甲方合同编号：SMXSZSJ2023005

乙方合同编号：SMXXY2023120023

三门峡市县一体化新型智慧城市建设（三期）

服务项目D包合同

二〇二三年十二月

甲方（采购方）：三门峡市政务服务和大数据管理局

地址：河南省三门峡市崤山东路银山大厦 2-8 层

法定代表人：李宝松

联系人：高银娜

电话：0398-2260112

电子邮箱：zsjxmglk@163.com

乙方（服务方）：三门峡崤云信息服务股份有限公司

地址： 河南省三门峡市五原西路传媒大厦 11 楼

法定代表人：党创业

联系人：张樊迪

电话：18003986067

电子邮箱：zhangfandi@smxxy.cn

鉴于甲方购买乙方提供的三门峡市县一体化新型智慧城市建设（三期）D 包相关项目服务，双方根据《中华人民共和国民法典》及其他有关法律、法规的规定，经过甲乙双方协商一致，达成如下合同，以资共同信守。

第 1 条 合同标的

乙方根据本合同约定和甲方要求提供三门峡市县一体化购买新型智慧城市建设（三期）服务项目 D 包（以下简称“项目”或“服务”）建设部署及相关服务，包括应急指挥平台（硬件）一期服务、15 个路口信号控制及电子警察服务。

1.1 服务范围

应急指挥平台（硬件）一期服务范围：三门峡市本级。

15 个路口信号控制及电子警察服务范围：三门峡市本级。

1.2 服务内容

（1）软件服务：乙方负责应急指挥平台（硬件）一期和 15 个路口信号控制及电子警察的部署运行。

（2）安全服务：服务期内，乙方提供平台安全设备及安全保障服务。

（3）平台维护：服务期内，乙方提供平台运维服务，后台 7*24 技术服务，平台上线后三个月 2 人驻场服务，项目验收完成后，乙方提供 2 人驻场运维服务；并提供第三方软件授权。

上述服务的具体要求详见本合同附件 2“技术规范书”。

1.2 服务期限

本合同服务期限为 3 年，自合同签订之日起，至 2026 年 12 月 28 日止。

第 2 条 合同金额及支付方式

2.1 本合同含税总金额为¥13,731,000.00（大写：壹仟叁佰柒拾叁万壹仟元），其中税金金额为：¥777,226.42（大写：柒拾柒万柒仟贰佰贰拾陆元肆角贰分）。合同价格清单如下：

序号	项目内容	数量/期限	小计（元）	备注
1	应急指挥平台（硬件）一期	1 项	7,189,000	
2	15 个路口信号控制及电子警察	1 项	6,542,000	
总计			13,731,000	

2.2 本合同总金额包含了甲方就乙方履行本合同所需支付的全部含税费用，除双方另有约定外，甲方无需向乙方另行支付任何其他费用。

2.3 本合同第 2.1 条约定的费用，按照如下方式进行结算和支付：

（1） 合同签订后自乙方向甲方提供合法发票后 10 个工作日内，甲方向乙方支付合同总金额的 10%作为首付款，即人民币壹佰叁拾柒万叁仟壹佰元（¥1,373,100.00）。剩余 90%款项依据绩效评价结果分三次支付。

（2） 2024 年 12 月 30 日前，甲方对乙方的项目服务进行第一次绩效评价，评价项目金额为人民币肆佰壹拾壹万玖仟叁佰元（¥4,119,300.00），实际服务费用依据绩

效评价结果进行支付。

（3） 2025年12月30日前，甲方对乙方的项目服务进行第二次绩效评价，评价项目金额为人民币肆佰壹拾壹万玖仟叁佰元（¥4,119,300.00），实际服务费用依据绩效评价结果进行支付。

（4） 2026年12月30日前，甲方对乙方的项目服务进行第三次绩效评价，评价项目金额为人民币肆佰壹拾壹万玖仟叁佰元（¥4,119,300.00），实际服务费用依据绩效评价结果进行支付。

