

合同登记编号:

信息化基础运维服务项目
--2022 年业务系统运维项目合同

甲 方: 北京市应急指挥保障中心



乙 方: 太极计算机股份有限公司



签订地点: 北京市通州区运河东大街 57 号

签订日期: 2022 年 7 月 12 日

甲方：北京市应急指挥保障中心
地址：北京市通州区运河东大街 57 号院 4 号楼
法定代表人：陆金周
联系电话：010-55573960 邮编：101117

乙方：太极计算机股份有限公司
地址：北京市朝阳区容达路 7 号
法定代表人：肖益
联系电话：010-57702888 邮编：100102

鉴于甲方有意委托乙方，双方特依据《中华人民共和国民法典》和相关的法律法规，按照平等互利的原则达成如下协议：

1、合同说明条款

1.1 甲、乙双方根据国家和北京市相关法律法规的规定，本着诚实守信、合作互利的原则，经过友好协商，就甲方委托乙方提供信息化基础运维服务项目-2022 年业务系统运维项目运维服务事宜签订本合同。

1.2 甲、乙双方之间任何与本合同有关的信函、电子邮件、电话，均使用并且只能使用下列双方确定的地址、传真号码、电话号码、电子邮件地址名。

单位名称	电话	传真	邮件	地址
北京市应急指挥保障中心	010-55573960			北京市通州区运河东大街 57 号院 4 号楼
太极计算机股份有限公司	010-57702888	010-57702889	zhangzhi@mail.taiji.com.cn	北京市朝阳区容达路 7 号

1.3 甲、乙双方之间有关合同的财务来往及结算，应通过甲方与乙方共同确认的银行及账户进行。本合同存续期间，一方若遇结算银行及账户变化，应在变化之日前 30 日内书面通告另一方，并在变化后 15 日内再次通知另一方。如变更一方未及时履行变更告知义务，由此产生的错付、误付的一切不利后果均由变更一方自行承担。

1.4 本合同的有效组成部分包括：本合同、合同附件、分包意向协议（如有）。

2、服务内容

2.1 服务内容

乙方负责 信息化基础运维服务项目-2022 年业务系统运维项目 运行维护服务，保证政府数据安全和信息交换安全。服务内容详细描述见附件一。

2.2 服务承诺

乙方在合同约定的期限内选派专业技术运维人员满足甲方的服务需求。乙方保证技术运维人员在为甲方提供服务的过程中，严格遵守甲方的各项规定、服从甲方安排。若甲方提出要求更换项目服务人员，乙方应于收到甲方通知之日起 10 日内进行更换。上述被更换的人员无甲方批准，不得重新参加相关工作。服务质量承诺详细描述见附件二。

2.3 服务期间

乙方为甲方提供运行维护服务的期间为 12 个月。

2.4 预留中小企业份额

本项目属于适宜由中小企业提供的情形，依法预留采购项目预算总额的【40%】专门面向中小企业采购，其中预留给小微企业的比例不低于预算总额的【28%】。对于预留份额，提供的服务由符合政策要求的中小企业承接。

3、合同价款

本合同总额为人民币（大写）叁佰玖拾万元整（¥3,900,000.00 元整，含税）。前述合同价款为含税价，是乙方在服务期间内全面履行本合同所有义务后，甲方所应支付的所有费用，除此之外甲方无需再支付乙方其他任何费用

4、支付条款

4.1 支付依据

乙方应向甲方汇报运维的工作情况，甲方根据乙方提交的年度运维报告及相关服务要求和约定，支付运维服务费。

4.2 支付方式

在双方签署合同后 10 个工作日内，乙方向甲方提供项目合同款总额 5%的履约保证金后，甲方以支票方式向乙方支付合同款的 60%作为项目启动款；

在开展项目技术服务 8 个月后乙方申请第 2 笔支付款，甲方需对技术服务时间予以确认，并在双方确认后 30 个工作日内以支票方式向乙方支付合同款的 30%；

年度运维工作结束且项目终验合格后乙方申请第 3 笔支付款，甲方需对技术服务时间予以确认，在双方确认后 30 个工作日内以支票方式向乙方支付合同尾

询报告、服务内容)与工作业务信息进行保密,未经甲方书面批准不得提供给第三方。如有违反,乙方应承担相应的法律责任。此保密协议不因合同的终止而免除。

7.2乙方必须与甲方签订《安全保密协议》。乙方因承接本《合同》服务所熟悉的甲方信息或甲方单位人员信息,以及在服务过程中所产生的全部甲方或甲方单位人员信息等均为甲方的保密信息,乙方应承担保密义务。见附件3。

