的全流程管理，结合回收站的资源回收及数据分层的结构优化，实现元数据的有效管控，助力数据资产的规范化与高效利用。 4.数据服务：包含服务分类、服务开发、服务管理和调用日志等子项，通过服务分类实现服务的有序归类，服务开发支持服务的创建，服务管理保障服务的有效运营，调用日志记录服务的使用情况，从而全面实现数据服务的分类、开发、管理及使用过程的可追溯，助力数据服务的高效应用与价值发挥。	1	15	15
7	数据交换系统	中国电信	定制	1.数据交换：基于数据统一服务设计理念，建设统一数据服务工具引擎，将全域数据中心前的数据提供给上层访问调用，实现数据的应用变现和数据的闭环。主要包括概览、待办任务、已办任务、目录编制、事项目录、目录变更、服务登记、资源申请、已申请资源、已共享资源、我的数据箱、交换任务、文件列表等功能。 2.数据服务：将数据和后端服务以 API 形式开放，简化分享数据或提供服务的过程，降低各委办局子系统之间对接的成本。提供不同语言的 API 和示例代码，简化各委办局新老系统以 API 形式开放后端服务的过程。主要包括服务分类、服务概览、服务开发、服务管理、数据查询、黑白名单、业务码管理 SDK 管理、服务授权、服务监控等功能。	1	12	12

8	数据开放系统	中国电信	定制	1.数据开放门户：数据开发门户是提供给个人或企业查看政府对外开放的数据，包括数据目录、数据接口、请求数据查看和申请、开放动态。主要包含互联网用户、政府用户、资源管理部门的领导用户、各委办局处理日常事务的业务用户及系统应用运维的系统管理员，前台数据展示包含所有用户。主要包括数据目录、数据接口、数据应用、统计分析、开发者中心、开放动态等功能。 2.数据安全管理：系统管理员通过配置敏感主题、敏感词词库、敏感词检测，对识别到的敏感数据脱敏显示。	1	10	10
9	数据级联系统	中国电信	定制	1.数据上报：数据上报是政务数据共享交换级联系统的重要功能，主要包括组织机构、目录分类、应用系统、目录信息、库表资源、文件资源、服务信息等内容的上报，可查看待上报和已上报的记录，并支持查询，通过这些操作实现本级数据向省级的级联上报。 2.系统管理：系统管理涵盖用户、角色、菜单及参数管理，通过用户权限控制、角色权限区分、菜单功能配置及系统参数维护，保障级联系统有序运行。 3.系统监控：系统监控包含在线用户管理、定时任务配置和数据监控功能，可记录并强制下线在线用户，自定义任务执行周期，监控数据源、SQL、防火墙等信息，保障系统稳定运行。 4.级联服务配置：主要包括服务信息配置、服务模型配置、SQL数据配置等功能。	1	17	17
			定制	1.国家平台、省级平台及市级业务系统平台数据接口对接 2.按照规范文档，展开接口的开发及调试 3.数据对接需遵循统一的数据格式与传输协议，确保字段映射准确、编码一致，通过接口实现数据的定时同步与实时交互。在开发过程中，需严格对照国家平台与省级平台的技术规范，完成身份认证、数据加密、异常处理等关键环节配置，并进行多场景联调测试，保障数据上报的完整性、准确性与及时性。	1	30	30

10	数据直达系统	中国电信	定制	1 基础信息对接管理：系统支持组织机构与应用系统的基础信息全流程管理，涵盖组织机构的上报、变更、下发等功能，以及应用系统的基础信息维护、上报、变更、下发、撤销等。主要包括省市组织机构对接、组织机构展示和查询、应用系统信息与组织机构绑定、应用管理等功能。 2. 数据目录对接管理：提供数据目录的全生命周期管理功能，支持数据目录的注册、上报、发布、下发、变更、撤销及审核等操作，确保数据目录的规范管理与动态更新。通过与上级平台和下级平台的无缝对接，系统能够及时同步数据目录信息，保证国家、省、市三级平台之间数据的一致性、完整性与及时性。同时，系统支持自动化流程与人工审核相结合，确保数据目录变更的准确性与合规性。 3. 数据资源对接管理：提供数据资源的全生命周期管理功能，支持数据资源的注册、上报、发布、下发、变更、撤销及审核等操作，确保数据目录的规范管理与动态更新。通过与上级平台和下级平台的无缝对接，系统能够及时同步数据目录信息，保证国家、省、市三级平台之间数据的一致性、完整性与及时性。系统采用自动化流程与人工审核相结合的方式，确保数据资源操作的准确性与合规性。 4. 数据申请对接管理：系统通过共享申请的提出、审核、上报、下发、撤销，支持跨层级、跨部门的协同处理。 5. 数据供需对接管理：通过数据需求的提出、受理、挂载、审核、上报、下发、撤销，实现跨层级、跨部门的数据需求处理闭环。需求部门提出数据需求后，由同级数据主管部门在时效内完成受理，并通过本级平台提交至上级平台。上级平台转发需求后，数源部门同级数据主管部门时效内完成受理，数源部门在时效完成审核。省级平台可通过查询接口实时获取审核进度与结果审核通过后，数源部门原则上在要求时效内完成数据资源注册，并与相关政务需求关联；审核不通过的，需明确驳回理由。 6. 数据异议处理对接管理：系统支持数据异议的提出、上报、审核、下发、撤销 实现数据异议的高效处理与闭环管理，确保数据共享的准确性与合规性。 7. 数据应用创新推广对接管理：支持数据应用案例的提出、上报、审核、下发、撤销，推动政务数据创新应用的推广与落地。各地区需求部门总结数据应用案例后，由本级平台通过数	1	20	20

				据接口提交至上级平台。上级平台接收后在时效内完成审核并发布，本级平台通过数据接口获取已发布的案例信息，并依托数据直达专区进行展示与发布。各级数据主管部门建立政务数据创新应用案例库，选取本级及上级案例库中的代表性案例，加强宣传推广，促进数据应用的广泛落地与使用。主要包括查询应用案例列表、我的案例、填报应用案例、更新应用案例、撤销应用案例等功能。 8.垂管系统对接管理：相关申请渠道，实现国家、省、市三级直连申请。垂管系统数据申请对接、垂管系统数据申请列表查询（申请列表、申请同步）垂管系统数据申请详情查询（基本信息、操作记录）垂管系统数据申请审核对接。主要包括资产超市列表、我的资源等功能。 9.运行监测：基于时间维度的动态数据展示，通过图形化界面直观呈现国家、省、市三级数据目录、数据资源、创新应用、供需对接、数据异议及共享申请的实时情况。同时，系统可清晰展示市到省、省到国家之间的数据交互流向与状态，帮助用户全面掌握跨层级数据共享的动态过程与成效，为数据管理与决策提供可视化支持。主要包括数据目录统计、数据资源统计、用户访问统计、资源访问统计、接口调用统计、数据交换统计、数据申请统计、供需对接统计、异议处理统计等功能。 10.数据直达专区构建：根据国家数据直达基层对接要求，持续提升平台的数据目录、资源管理、数据申请、基础信息、数据供需、数据异议、应用创新、垂管系统对接等能力。完成一体化大数据平台国家、省、市三级节点对接，实现跨层级、跨地域之间的数据目录通、数据资源通、业务流程通，持续推动数据共享应用。主要包括基础系统、对接测试、数据直达专区等功能。			
（二）数据安全管理平台							
序号	名称	品牌	型号	技术参数	数量	单价	合计
1	数据安全	中国电信	定制	数据安全中心 1：用于敏感数据识别、分类分级标识等数据安全管理工作。系统规	2	33	66