2.4 甲方付款前，乙方应开具合格的增值税发票（增值税率6%）。乙方提供发票不符合要求的，甲方有权延期付款且不承担违约责任。

2.5 甲方开票信息如下，甲方如需改变账户，应提前十(10)日书面通知乙方：

甲方名称：三门峡市政务服务和大数据管理局

纳税人识别号：11411200MB1851405M

开户行：建设银行股份有限公司三门峡分行财政大厦支行

帐号：41050169864608000355

2.6 乙方结算账户信息如下，乙方如需改变账户，应提前十(10)日书面通知甲方：

乙方名称：三门峡崤云信息服务股份有限公司

纳税人识别号：91411200MA442EYM3D

开户行：建设银行股份有限公司三门峡分行财政大厦支行

帐号：41050169864600000093

第3条 甲方的权利和义务

3.1 甲方有权要求乙方按照单一来源采购文件、响应文件内容提供项目服务。

3.2 甲方对服务内容产生的所有数据具有所有权。

3.3 甲方负责在约定期限内，完成付款并及时组织项目验收。

3.4 甲方负责支持、协助、配合乙方做好项目的相关工作，为乙方在合同履行过程中与相关政府部门及其他第三方的沟通、协调提供必要的协助。

第4条 乙方的权利和义务

4.1 乙方负责按照本合同及响应文件中约定的内容提供三门峡市县一体化新型智慧城市建设（三期）服务项目D包的建设部署及相关服务并收取费用。

4.2 乙方在项目范围内，对服务中出现的问题及时调整或完善。因乙方原因未及时对出现问题调整完善造成甲方损失的，乙方应承担甲方因此所遭受的全部损失。

4.3 乙方应保证其交付的服务成果不侵犯任何第三方的合法权益。若乙方交付的服务成果侵犯他人合法权益，乙方应承担因此所产生的所有法律后果及全部损失。

4.4 因乙方自身原因导致乙方及其人员在服务期内发生的一切事故责任和由此产生的一切费用和损失，全部由乙方自行承担，与甲方无关，给甲方造成的一切损失

（包括但不限于由此引起诉讼所发生的诉讼费、律师费等全部费用和一切经济赔偿损失）全部由乙方承担，若甲方已经承担的，则有权向乙方追偿。

4.5　乙方按照国家关于政务信息系统及政务数据有关要求进行项目管理，不得留存、使用、泄露或向他人提供数据，不得将数据用于商业用途。

第5条　验收

5.1　乙方按照本合同约定完成平台部署及上线后，应向甲方提交验收申请，甲方在收到申请后五个工作日向乙方书面进行答复是否组织验收，甲方未书面回复验收或未组织验收的，自乙方提交验收之日起十五个工作日后视为验收通过，若同意验收，甲方在十个工作日内对项目进行验收（项目验收费用由乙方承担），验收合格后双方签署验收报告。如验收不合格，甲方需明确整改要求，乙方应立即进行更正修改，直至符合“技术规范书”的要求。若经两次验收仍达不到“技术规范书”的要求，甲方可以解除合同，将该项目所涉服务交由第三方完成，乙方应当予以配合进行交接，由此给甲方造成的损失应当由乙方予以赔偿。”项目验收后，乙方应按照“技术规范书”的要求和甲方实际需求，免费为甲方指定的人员提供不限次技术指导和培训，使参加受训的人员理解并掌握软件的操作和维护。

5.2　在项目服务期内，因政策调整导致平台功能调整的，乙方应根据甲方相关要求进行调整，不得额外收取费用。甲方由于业务变化以及需求增加引起的新模块增添或表单与工作流程的大量调整，由乙方与甲方共同评估工作量及费用，达成一致签订补充协议后进行开发。

5.3　项目验收后，甲方在合同期内，针对乙方提供的项目及时进行绩效评价，保障项目稳定运行。

第6条　知识产权

6.1　本合同生效时已经存在并为各方合法拥有或使用的技术、资料和信息，其知识产权和其他权益仍归原权利人所有。甲方享有乙方交付软件的永久使用权。

6.2　乙方及其工作人员在为甲方提供服务的期间所产生的合法原创知识产权归乙方所有。

6.3　乙方保证其在本合同项下提供的服务不会侵犯第三方的知识产权和其他合法权益。如果甲方因接受乙方服务而侵犯第三方的合法权益，并因此涉入诉讼、仲裁或其他司法程序，乙方应就诉讼策略及其他事宜向甲方提供充分的支持与协助，并承担甲方因此而产生的全部损失及全部法律后果；如有生效的法律文书禁止甲方继续使用相关服务或要求甲方向第三人支付使用费，乙方应采取相应的补救措施，并赔偿由此给甲方造成的全部损失。

第7条　保密

7.1　本合同拥有信息的一方（“提供方”）根据本合同向另一方（“接收方”）

提供的信息，包括但不限于技术性信息、商业性信息、文件、程序、计划、技术、图表、模型、参数、数据、标准、专有技术、业务或业务运作方法以及其他专有信息，本合同履行过程中形成的所有信息、数据、资料、阶段性成果和最终成果，本合同的条款和与本合同有关的其他商业信息和技术信息(以下统称“保密信息”)，只能由接收方及其人员为本合同目的而使用。除本合同另有规定外，对于提供方提供的任何保密信息，未经提供方的书面同意，接收方及其知悉保密信息的人员均不得直接或间接地以任何方式提供、披露或转让给任何第三方，或许可第三方使用，或以保密信息为任何第三方提供任何意见或建议。

7.2 提供方向接收方提供或披露的保密信息，仅可由接收方为执行本合同需要披露给指定的雇员，并且仅在为执行本合同所需的范围内进行该等披露；但是，接收方在采取一切合理的预防措施之前，不得向其雇员披露任何保密信息，该等预防措施包括但不限于告知该等雇员将要披露信息的保密性质，由该等雇员做出至少与本合同保密义务一样严格的保密承诺等，以防止该等雇员为个人利益使用保密信息或向任何第三方做出未经授权的任何披露。接收方雇员违反保密义务的，视为接收方违反保密义务。

7.3 接收方的律师、会计师、承包商和顾问为提供专业协助而需要了解保密信息时，接收方可向其披露保密信息，但是，其应要求上述人员签订保密协议或按照有关职业道德标准履行保密义务。

7.4 如相关政府部门或监管机构要求接收方披露任何保密信息，接收方可在该政府部门或机构要求的范围内做出披露而无需承担本合同项下的责任。但前提是，该接收方应立即将需披露的信息书面通知提供方，以便提供方采取必要的保护措施，且该等通知应尽可能在信息披露前做出，并且接收方应尽商业上合理的努力确保该等被披露的信息获得有关政府机关或机构的保密待遇。

7.5 在任何情形下，本条所规定的保密义务应永久持续有效。

7.6 当本合同解除或终止时，接收方应立即停止使用且不得许可第三方使用提供方的保密信息，同时，接收方应按照提供方的书面要求，将提供方提供的保密信息退还提供方或予以删除或销毁，不得以任何形式留存。

