



甲方合同编号：【

乙方合同编号：【

合同格式
已审核：20240408

中国移动通信集团河南有限公司与河南省新郑监狱

关于【警务对讲通讯服务】项目合作协议

甲方：【河南省新郑监狱】（盖章）

法定代表人：张立志

住所：河南省新郑市炎黄大道1号

授权代表签字：刘源鹏

电话：18595617069

联系人：刘源鹏

乙方：【中国移动通信集团河南有限公司】（盖章）

法定代表人：首建国

住所：郑州市经三路48号

授权代表签字：赵喆

电话：13700861526

联系人：赵喆

合同签订日期：【2024】年【6】月【19】日

合同签订地点：【郑州】





根据《中华人民共和国民法典》、《中华人民共和国电信条例》及其他有关法律、法规的规定，在平等、自愿、公平、诚实、信用的基础上，双方就【警务对讲通讯服务】项目有关事宜协商一致，达成合同如下：

第一条 合作内容

1.1 乙方在现有技术条件下、现有网络覆盖范围内，为甲方有偿提供【警务对讲通讯服务】项目信息化服务具体内容为【警务对讲通讯服务（综合指挥），搭建警务对讲平台（终端管控），能够实现安全、稳定、高质量的实时对讲、电话通讯、移动办公等功能，同时配备终端管控服务、办公通讯服务及相应警务对讲通讯服务】项目的需求，甲方委托乙方完成该项目的集成工作。

1.2 乙方为甲方提供的具体服务相关具体要求详见【附件 1：服务清单及技术规范】。

第二条 资费标准和支付方式

2.1 本合同项下甲方应当向乙方支付的合同款项包括集成服务费。

2.2 本合同项下甲方应当向乙方支付的合同款项（含税）共计【3166812】元（大写：人民币叁佰壹拾陆万陆仟捌佰壹拾贰元整），详见下表。

2.3 合同项下所有款项由甲方向乙方以如下方式支付：

项目名称	合同内容	未含税总价 (元)	税率	增值税税额 (元)	含税总价 (元)	备注
河南省新郑监狱警务对讲通讯服务	办公通讯服务	39349.98	9%	3541.5	42891.48	无
		364172.94	6%	21850.38	386023.32	无
	警务对讲平台服务、综合调度以及管控平台	2506121.89	6%	150367.31	2656489.2	无
	数据专线	24770.64	9%	2229.36	27000	无
	5G 双域专网	51328.3	6%	3079.7	54408	无
合计		2985743.75	/	181068.25	3166812	无

本合同项下甲方应当向乙方支付的合同款项（含税）共计【3166812】元（大写：人民币叁佰壹拾陆万陆仟捌佰壹拾贰元整）。甲方向乙方分期付款，首期款项在本合同签订后 15 个工作日内支付，支付金额为含税 527802 元（大写：人民币伍拾贰万柒仟捌佰零贰元整）。剩余费用分 5 期按半年度支付，项目经验收通过后，在每年 6 月和 12 月底前进行支付，每期甲方向乙方支付项目费用含税 527802 元（大写：人民币伍拾贰万柒仟捌佰零贰元整）。

2.4 双方银行账户信息

甲方名称：【河南省新郑监狱】

纳税人识别号：【114100004158008273】

户名：【河南省新郑监狱】





开户行：【中行新郑市支行】
账号：【263700626333】
地址：【河南省新郑市炎黄大道1号】
联系电话：【0371-68335000】

乙方名称：【中国移动通信集团河南有限公司】
纳税人识别号：【91410000719172532Q】
户名：【中国移动通信集团河南有限公司】
开户行：【中国银行股份有限公司郑州花园支行】
账号：【258500874653】
地址：【郑州市经三路48号】
联系电话：【0371-68588012】