	中心			格：最大支持数据源数：1000。 数据安全中心 2：用于数据安全集中管理，用于集中管理数据安全系列组件，实现统一认证、账户审计、设备管理、状态检测等功能。系统规格：最大接入数据安全设备数：100。 1、产品支持丰富的文档类型，包括办公文档 WPS 软件格式及版本（doc/docx、xls/xlsx、ppt/pptx、pdf、txt、ofd 等）、压缩包（rar、zip、7z 等）、图片（bmp、png、jpg、gif 等）、源代码（xml、sh、c 等）支持识别多层嵌套压缩文件中文档内容。 2、内置敏感数据特征库功能，包含 60+类特征规则，包括姓名、身份证号、电话号码等关键个人隐私数据。 3、支持通过数据识别规则对数据资产（表、簇、目录、字段、文件等）进行分类分级打标，并查看打标结果。 支持通过数据特征和资产属性构建识别规则。可针对数据特征（特征项）、资产属性（表名、表注释、字段名、字段注释等）设定单一规则。也可针对多规则之间以“与”、“或”等逻辑关系进行组合形成规则集。 4、支持资产热度分析，统计数据资产使用情况，可覆盖表级，方便用户了解高频资产、低频资产、静默资产等。 5、支持对同标段中的数据库审计、数据静态脱敏、API 审计、网络防泄漏产品的接入集中管理。 6、支持对同标段中的数据库审计、数据静态脱敏、API 审计、网络防泄漏产品的状态监控，并支持资源信息的监控（CPU 使用率、内存利用率、剩余磁盘） 7、 支持对同标段中的数据库审计、数据静态脱敏、API 审计、网络防泄漏、数据库加密网关、数据库运维管控产品的单点登录。 8、支持发现僵尸库表、敏感数据篡改、数据下载量异常、异常时间下载敏感数据、登录地址异常、登录时间异常等风险。 9、支持针对采集日志进行时间窗口的周期配置，制定具体时间窗内口触发的次数			

				阈值以分析生成告警。 10、支持 kafka 和 syslog 类型的日志外发采集，支持自定义解析规则上传后进行日志解析。 11、支持忽略、手工处理、工单处理、白名单等方式进行告警处理。 12、支持根据告警相关条件进行智能批量处理。如可根据事件名称、风险类型、风险等级、客户端 IP、关联资产类型、关联资产等条件进行类似告警的批量处置。 13、支持后期扩容，对其他业务系统提供数据安全和网络安全支撑。			
2	数据库加密网关	中国电信	定制	1、可依据数据分级分类的标准，对于敏感数据、内部数据等重要数据在存储时进行加密处理。加密后的数据以密文的形式存储，保证存储介质丢失或数据库文件被非法复制情况下数据的安全。加密速率 70000 单元格/秒，最大并发连接数 7000，数据库实例 20 个。 2、支持国密浏览器，采用国密证书和国密算法，支持基于 ukey 的认证双因子认证，满足密评的要求 3、支持 MySQL、Oracle、达梦、海量、Kingbase、GaussDB A、PostgreSQL、SQLServer、MariaDB、HighGO、DWS 国产数据库类型，且以上数据库类型都支持列加密和国密算法 4、支持 HotDB、TDSQL、TBASE 等大数据数据库的加密，并且以上均支持列加密和国密算法 5、支持全面的业务感知能力，包括访问请求趋势 QPS、风险 TOP5、访问请求 TOP5（基于数据源和账号）、并发数、流量等趋势图，并可基于 1 小时、1 天、7 天、30 天查看相应的历史折线图 6、支持在数据源管理页面查看安全规则、加密规则、脱敏规则以及相应的规则数量，并可一键进入相应规则配置页面进行规则配置 7、可基于某个数据源配置业务透传，直接从底层进行转发，保证业务正常运行，支持代理级和业务级两种模式 8、支持静默扫描、性能扫描两种扫描模式，支持跨数据源多表同时扫描，配置扫	2	17.5	35

		描例外表，支持根据数据结构、数据特征标签库进行针对性扫描，可选择扫描单次、每日、每周、每月对数据资产进行敏感数据和分类分级标识，扫描进度的百分比可实时查看 9、支持自动检测表新增列、修改列的分类分级信息，并自动刷新到相应脱敏策略，自动基于新增列、修改列进行脱敏，无需人为参与 10、支持查看每个数据源下的数据资产分类分级详情，一个数据资产可命中多个标签库，并可给出是否可加密、脱敏的标识，支持一键快速创建脱敏和加密策略 11、安全规则按照页面显示顺序的优先级进行匹配，支持鼠标拖动调整优先级，支持默认规则，可对所有未命中规则的流量做统一的处理，且每条安全规则有命中次数统计，方便实时查看每条安全规则的使用情况，以便进行策略调优 12、支持基于多表、分类分级配置加解密规则，并支持各阶段任务进度的可视化展示，包括智能分析结果/时长，加解密结果/进度，实时加密防护状态等 13、支持自定义添加或从智能分析结果中同步存在 Join 关系的加密列，将其配置为共享列密钥，以保证密文列的关联查询、写入等 14、支持自动和手动创建密文索引，支持在管理页面上创建密文索引，并可自定义索引长度，以提升数据加密后的查询效率 15、支持标准的主密钥(RK)、密钥加密密钥-库密钥(DSK)、数据密钥-列密钥(DEK)三级密钥管理技术保障密钥安全 16、支持基于数据对象组、自定义脱敏对象、数据库账号、数据库账号组、数据分类、数据分级、脱敏模版等条件创建动态脱敏规则 17、记录敏感数据类型、敏感字段数以及具体的表名、字段名、数据分类、数据分级、识别位置、是否敏感等详情 18、记录各个安全策略命中日志详情，包含该日志命中的防护规则、脱敏规则、加密规则名称和风险等级等信息。另外数据加解密信息还包括：加密表名、加密列名、加密方式、加密算法、校验算法、加解密数量；记录数据脱敏信息包括表名、脱敏列名、数据类型、脱敏算法、脱敏数量等		

				19、支持业务日志基本信息、分类分级信息、策略命中日志详情在一条日志中记录和查看，支持业务语句翻译功能 20、支持使用离线密文恢复工具将密文恢复成明文，防止不可预测原因导致系统宕机后数据库数据不可解密，支持对单表进行密文恢复。 21、支持后期扩容，对其他业务系统提供数据安全和网络安全支撑。			
3	网络数据防泄漏	中国电信	定制	1、可通过流量牵引技术，可对受控区域内的外发流量进行深度解析、内容恢复和敏感度扫描，及时发现受控区域内通过网络泄漏数据、传播数据的行为，并进行拦截、告警、审计等措施。系统能够根据网络环境和监控需求，进行灵活多变的部署。内含：（1）旁路镜像模式部署；（2）网络流量恢复；（3）传输内容识别；（4）支持2000M及以下镜像流量；（5）内容扫描速度不高于40MB/S等。 2、支持针对Windows，Linux服务器安装插件（非终端DLP），插件支持安装在Windows，CentOS，Redhat，Ubuntu，统信、银河麒麟等国产系统，基于插件抓取目标服务器的流量进行敏感内容分析，插件能够对目标服务器进行网卡，IP，端口等进行抓包过滤，支持对插件的统一管理，包括状态监控，版本管理等 3、支持基于正反向样本的机器学习算法；支持基于正反向样本的机器学习算法；支持将误报文件自动加入到训练模型的反向样本中进行再次训练，提升模型的识别准确度 4、对于常见压缩文件能够判断文件嵌套或压缩的深度，深度识别出100层；同时，也可以将每个被嵌套的文件进行单独的内容识别，判断要识别的内容是否都在一个被嵌套文件中，还是分散在多个嵌套文件中 5、支持对网络中的HTTP、HTTPS、SMTP、SMTPS、POP3、POP3S、IMAP、IMAPS、FTP、FTPS、NFS、SMB等协议进行监控，并能够完整地恢复流量中传输的内容，同时支持上述协议自定义端口的流量进行文件恢复和内容识别 6、支持对MPLS、PPPoE、VLAN、VXLAN、IPv6、GRE、双栈封装、ERSPAN等协议流量进行协议识别和内容识别，并且能够在Web对上述协议的识别进行控制；对IPv6的支持产品应提供IPv6 Ready证书	1	15.7	15.7