7.3乙方必须遵守甲方的各项规章制度,严格按照工作规范组织进行运维工作,制定切实可行的措施保障人员安全、设备安全、生产安全。

7.4乙方必须制定合理的措施对运维人员进行管理与思想教育,加强保密意识,安全生产意识。

7.5乙方如违反《安全保密协议》,乙方必须承担全部责任并赔偿甲方的一切损失,甲方有权追究乙方的法律责任并终止本合同。

7.6甲、乙方应积极配合信息安全主管部门对信息安全进行监督检查。

8、知识产权条款

8.1乙方保证甲方在使用乙方提供的任何产品、服务时,不受第三方提出侵犯知识产权指控。如果任何第三方提出与乙方提供的任何产品、服务有关的侵权指控,乙方须与第三方交涉并承担因此发生的一切法律责任和费用。

8.2本项目实施所产生的信息资源及完成的所有技术成果(包括但不限于软件、源代码及技术资料)的知识产权(包括但不限于著作权、专利权、商标权、专有技术等权利)及衍生权利均由甲方享有,凡有必要或者可能申请专利的技术成果,均需要通过甲方办理专利申请。

8.3对在运维过程中获知的甲方或为甲方提供服务的第三方的知识产权,都受本条款的保护。

9、不可抗力

9.1如果合同任何一方因战争、火灾、洪水、台风、地震和其他不可抗力原因,影响了合同的履行,则可根据受影响的程度顺延合同履行期限,这一期限应相当于事故所影响的时间、并可根据情况部分或者全部免于承担违约责任。但若一方违约在先,不得以此后发生不可抗力为由免除其违约责任。

9.2受不可抗力影响的一方应在事件发生后,立即通知对方,并在十日内以书面方式向对方提供该不可抗力事件的证明文件(如政府公告、新闻报道等),

并应于不可抗力事件结束后，立即恢复对本合同的履行。

9.3 如果不可抗力事件后果影响本合同执行超过 180 天，双方则就未来合同的履行另行商议。

10、争议解决条款

10.1 争议的解决

因履行本合同而发生的或与本合同有关的一切争议，甲、乙双方应首先通过协商方式解决，若协议不成，向甲方所在地区的人民法院提起诉讼。

10.2 争议期间服务的连续性

如果甲方和乙方之间发生争议，乙方有义务继续按照服务内容条款中的要求提供服务，不得中断。

11、其他条款

11.1 本合同生效后，除出现不可抗力，继续履行将损害国家利益和社会公共利益的情形外，未经协商，任何一方不得擅自变更、中止或者终止本合同。甲方需追加与合同标的相同的服务的，在不改变合同其他条款的前提下，可以与乙方协商签订补充合同，但所有补充合同的采购金额不得超过原合同采购金额的百分之十。

11.2 本合同的附件为本合同不可分割的部分，与本合同正文具有同等效力。

11.3 如本合同附件中的条款或本合同签署之前所签署的任何文件与本合同的条款相冲突或不一致，以本合同为准。

11.4 履约验收方案

11.4.1 履约验收的主体、时间、方式

供应商完成全部工作内容提交项目成果后，采购人有权组织 1 次不少于 5 名专家的评审会。

11.4.2 履约验收的程序

根据验收标准，对项目服务成果进行验收，出具专家验收意见，验收意见应包含对各项服务成果的分项验收意见，专家费用由投标人支付。

11.4.3 履约验收的内容和验收标准

根据合同条款要求、招标文件要求、投标文件响应及国家行业有关标准，针对本招标文件对应的合同中每一项商务、技术要求履约情况进行履约验收。

12、合同的终止与解除

12.1 违约的解除

甲乙双方不得随意解除本合同，因解除合同给对方造成损失的，除不可归责于该当事人的事由外，应当赔偿守约方的全部损失。如乙方要求解除该合同，必须提前 10 日以书面形式通知甲方，并退还甲方已支付的全部款项，乙方应向甲方支付本合同服务费总额 0.5% 的违约金，还应赔偿甲方因此造成的损失。