第 8 条 违约责任

8.1 任何一方不履行本合同约定的义务或履行义务不符合本合同约定的，视为违约，应停止违约行为，并按守约方的要求继续履行、采取补救措施或赔偿损失，乙方不能满足附件 2“技术规范书”的服务要求，即视为乙方违约。

8.2 如乙方未能按本合同约定向甲方提供服务，每逾期一(1)日，应按当期应付服务费用的万分之五(0.05%)向甲方支付逾期违约金。逾期超过三十(30)日，甲方有权单方解除本合同，同时，乙方应向甲方支付当期应付服务费用的百分之二十(20%)的违

约金，违约金不足以弥补甲方的全部损失的，乙方还应予以赔偿。

8.3　如甲方未能按本合同约定向乙方支付费用，每逾期一(1)日，应按当期应付服务费用的万分之五(0.05%)向乙方支付逾期违约金。逾期超过三十(30)日，乙方有权单方解除本合同，同时，甲方应向乙方支付当期应付服务费用百分之二十(20%)的违约金，违约金不足以弥补乙方的全部损失的，甲方还应予以赔偿。

8.4　任何一方违反本合同所约定的保密义务给对方造成了负面影响或损失，违约方应按本合同总价的20%支付违约金。如包括利润在内的实际损失超过该违约金的，受损失一方还有权要求对方赔偿超过部分的损失。

第 9 条　不可抗力

9.1　合同所指不可抗力，是指不能预见、不能避免并不能克服的客观情况。

9.2　由于不可抗力事件，致使一方在履行其在本合同项下的义务过程中遇到障碍或延误，不能按约定的条款全部或部分履行其义务的，遇到不可抗力事件的一方（“受阻方”），只要满足下列所有条件，不应视为违反本合同：

（1）受阻方不能全部或部分履行其义务，是由于不可抗力事件直接造成的，且在不可抗力发生前受阻方不存在迟延履行相关义务的情形；

（2）受阻方已尽最大努力履行其义务并减少由于不可抗力事件给另一方造成的损失；

（3）不可抗力事件发生时，受阻方立即通知了对方，并在不可抗力事件发生后的十五(15)日内提供有关该事件的公证文书和书面说明，书面说明中应包括对延迟履行或部分履行本合同的原因说明。

9.3　不可抗力事件终止或被排除后，受阻方应继续履行本合同，并应尽快通知另一方。受阻方应延长履行义务的时间，延长期应相当于不可抗力事件实际造成延误的时间。

9.4　如果不可抗力事件的影响持续达三十(30)日或以上时，双方应根据该事件对本合同履行的影响程度协商对本合同的修改或终止。如在一方发出协商书面通知之日起十(10)日内双方无法就此达成一致，双方可根据本平台服务时间结算已产生的费用，多余费用乙方应在七（7）日内退还甲方指定账户，经结算后任何一方均有权解除本合同而无需承担违约责任。

第 10 条 通知与送达

10.1　根据本合同需要发出的全部通知，均须采取书面形式，以专人递送、传真、电子邮件、特快专递或挂号信件发出。特快专递或挂号信件的交寄日以邮戳为准。上述书面通知均须标明合同对方为收件人。

10.2　上述书面通知按对方在本合同首页中所列的地址发出，并按本合同条款规定时间被视为已经送达。如双方中任何一方的地址有变更时，须在变更前十日以书面

形式通知对方，因迟延通知而造成的损失，由延迟通知方承担责任。

10.3 双方将按如下规定确定通知被视为正式送达的日期：以专人递送的，接收人签收之日视为送达；以传真方式发出的，发件方发送后打印出的发送确认单所示时间视为送达；以电子邮件方式发出的，电子邮件到达接收方指定电子邮箱的时间视为送达；以特快专递形式发出的，发往本市内的，发出后第 3 日视为送达，发往国内其他地区的，发出后第 3 日视为送达；以挂号信件方式发出的，发往本市内的，邮寄后第 7 日视为送达，发往国内其他地区的，邮寄后第 15 日视为送达。

第 11 条 法律适用和争议解决

11.1 双方就本合同的解释和履行发生的任何争议，应通过友好协商解决。协商不成的，应提交三门峡仲裁委员会按照申请仲裁时现行有效的仲裁规则进行仲裁。仲裁地点在三门峡。仲裁裁决是终局的，对双方均有约束力。

11.2 争议解决过程中，除双方有争议的部分外，本合同其他部分仍然有效，双方应继续履行。

11.3 本合同全部或部分无效的，本条（即第 11 条法律适用和争议解决）依然有效。

第 12 条 其他

12.1 本合同由双方法定代表人或授权代表签字并加盖公章或合同专用章后生效。合同将保持其效力直至双方已完全履行合同项下的所有义务并且双方之间的所有付款和索赔已结清。

12.2 未经另一方书面同意，任何一方不得转让本合同项下任何权利义务。

12.3 本合同未尽事宜，应由双方友好协商解决。如需对本合同及其附件作任何修改或补充，须由双方以书面做出并经双方签署后方为有效。补充协议与本合同具有同等法律效力，补充协议与本合同存在不一致之处的，以补充协议为准。