任何一方如需改变上述账户信息，应提前十（10）日以书面通知另一方。如一方未按本合同规定通知而使另一方遭受损失的，应予以赔偿。

2.5 结算周期内甲方向乙方支付的费用为：结算金额=Σ（服务费±违约金）（说明：如甲方违约则使用“+”，若乙方违约则使用“-”）。

2.6 结算方式采用【转账】（现金/转账等）的形式。

2.7 在甲方支付本合同项下的服务费之前，乙方应当向甲方开具相应金额的增值税【普通】（普通/专用）发票。

第三条 服务期限

本合同自双方签字盖章之日起生效，乙方应自合同生效之日起【30】日内完成平台集成及调测，达到交付验收标准。

自项目验收通过之日起乙方为甲方提供质保服务，直到质保期结束，质保期为【3】年。

第四条 集成验收

4.1 集成验收

4.1.1 根据中华人民共和国国家和履约地相关质量标准、行业技术规范标准、采购文件的要求及乙方的响应承诺验收。

4.1.2 在乙方完成集成服务【7】个工作日内，双方应对项目成果进行验收，各项功能及指标符合要求的，由双方签署项目验收合格报告。

4.1.3 甲方自收到乙方提交的验收申请后【7】个工作日内未组织验收，且自乙方催告后【3】个工作日内仍未组织验收的，视为验收通过。

第五条 售后服务

乙方质保具体内容如下：





5.1 为保证系统正常运行所需的预防性维护、日常维护支持、网络调整支持、数据备份支持等工作。

5.2 提供每周7天每天24小时的技术支持服务。如果出现紧急技术问题，在甲方通过电话或传真通知乙方的情况下，乙方的工程师应在1小时内予以答复。如果甲方要求紧急处理，乙方应在收到甲方通知后的4小时内赶到现场。当合同系统提供的业务中断时，乙方在提供远端服务的同时，须在收到甲方通知后2小时内赶到现场；因不可抗力致使乙方未按时到达现场的除外。

第六条 双方的权利与义务

6.1 甲方的权利和义务

6.1.1 在本合同有效期内，甲方有权要求乙方根据本合同约定和产品使用说明书的描述向甲方提供相应的产品和服务，所需的硬件设备由甲方提供。

6.1.2 甲方同意乙方有权协同第三方从事部分合同约定的乙方服务工作。但是，乙方应对第三方的服务行为向甲方承担责任。

6.1.3 甲方应当根据其所使用的业务的要求向乙方提供真实有效的证件、资料和信息（包括但不限于甲方单位及相关授权人真实有效的营业执照、身份证、授权委托书等证件，以及白名单的相关资料等）。

6.1.4 甲方承诺并保证不利用乙方提供的质保服务进行任何违反国家政策、法律法规以及侵犯乙方或第三方合法权益的行为。否则，乙方有权立即停止向甲方提供所有产品和服务并解除本合同，一切后果由甲方承担。

6.1.5 甲方应本合同的约定，及时足额向乙方支付各项费用。

6.1.6 甲方应授权一名员工作为联系人，负责甲乙双方信息传递、服务实现、业务受理等方面的组织协调工作。甲方联系人需提供乙方所需的身份确认资料。甲方联系人如发生变更，需以书面形式通知乙方。

6.1.7 甲方使用乙方提供的本合同约定产品或服务时，需遵守对应的产品使用说明。甲方未按约定和相关要求使用产品的，相关责任由甲方承担。

6.1.8 甲方成为乙方集团客户后，如果乙方提供了服务账号，甲方应妥善保管乙方提供的服务账号和甲方设定的服务密码。服务账号和密码是甲方办理相关业务的凭证，凡使用服务密码进行的任何操作行为均被视为甲方或甲方授权行为。如因甲方服务账号和密码保管不善等原因发生服务中断、业务变更、高额费用等情况，甲方应立即以书面形式通知乙方，乙方应采取可行的补救措施。甲方应当承担因账号和密码保管不善产生的费用。

6.1.9 如因甲方提供的相关资料不准确、不真实、不完整或变更后未通知乙方等原因，使乙方无法将服务提供给甲方，甲方承担由此造成的责任和后果。

6.1.10 甲方负责系统建设验收后的后期维护工作，本合同另有约定的除外。

6.1.11 未经乙方同意，甲方不得将乙方的软件、技术、设施、设备等用于双方合作项目以外





的其他用途，且不得向第三方透漏、转让。若甲方违反本条款，乙方有权要求甲方赔偿损失，撤回设备，终止协议。

6.1.12 未经乙方书面同意，甲方不得擅自使用中国移动的企业及品牌名称和标识、乙方的地方性品牌的名称和标识。否则，乙方有权解除合同并要求甲方赔偿损失。

6.2 乙方的权利和义务

6.2.1 乙方应按合同约定向甲方提供系统集成工作，乙方人员携带相关证件及单位证明，与甲方相关部门联系并办理相关手续，甲方应及时提供相关配合。

6.2.2 乙方进行检修线路、设备搬迁、工程割接、网络及软件升级或其他网络设备进行调试、维护工作，或因其他可预见性的原因可能影响甲方使用本合同约定产品或服务的，应提前通知甲方，甲方应给予必要的配合。