乙方在连续 2 个月的运维服务质量考核中不合格的，乙方在甲方发出要求乙方纠正违约行为的书面通知之日起 30 天内未能纠正违约行为并赔偿损失的，甲方有权解除合同。

乙方在提供运维服务过程中出现重大安全事件的，或甲方因特殊情况或其他合法正当原因要求乙方停止本合同约定的服务的，甲方有权解除合同。

13、合同的生效

13.1 本合同有效期限为 12 个月，合同自签订双方代表人签字并加盖单位合同章或者公章后生效。


13.2 本合同一式捌份，甲方执陆份、乙双方各执贰份，具有同等法律效力。

13.3 本合同未尽事宜，凡需对本合同条款进行修改，应经双方协商后补充协议方式明确。

甲方：北京市应急指挥保障中心
法定代表人：
法定地址：北京市通州区运河东大街57号

邮编：101117
传真：
电话：010-55573960

签约日期：2022.7.12

乙方：太极计算机股份有限公司
法定代表人：
法定地址：北京市海淀区北四环中路211号

邮编：10083
传真：010-57702889
电话：010-57702888
开户行：工行北太平庄支行
税务登记号：91110000101137049C

签约日期：2022.7.12

附件1

运维外包技术服务条款

1. 基本要求

1.1 采购标的需实现的功能或者目标

满足采购人日常工作开展需要，保证本项目包含全部系统安全稳定运行。

1.2 需执行的国家相关标准、行业标准、地方标准或者其他标准、规范

1.2.1 采购人内部管理规范；

1.2.2 《中华人民共和国网络安全法》；

1.2.3 GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》；

以上规范如有更新，以国家、地方、行业最新标准为准。在实施本项目期间除应遵循上述规范外，还应遵循未列出的其它相关国家、地方、行业标准及规范。

2. 服务内容及要求

2.1 运维系统及要求

序号	运维项目	运维主要内容
1	数据库系统运维	数据库系统运维内容包括： 1、数据库系统软件的按需或定期关闭和启动。 2、数据库运行状态监控。 3、数据的安全管理及备份，进行本地、异地备份，并对备份数据进行管理。 4、数据库参数配置检查、调整和优化。 5、数据库安全加固等。 6、数据库故障处置：对数据库问题进行诊断、处置。 7、技术文档管理服务。根据数据库系统运维需要，及时总结技术维护文档，并对技术文档进行动态更新、管理。
2	数字证书运维服务	数字证书运维服务包括： 1、数字证书统计管理。 2、为新入职人员申请办理数字证书。 3、当用户证书即将过期时为用户提供数字证书更新。 4、为锁定的用户的数字证书进行解锁。 5、当用户的数字证书丢失或者损坏时为用户重新办理个人数字证书。 6、根据市应急管理局人员安排，为离职人员注销数字证书。 7、技术文档管理服务。
3	业务相关系统运维（烟花爆竹、安全监管移动执法系统、安全生产专职安全员检查系统（离线版）、应急值守以及应急相关系统、地理信息系统、行政审批系统运维	烟花爆竹、安全监管移动执法系统、安全生产专职安全员检查系统、专职安全员检查系统（离线版）、应急值守以及应急相关系统、地理信息系统、行政审批系统运维内容包括： 1、系统巡检维护。对重要业务系统进行7*24可用性巡检，对其他系统每日检查系统的可用性、系统功能完整性。 2、系统性能优化服务。优化系统功能、调整系统栏目，满足日常业务开展中对系统优化的需求；优化系统代码，提升系统运行效能；解决系统漏洞，对系统进行应用层面的安全加固。使系统更健壮，可用性更强。