12.4 本合同一式肆(4)份，双方各执贰(2)份，具有相同法律效力。

12.5 本合同附件是本合同不可分割的部分，若附件与合同正文冲突，以本合同正文为准。

附件：1.功能清单

2.技术规范书

（本页无正文，为《三门峡市县一体化新型智慧城市建设（三期）服务项目D包合同》的签署页）

甲　　方（盖章）：三门峡市政务服务和大数据管理局

法定代表人或授权代表（签字）：高银娜

日　　期：2023.12.29

乙　　方（盖章）：三门峡崤云信息服务股份有限公司

法定代表人或授权代表（签字）：张俊山

日　　期：2023.12.29

附件 1：

功能清单

项目名称	功能模块
应急指挥平台（硬件）一期	应急指挥中心场所规划布局
	指挥中心建设
	地面光纤网络系统
	融合通信系统
	视频会商系统
	图像接入系统
	传感监测网接入系统
	卫星通信系统
	网络安全防护系统
15 个路口信号控制及电子警察	五原路向青路、甘棠路河堤北路、五原路上阳路、五原路永安街、文明路茅津路、上官路向青路、上官路和平路、黄河路上官路、黄河路经二路、建工路六峰路、黄河路崤山路、五原路草堂路、虢国路永安街、黄河路火车站、分陕路三门路

附件 2：

技术规范书

一、服务内容及要求

1.1 平台建设部署

1.1.1 指派专职人员配合完成应急指挥平台（硬件）一期、15 个路口信号控制及电子警察部署上线准备工作，需提供平台试运行服务、调测优化服务、调测优化服务、系统用户及管理人员的操作培训服务等。

1.1.2 根据甲方时间节点要求，完成应急指挥平台（硬件）一期、15 个路口信号控制及电子警察相关软件模块部署上线，各模块及功能参照“附件 1”。

1.1.3 针对产品的操作使用，配合甲方组织用户培训工作。

1.1.4 具备平台个性化开发能力，定制开发费用根据具体功能点另行测算，不包含在本次服务内。

1.2 安全设备

乙方配备安全设备（设备归乙方所有），为甲方提供安全保障服务。安全设备配置清单如下：

产品名称		性能参数	数量
边界安全防护	WEB 应用防护	含交流冗余电源模块，USB 接口≥2 个，1 个 RJ45 口，RJ45 串口≥1 个，网络接口≥4 个千兆电口（2 对 Bypass），≥1 个接口扩展槽（4GE/4SFP/2SFP+），HTTP 应用层吞吐量≥800Mbps。	1
数据中心防护	日志审计	包含交流冗余电源模块,USB 接口≥2 个,RJ45 串口≥1 个,管理口≥1 个千兆电口，网络接口≥6 个千兆电口，≥4 个千兆光口，≥1 个接口扩展槽位，有效存储容量≥4T。日志源接入授权≥60 个，内置 1 个采集器。	1
	漏洞扫描	包含 1 个管理口、RJ45 Console 口≥1 个， USB 接口≥2 个，网络接口≥4 个千兆光口，≥4 个千兆电口，≥1 个接口扩展槽位。可扫描总数量≥500 个 IP，并发扫描≥60 个 IP。支持 Linux 系统扫描（包含 UOS、麒麟等国产化系统），支持扫描的漏洞数量≥190000 个。	1
	数据库审计	内存≥16G，硬盘≥2T，≥6 个千兆电口，≥4 个千兆光口，≥1 个接口扩展槽位，2 个 USB 接口，1 个 RJ45 串口。数据库实例数≥30 个。支持达梦、MySQL、Oracle、SQL-Server、DB2、Informix、Sybase、PostgreSQL、Teradata、Cache、人大金仓、南大通用、神通、高斯、MongoDB、redis、Hbase、hive、ES 等数据库审计。	1

产品名称		性能参数	数量
数据中心防护	安全管理中心	包含冗余电源，支持专用千兆硬件平台和安全操作系统，≥2 个 USB 接口，≥2 个千兆电口，≥4 个千兆光口，≥3 个接口扩展槽位，有效存储容量不低于 32TB。支持内置 300+设备日志解析规则查看以及筛选，包括但不限于网络设备（防火墙、交换机、网关）、安全设备（入侵检测设备、WEB 攻击防护设备、APT 检测设备、防火墙、网络审计、流量探针等）、终端主机日志、数据库等。	1
高级威胁检测	融合威胁检测探针	接口≥1 个管理口、≥6 个千兆电口、≥4 个千兆光口，≥1 个接口扩展槽，≥2 个 USB 接口；≥1 个 RJ45 串口；应用层吞吐量≥1000Mbps；最大并发会话数≥300 万；每秒新增会话数≥2 万；SATA 硬盘容量不低于 10T。支持收集 IDS、WAF、威胁情报和全流量行为日志，支持对接第三方大数据平台的多功能融合探针。	1
零信任安全体系	安全认证网关	支持虚拟化部署，能够和飞天云平台进行对接，支持 X86、ARM 架构，提供定制客户端 SDK 实现对移动侧 app 加固，实现安全接入。每秒新建 SSL 连接数不少于 5000/s，并发在线用户数不少于 200 个/S，可管理设备用户数≥1000。客户端支持 Win7, Win8, Win10 操作系统、OSX 10.12 及以上版本、Linux 操作系统（Ubuntu 16 及其以上版本）、Android 5.0 及以上版本，提供定制化 SDK 接入客户应用，实现移动安全接入。	1

从业务、终端、数据、网络、基础设施等方面，全面构建系统平台的安全防护体系。整体平台安全建设需要满足 GBT25070-2019《信息安全技术 网络安全等级保护安全设计技术要求》中第三级的相关要求。系统主要安全服务如下：