6.2.3 乙方受理甲方的故障申报，应及时安排故障处理。乙方按维护及业务规程的有关规定，为甲方提供优质服务。

6.2.4 在合同有效期内，乙方有责任按照国家标准负责系统的日常运行维护工作。保障系统的正常运行，如发生故障，及时响应。

6.2.5 因第三方实施破坏、网络攻击等非乙方原因导致甲方不能正常使用乙方产品和服务的，不视为乙方违约，乙方不承担相应责任。

6.2.6 乙方有权根据本合同约定要求甲方及时足额支付各项费用。

6.2.7 乙方应对其所委托的代为向甲方提供本合同项下服务的第三方的服务行为向甲方承担责任，包括保证其提供的服务质量符合本合同约定，并对其服务瑕疵向甲方承担违约责任。

6.2.8 因甲方员工与乙方存在电信服务合同关系，若在本合同履行过程中，甲方员工就与本合同有关的服务提出异议时，为保证甲方员工利益，乙方有权对提出异议的甲方员工暂停提供与本合同有关的甲方员工个人服务，并由三方进行协商。待三方意见一致时，再向提出异议的甲方员工恢复本合同服务，乙方无需因此向甲方承担违约责任。甲方员工如对已经提供的服务要求乙方承担责任时，该责任由甲方向乙方承担。

第七条 保密条款

7.1 “保密信息”是指本协议拥有信息的一方（“提供方”）根据本协议向另一方（“接受方”）提供的信息，或接受方在本协议履行过程中从提供方处获知的信息。保密信息包括但不限于的：技术信息、商业信息、商业秘密、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和其他保密信息，本协议的条款和与本协议有关的其他信息，本协议履行过程中形成的所有信息、数据、资料、意见、建议等。

7.2 保密信息只能由接受方及其人员为本协议目的而使用。除非本协议另有约定，对于提供方提供的任何保密信息，未经提供方事先书面同意，接受方及其知悉保密信息的有关人员均不得直接或间接地以任何方式提供或披露给任何第三方。甲方理解并同意，乙方及其关联公司可通过业务受





理系统登记、纸质档案，通过网络接收、读取并记录等方式，以提供电信服务为目的，在业务活动中收集、使用甲方提供的和甲方使用服务过程中形成的信息。乙方有权依法对包含甲方在内的整体用户数据进行分析并加以利用。未经甲方同意，乙方不向除乙方关联公司外的第三方提供甲方信息。乙方关联公司，是指中国移动通信集团公司及其在中华人民共和国境内直接或间接控股的主营通信业务的公司，以及上述公司的合法继承公司。

7.3 双方不得向任何人透露用户的信息、资料以及交易记录，除国家法律、行政法规另有规定外，双方均有权拒绝除用户本人以外的任何单位或个人的查询；同时，双方应尽合理努力将电子支付交易数据以安全方式保存，并防止其在公共、私人或内部网络上传输时被擅自查看或非法截取。

7.4 接受方的律师、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，接受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。接受方应向提供方承担因己方聘请的上述专业顾问违反保密约定而给提供方造成的任何损失。

7.5 如相关政府部门或监管机构要求接受方披露任何保密信息，接受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协议项下的保密责任。但前提是，该接受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，并且接受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。保密信息不包括以下任何信息：（1）非因违反本协议所致，已进入公众领域的信息；（2）在提供方依据本协议做出披露前，接受方已合法拥有的信息；（3）接受方从有权披露的第三方获得的信息；及（4）接受方独立开发的信息，未使用任何保密信息。

7.6 双方应严格遵守保密条款之约定，严格履行保密义务，直至有关保密信息合法公开之时止。本协议或其任何条款的终止、中止、失效、无效均不影响本保密条款的有效性及对甲乙双方的约束力。

7.7 由于保密信息接受方未履行保密义务给提供方造成损失的，接受方应当赔偿由此给提供方造成的损失。

7.8 在任何情形下，本合同约定的保密义务应永久持续有效。

第八条 违约责任

8.1 甲方未按照本合同约定的期限支付合同款项的，从逾期的次日起计算违约金，每滞后1天收取未缴金额的【1%】。违约金总额超过所欠金额的【6%】时，乙方有权解除本合同，并保留进一步追偿的权利。