				7、支持对SSH、SFTP协议流量进行协议识别和内容识别，并且能够在Web对上述协议的识别进行控制，同时支持上述协议自定义端口的流量进行文件恢复和内容识别 8、支持加密流量的识别和检测，支持自动检测安装证书情况，对于未安装证书的终端，支持提供在线证书下载页面，用户可自助下载证书，一键安装证书 9、支持基于用户的分析溯源能力，包括异常用户行为告警，单用户行为分析，用户行为追溯；支持对用户进行风险评分，定义风险等级，用户命中策略TOP，用户行为溯源追溯，用户风险象限等级分布等； 10、支持泄漏流转标注地理属性，能够直观的了解数据流转的地理信息，知晓是否有跨境传输的风险，地理属性支持到城市级，所属运营商，支持IP地址库校准 11、支持常见的运维管理功能，包括网络抓包、网络连通性检测、路由追踪、服务连通性检测、系统服务连接展示、一键采集诊断信息等功能，且上述所有功能可以在Web进行自行配置和管理，也可以展示详细的执行结果 12、支持多重业务保障能力，能够基于Web灵活配置相关参数，包括硬件状态感知，能够基于CPU，内存，硬盘的使用阈值是否启动业务保障能力，也支持周期性的服务状态感知及实时的内容扫描性能感知，当服务异常或性能过载时能够优先保障业务，也支持Web一键关闭安全服务，优先保障业务； 13、产品应支持和第三方系统对接能力，包括事件能够支持syslog、Kafka外发；支持策略API接口，第三方系统能够调用API接口直接进行策略下发，策略也能够支持Kafka外发；内容识别能力支持API接口，第三方系统能够直接调用API接口传送文件进行内容识别并返回识别结果，上送系统对接能力需在同一台设备上实现，并提供详细的对接文档。 14、支持后期扩容，对其他业务系统提供支撑。			
4	数据库审计	中国电信	定制	1、可实现对数据库访问行为的全程监控、高危操作的实时告警和安全事件的审计和追溯。纯软件，默认支持数据库实例：64个，数据库流量：800Mbps，SQL峰值处理能力：80000条/秒，SQL日志存储数量：160亿条。	1	9	9

				2、支持对安装插件的主机进行监控，可采集展示主机名称、操作系统、平台、CPU使用率趋势、内存使用率趋势和流量趋势等； 3、支持插件抓包网卡设置和采集流量过滤设置，过滤条件至少支持客户端IP、客户端端口等，支持将插件设置的过滤条件作为模板应用到其他插件； 4、支持插件阈值设置，可设置数据库服务器的CPU利用率、内存利用率、带宽等阈值或插件自身占用的CPU利用率、内存利用率、磁盘空间占用、带宽阈值，当超过阈值时审计采集插件自动休眠，临时暂停抓包工作，避免与数据库服务器抢占资源。 5、支持Hive与Kerberos集成，Hive传输加密的解析 6、支持敏感数据标签管理，系统内置包括个人信息安全规范标签库，内置敏感数据标签包含港澳居民来往内容通行证、性别、名族、统一社会信用代码、港澳通行证、IP地址、IPv6地址、MAC地址、IMEI、MEID、企业单位名称、电子邮箱、中文地址、固定电话、手机号、银行卡号、军官证号、社保证号、护照号、驾驶证、身份证号、中文姓名等22条敏感数据规则，内置其他标签库共14条敏感数据标签规则； 7、支持敏感数据识别规则，可通过配置识别策略，通过流量动态识别方式对资产访问中的敏感数据进行识别并标记； 8、支持按照资产维度展示其表、字段敏感数据识别的数据标签和敏感等级； 9、支持发现数据库所在的服务器的异常网络通讯行为，包含访问数据库服务器上的非数据库协议通讯审计全记录。 10、支持发现数据库服务器主动外联通讯行为，外联审计结果全记录可追溯。 11、支持通过审计日志快速添加黑白名单、自定义规则、更新用户行为模型，审计规则和用户行为模型自动引用审计日志内容作为规则或模型条件。 12、支持对告警日志进行多维下钻分析、自定义选择图类型（饼图、柱状图），展示分析结果，支持自定义选择下级维度，下钻层数不小于18层。 13、支持通过审计日志进行SQL模板响应分析，对资产选定时间范围内的SQL模板			

				访问数、平均执行时长、平均影响行数进行分析； 14、支持SQL模板数趋势分析，对资产选定时间范围内新增SQL模板数和使用SQL模板数进行趋势分析； 15、支持通过分析条件生成报表模板； 16、支持后期扩容，对其他业务系统提供数据安全和网络安全支撑。			
5	数据库运维管控	中国电信	定制	1、可针对数据库运维人员的访问进行安全管控。系统通过多因素认证、权限控制、操作审批、动态脱敏、误删恢复、行为审计等功能，对运维行为进行全周期管理，做到事前审批、事中管控、事后审计。主要参数：可支持数据库实例：40个 SQL峰值处理能力：32000条/秒 2、支持针对业务的实时统计，包括实时访问请求趋势、访问请求TOP5、并发趋势、流量趋势等信息，并可基于最近1小时、24小时、最近7天、最近一个月和自定义时间，以折线图的方式直观展现趋势图。 3、支持在数据源管理页面查看安全规则以及相应的规则数量，并可一键进入相应规则配置页面进行规则配置 4、可基于某个数据源配置业务透传，直接从底层进行转发，保证业务正常运行，支持代理级和业务级两种模式。 5、支持静默扫描、性能扫描两种扫描模式，支持全量和增量两种扫描策略，可选择扫描单次、每日、每周、每月对数据资产进行敏感数据和分类分级标识，扫描进度的百分比可实时查看。 6、支持查看每个数据源下的数据资产分类分级详情，一个数据资产可命中多个标签库，并可给出是否可脱敏的标识，支持一键快速创建脱敏策略。 7、安全规则按照页面显示顺序的优先级进行匹配，支持鼠标拖动调整优先级，支持默认规则，可对所有未命中规则的流量做统一的处理，且每条安全规则有命中次数统计，方便实时查看每条安全规则的使用情况，以便进行策略调优。 8、可支持强制安全客户端认证，用户必须使用设备自带安全客户端工具才能访问该数据源，保证用户身份可信；支持基于运维账号做管控，实现隐藏数据库真实账	1	16.5	16.5