1.2.1 WEB 应用防护服务

主要针对 Web 应用防护建设，在政务外网核心交换机旁挂部署 Web 应用防护设备，实现对 Web 网站的安全防护，确保业务稳定运行。

（1） 提供透明串联部署、基于路由牵引回注的旁路部署、反向代理部署、以及镜像监听检测模式部署。

（2） 提供盗链防护，有效识别网页盗链行为，避免用户网页资源被滥用；支持 Cookie 安全机制；支持敏感关键字自定义。

（3） 提供业务合规功能，可对业务进行恶意试探、恶意撞库、恶意登录等行为进行检测及拦截。

（4） 提供对注入、XSS、SSI 指令、Webshell 防护、路径穿越及远程文件包含的攻击防护。

（5） 提供源访问区域控制功能，可按照国家，区域等进行地址访问限制，防止区域性攻击对 Web 网站造成影响。

（6） 提供扫描防护，包括阈值告警、请求量统计、应答分布统计等防护手段。

（7） 支持获取 Web 安全事件的原始攻击信息，支持和安全管理中心联动。

1.2.2 日志审计服务

在安全管理区域旁路部署日志审计设备，针对网络设备、安全设备日志进行实时收集存储，满足合规要求。

（1） 提供 SNMP Trap、Syslog、ODBC、JDBC、WMI、FTP、SFTP 等多种方式完成日志收集功能。

（2） 提供统一的日志管理过程，如日志范式化处理等，将采集来的海量的异构的日志信息进行集中化的解析和存储，支持范式化字段包括事件接收时间、事件产生时间、用户名称、源地址、源端口、操作、目的地址、目的端口、事件名称、事件摘要、事件类型、网络协议、设备地址、设备名称、设备类型等。

（3） 提供将日志中的 IP 地址、等信息进行资源自定义，为规则所引用。支持基于资产的拓扑视图，可以按列表或拓扑等模式显示资产拓扑节点；可查看每个资产设备本身产生的事件信息、关联告警信息，并且支持向下钻取，直接进入事件列表、关联告警列表。

（4） 提供日志时间、行为关联分析，支持描述日志之间行为相关关系的事件拓扑图等分析工具。

（5） 提供日志转发功能，支持日志转发多个目标地址，可实现原始日志、范式化日志的转发，且不丢失原始日志源 IP 信息，支持以 NFS 网络共享存储扩展等方式进行日志存储扩展。

（6） 提供知识库功能，内置交换机事件编码知识库，内置 Windows、Linux 操作系统的事件 ID 知识库，内置 MySQL、Oracle、SQL Server 等主流数据库的事件编码知识库，能够查看系统内置的事件库中事件类型名称及其描述信息。

1.2.3 漏洞扫描服务

在安全管理区域旁路部署漏洞扫描设备，针对云平台、安全设备、网络设备进行定期扫描出具扫描报告。

（1） 可对主流数据库进行识别与扫描，包括 mysql、达梦、Oracle、Sybase、GBASE、GaussDB、人大金仓、优炫等，扫描数据库漏洞扫描方法≥2600 种。

（2） 提供主流虚拟化软件平台扫描功能，包括 OpenStack 、KVM、Vmware、Xen、Docker、Huawei FusionSphere 等，提供扫描虚拟化软件平台漏洞的扫描方法≥600 种。

（3） 提供国产应用软件的识别与扫描功能，支持范围包括 Foxit、WPS、永中、数科、用友等。

（4） 支持 20 种以上默认扫描策略模板，如常规安全扫描、中高危漏洞扫描、

高危漏洞扫描、web 服务组件扫描、云平台漏洞扫描、虚拟化扫描、主机信息收集、攻击性扫描、视频监控类扫描等，针对市场应急响应的漏洞提供应急响应策略模板，支持自定义策略模板。

（5） 支持专门针对 DNS 服务的安全漏洞检测，包括 DNS 投毒等漏洞检测能力；支持“幽灵木马”检测。

1.2.4 数据库审计服务

在应用服务器区部署一套数据库审计设备，并通过镜像方式或者 agent 方式获取云管平台数据库的日常维护、运维操作，并进行实时审计，对违规行为进行预警。

（1） 提供针对数据库的 XSS 攻击、SQL 注入、CVE 高危漏洞利用、口令攻击、缓冲区溢出等攻击行为审计服务。支持访问数据库的源主机名、源主机用户、SQL 操作响应时间、数据库操作成功、失败的审计。

（2） 自动建立数据库操作行为基线，行为基线包括数据库账号、操作类型（SQL 模板）等行为特征，对超出数据库操作行为基线的操作可自动识别，并及时告警。

（3） 支持数据库和资源账号、表名的自动发现，支持数据库中敏感信息的自动发现，定位敏感数据存储的服务器、库名、表名、列名，并形成针对敏感信息的审计规则。支持对敏感信息敏感级别进行定义，敏感数据发现支持 mysql、Oracle、ms-sql、DB2、PostgreSQL、ES 等常见关系型数据库与大数据库协议，支持探测器和正则表达式两种方式，探测器包含姓名、地名、银行卡、身份证、IP 地址、密码等多种探测器。