因乙方原因导致乙方未按照本合同约定时间完成项目的，每逾期一天应向甲方支付合同金额1%的违约金。

8.2 如甲方未按本合同约定或国家法律法规规定及时办理相关备案或审批手续，因此产生的一切责任和后果均由甲方承担。根据国家法律法规、通信管理部门的规定或通知，乙方有权中断、终止为甲方提供本协议项下的全部或部分业务，且无需承担任何违约责任。





8.3 乙方在进行网络调整和维护时需要短时间中断服务,或者由于 Internet 上骨干网通路的阻塞造成甲方服务器访问速度下降,甲方认同属于正常情况,不视为乙方违约。

8.4 下列情况下乙方有权单方终止本合同,并停止向甲方提供服务。由此给甲方造成的损失,乙方不承担责任,并有权要求甲方承担违约和赔偿责任:

- (1) 甲方(包括联系人)提供虚假证照的;
- (2) 甲方利用乙方提供的产品和服务实施违反国家法律、法规和政策的活动;
- (3) 甲方利用乙方提供的产品和服务从事其他不当用途(如:甲方将乙方提供用于本合同业务的相关设备转售、租赁、转借第三方,或将乙方提供的设备、产品和服务接入其他通信服务提供商的业务)或侵犯第三方的合法权利;
- (4) 乙方根据国家有关部门的要求停止为甲方提供相关服务。
- (5) 甲方所使用的所有产品和服务中有一项产品欠费超过三个月,或有二项以上产品欠费均超过一个月。

8.5 乙方仅对因其过错给甲方造成的直接损害结果承担赔偿责任,且不包括第三方提出的索赔要求、数据丢失或损坏的损失,不包括经营损失等一切间接损失。无论何种情况,乙方对本协议项下的违约赔偿总额不超过本协议项下已支付的服务费用的总和。

第九条 不可抗力及免责条款

9.1 本合同所指不可抗力,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)天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迟延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。受阻方可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,任何一方均有权解除本合同而无需承担违约责任。

9.5 乙方对下述事项不承担责任:(1)第三方对甲方提出的索赔要求;(2)甲方的记录或数据的丢失或损坏;(3)甲方的经营损失等一切间接损失。

9.6 如因乙方难以避免、难以排除的技术或网络故障或第三方原因造成甲方无法使用本协议项下服务的,不视为乙方违约,但乙方应尽合理努力争取在最短时间内解决,对此双方无异议。鉴于





计算机、移动通信网络及互联网的特殊性，因黑客、病毒、电信部门技术调整和骨干线路中断等引起的事件，在乙方能够出具相关合理证明材料的情况下，甲方亦认同不属于乙方违约。

第十条 争议解决

10.1 本合同的成立、有效性、解释、履行、签署、修订和终止以及争议的解决均应适用中华人民共和国法律。

10.2 如果任何争议或权利要求起因于本合同或与本合同有关或与本合同的解释、违约、终止或效力有关，都应由双方通过友好协商解决。协商应在一方向另一方送达关于协商的书面要求后立即开始。

10.3 如果在一方提出协商要求后的十(10)天内，双方通过协商不能解决争议，则双方同意向乙方住所地人民法院提起诉讼。

10.4 诉讼进行过程中，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。本合同全部或部分无效的，争议解决条款依然有效。

第十一条 其他约定

11.1 本合同一式【肆】份，双方各持【贰】份，具有同等法律效力。

11.2 对于合同未尽事宜、双方可签订补充合同对本合同中的问题做出补充、说明、解释。本合同的补充合同作为本合同不可分割的一部分，与本合同具有同等的法律效力。

11.3 本协议附件作为本协议的一部分，与本协议具有同等法律效力。

11.4 在本协议有效期内，双方可以通过友好协商，对本协议相应条款进行变更或者解除本协议。任何一方欲变更或解除本协议，应提前30日向另一方提交书面说明。单方面解除协议的一方，应对另一方因此遭受的损失承担全部赔偿责任。

第十二条 本合同附件

附件1：服务清单及技术规范

附件2：网络与信息安全承诺书

(以下无正文)