序号	运维项目	运维主要内容
	安全员检查系统、专职安全员检查系统（离线版）、应急值守以及应急相关系统、地理信息系统、行政审批系统、特种作业考试系统、台账系统）	<p>3、系统故障处置和恢复。及时处置系统故障，对系统故障事件进行快速响应，进行故障原因排查，恢复系统服务。</p> <p>4、系统优化。根据调整安排，提供系统部署，硬件支撑资源调整、业务系统优化等服务。</p> <p>5、业务系统上、下线技术支持。配合软件建设单位准备应用系统上线、下线，准备业务应用系统上线所需基础技术环境以及业务应用系统下线所需技术支持工作。</p> <p>6、应用系统数据备份及恢复管理服务。制定合理的备份策略，定期备份生产系统的数据及应用系统程序文件，并检查备份执行情况是否正常；定期开展备份数据恢复测试工作，检查备份数据有效性。</p> <p>7、系统安全加固。对系统进行安全风险评估，对系统存在的信息安全隐患进行安全加固、策略调整和配置优化等。</p> <p>8、技术文档管理服务。根据业务系统运维需要，及时总结技术维护文档，并对技术文档进行动态更新、管理。</p> <p>9、应急演练工作。根据业务需要，定期开展办公和业务系统应急演练工作。</p> <p>10、其他技术服务。根据业务需要，对业务系统使用人进行培训服务等。</p> <p>特种作业考试系统运维内容包括：</p> <p>1、系统巡检维护。对业务系统进行日常巡检，检查系统的可用性、系统功能完整性。</p> <p>2、单机版软件维护。参照培训单位软硬件条件，向培训单位提供单机版安装及使用的技术指导服务。</p> <p>3、系统故障处置和恢复。及时处置系统故障，对系统故障事件进行快速响应，进行故障原因排查，恢复系统服务。</p> <p>4、远程协助。通过远程协助，对各类客观原因导致的突发问题进行处理。</p> <p>5、考试数据上传确认。考点理论考试结束完成数据上传后，对已上传考试数据进行核对，确认数据入库情况。</p> <p>6、其他技术服务。根据业务需要，对业务系统使用人进行培训服务等。</p> <p>台账系统运维内容包括：</p> <p>1、系统巡检维护。对业务系统进行日常巡检，检查系统的可用性、系统功能完整性。</p> <p>2、系统故障处置和恢复。及时处置系统故障，对系统故障事件进行快速响应，进行故障原因排查，恢复系统服务。</p> <p>3、远程协助。通过远程协助，对各类客观原因导致的突发问题进行处理。</p> <p>4、数据处理。对于业务系统界面上数据已进入审核、审批、办理、办结、归档等业务流程中无法直接修改数据的情况，根据用户要求进行更新、修改。</p>
4	应急管理数据对接技术支持	<p>应急管理数据对接技术支持内容包括：</p> <p>1、开展日常巡检，保障应急管理共享交换平台的安全、稳定运行，按要求记录巡检时间和巡检内容，发现问题按程序及时报告，并提供必要的技术支持。</p> <p>2、根据采购人要求，对各区应急局、委办局、局内业务系统、其他单位提供数据共享交换技术支持。</p> <p>3、配合采购人，做好资源目录、数据开放建议清单梳理工作。</p> <p>4、负责因经信局共享交换平台升级和共享交换平台上云而引起的功能升级和服务方式的变更工作。</p> <p>5、如果针对某些数据需要开发接口，按要求做好本系统服务接口的开发、维护、更新和扩展工作</p>
5	应急管理	应急管理门户运维内容包括：

序号	运维项目	运维主要内容
	门户运维及政务网站运维	<p>1、系统巡检维护。对业务系统进行日常巡检，检查系统的可用性、系统功能完整性。</p> <p>2、系统故障处置和恢复。及时处置系统故障，对系统故障事件进行快速响应，进行故障原因排查，恢复系统服务。</p> <p>3、系统性能优化服务。优化系统功能、调整系统栏目，满足日常业务开展中对系统优化的需求；优化系统代码，提升系统运行效能；解决系统漏洞，对系统进行应用层面的安全加固。使系统更健壮，可用性更强。</p> <p>4、信息专题制作。根据采购人要求，开展专题业务设计，新增业务专题页面等工作。</p> <p>5、数据处理。对于业务系统界面上数据已进入审核、审批、办理、办结、归档等业务流程中无法直接修改数据的情况，根据用户要求进行更新、修改。</p> <p>政务网站主要运维工作包括：</p> <p>1、网站信息发布及维护。根据相关的局内信息审批流程，对普通内网信息、区县信息、弹出信息、外网信息的内容进行更新。</p> <p>2、政务网站巡检。按照应用系统运维规范，定期对政务网站所有模块的业务可用性、内容准确性、域名和IP访问、首页、二级页面、三级页面以及嵌套页面等进行巡检等。</p> <p>3、政府信息公开内容管理系统维护。</p> <p>4、数据维护。进行网站业务数据的管理、维护、归档工作，并根据相关规定，每日上传日志文件到首都之窗。处理因用户操作失误等特殊原因导致的需要进行数据干预的维护服务。</p> <p>5、网站安全加固。对应急管理局外网网站进行安全加固，修补安全漏洞。</p> <p>6、网站功能调整需求。北京市应急管理局网站的页面、版式、图片等内容的修改。</p> <p>7、网站错误扫描。对网站的错字、错链进行扫描检测，检测网站是否存在不合法信息，并提供检测报告。</p> <p>8、故障处置和系统恢复技术服务。处理网站突发故障、及时恢复网站访问服务。</p> <p>9、系统数据管理服务。制定合理的备份策略，定期备份生产系统的数据，并检查备份执行情况是否正常；定期开展备份数据恢复测试工作，检查备份数据有效性。</p> <p>10、政务网站应急演练：定期开展政务网站主备机切换、宕机等应急演练工作。</p> <p>11、政务网站特殊时期值守工作：特殊时期安排工程师现场技术值守工作。</p> <p>12、技术文档管理服务。根据政务网站运维需要，及时总结技术维护文档，并对技术文档进行动态更新、管理。</p>