				号，提升数据源的运维安全的目的。 9、记录敏感数据类型、敏感字段数以及具体的表名、字段名、数据分类、数据分级、识别位置、是否敏感等详情。 10、记录各个安全策略命中日志详情，包含该日志命中的防护规则、脱敏规则、工单审批规则名称和风险等级等信息。记录数据脱敏信息包括表名、脱敏列名、数据类型、脱敏算法、脱敏数量等。 11、支持业务日志基本信息、分类分级信息、策略命中日志详情在一条日志中记录和查看，支持业务语句翻译功能。 12、支持业务字典功能。用户可在业务字典中配置业务 IP、业务账号、业务操作、业务操作对象、语句模板等维度对应的业务语句，为用户查询日志时提供经过翻译更易读的 SQL 语句 13、支持通过数据源和会话两个维度呈现可视化图表方式展现业务数据：业务流量包括上下行流量、在线会话数、新建会话数、SQL 请求速率等；业务安全风险包括风险告警数、语句拦截次数、会话阻断次数、IP 黑名单命中次数、虚拟补丁命中次数等。 14、支持后期扩容，对其他业务系统提供数据安全和网络安全支撑。			
6	静态脱敏	中国电信	定制	1、可通过数据脱敏机制对某些敏感信息通过脱敏规则进行数据的变形，实现敏感数据的可靠保护。在不影响数据共享规则条件下，对真实数据进行改造并提供使用。性能规格：峰值脱敏速度：60G/h ，最大脱敏能力：810000 单元格/秒，视用户数据库吞吐性能而定授权：默认支持数据库实例：20 个 2、支持 Oracle，MySQL，SQL Server，PostgreSQL，DB2，informix，GaussDB，神通，人大金仓，达梦，GBASE，Greenplum，TeraData，HIVE，HBASE，HDFS，MongoDB，TiDB，ClickHouse，ODPS 等数据库。 3、支持用户通过 Java 函数自定义编写脱敏算法，满足用户多样化的脱敏需求。 4、支持对已脱敏的数据进行逆向脱敏查询，得到真实数据，便于用户校验数据的可使用性。	1	10.5	10.5

				5、提供快速导出方案能力，支持配置最低匹配率和脱敏算法后进行扫描，扫描结果无需手动导出，即可自动生成方案使用。 6、支持扫描任务定时执行，提高扫描配置化管理。 7、支持异构数据库脱敏，如 Oracle 到 SQLServer、Oracle 到 MySQL 的异构脱敏等。 8、支持周期性调度作业任务，可根据需求设定任务单次或多次调度执行的时间，进行任务定时脱敏。 9、支持保留数据库对象脱敏，包括索引、约束、触发器、视图、存储过程、函数等。 10、支持数据库增量脱敏，根据自定义的增量判断字段，自行识别数据库增量数据，并对其执行脱敏操作。 11、支持生成脱敏任务历史记录，对于生成的历史记录可以在版本之间切换，无需重复进行任务配置，提高业务效率。 12、支持文件资产自定义简单/复杂分隔符脱敏。 13、支持 dmp 到 dmp 的分发方式，支持 dmp 到库的分发方式。支持脱敏任务运行中状态监控，实时展示包括任务执行速度、执行时间、执行进度等信息。 14、系统支持脱敏敏感数据的同时增加水印信息，提高敏感数据多渠道分发的安全指标。 15、系统支持自定义水印信息，满足各类场景水印内容需求，规范数据交互。 16、系统支持水印脱敏文件溯源，在发生数据泄漏安全事件后能快速定位泄漏源。 17、支持后期扩容，对其他业务系统提供数据安全和网络安全支撑。			
7	API 审计	中国电信	定制	1、通过旁路部署侦听的工作模式，可以对 web 业务系统的接口进行深度解析与审计分析，解决客户的核心业务面临的“敏感信息外发、接口盗用、违规权限、业务风险”等安全威胁，满足各类法令法规对业务接口审计的要求，可以帮助用户提升业务运行监控的透明度，降低人工审计成本，真正实现业务全业务运行可视化、日常操作可监控、危险操作可控制、所有行为可审计、安全事件可追溯。性能要求：HTTP 流量解析不低于 1500Mbps；HTTP 峰值处理能力 15000QPS	1	18.5	18.5

				2、支持根据应用域名以及应用的业务重合度，深度结合 AI 技术进行资产合并智能推荐，支持应用拆分； 3、支持内置 IP 库，可对应用的部署域和客户端 IP 所在地进行识别；支持 IP 地址段所属域自定义，如内网、外网、DMZ 区等，并能更细粒度定义内网的各个业务域； 4、支持应用关系图谱分析，可在根据应用域名进行应用查询，并可视化展示被查询应用与其他应用服务之间的调用关系，清晰掌握应用间接口调用走向和调用数据等； 5、支持二次封装接口识别和标识，并支持接口封装前后样例对比和查看； 6、支持客户端 IP 列表，展示所有调用接口的客户端 IP 基本信息，关联信息、风险标签等信息； 7、基于大数据分析、行为分析以及 AI 技术，对应用、接口、账号、客户端 IP、数据维度建立全面的资产画像分析，包含资产基本信息、统计数据和周期时间内的访问趋势和敏感数据访问分析、访问基线、访问时间偏好分布、关联风险（脆弱性）等。 8、支持根据会话关联接口请求日志，帮助会话还原。会话信息包括：会话开始时间、持续时长、客户端 IP、目标服务端 IP、应用账户、请求总数以及各风险级别请求数等。 9、支持根据会话中的请求顺序进行会话回放。 10、支持告警记录、审计日志通过 SYSLOG、KAFKA、企业微信等多种方式外发。 11、支持对审计日志进行多维条件下钻分析。根据查询条件可自定义选择图表样式，可对分析结果进行可视化查看，也可下载查看；可支持多维分析条件生成自定义报表模板； 12、支持基于账号和 IP 的历史对比分析，分析本周与上周访问应用数、访问次数、访问数据量、下载文件数、访问时间段和访问终端的对比差异。			
8	终端数据防泄漏	中国电信	定制	1、部署在终端设备上，可通过操作系统底层技术和对接机制，对终端电脑上的泄漏风险，如 U 盘拷贝、文件打印、微信消息、屏幕截屏、电子邮件、文件上传等行	1	30	30

				为进行实时监控，阻止终端使用人员私自将获取到的敏感数据泄漏，同时对离开终端电脑的数据提供溯源手段。管理能力主要包括：1.终端 DLP 插件统一管理；2.终端 DLP 策略统一管理；3.终端 DLP 事件统一管理；4.至少支持 500 终端在线。 2、具备图章识别能力，能够发现常见的文档、图片中是否携带有图章，并可以识别图章中的文字。 3、能够识别各种文档类型，系统内置不少于 150 种文档类型，对于不在内置范围的文档可以通过自定义文档特征进行识别，支持 dwg、dxf、pcb、brd 等常见图纸文件的文本内容。 4、支持将误报文件自动加入到训练模型的反向样本中进行再次训练，提升模型的识别准确度。 5、对于常见压缩文件能够判断文件嵌套或压缩的深度，深度能识别出 100 层；同时，也可以将每个被嵌套的文件进行单独的内容识别，判断要识别的内容是否都在一个被嵌套文件中，还是分散在多个嵌套文件中。 6、支持自动采集并监控终端新增的应用信息，能够对未知应用进行监控，禁止运行高危应用程序、外置应用程序，降低系统风险。 7、支持监控打印机打印和虚拟打印行为；支持添加打印水印，提供文字、图片、二维码选择、矢量水印和其他自定义格式设置；支持暗水印，将不容易识别的数字水印隐藏在打印文件中，可进行水印溯源。 8、支持禁止对敏感文件的截屏、录屏行为，支持系统自带的截屏、录屏软件和第三方的截屏、录屏软件。 9、敏感文件因业务需要必须外发时，支持制作加密、离线权限管控的安全外发包；支持设置密码，设置复制权限、截屏权限、打印权限、文件有限期、打印水印、阅读水印等。 10、可配置策略对敏感文件进行自动加密（加密方式支持内部通用加密、根据文件分级进行加密，根据用户级别控制打开权限），内部流转根据权限打开文件，拷贝至未安装 DLP 客户端软件的终端时无法读取。			