附件 1：服务清单及技术规范

服务项目	服务名称	单位	数量	技术参数	税率	含税价
警务对讲平台服务	基础功能	项	1	1. 用户身份认证功能:应对管理平台的用户身份进行合法性认证,只有通过身份认证的用户才能访问管理平台。 2. 语音功能:支持监控中心之间的语音双向对讲功能;支持监控点和监控中心之间双向对讲或语音广播功能。 3. 登录认证功能:平台具有终端和 WEB 端登录认证功能,登录时进行密码认证,密码认证成功后方可登录到平台,否则不予登录。 4. 设备接入功能:平台支持执法记录仪、Android 终端及 PC 调度台等类型的设备登录接入。 5. 对讲组管理功能:平台支持对对讲组管理功能,通过调度员账号登录后,可对对讲组进行增加、删除、修改及成员管理操作。 6. 用户容量:平台单系统节点具备容纳管理 20000 个用户、1000 个组的能力。具备国家安全防范报警系统产品质量监督检验中心出具的检验报告。 7. SIP 接入功能:平台支持 SIP 协议、RTP 协议,支持通过 SIP 协议接入。	6%	20000
	语音功能	项	1	1. 单呼功能:接入平台的设备支持设备之间、平台与设备之间一对一全双工语音呼叫功能。 2. 强拆功能:平台具有强行拆除当前正在呼叫的通话链路。 3. 组呼功能:平台具有数字集群组呼对讲功能(点对多点的半双工语音通信方式),支持 5 级的组呼话权权限划分,高话权优先级的用户可抢占低用户优先级的话权讲话。具备国家安全防范报警系统产品质量监督检验中心出具的检验报告。 4. 音频存储功能:平台具有对终端之间以及调度台与终端之间的语音通话进行存储和查询功能,平台支持按 ID 和时间进行检索,并可下载和回放。 5. 紧急呼叫响应功能:平台具有接受紧急呼叫的功能,终端支持一键紧急呼叫,平台收到终端紧急呼叫时自动调用终端实时视频,获取终端的 GPS 位置,在地图界面闪烁报警。具备国家安全防范报警系统产品质量监督检验中心出具的检验报告。 6. 对讲机接入功能:平台支持通过对讲网关和模拟对讲机、数字对讲机进行语音对讲。具备国家安全防范报警系统产品质量监督检验中心出具的检验报告。 7. 平台能收到实体健报警的报警讯息。	6%	25260





	<p>视频功能</p>	<p>项</p>	<p>1</p>	<p>1. 视频通话功能:接入平台的设备,支持设备与设备、设备与平台之间一对一全双工视频通话功能,视频通话支持 H.264 视频编码格式,视频通话分辨率支持 QVGA、VGA、720P。</p> <p>2. 视频监控功能:平台支持远程监控服务的实时摄像头视频画面功能,监控视频支持 H.264 编码格式,监控视频分辨率支持 QVGA、VGA、720P、1080P。</p> <p>3. 监控过程存储功能:平台支持调度台与终端视频监控过程中,随时开启视频录制存储监控视频。</p> <p>4. 视频窗口分屏显示功能:平台支持同时查看多路视频,并可设置对视频窗口分屏显示方式。</p> <p>5. 视频轮巡播放功能:平台具有多路视频轮巡播放功能。</p>	<p>6%</p>	<p>33680</p>
	<p>即时通讯功能</p>	<p>项</p>	<p>1</p>	<p>1. 文件上传接收功能:平台支持终端文件传输接收功能,终端可将本地录制的视音频文件上传至平台,平台可根据终端 ID 和时间进行检索、回放和下载。具备国家安全防范报警系统产品质量监督检验中心出具的检验报告。</p> <p>2. 视音频文件存储功能:平台支持将终端上传的视音频文件、后台语音通话录音、视频监控录像、视频通话录像等文件进行存储;平台支持按照终端 ID 和时间进行条件检索、查看、下载和删除。</p> <p>3. 框选调度功能:平台支持在电子地图界面框选区域选择终端建立临时组,框选范围内的终端自动勾选,并可一键发起临时对讲。</p> <p>4. 点对点多媒体即时信息收发功能:平台与接入设备之间支持点对点即时信息收发功能,消息支持文字、图片、语音格式;支持对离线用户发送消息,用户可在上线后进行接收。</p> <p>5. 群组多媒体即时信息收发功能:平台支持群组即时信息收发功能,消息支持文字、图片、语音格式,发送到群组的消息,群组成员均可收到,离线的用户上线后可进行接收。</p> <p>6. 任务通知功能:平台支持向一个或多个接入平台的终端下发任务通知,通知支持文字、图片和视频文件下发;平台可按时间、消息类型等条件检索已下发的任务通知记录。具备国家安全防范报警系统产品质量监督检验中心出具的检验报告。</p> <p>7. 平台告警接收及统计功能:平台可接收的终端上报的 SOS 紧急呼叫功能、异常告警(久坐提醒、低电告警、低容量告警)并进行告警提示,支持记录告警历史,并可根据终端 ID 和时间等条件进行检索。具备国家安全防范报警系统产品质量监督检验中心出具的检验报告。</p>	<p>6%</p>	<p>12000</p>