2.2 北京市应急管理局信息化现状

2.2.1 市应急管理局信息化概况

市应急管理局一直以来努力探索建立符合应急管理工作和规律的信息信息化建设、应用及管理的新模式，在信息化建设取得了一定成果，信息化应用的推广工作取得了全面进展，信息化已经完全融入了市应急管理局的业务和办公工作，成为了重要的、不可或缺的工作方式。

2.2.2 软件系统现状

2.2.2.1 信息化建设历程

北京市应急管理局信息化工作起步于 2018 年，在原安监局信息化工作的基础上，又经过几年的发展过程，信息化工作紧密结合业务需求，不断迭代更新和深化应用，由分散和封闭走向统一和开放，正处于全力推进系统整合应用和数据深度分析应用的重要历史时期。目前已建设有 3 级网络、4 级信息平台，7 大业务应用、1 个数据中心、1 个应急指挥中心，以及视频会议及图像监控 2 套支撑系统，集成协同办公、执法检查、隐患管理、公共服务、应急通讯、指挥调度等多项功能。

2014 年，原安监局局党组将信息化列为“四化三体系双基”（“四化”：法治化、标准化、信息化和社会化；“三体系”：隐患排查治理体系、安全预防控制体系和安全生产责任体系；“双基”：基层基础工作）总任务的重要内容，成立了信息化领导小组，制定下发信息化总体建设方案，大力推进信息化资源整合与应用。2015 年开展全市生产经营单位普查，全面摸清我市生产经营单位情况。2016 年，完成行政审批系统升级改造，支持市区两级应用。按照“一企一标准、一岗一清单”模式建设隐患排查治理系统；2017 年制定了信息化顶层设计方案，开展数据中心建设，整合优化信息化数据资源。当年为全市近 5000 余名专职安全员研发移动检查系统，实现全市生产经营单位检查的全覆盖；2018 年，在原国家安监总局的支持下对我局监管信息平台进行全面优化，开展移动执法系统和办公 OA 系统升级改造，加强业务系统整合，重要业务系统全部实现“云部署”，数据中心初步建成，数据资源共享程度得到显著提升。

2.2.2.2 主要业务系统功能

1. 应急管理信息平台建设

按照“集中建设、分级使用”的原则，组织建设了 4 级监管信息平台，市、区、街乡、企业 4 级信息平台根据实际业务需要各有侧重，实现各类业务“全覆盖”，满足不同人员使用需要。其中，市级平台实现了 43 项业务功能、区级平台实现了 35 项业务功能、街乡平台实现了 9 项业务功能、企业平台提供了 21 项服务功能，显著提高了工作效率。

2. 局政务网站建设

局政务网站自 2005 年开通，先后历经 3 次改版，目前运行版本为 2019 年改版，目前运行的政务网站共有 6 个一级栏目、46 个二级栏目、15 个专题专栏，在传播安全文化知识、解读安全生产法律法规、展现应急管理系统工作等方面发挥了重要的窗口作用。政府网站突出特色栏目，整合应急管理、地质灾害防治、防汛抗旱、森林防火专题网站的信息资源，丰富和完善网站内容及功能；同时结合国家、北京市政府相关考核评测体系，深度整合信息、业务和服务，提升用户体验。

3.企业台账管理系统

为了摸清全市生产经营单位底数，进一步夯实首都安全监管基础工作，在 2015 年生产经营单位普查工作的基础上，2017 年我局启动生产经营单位台账系统建设，依托专职安全员日常检查，实现了生产经营单位的应统尽统和台账数据的动态更新，数据质量和准确率得到明显提升。

目前，该系统还与行政执法、隐患排查、标准化达标、专职安全员检查等多个业务系统实现对接，与 10 余个区安监局实现数据共享，真正实现了全市共用一本账，业务工作深度融合，也为下一步全市生产经营单位分级分类监管和大数据分析奠定了坚实基础。