				11、支持暗水印追溯：支持屏幕水印暗水印溯源，支持拍照截屏溯源，支持在外发时对文档打标，标识外发用户、外发时间、分类分级信息，通过溯源系统追溯到文件的外发流转过程 12、对受控程序文件进行编辑操作时，实现文件自动、强制、透明加解密；受控程序之间相互信任；受控程序与非受控程序相互隔离；加密文件增加加密图标，在安装客户端的电脑上打开加密文件，以明文显示，不影响用户工作习惯；支持指定 url 实现上传解密，下载加密，用户无需手动操作。 13、针对受控程序文件制作外发文件包，支持在未安装客户端的终端打开外发文件包，用于发送客户或合作伙伴； 外发文件包可对文件设置口令校验、限制打开次数/打印次数、限制文档有效期、权限（打印、编辑、截屏、复制、解密、打印水印、阅读水印）； 14、支持软件停用功能，管理员可以直接停用指定终端的防护功能，用户也可以根据需要通过审批流程提前申请停用时间。 15、支持后期扩容，对其他业务系统提供数据安全和网络安全支撑。			
9	数据安全分类分级服务	中国电信	定制	提供数据分类分级服务，建立数据分类分级目录，覆盖各行业数据库及相关表格字段，并完成现有数据的分类分级工作，并完成后期上线的系统做好支撑。 (1)数据分类分级体系建设服务交付物要求 《数据分类分级管理办法》 (2)数据分类分级规范设计服务交付物要求 《数据安全分类分级规范》 《数据安全分类分级操作指南》 (3)数据分类分级标识服务交付物要求 《数据资产清单》 《数据分类分级清单》	1	29	29

10	数据安全风险评估服务	中国电信	定制	提供数据安全风险评估服务，根据评估目的、行业特征、监管动向等选取合适的法律法规或标准作为评估依据，通过专业评估过程识别发现政务数据安全和隐私风险，输出评估报告。 (1)数据安全风险评估准备交付物要求 《数据安全风险评估调研表》 《数据安全风险评估方案》 (2)数据安全调研评估交付物要求 《数据流转图》 《数据处理活动一览表》 《数据安全评估结果表》 (3)数据安全风险分析交付物要求 《数据安全问题清单》 《数据安全风险清单》 (4)数据安全评估总结交付物要求 《数据安全风险处置建议表》 《数据安全风险评估报告》	1	30	30
		中国电信	定制	数据标识及风险评估调研及相关服务	1	16.8	16.8
（三）网络安全升级优化							
序号	产品名称	品牌		技术指标	数量	单价	合计
1	防火墙系统	绿盟	NFNX5-HH2050	1、绿盟防火墙产品 NFNX5-HH2050 为标准 2U 机架设备，含交流冗余电源，配备银河麒麟 V10 操作系统，海光 3250 CPU，硬盘 4T 机械硬盘+256G 固态硬盘；配置 1*RJ45 串口，1*RJ45 管理口，2*USB 接口，配置 8 个千兆电口，8 个千兆光口，8 个万兆光口，5 个接口扩展槽位；1 个 Console 口，防火墙吞吐量 20G，应用层吞吐量 16G，并发连接 400 万，每秒新建 30 万，提供三年硬件维保及系统升级服务。	1	3.43	3.43

				2、绿盟防火墙产品 NFNX5-HH2050 支持基于 IPV4/IPV6 的安全域、地址、服务、应用和时间的防火墙访问控制策略。 3、绿盟防火墙产品 NFNX5-HH2050 可基于多种条件设定入侵防御模块的检测事件及响应方式。一条策略可同时引用多种安全防护模板。 4、绿盟防火墙产品 NFNX5-HH2050 支持对服务器、客户端进行的口令暴力破解的攻击防护。 5、绿盟防火墙产品 NFNX5-HH2050 支持并开通 IPSec VPN、GRE VPN，并且支持从管控平台查询到每条 grc over ipsec 的实时数据以图形化界面进行展示。 6、绿盟防火墙产品 NFNX5-HH2050 支持基于心跳信号丢失、链路断开等多种方式的 HA 切换条件及逻辑，支持双路 HA 物理心跳线确保 HA 运行稳定可靠。 7、绿盟防火墙产品 NFNX5-HH2050 支持日志审计可记录所有用户的操作日志，包括用户登陆、查看配置、修改配置、删除和添加配置等各类详细动作。 8、绿盟防火墙产品 NFNX5-HH2050 支持威胁可视化技术和流量可视化技术，可提供详细的分析展示图表。 9、绿盟防火墙产品 NFNX5-HH2050 支持整机威胁统计和展示。 10、绿盟防火墙产品 NFNX5-HH2050 自带 SSL VPN 和 Ipsec VPN 能力，免费提供。 11、绿盟防火墙产品 NFNX5-HH2050 具备信息技术产品安全测评证书 12、绿盟防火墙产品 NFNX5-HH2050 能够全面支持 IPV4 和 IPV6 的网络配置和安全防护，能够提供 IPV6 Ready 认证证书。 13、绿盟防火墙产品 NFNX5-HH2050 产品需具备《网络安全专用产品安全检测证书》。 14、绿盟防火墙产品 NFNX5-HH2050 能够提供国产化 CPU 和国产化操作系统的兼容性证明，且产品所采用的 CPU 和操作系统均应符合安全可靠测评要求，能够提供可验证的证明材料。 15、绿盟防火墙产品 NFNX5-HH2050 与现有网络设备能够实现主备部署			
2	网络入侵防护系统	绿盟	NIPSNX5-HH4050	1、绿盟网络入侵防护系统 NIPSNX5-HH4050 为标准 2U 机架式设备，配置银河麒麟 V10 操作系统和海光 3250 CPU，含交流冗余电源，4 个扩展槽位，2*USB 接口，1*RJ45	2	6.95	13.9

				串口，2*千兆电口（1*管理，1*热备），8个千兆电口（3路bypass），4个千兆光口插槽，4个万兆光口，256G SSD，4T硬盘，应用层吞吐量6G，网络层吞吐量20G，并发连接400万，每秒新建25万。含三年原厂质保及系统、特征库升级服务。 2、绿盟网络入侵防护系统NIPSNX5-HH4050提供入侵规则分类，帮助更便捷的制定防护策略，攻击特征库数量15000+条 3、绿盟网络入侵防护系统NIPSNX5-HH4050能够有效抵御SQL注入、XSS注入、wobshell等多种常见的应用层安全威胁，并可配置SQL注入白名单。 4、绿盟网络入侵防护系统NIPSNX5-HH4050支持多种抗逃避或欺骗检测技术，能检测出的躲避行为。 5、绿盟网络入侵防护系统NIPSNX5-HH4050支持国密加密证书和国密签名证书导入，并对国密加密流量进行解密检测。 6、绿盟网络入侵防护系统NIPSNX5-HH4050提供服务器外联异常告警功能，可以手动添加或自学习服务器外联行为，并以此为基线检测服务器非法外联行为并告警。 7、绿盟网络入侵防护系统NIPSNX5-HH4050能够对高危漏洞、高危端口、弱口令进行有效识别，支持场景化配置与展示，支持关联高频高危漏洞、关联高危端口配置，支持关联漏洞动作自定义设置，支持开启高危端口访问拦截 8、绿盟网络入侵防护系统NIPSNX5-HH4050可通过各种统计分析自行选择呈现当前整体威胁状态：如威胁事件级别分布、入侵事件-攻击类别分布、攻击类别趋势、TOP入侵事件目的IP、入侵事件发生趋势等等，支持TOP5、10展示。 9、绿盟网络入侵防护系统NIPSNX5-HH4050能够提供公网地理库，能够在日志中展示攻击源IP的地理信息，并能够自定义私网IP地址或地址段，避免与公网重合时误展示为公网地址。 10、绿盟网络入侵防护系统NIPSNX5-HH4050能够基于在告警、日志中攻击事件的IP地址进行溯源，情报查询可基于IP、文件MD5、URL等进行溯源；溯源可展示地理信息、开放端口、对外提供的服务、相关联域名、ASN信息、Whois信息等。 11、绿盟网络入侵防护系统NIPSNX5-HH4050能够全面支持IPV4和IPV6的网络配			