	扩展功能	项	1	<ol style="list-style-type: none"> 1. 加入快照功能:平台支持将一个或多个加入快照功能,并在窗口中显示定期拍摄上传的照片。 2. IP 摄像机接入功能:平台支持通过 SIP 协议接入 IP 摄像机,平台可查看 IP 摄像机实时视频画面。 3. 布控球接入功能:平台支持通过 SIP 协议接入布控球,平台可查看布控球的实时视频画面。具备国家安全防范报警系统产品质量监督检验中心出具的检验报告。 4. 云台控制功能:平台支持通过 SIP 协议接入云台摄像机 / 布控球,可通过平台的云台控制界面实现远程云台控制,控制云台上下左右移动及镜头拉远拉近。 5. 视频转发功能:平台在调用终端视频的过程中可将该视频转发至其他终端。 6. 视频水印:平台支持接收终端实时上传的添加水印标记的视频,水印包含时间、终端 ID、名称、位置经纬度等信息。 	6%	20000
	警务对讲通讯 配套服务	项	421	<ol style="list-style-type: none"> 1. 运行环境要求国产,不低于八核; 2. 运行内存不低于 (RAM) 16GB; 3. 支持北斗、支持 NFC、指纹识别、蓝牙等对接服务,提供前置不低于 2000 万像素视频传输; 4. 具有安全管控专网及互联网双系统软件。 5. 生活模式与工作模式可一键切换; 6. 生活模式与工作模式下数据彼此隔离,不能互相访问; 7. 语音功能:生活模式与工作模式都能接电话,当前模式接电话的通话记录只保存在当前模式下,通话记录相互不能访问; 8. 短信息:生活模式与工作模式都能收发短信,当前模式收发信息只保存在当前模式下; 9. 另支持执勤模式,执勤模式下只能拨打亲情白名单内的号码。 	6%	2144574
管控平台 服务	基础功能	项	1	<ol style="list-style-type: none"> 1. 显示设备状态:显示当前终端的在线数量(最近上线时间 15 分钟内); 2. 用户信息:显示当前平台上的用户总数和已激活设备的用户数。 3. 系统状态监控:显示当前系统 CPU 和内存的空闲状态,以及 NPNS 通讯状态、远程控制服务、文档管理服务和平台服务的状态。 4. 设备状态:以条形图的形式显示当前有病毒、Rooted/越狱、已丢失、已淘汰、已擦除的设备数。 5. 设备违规情况:以环形饼状图的形式显示违规设备数与正常设备数的占比。 6. 设备归属分布:以环形饼状图的形式显示设备归属单位、用户和其他类型的占比。 7. 策略执行情况:以柱状图的形式显示策略已应用和已分发 	6%	50000