4.行政执法信息系统

我市新版安全生产行政执法系统于 2018 年 1 月上线试运行。该系统的应用使全市执法人员可利用 PAD 开展现场执法，在执法文书中嵌入电子签章，实现了执法文书的电子印章集成化。系统还将执法系统与局网站政务公开、市政府法制办执法考核、安全员检查等业务系统有效对接，实现执法数据的“一方录入、多方共享”，有效提升了行政执法信息化、规范化、标准化水平。

5.专职安全员检查系统

近年来，为配合安全员日常检查工作，2016 年初，我局建成专职安全员检查系统并上线运行。安全员使用手机 APP 中集成的 15 项常规检查标准，实现了安全生产隐患的全流程动态监管和检查文书电子化送达。

6.数据中心建设

随着业务不断深化，各类数据不断丰富和完善，我局组织建设了数据中心，将企业台账数据、知识数据、业务数据、物联网数据纳入数据中心进行集中管理，努力实现对我市各类安全生产和应急数据资源的“统一管理、统一共享、统一服

务”，通过数据中心向各业务系统提供统一的数据服务，提升数据共享和使用效率。同时，开展大数据可视化分析平台建设，依托企业台账数据，开展数据综合分析和展示，实现以企业画像和监管力量画像为核心的集中分析展示。

2.2.3 运维管理

市应急管理局信息化建设和运维工作在市经信局业务指导下，通过采取一系列有力措施，健全制度，加快硬件建设，强化治理服务，取得了较好的成绩。信息化运维工作在推进调整中，逐步完善了运维体系的建设，规范化了运维体系的制度和流程，但由于信息化发展迅速，信息化运维保障能力仍需要进一步提升。

2.3 运维范围及内容

2.3.1 数据库系统运维

2.3.1.1 数据库系统运维范围

市应急管理局数据库系统软件运维的范围如下表所示：

序号	维护类型	维护范围	数量
1	数据库系统维护	SQL 数据库	2 套
2		Oracle 数据库	33 套
3		MY SQL 数据库	12 套

2.3.1.2 数据库系统软件运维内容

数据库系统运维内容包括：

- (1) 数据库系统软件的按需或定期关闭和启动。
- (2) 数据库运行状态监控（包括数据库软件文件系统空间状态、数据库数据文件系统空间状态、数据库归档文件系统空间状态、表空间使用状态、数据库连接数信息、数据库监听是否正常等），数据库日志检查分析。
- (3) 数据的安全管理及备份，进行本地、异地备份，并对备份数据进行管理。
- (4) 数据库参数配置检查、调整和优化。
- (5) 数据库安全加固等。
- (6) 数据故障处置：对数据库问题进行诊断、处置。
- (7) 技术文档管理服务：根据数据库系统运维需要，及时总结技术维护文档，并对技术文档进行动态更新、管理。

2.3.1.3 数据库系统软件运维方式

数据库系统软件维护方式包括驻场监控、现场巡检、现场支持、应急支持。当数据库系统软件配置改变或应用系统更新需要对数据库进行调试和测试时，需要安排高级工程师到现场，并在驻场工程师的协助下完成相关工作；当出现驻场工程师不能解决的技术问题或出现紧急情况时，需要指派工程师赶赴故障现场，解决故障。

2.3.2 数字证书服务

2.3.2.1 数字证书服务范围

市应急管理局数字证书运维服务的范围如下表所示：

序号	维护类型	维护范围
1	数字证书服务	CA 数字证书

2.3.2.2 数字证书运维服务内容

数字证书运维服务包括：

- (1) 数字证书统计管理。
- (2) 为新入职人员申请办理数字证书。
- (3) 为当用户证书即将过期时为用户提供数字证书更新。
- (4) 为锁定的用户的数字证书进行解锁。
- (5) 当用户的数字证书丢失或者损坏时为用户重新办理个人数字证书。
- (6) 为离职人员注销数字证书。

2.3.2.3 数字证书运维服务方式

数字证书运维：负责我局数字证书管理，为新入职办理证书、为即将过期的数字证书用户进行更新服务、为锁定的用户进行数字证书解锁，以及为丢失的数字证书进行补办、重签发等数字证书维护服务工作。