				置和安全防护，能够提供 IPV6 Ready 认证证书。 12、绿盟网络入侵防护系统 NIPSNX5-HH4050 具备《网络关键设备和网络安全专用产品安全认证证书》 13、绿盟网络入侵防护系统 NIPSNX5-HH4050 能够提供国产化 CPU 和国产化操作系统的兼容性证明，且产品所采用的 CPU 和操作系统均应符合安全可靠测评要求，能够提供可验证的证明材料。 14、绿盟网络入侵防护系统 NIPSNX5-HH4050 能与现有网络设备能够实现主备部署			
3	安全审计系统	三六零	NT-IBASGC 2000	1、标准机架式设备，配置国产化操作系统和国产化 CPU，含交流冗余电源，硬盘容量 256GSSD+4T，2*USB 接口，1*RJ45 串口，2*GE 管理口，专用带外管理 MGT 口，6 千兆电口，4 千兆光口，2 扩展网卡插槽，网络层吞吐量 24G，应用层吞吐量 18G，日志入库性能 15000 条/秒。含三年原厂质保及系统、特征库升级服务。 2、支持基于域名、关键字等多种组合的主动内容审计策略，可扫描指定网站，分析网页页面是否含有非法敏感信息。 3、通过扫描指定网站，分析检测网页是否被挂马，并实时告警响应记录。 4、支持对 70+应用进行审计，记录使用的 IP、访问的时间、使用的应用等具体信息。应用类型包括商业系统、媒体、协作应用、网络应用。 5、可对 P2P 下载、在线视频、网络游戏、炒股软件等行为进行审计，支持基于 IP 地址、用户组、时间、协议等组合审计策略，记录日志包括源 IP 地址、目的 IP 地址、时间、应用名称等。 6、通过对互联网资源（域名、IP 地址、URL 等）进行威胁分析，与威胁情报进行匹配发现恶意网站，达到识别含有恶意代码的高风险网站，实现对终端用户的安全评估和保护。 7、支持流量审计：支持基于时间、协议、IP 地址等组合流量审计策略。支持统计各种应用协议的总流量、上下行流量及 TOP10 排名；针对协议 TOP10 排名， 可查看使用当前协议的 IP 及其流量。支持统计各 IP 的总流量、上下行流量及 TOP10 排名；针对 IP TOP10 排名，可查看当前 IP 使用的协议及其流量。	1	6.2	6.2

				8、投标产品能够全面支持 IPV4 和 IPV6 的网络配置和日志审计。 9、产品需具备《网络关键设备和网络安全专用产品安全认证证书》和《网络安全专用产品安全检测证书》 10、投标产品符合国产化要求，需提供国产化 CPU 和国产化操作系统的兼容性证明。			
1	网络安全漏洞扫描系统	三六零	NT-VSSGC5060	1、国产化操作系统，国产 CPU，硬盘 6T 机械硬盘；配置 8 个千兆电口，4 个千兆光口，2 个网卡扩展插槽；内存 32G 2、支持对多个扫描任务并发执行，配置系统漏洞扫描、web 应用扫描、弱口令扫描、云计算平台漏洞扫描、大数据组件漏洞扫描、物联网设备漏洞扫描，不限制评估的 IP 地址数量，同时并发 128IP 扫描。 3、概要报表汇总了当前扫描任务中涉及的所有主机信息，并提供了按主机分类的漏洞汇总概览。而详细报表则在概要报表的基础上进行了深度拓展，包含了所有主机的基本信息和漏洞汇总，深入展示了每个资产上所有漏洞的详细情况，如漏洞类型、风险等级、CVSS 评分、CVE 编号、漏洞描述以及相应的解决方案等关键数据。 4、投标产品支持超过 53 个漏洞分类，漏洞库积累超过 43w，设备内置漏洞数量不少于 35W。 5、支持多样化的资产活跃性检测配置，具体方式涵盖：ICMP Ping 探测、TCP 连接、UDP 包探测以及 ARP Ping 探测。 6、支持漏洞详细*信息展示，包括但是不限于：CVE 编号、CNNVD 编号，原厂链接，漏洞风险，分类细节、漏洞发布时间、严重性分类等。 7、支持漏扫管理员的访问密码相关策略配置，支持密码复杂度要求配置、支持密码重试次数上限配置等 8、支持对多种常见协议进行口令强度检测，协议包括 SSH、TELNET、FTP、SMB、RDP、MYSQL、POSTGRES 协议 9、支持操作系统：Windows（win7、win10、win2008、win2012、win2016、win2019）、Linux（Contos7、Debian9、Fedora、Rodhat、Susc、Ubuntu18）、国产操作系统（kylinos10-S、kylinos10-D）。	1	8.9	8.9

				10、支持国际 CVE 标准和国内 CNNVD 标准。 11、配置 3 年系统漏洞库、Web 漏洞库、数据库漏洞库、中间件漏洞库、虚拟化漏洞库、网络设备漏洞库、容器漏洞库升级及 3 年原厂维保。 12、投标产品应该是被广泛应用的成熟产品，具备合格证书。 13、产品具备确保漏洞扫描产品能够全面支持 IPV4 和 IPV6 的网络配置和安全检测。 14、产品具备《网络关键设备和网络安全专用产品安全认证证书》和《网络安全专用产品安全检测证书》。 15、投标产品符合国产化要求，提供国产化 CPU 和国产化操作系统的兼容性证明。			
5	WAF	三六零	（HT-8000-WAFYGC4000）	1、国产化操作系统，国产 CPU，硬盘 4T 机械硬盘+256G 固态硬盘；配置 8 个千兆光口，8 个千兆电口，4 个万兆光口，2 个接口扩展槽位；吞吐量 40G，HTTP 吞吐 15G，HTTP 新建 15W，HTTP 并发连接数 600 万 ，含 3 年原厂维保及 WAF 特征库升级服务。 2、支持 SSL 透明代理，可以对 HTTPS 国密网站进行保护，一个站点同时防护国密及商密网站。 3、系统具备注入攻击防御能力，可以对 SQL 注入、LDAP 注入、SSI 指令注入、Xpath 注入、命令注入、远程文件包含以及其他注入进行防御 4、系统具备跨站攻击防御能力，可以对 XSS 和 CSRF 攻击进行防御 5、系统具备 Web 访问控制能力，可以对扫描器的扫描行为、爬虫行为、目录遍历行为进行防御，支持基于扫描防护。 6、支持对保护站点的流量进行智能学习，并根据学习结果生成针对性的防护策略。 7、提供丰富的日志信息，包括设备管理日志、网络安全日志、网页安全日志、防篡改日志、访问控制日志、、Web 访问日志等 8、提供集中展示功能，可展示威胁事件风险分布、威胁事件类型分布、实时威胁事件、等内容。 9、支持页面动态混淆防护，在保证业务和页面展示效果的情况下，对响应页面中的 Form 表单、a 标签、Javascript 文件等关键信息进行混淆，支持对例外 URL 不	1	11.4	11.4