（4） 支持根据风险操作、SQL 注入、漏洞攻击检测、语句管理等模块定义告警规则，支持高、中、低风险告警，支持系统资源监控与告警。

（5） 支持敏感信息掩码，可以针对姓名、身份证号、手机号、银行卡号、住址以及自定义信息进行敏感信息掩码配置，防止敏感信息在审计系统中进行泄露。

（6） 根据不同的安全级别采用不同的响应方式，包括记录、告警；告警方式包括：邮件、短信、SYSLOG、SNMP 等。

（7） 通过模式匹配的方式对 SQL 访问进行监测与告警，判断是否为可疑 SQL 注入，并提供 SQL 注入特征库。

1.2.5 安全管理中心服务

在安全管理区，通过部署一套安全管理中心设备，为实现网络安全等级保护要求提供集中安全管理功能服务，成为安全应用系统安全策略部署和控制的中心。

（1） 提供失陷资产判定功能，同时提供失陷资产的判定依据，包括但不限于失陷资产概要信息、攻击结果、攻击链分布阶段、失陷资产的攻击过程及过程判定依据如攻击特征、流量上下文、关联的告警日志及流量日志以及 pcap 包下载，并可快速扩展该失陷资产的全部攻击事件以及该失陷资产攻击者发起的攻击、该失陷资产的同类型威胁事件。

（2） 提供监测网络安全情况的态势呈现能力，态势呈现包括但不限于综合态势、威胁态势、脆弱性态势、环境感知态势、运维响应态势。

（3） 提供对网络环境中威胁、漏洞、资产各种事件多种运维方式的可视化呈现，包括但不限于人工处置的各类型运维事件的状态统计、数量统计、自动化编排和响应的时长统计、数据量统计以及任务数统计等。

（4） 提供针对 IP、域名、会话进行封堵，支持黑名单、流量牵引等方式联动设备进行封堵，设备类型包括但不限于抗拒绝服务系统、WEB 应用防火墙、网络流量探针、网络入侵保护系统、防火墙等。

（5） 提供根据漏洞扫描结果自动生成漏洞处置单的能力，支持对漏洞处置单闭环处理，可设置漏洞处置单状态包括但不限于：新增、待修复、已修复、已验证、单次忽略、永久忽略。

1.2.6 威胁安全检测服务

在安全管理区旁路镜像部署一台融合威胁检测探针设备，集 IDS、WAF、威胁情报和全流量行为日志于一身,支持对接第三方大数据平台的多功能融合探针，集成了入侵防护、WEB 安全、威胁情报、恶意文件和 WEBshell 检测能力能快速精准的发现威胁，能对威胁进行研判和分析，利用自身的策略对攻击者进行封堵，提高重大事件的响应速度。

（1） 提供入侵行为检测、WEB 应用检测、恶意文件检测、威胁情报检测、弱口令检测、拒绝服务攻击检测等服务。支持对检测的告警事件结合双向检测机制、元数据、原始数据包和研判模型进行深层次研判给出告警事件的攻击结果。

（2） 提供本地授权认证。

（3） 提供流量采集、元数据提取、存储等功能。

（4） 提供对实时流量采集的 pcap 包进行全量存储，供追溯分析和取证使用。

（5） 提供针对 TCP、UDP、SCTP、ICMPv4、ICMPv6、GRE、Ethernet、PPP、PPPoE、Raw、SLL、VLAN、QINQ、MPLS、ERSPAN、HTTP、SSL、TLS、SMB、DCERPC、SMTP、FTP、SSH、DNS、NFS、NTP、DHCP、TFTP、KRB5、IKEv2 等常见协议的深度解析和还原。

（6） 提供资产自动化精准识别，粒度包含设备类型，资产名称，操作系统类型、MAC 地址、IP 地址、端口等资产信息。

1.2.7 零信任安全防护服务

针对安全认证网关的建设，在互联网区核心交换区部署安全认证网关，同时与统一身份认证平台联动，对外提供零信任安全能力。安全认证网关采用反向代理部署模式，可以隐藏真实应用，减少威胁暴露面。

（1） 提供用户访问时间、访问地理位置、访问行为进行分析和评估，识别是否

存在异常的暴露破解，异地登录，或非注册终端的登录等异常访问行为，可以对检测出的异常情况进行告警。

（2） 提供统计授权次数、授权成功、授权失败次数等数据分析功能。

（3） 提供访问终端的活跃趋势统计，展示在线终端数以及总终端数等情况。

（4） 支持根据用户组/地理位置/网络地址/访问时间来定义用户的认证方式，精细化管理用户认证策略。

（5） 提供认证通过前对应用的隐藏功能，避免被扫描器扫描到应用对外的端口和信息。

（6） 提供 TCP 端口关闭功能，在客户端发起 SPA 和得到验证前，不接收任何客户端的连接请求，避免自身成为被攻击对象。

1.3 平台运维服务

服务期内，乙方提供平台运行服务，为甲方提供平台稳定运行保障服务。服务清单如下：

序号	服务名称		服务内容
1	驻场服务	驻场服务	平台部署上线后，提供 2 人的驻场服务，配备人员需熟悉应急指挥平台（硬件）一期、15 个路口信号控制及电子警察业务逻辑、数据流向及架构设计思路，对于系统的各个功能模块的运行提供技术支撑服务，保证应急指挥平台（硬件）一期、15 个路口信号控制及电子警察的正常运行，能够对提出的问题进行答疑。
2	数据及配置维护	用户信息管理维护服务	针对平台运行中，各单位报送人员调整后，需要及时调整平台中的用户数据信息，包括新增用户、删除用户、冻结用户、解冻用户、调整用户角色、职位等，并提供用户忘记密码后的密码重置服务。严格保障用户信息的数据安全。
3	系统优化更新升级服务	补丁程序及版本更新	按季度对系统的补丁、版本等进行分析，并提交补丁升级建议报告。报告中详细描述演变信息，例如修正了哪些缺陷，或改善了哪些环节。根据系统运行需求提供是否安装及安装哪些补丁及版本更新。
4		系统升级	针对系统使用中，用户提出的个性化需求，调整系统功能。
5	系统运行保障服务	系统运行监控服务	针对系统的可靠性和安全性，提供软件的运行监控服务，监控软件系统运行状态，当发现系统故障时，及时通知到相应人员，并及时处理。