			<p>比例。</p> <p>8. 在线设备量统计:以柱状图的形式显示设备在线时间分布。</p> <p>9. 消息提醒:包括但不限于设备 Rooted/越狱提醒、新增激活设备提醒、设备失联提醒、流量超额提醒、SIM 卡变更提醒。</p>		
用户管理功能	项	1	<p>1. 创建用户和用户组:支持文件导入用户和组织架构/设备信息/头像信息/亲情号。</p> <p>2. 锁定账号:支持锁定账号和解锁账号。</p>	6%	42100
应用商店	项	1	<p>1. 上传应用:支持上传同一个应用的多个版本。</p> <p>2. 查询/筛选/排序应用:支持按应用名称模糊查找应用、支持按条件筛选目标应用、支持按应用按名称、状态、分类、更新时间进行排序。</p> <p>3. 维护管理:支持应用下架/删除/更新等,用户组织架构变更时,自动删除该用户在原来组织结构下已推送的应用。</p> <p>4. 导出已下发应用的详情:支持导出已下发应用下发的用户、设备等详情</p> <p>5. 一键向未安装/未更新的设备分发应用</p> <p>6. 查看/更改应用下发关系:支持查看应用下发给了哪些用户/用户组/设备/设备组,支持按用户/用户组/设备/设备组删除下发关系。</p>	6%	20000
设备管控	项	1	<p>1. 查看设备详情:支持查看设备状态及基本信息、设备上安装的应用程序、设备策略、文档内容、杀毒信息、应用耗电量</p> <p>2. 机卡绑定:终端与 sim 卡绑定在一起,私自换卡向管理员发送违规提醒。</p> <p>3. 切换终端模式:可远程切换设备至个人模式或安全模式</p> <p>4. 锁定终端模式:可远程将设备的个人模式或安全模式锁定。</p> <p>5. 执勤模式:可将终端切换至执勤模式,在该模式下只允许使用管理员指定应用和拨打亲情号码。</p>	6%	84200
管理策略	项	1	<p>1. 限制策略:可向终端下发的管理策略包括但不限于允许/禁止使用相机、允许/禁止使用 WiFi、强制开启/关闭移动数据、允许/禁止使用蓝牙、允许/禁止允许移动热点、强制开启/关闭定位、允许/禁止更改日期或时间、允许/禁止安装未知来源的应用、允许/禁止启用 USB 调试模式、允许/禁止 USB 使用 MTP 数据传输、允许/禁止截屏、允许/禁止恢复出厂设置。具备国家安全防范报警系统产品质量检验检测中心出具的测试报告。</p> <p>2. 亲情通话管理:用户的亲情号码由管理员进行审核后录入系统,当终端切换到执勤模式后,除白名单号外只能与亲情号码通讯,除此之外不能接打其他电话或者发送短信。</p> <p>3. 地理围栏管理:提供地理围栏功能,在限定的围栏范围内可以强制将终端切换至执勤模式。</p>	6%	29470





	文档管理	项	1	1. 上传文件：支持单个或批量上传文档、图片、音频或视频等格式的文件，支持修改文档简介。 2. 远程推送文档：支持手动推送文档，支持用户组织架构变更后，自动向用户推送其当前所在用户组下的已推送的文档。 3. 远程启用/禁用文档：支持管理员控制文档是否可用 4. 远程删除文档：支持按下发关系删除文档，实现文档只对一部人可见	6%	20000
	信息展示服务	项	1	1. 进出监狱区（监区 AB 门）处的人员进出信息展示，语音播报、监狱内外人员统计、监狱时时执勤人员统计等信息。 2. 提供大屏数据展示功能：在显示大屏上实时展示门禁进出情况。Android 操作系统，展示环境不低于 4K 超清、三级能效。	6%	40000
	运行服务	项	1	1. 提供支持国产，具有自主知识产权的运行环境； 2. 系统运行环境不低于内存 64GB、硬盘 2T*8、内置存储 2*M.2 SATA SSD 和支持硬 RAID1 等	6%	69000
	网络配置服务	项	1	网络配置不低于交换容量 336Gbps，包转发率：96Mpps	6%	3515.2
门禁监控服务	虚拟换证管理系统	项	1	开放对接警务通 APP 模式切换源码	6%	42690
	读卡服务	项	1	支持下发密码开门 需满足内置蜂鸣器、反破坏开关、看门狗等数据上传 读卡服务对接需要支持密码键盘、RFID、报警等		
	虚拟换证 CPU 读卡服务	项	1	运行环境需要支持 CPU 识别码切换		
	门禁服务	套	2	可脱机使用，亦可联网。多组维度输入口，可透过软件设定。 透过计算机设定所有参数，也可由键盘设定基本参数。 支持主动上传功能(V5A) 支持 TCP/IP WiFi 通讯 (SY230NT2-N-PV5A)		
	人脸识别服务	套	2	服务运行环境要求： 操作系统 Android 7.1 及以上多国语言版、 运行内存 RAM2GB LPDDR4/1600MHZ、 储存内存 ROM16/32 GB eMMC5.1		
	监控服务	套	1	武警门人员进入抓拍布控高转闸人员外出抓拍布控		
通讯服务	办公通讯服务	项	421	每个号码每月不低于 1500 分钟语音通话 100G 流量 内部通话 1000 分钟 全国接听免费，套餐期限为 3 年；	9%	42891.48
				6%	386023.32	
	50M 专线	项	1	提供 3 年 50M 数据专线；	9%	27000
	5G 加密服务	项	1	提供 3 年 5G 双域网；	6%	54408





附件 2: 网络与信息安全承诺书

网络与信息安全协议书

甲方应按照《中华人民共和国网络安全法》等法律法规的要求,履行相关网络安全义务,承担网络安全责任。

第一条 甲方承诺不利用乙方提供的服务及设备设施进行下列任何活动或发布、传播下列任何信息:

(1) 从事危害国家安全、泄露国家秘密等犯罪活动;从事国家法律、法规、政策所禁止的活动或违背公共道德的活动;

(2) 散布谣言,扰乱社会秩序,破坏社会稳定;散布垃圾邮件、病毒程序;黑客行为;侵权行为;博彩、赌博游戏等;

(3) 危害国家安全、泄露国家机密、颠覆国家政权、破坏国家统一的信息;损害国家荣誉和利益的信息;煽动民族仇恨、民族歧视、破坏民族团结的信息;违反国家宗教政策的信息;宣扬邪教和封建迷信的信息;淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的信息;侮辱或者诽谤他人,侵害他人合法权益的信息;妨碍互联网运行安全的信息;其他有损于社会秩序、社会治安、公共道德的信息或内容;

(4) 发布、传播其他违反国家法律、法规、政策内容的。

甲方同时承诺不为他人从事上述活动或发布、传播上述信息提供任何便利,如因甲方违反上述约定产生的一切责任和后果均由甲方承担。甲方认可乙方有权判断本协议项下甲方从事的活动或甲方发布的信息是否违法、违规或违反本协议有关规定,且乙方有权在提前通知甲方的情况下采取一切必要措施,包括但不限于暂停或终止提供本协议项下的服务、要求甲方进行整改等,但乙方上述权利不应被视为乙方有审核甲方行为或信息内容的义务或保证其合法合规的任何责任。

第二条 甲方不得有下列危害电信网络安全和信息安全的行为:

(1) 对电信网络的功能或者存储、处理、传输的数据和应用程序进行违法删除或者修改。

(2) 利用电信网络从事窃取或者破坏他人信息、损害他人合法权益的活动。

(3) 故意制作、复制、传播计算机病毒或者以其他方式攻击他人电信网络等电信设施。

(4) 危害电信网络安全和信息安全的其他行为。

若甲方存在上述任一情形的,乙方有权按相关规定暂停或停止提供服务、断开网络接入,保存有关记录,并向政府主管部门报告,由此引起的一切后果和责任由甲方负责。同时,乙方有权终止合同,并不承担任何责任。

第三条 甲方不得将接入设备转借或租赁给其它单位和个人使用,以防止非法信息的传播;否则,由其承担相关责任,乙方有权立即停止相关服务。

第四条 甲方应承担如下管理责任:





- (1) 向所属员工或使用者宣传国家及电信主管部门有关电信安全的法规规定。
- (2) 建立健全使用者档案，加强对使用者的管理、教育工作。
- (3) 有健全的网络安全保密管理办法。

第五条 甲方有责任对其自身系统的网络安全状况负责，并定期对其系统的安全状况进行检查，若发生网络攻击、信息泄露等网络安全事件，乙方不承担相关责任。

第六条 甲方侧数据由甲方负责，如出现信息泄露、信息篡改等安全事件，乙方不承担责任。

第七条 甲方承诺采取技术措施和其他必要措施，保障网络安全、稳定运行，有效应对网络安全事件，防范网络违法犯罪活动，维护网络数据的完整性、保密性和可用性。不得从事以下行为：

- (1) 利用自己或他人的机器设备，未经他人允许，通过非法手段取得他人机器设备的控制权；
- (2) 非授权访问、窃取、篡改、滥用他人机器设备上的信息，对他人机器设备功能进行删除、修改或者增加；
- (3) 向其他机器设备发送大量信息包，干扰其他机器设备的正常运行甚至无法工作；或引起网络流量大幅度增加，造成网络拥塞，而损害他人利益的行为；
- (4) 资源被利用进行网络攻击的行为或由于机器设备被计算机病毒侵染而造成攻击等一切攻击行为。
- (5) 有意通过互联网络传播计算机病毒；
- (6) 因感染计算机病毒进而影响网络和其它客户正常使用的行为。

第八条 甲方业务如使用乙方提供的 IP 地址，甲方需承诺并确认：甲方所提交的所有备案信息真实有效，且备案信息不得出现乙方任何内容。当提供的备案信息发生变化时应及时到备案系统中提交更新信息，如因未及时更新而导致备案信息不准确，乙方有权依法采取停止提供服务、断开网络接入等关闭处理措施。如因甲方原因造成信息未及时通知，引发相关网络信息安全事件的，由甲方自行承担相关责任。



甲方签字盖章：

2024年6月19日