				进行混淆操作。 10、产品具备信息技术产品安全测试证书 11、投标产品产品能够全面支持 IPV4 和 IPV6 的网络配置和安全防护。 12、产品具备《网络关键设备和网络安全专用产品安全认证证书》或《网络安全专用产品安全检测证书》。 13、投标产品符合国产化要求，提供国产化 CPU 和国产化操作系统的兼容性证明。 14、设备支持标准的双机主备协议，支持双主、主备部署。			
6	日志审计系统	三六零	NT-IBASGC 2000	1、标准机架式设备，配置国产化操作系统和国产化 CPU，含交流冗余电源，硬盘 4T 机械硬盘+128G 固态硬盘，2*USB 接口，1*RJ45 串口，专用带外管理 MGT 口，6 千兆电口，4 千兆光口，2 扩展网卡插槽，网络层吞吐量 24G，应用层吞吐量 18G，日志入库性能 15000 条/秒。含三年原厂质保及系统、特征库升级服务。2、支持基于域名、关键字等多种组合的主动内容审计策略，可扫描指定网站，分析网页页面是否含有非法敏感信息。3、通过扫描指定网站，分析检测网页是否被挂马，并实时告警响应记录。4、支持对 70+应用进行审计，记录使用的 IP、访问的时间、使用的应用等具体信息。应用类型包括商业系统、媒体、协作应用、网络应用。5、可对 P2P 下载、在线视频、网络游戏、炒股软件等行为进行审计，支持基于 IP 地址、用户组、时间、协议等组合审计策略，记录日志包括源 IP 地址、目的 IP 地址、时间、应用名称等。6、通过对互联网资源（域名、IP 地址、URL 等）进行威胁分析，与威胁情报进行匹配发现恶意网站，达到识别含有恶意代码的高风险网站，实现对终端用户的安全评估和保护。7、支持流量审计：支持基于时间、协议、IP 地址等组合流量审计策略。支持统计各种应用协议的总流量、上下行流量及 TOP10 排名；针对协议 TOP10 排名， 可查看使用当前协议的 IP 及其流量。支持统计各 IP 的总流量、上下行流量及 TOP10 排名；针对 IP TOP10 排名，可查看当前 IP 使用的协议及其流量。8、投标产品能够全面支持 IPV4 和 IPV6 的网络配置和日志审计。9、产品需具备《网络关键设备和网络安全专用产品安全认证证书》和《网络安全专用产品安全检测证书》10、投标产品符合国产化要求，需提供国产化 CPU 和国产化操	1	6.38	6.38

				作系统的兼容性证明。			
7	运维安全管理系统V3	天融信	TopSAG（FT-B）V3 NSAG-SUP-1Y	TopSAG（FT-B）V3 NSAG-SUP-1Y，一年软件升级增值服务包，覆盖功能模块升级、漏洞修复、合规性配置更新等内容，附赠专家级技术支持响应，确保设备全年稳定运行。	1	0.5	0.5
8	网络审计系统	天融信	TA-NET（FT-A）V3 BUNDLE-LIC-D-DB-XC-1Y	TA-NET（FT-A）V3 BUNDLE-LIC-D-DB-XC-1Y，一年特征库升级增值服务包，包含攻击检测规则库、僵尸主机规则库更新，同步适配最新攻防技术，保障设备防护能力处于前沿水平。	1	2.15	2.15
9	负载均衡系统V3	天融信	定制	一年原厂硬件保修增值服务包，覆盖设备核心部件与整机故障，提供7*24小时原厂技术支持响应，包括故障响应、硬件诊断、配件更换及修复验证全流程服务。	1	1.5	1.5
10	防火墙系统V3	天融信	NGFW4000-UF（FT-A60）（万兆）V3 IDP-LIC-B-XC-1Y	NGFW4000-UF（FT-A60）（万兆）V3 IDP-LIC-B-XC-1Y，一年特征库升级增值服务包，包含IDP攻击规则特征库更新，同步适配最新攻防技术，保障设备防护能力处于前沿水平。	2	4.3	8.6
		天融信	NGFW4000-UF（FT-A60）（万兆）V3 IDP-LIC-B-XC-1Y	NGFW4000-UF（FT-A60）（万兆）V3 AVPRO-SMT-LIC-B-XC-1Y，一年特征库升级增值服务包，包含专业版快速查杀病毒库更新，同步适配最新病毒检测规则，保障设备能够检测已知病毒和变种病毒文件。			

		天融信	NGFW4000-UF(FT-A60)(万兆)V3 IDP-LIC-B-XC-1Y	NGFW4000-UF(FT-A60)(万兆)V3 AV-LIC-B-XC-1Y，一年特征库升级增值服务包，包含应用识别特征库更新，同步适配最新应用及协议识别技术，确保设备能够识别各种传统应用及新兴应用协议流量。			
11	备份一体机（新购）	鼎甲	DP4000	DP4000：4U 机架式 CPU：2*Kunpeng 920 主频 2.6GHz/48 核 内存：256GB，32 个 DIMM 插槽，最大支持 4T RECC 内存 系统盘：2*960GB SSD 数据盘：24*12TB SATA 阵列卡：2GB 缓存 RAID 卡（含掉电保护） 网络接口：4*1GE 电口，4*10GE 光口（含多模光纤模块） 扩展槽位：2 个可用 PCIe 插槽 国产版 备份软件具备防勒索病毒能力提供重复数据删除和远程复制，本次提供三年硬件质保服务和技术支持服务。	2	10	20
12	备份一体机（授权扩容）	爱数	定制	每台设备扩容 20TB 后端容量备份代理，按照容量授权模式进行授权的基础容量授权（包含和原有系统匹配的备份软件功能），扩容 4 块 12TB SATA 硬盘。包含一年软件金牌运维服务，一年硬件延保服务，（包括 7*24 小时热线电话支持；5*10 小时网络远程支持；事件优先处理；支持分析报告；指定城市 7×24×下一工作日现场故障处理；每购买 12 个月提供 2 次远程巡检服务或者 1 次现场巡检服务；提供软件更新权益，包含软件补丁和小版本授权。）	2	6	12
13	集成服务	定制	定制	提供整体平台系统资源部署及调试，平台软硬件系统集成服务	1	17.04	17.04
14	合计：705 万元						

附件二：

数据安全及保密协议

委托方（甲方）：[铜川市数据中心]
地址：[铜川市正阳路 9 号]
法定代表人/负责人：[白永琦]
项目联系人：[杨凡]
电话：[18590985543]

受托方（乙方）：中电信数智科技有限公司
地址：[北京市海淀区复兴路 33 号 13 层东塔 13 层 1308 室]
法定代表人/负责人：[陆良军]
项目联系人：[刘珍]
电话：[18991230602]

鉴于甲乙双方（“双方”）正在进行铜川市一体化政务大数据平台暨数据安全底座项目的业务合作，为加强网络数据和信息保护，根据国家法律法规，经双方友好协商，达成本协议。

第一条保密内容和范围

本协议约定的需保密的网络数据和信息包含：

项目建设过程中收集、存储、传输、处理和产生的各种数据，主要包含业务运营数据，行业、公众用户信息，网络、平台以及上层应用的运行与维护数据等。

第二条双方权利和义务

2.1 乙方应严格遵守国家法律法规和甲方的保密规定，完善网络数据和信息保护制度流程，采取必要的管理和技术措施，妥善管理各类系统登录账号、工号，确保网络数据和信息安全。