6		预防性维护	在平台运行期间，每月安排工程师提供检查服务，定期检查错误日志、软件版本、协助用户建立数据备份，在重大保障时，提供巡检等内容。
7		节假日保障	在节假日期间，提前制定节假日保障计划，安排工程师在节假日期间提供技术保障。
8		紧急故障处理	当系统发生紧急故障时，及时响应并进行故障处理，通过多种渠道提供技术支持服务。可根据需要派遣工程师并在规定时限内赶到现场，提供不间断故障处理服务。
9		安全漏洞整改	平台运行中，根据需要，安排工程师进行软件基线扫描以及安全漏洞扫描，对发现的安全漏洞进行梳理及整改。
10		软件隐患排查及整改	为保证平台稳定运行，对日常维护过程中的软件高故障率分析，分析系统瓶颈，并提供超期服务软件重点监控及应用部署建议。
11	技术支持	热线电话支持服务	针对用户在使用中，遇到的问题，进行答疑，常见的包括登录问题、数据填报问题、督办系统使用问题等，提供 7*24 小时问题答疑服务，及时解答使用中的问题。
12		远程接入支持服务	在具备远程接入的条件下，以提供远程接入方式对系统问题进行检查、诊断和分析。
13		现场技术支持服务	针对平台运行中，需要工程师到现场提供技术支持的服务要求时，及时指派工程师提供现场支持服务。
14		应用变更现场技术支持	在进行重要系统变更，如系统升级、切换演练等操作时，派工程师配合进行前期信息梳理，风险分析及评估，并在重要变更操作过程中提供现场支持服务。

1.3.1 驻场运维

平台部署上线后乙方提供 2 人的驻场服务，配备人员需熟悉应急指挥平台（硬件）一期、15 个路口信号控制及电子警察业务逻辑、数据流向及架构设计思路，对于系统的各个功能模块的运行提供技术支撑服务，保证应急指挥平台（硬件）一期、15 个路口信号控制及电子警察的正常运行，能够对提出的问题进行答疑。

运维期间，对平台软件免费升级、Bug 修复、巡检、监控及故障处理。

1.3.2 用户信息管理维护服务

平台部署上线后服务期内，针对平台运行中，各单位报送人员调整后，乙方需要及时调整平台中的用户数据信息，保障平台用户能正常使用系统，严格保障用户信息的数据安全。用户信息维护内容如下：

（1）单位领导调整后，需要新增用户、删除用户服务。

（2）平台用户手机号或职务调整后，需要调整用户角色、职位等内容。

（3）平台用户忘记密码或多次密码输入错误导致账号冻结，需要提供用户密码重置、账号解冻服务。

（4）平台用户手机遗失等原因需要解除设备绑定时，提供用户账号解除设备绑定服务。

1.3.3 补丁程序及版本更新

乙方应按季度对客户现场软件的补丁、版本等进行分析，并提交客户季度性补丁升级建议报告。报告中详细描述演变信息，例如修正了哪些缺陷，或改善了哪些环节。甲方将最终根据系统运行需求决定是否安装及安装哪些补丁及版本更新。

1.3.4 系统升级

乙方应提供软件升级服务，包括补丁安装及软件小版本升级。乙方负责实施软件升级服务、配合甲方进行软件升级完成后的测试、提交软件升级实施报告和测试报告等环节。服务内容包括但不限于以下内容：

乙方应指派工程师每半年检查甲方系统软件的补丁程序的安装情况和软件版本状况，根据软件运行状况决定是否安装新的补丁程序或进行软件小版本升级。乙方应确保补丁程序的安全性。

乙方应指派工程师负责对甲方软件进行补丁安装或软件小版本升级，实施工作完成后应进行软件测试和跟踪。服务的具体内容包括但不局限于以下方面：

（1）乙方工程师应向甲方提交补丁安装或软件小版本升级实施方案，明确实施过程、实施时间以及实施中可能出现的问题和风险；

（2）乙方工程师应提前向甲方提出补丁安装或软件小版本升级过程中需要甲方进行配合的工作及要求；

（3）安装或升级前，乙方工程师应向甲方提供失败情况下的回退方案；

（4）乙方工程师在安装或升级完成后，应进行安装或升级后的标准测试；

双方共同协商制订补丁安装及软件小版本升级服务实施方案（包括对系统回退可能性的评估）。乙方应承诺严格按照双方批准的实施方案进行补丁安装及软件小版本升级的实施。在安装或升级过程中，系统允许回退的前提下，甲方可根据业务时限要求或系统运行情况，提出中止安装或升级过程，要求实施回退方案，乙方应在甲方要求下保证系统安全回退。

1.3.5 系统运行监控服务

针对系统的可靠性和安全性，提供软件的运行监控服务，监控软件系统运行状态，当发现系统故障时，及时通知到相应人员，并及时处理。

1.3.6 预防性维护

乙方至少每个月 1 次指派固定服务工程师提供检查服务。乙方服务工程师应于每

次检查前 3 日提交检查计划给甲方审批，并在检查结束后的 3 日内提供检查报告给甲方审核确认。乙方所提供的预防性检查服务内容应包括以下检查项目但不仅限于以下内容：