2.3.3 业务相关系统运维

2.3.3.1 运维范围

运维范围：我局现有业务系统分为内部管理类、行业领域类、专项业务类、重点工作类以及其他系统。包括：烟花爆竹、安全监管移动执法系统、安全生产专职安全员检查系统、专职安全员检查系统（离线版）、应急值守以及应急相关系统、地理信息系统、行政审批系统、特种作业考试系统、台账系统等。

2.3.3.2 运维内容

2.3.3.2.1 烟花爆竹、安全监管移动执法系统、安全生产专职安全员检查系统、专职安全员检查系统（离线版）、应急值守以及应急相关系统、地理信息系统、行政审批系统：

（1）系统巡检维护。对重要业务系统进行 7*24 可用性巡检，对其他系统每日检查系统的可用性、系统功能完整性。

（2）系统性能优化服务。优化系统功能、调整系统栏目，满足日常业务开展中对系统优化的需求；优化系统代码，提升系统运行效能；解决系统漏洞，对系统进行应用层面的安全加固。使系统更健壮，可用性更强。

（3）系统故障处置和恢复。及时处置系统故障，对系统故障事件进行快速响应，进行故障原因排查，恢复系统服务。

（4）系统优化、迁移调整。根据调整安排，提供系统迁移部署，硬件支撑资源调整、业务系统优化等服务。

（5）业务系统上、下线技术支持。配合软件建设单位准备应用系统上线、下线，准备业务应用系统上线所需基础技术环境以及业务应用系统下线所需技术支持工作。

（6）应用系统数据备份及恢复管理服务。制定合理的备份策略，定期备份生产系统的数据及应用系统程序文件，并检查备份执行情况是否正常；定期开展备份数据恢复测试工作，检查备份数据有效性。

（7）系统安全加固。对系统进行安全风险评估，对系统存在的信息安全隐患进行安全加固、策略调整和配置优化等。

（8）技术文档管理服务。根据业务系统运维需要，及时总结技术维护文档，并对技术文档进行动态更新、管理。

（9）应急演练工作。根据业务需要，定期开展办公和业务系统应急演练工作。

（10）其他技术服务。根据业务需要，对业务系统使用人进行培训服务等。

2.3.3.2.2 特种作业考试系统运维内容包括：

（1）系统巡检维护。对业务系统进行日常巡检，检查系统的可用性、系统功能完整性。

(2) 单机版软件维护。参照培训单位软硬件条件，向培训单位提供单机版安装及使用的技术指导服务。

(3) 系统故障处置和恢复。及时处置系统故障，对系统故障事件进行快速响应，进行故障原因排查，恢复系统服务。

(4) 远程协助。通过远程协助，对各类客观原因导致的突发问题进行处理。
(包括：理论考试考生机无法连接服务器、考官无法正常进行打分)

(5) 考试数据上传确认。考点理论考试结束完成数据上传后，对已上传考试数据进行核对，确认数据入库情况。

(6) 其他技术服务。根据业务需要，对业务系统使用人进行培训服务等。

2.3.3.2.3 台账系统运维内容包括：

(1) 系统巡检维护。对业务系统进行日常巡检，检查系统的可用性、系统功能完整性。

(2) 系统故障处置和恢复。及时处置系统故障，对系统故障事件进行快速响应，进行故障原因排查，恢复系统服务。

(3) 远程协助。通过远程协助，对各类客观原因导致的突发问题进行处理。

(4) 数据处理。对于业务系统界面上数据已进入审核、审批、办理、办结、归档等业务流程中无法直接修改数据的情况，根据用户要求进行更新、修改。

2.3.3.3 运维方式

业务系统运维方式包括驻场监控、现场巡检、现场支持、应急支持。当办公和业务系统更新、调试和测试时，需要指派高级工程师到现场，并在驻场工程师的协助下完成相关工作；当出现驻场工程师不能解决的技术问题或出现紧急情况时，需要安排二线工程师到现场解决故障。

特种作业考试运维方式包括远程监控、系统巡检、现场支持、应急支持。当出现技术支持工程师不能解答的技术问题或出现紧急情况时，需要安排技术工程师进行远程协助支持服务。提供每周 5*8 电话客服咨询服务。

台账系统运维方式包括远程监控、系统巡检、现场支持、应急支持。当出现技术支持工程师不能解答的技术问题或出现紧急情况时，需要安排技术工程师进行远程协助支持服务。提供每周 5*8 电话客服咨询服务。