2.2 乙方不得窃取或者以其他非法方式获取网络数据和信息。

2.3 乙方保证所获取的网络数据和信息仅用于与甲方合作业务有关的合法用途，不得利用网络数据和信息牟取非法利益。

2.4 除合作业务之外，乙方不得对网络数据和信息进行复制和存储。

2.5 乙方对在业务活动中收集的网络数据和信息必须严格保密，不得泄露、篡改、毁损，不得出售或者非法向他人提供。

2.6 对于甲方为合作业务提供给乙方的网络数据和信息资料或乙方在合作业务中获取的网络数据和信息资料，乙方应在双方规定时间或双方终止合作业务时及时交还甲方，并不得留存和使用。

2.7 乙方应加强对员工的保密管理，强化对员工的保密教育培训和监督检查，及时与接触甲方网络数据和信息的员工签订网络数据和信息保密协议。

2.8 由于法律的适用，公安机关或其他国家有权机关依法要求乙方提供或披

露网络数据和信息时，乙方应事先征得甲方同意。

2.9 乙方如发现网络数据和信息泄露，应采取有效措施防止泄密进一步扩大，并及时告知甲方。

第三条保密期限

只要网络数据和信息未被公众所知悉，乙方须继续履行保密义务。

第四条保密协议的终止或例外

乙方未履行或未完全履行本协议项下的条款均构成违约，甲方有权立即终止双方业务合作，暂停支付相关费用，并要求乙方承担全部责任，赔偿因此而给甲方造成的一切损失，包括但不限于甲方因调查违约行为而产生的合理费用。

第五条争议解决方式

所有因本协议引起的或与本协议有关的任何争议将通过双方友好协商解决。如果不能通过友好协商解决，则任何一方均有权向有管辖权的人民法院起诉。

第六条协议生效及其他

6.1 本协议一式肆份，自双方盖章之日起生效，双方各执贰份，具有同等法律效力。

6.2 本协议签订后，如双方之前涉及数据安全及保密协议相关协议约定与本协议不一致的，以本协议为准。

甲方：铜川市数据中心
法定代表人/负责人
或授权代表：

2026年 1月30日

乙方：中电信数智科技有限公司
法定代表人/负责人
或授权代表：

2026年 1月5日

附件三

交付内容

一、项目启动阶段

项目启动阶段作为本项目建设的开篇环节，核心聚焦目标锚定、路径规划与组织保障。通过召开项目启动会明确核心建设目标，系统梳理各委办局业务需求边界与数据共享诉求，组建涵盖业务、技术、安全等多领域的专项工作组，明确各方职责权限与沟通协作机制。同时，结合项目规模、技术复杂度及建设要求，制定科学合理的总体实施框架、分阶段推进计划与资源配置方案，预判项目实施过程中可能面临的风险并制定应对策略，确保项目从起步阶段就具备清晰的方向指引和完善的保障体系。

成果物：《项目实施方案》、《项目排期计划》。

二、调研分析阶段

调研分析阶段是平台建设的基础性环节，旨在全面摸清政务数据资源底数、业务应用需求及现有建设基础。通过跨部门实地走访、座谈访谈、问卷调研等多种方式，深入了解各业务部门的数据采集范围、存储现状、流转流程及应用场景，完成全域数据资产盘点与分类统计；系统梳理各部门在数据共享、业务协同、数据分析等方面的核心需求与潜在诉求，明确平台功能优先级；同时，对现有政务信息系统的技术架构、接口规范、数据格式及运行状态进行全面排查，开展兼容性与扩展性评估，分析现有系统与目标平台的衔接要点及改造需求，为后续规划设计提供详实、准确的决策依据。

成果物：《项目调研计划》、《项目调研报告》、《数据资产目录清单》、《市级政务数据共享责任清单》。

三、开发建设阶段

开发建设阶段是将设计方案转化为实际成果的核心实施环节，聚焦软硬件开发、部署与集成适配。按照设计方案，组织技术团队开展平台核心系统的代码开发、功能实现与单元测试，完成数据服务门户、数据治理系统、数据共享交换系统等核心软件的定制化开发；同步推进硬件设备的采购、安装与部署，包括服务器、存储设备、网络安全设备等，搭建稳定可靠的硬件运行环境；开展各系统间的接口对接与集成调试，实现数据在不同系统间的顺畅流转与共享；推进数据治理工作，完成数据清洗、转换、标准化处理及资产编目，构建高质量的数据资源池；在开发建设过程中，建立严格的质量管控与进度跟踪机制，及时解决实施过程中出现的技术问题与业务适配问题，确保项目按计划推进。

本次项目建设7个数据库，包含人口库、法人库、社会信用库3个基础库，4个专题库（具体以甲乙双方商定为准）。各基础库、专题库辐射范围均以铜川市县两级业务数据为范围；

交付效果为3个基础库和4个专题库分别实现对应领域数据的标准化归集、结构化存储、合规管控及快速检索调取，满足数据基础管理与提取需求。乙方在甲方按约定提供完整、合规的基础数据源及必要配合的前提下，完成基础库与专题库的设计、搭建等工作。

成果物：《软件开发计划》、《需求规格说明书》、《软件概要设计说明书》、《软件详细设计说明书》、《数据库设计说明书》、《测试总结报告》

五、验收阶段

验收阶段聚焦平台功能、性能、安全等多维度验证，确保平台满足建设要求与业务需求。组织专业测试团队开展全面测试工作，包括功能测试、性能测试、安全测试、压力测试及兼容性测试；针对测试过程中发现的问题，制定整改方案并限期整改，形成问题整改闭环；联合建设方、监理方开展阶段性验收与整体验收，对照合同约定与设计方案，对平台功能、性能指标、安全防护、文档资料等进行全面核查，确保平台达到交付标准。

成果物：《问题整改报告》、《验收报告》

六、培训阶段

培训阶段聚焦用户赋能，确保不同角色用户能够熟练、规范使用平台各项功能。基于平台使用场景与用户角色分类，定制差异化培训方案，涵盖理论讲解、实操演练、案例分析、答疑解惑等多元化培训形式。培训内容重点包括平台核心功能操作流程、数据归集、数据编目、数据共享及数据查询与应用方法、数据安全管理规范、常见问题处理技巧等；针对关键岗位人员开展专项强化培训，通过实操考核、场景模拟等方式确保培训效果。

成果物：《用户操作手册》、《用户培训课件》、《培训签到表》

七、运维阶段

运维阶段作为平台长期稳定运行的核心保障环节，聚焦建立常态化、规范化的运维管理体系。制定详细的运维管理办法，明确运维团队职责、日常巡检流程、问题响应机制与服务等级标准；建立完善的问题反馈与处置闭环机制，对用户反馈的问题进行分类登记、快速响应、限期解决，并做好记录归档；编制应急处置预案，针对系统故障、数据安全事件、硬件损坏等突发情况，制定标准化处置流程与恢复方案，定期开展应急演练；提供持续的系统优化升级服务，根据业务需求变化与技术发展趋势，定期对平台功能、性能及安全防护进行优化迭代，确保平台长期稳定、高效、安全运行。

时间：合同签订起三年免费运维服务。

成果物：《运维管理办法》、《运维报告》、《问题处置报告》