（1）定期检查错误日志，并对错误日志进行分析，消除故障隐患。

（2）对软件进行版本检查，并在乙方专家的指导下,在必要的时候进行升级。

（3）协助用户建立数据备份，保存及恢复方法。

（4）协助用户进行软件配置信息备份。

（5）甲方进行重大保障时，乙方应按照甲方要求安排巡检等。

1.3.7 节假日保障

在节假日期间，乙方应提前制定节假日保障计划并获得甲方认可，指定工程师在节假日期间提供技术保障

1.3.8 紧急故障处理

紧急故障：指导致关键业务应用不可用的故障。

当甲方系统发生紧急故障时，乙方应及时响应并进行故障处理，通过多种渠道提供技术支持服务。乙方在接到甲方故障申告后应于 20 分钟内由相关工程师做出响应并开始处理，同时应根据甲方要求立即派遣工程师并在规定时限内赶到甲方现场，提供不间断故障处理服务。

乙方在系统恢复正常运行后，应对系统运行情况进行跟踪，并结合故障现场信息对故障产生原因进行分析，3 个工作日内提交故障分析报告。

1.3.9 安全漏洞整改

根据甲方的需要，乙方应指定工程配合甲方进行软件基线扫描以及安全漏洞扫描，对发现的安全漏洞进行梳理及整改。

1.3.10 软件隐患排查及整改

软件隐患排查及整改主要包括：

（1）日常维护过程中的软件高故障率分析。

（2）软件性能瓶颈分析。

（3）不定期发布的系统 bug 进行整改。

（4）超期服务软件重点监控及应用部署建议。

1.3.11 技术支持

乙方应提供一整套规范的技术支持服务运作体系和流程，指定专职项目经理以及稳定的维护服务队伍，提供故障诊断、技术咨询等全方位的技术支持服务。

乙方应为甲方提供多种技术支持方式，包括但不限于热线电话支持、远程接入支持、现场技术支持等，并对甲方所提交问题指派专职服务队伍进行解答提供相关建议，对未能彻底解决的问题应进行跟踪、反馈并及时处理。

（1）热线电话支持服务

乙方提供 7×24 小时响应的热线服务电话，当甲方出现疑难问题时，乙方应有相应的应急机制，允许甲方和乙方的技术专家直接沟通,帮助解决甲方提出的疑难问题。在相应服务时段内，相关工程师做出响应并开始解答的时间不超过 30 分钟，对于以前出现并解决过的问题，处理完成时间不超过 24 小时。

（2）远程接入支持服务

乙方在具备远程接入的条件下，应提供远程接入方式对甲方系统问题进行检查、诊断和分析。乙方工程师仅在得到甲方许可的情况下方可访问甲方系统，并且乙方应确保所访问系统的安全，同时保证数据完整性。

（3）现场技术支持服务

按照甲方要求，乙方在下列情况下应及时指派工程师提供现场支持服务。工程师必须在服务完成，并得到甲方确认后方可离开现场。

(i) 故障处理

乙方应提供现场软件故障定位、处理服务。相关服务标准参照服务级别。

(ii) 配合甲方进行系统故障定位

甲方出现与各类软件相关但难以准确定位故障原因的系统问题时，为了保证故障得到及时、准确的定位和处理，乙方工程师应根据甲方的合理安排到达现场提供技术支持服务。乙方工程师应配合甲方对故障进行分析定位并及时解决。

1.3.12 应用变更现场技术支持

在甲方进行重要系统变更，如系统升级、切换演练等操作时，乙方应派工程师配合进行前期信息梳理，风险分析及评估，并在重要变更操作过程中提供现场支持服务。

在甲方应用部门进行重要变更，如新应用版本发布，平台变更等应用调整时，乙方应根据甲方要求提供现场技术支持服务。

二、项目其他要求

2.1 响应要求

乙方在与甲方签订服务采购合同后，须在最短时间内按要求提供相应的技术服务人员，乙方不得因任何情形影响人员的部署。

2.2 服务要求

乙方应具有规范的服务响应体系以及质量管控体系，能保障维保项目的顺利实施。乙方应承诺合同签订后一周内，在本地建立符合项目要求的服务团队，合同期内提供 7×24 小时技术支持服务。

（1）如果提供人员不能满足项目实际需要，则需在接到甲方反馈后，第一时间替换相关人员，如两次替换仍不能满足项目需要，严重影响项目进度的，甲方有权追究乙方责任。

（2）相关人员必须严格执行保密规定，未得甲方管理人员许可，不得随意分发、泄漏项目资料，如有违反，将按照有关规定给予处罚。

同时，乙方须承诺提供 7×24 小时的投诉渠道，及时受理甲方对服务方面不满意的投诉意见，并说明相关管理流程。

2.3 维保服务流程

乙方应具有清晰流畅、责任明确的维保服务界面和具体服务流程，以确保迅速有效地解决客户系统的问题或故障。

三、对技术人员的要求

3.1 针对本项目乙方应在平台部署上线后三个月内提供专职运维人员集中现场办公，负责软件 Bug 修复、升级等工作。

3.2 乙方服务团队稳定，服务团队要求 1 名本项目负责人，明确项目联络人员。

3.3 乙方还须承诺：参与本项目的工程师在合同生效之日起必须固定下来，如需更换须保证替换人员的认证资质和从业经验不低于原有人员，并须提前一个月向甲方提交书面申请并经相关软件维护人员签字同意。未经甲方同意人员不得随意更换，如出现随意更换的情况，甲方有权采取投诉、罚款等处罚措施直至解除合同。

3.4 甲方如对乙方所指派的服务工程师的服务质量不满意（包括技术能力、服务态度等），甲方有权通过书面形式提出撤换该工程师的要求，乙方应予以执行。