2.3.4 应急管理门户运维及政务网站运维

2.3.4.1 运维范围

运维范围：系统管理门户运维及局政务网站运维

市应急管理局政务网站作为展示北京市应急管理局工作的整体形象的窗口，主要目的是充分发挥互联网的优势，做好政府信息公开、更好的为民服务，咨询服务、网上办事等主要功能。

2.3.4.2 运维内容

2.3.4.2.1 政务网站主要运维工作包括：

(1) 网站群信息发布及维护。根据相关的局内信息审批流程，对普通内网信息、区局信息、弹出信息、外网信息的内容进行更新。

(2) 政府信息公开内容管理系统维护。政府信息公开管理系统由首都之窗提供，负责登录该系统维护政务公开的信息。公开的信息由办公室提供，做到及时公开，对于由局办公室确认不公开的信息及时撤下。

(3) 数据维护。进行网站业务数据的管理、维护、归档工作，并根据相关规定，每日上传日志文件到首都之窗。处理因用户操作失误等特殊原因导致的需要进行数据干预的维护服务。

(4) 网站安全加固。对应急管理局外网网站进行安全加固，修补安全漏洞。

(5) 网站功能调整需求。北京市应急管理局网站的页面、版式、图片等内容的修改。

(6) 网站监控服务。对应急管理局网站进行每周 7*24 监控服务，检测网站的连通性以及是否存在不合法信息，并及时采取措施进行处理。

(7) 故障处置和系统恢复技术服务。处理网站突发故障、及时恢复网站访问服务。

2.3.4.2.2 应急管理门户运维工作包括：

(1) 系统巡检维护。对业务系统进行日常巡检，检查系统的可用性、系统功能完整性。

(2) 系统故障处置和恢复。及时处置系统故障，对系统故障事件进行快速响应，进行故障原因排查，恢复系统服务。

(3) 系统性能优化服务。优化系统功能、调整系统栏目，满足日常业务开展中对系统优化的需求；优化系统代码，提升系统运行效能；解决系统漏洞，对系统进行应用层面的安全加固。使系统更健壮，可用性更强。

(4) 信息专题制作。根据采购人要求，开展专题业务设计，新增业务专题页面等工作。

(5) 数据处理。对于业务系统界面上数据已进入审核、审批、办理、办结、归档等业务流程中无法直接修改数据的情况，根据用户要求进行更新、修改。

2.3.4.3 运维方式

政务网站运维方式包括驻场监控、现场巡检、现场支持、应急支持。当政务网站参数配置变更或应用系统更新需要对应用系统进行调试和测试时，需要指派中级工程师到现场，并在驻场工程师的协助下完成相关工作；当出现驻场工程师不能解决的技术问题或出现紧急情况时，需要安排二线工程师到现场解决故障。

2.3.5 应急管理数据对接技术支持

2.3.5.1 服务范围

开展应急管理数据对接技术支持工作

2.3.5.2 服务内容

(1) 开展日常巡检，保障应急管理共享交换平台的安全、稳定运行，按要求记录巡检时间和巡检内容，发现问题按程序及时报告，并提供必要的技术支持。

(2) 根据采购人要求，对各区应急局、委办局、局内业务系统、其他单位提供数据共享交换技术支持。

(3) 配合采购人，做好经信局要求的资源目录、数据开放建议清单梳理工作。

(4) 负责因经信局共享交换平台升级和共享交换平台上云而引起的功能升级和服务方式的变更工作。

(5) 如果针对某些数据需要开发接口，按要求做好本系统服务接口的开发、维护、更新和扩展工作。

2.3.5.3 服务方式

(1) 电话支持

工程师通过电话提供技术问题咨询和故障诊断。

日常维护服务时间为星期一到星期五的工作时间（上午九点至下午六点）。

技术支持人员手机提供每周 7*24 小时服务，公共假日无休。

(2)时刻在线的电子化支持

通过 Email 电子化方式报告的软件技术问题，提供每周 7*24 小时在线提交。

(3)远程在线诊断和故障排除

公司为客户提供远程支持服务。在得到客户授权的前提下，公司技术支持人员将通过广域网或电话网，直接登录到客户的路由器，服务器或数据库服务器，对其问题进行远程诊断。除非得到客户的书面授权，公司技术人员将不对客户的应用系统和数据进行修改，同时不对客户的数据进行下载。

(4)现场服务

公司将在下列两种情况下，为客户供现场技术服务：一、公司认为有必要到现场解决问题；二、客户要求提供现场支持，且公司认可的要求。

(5)重大活动现场支持服务

重大活动当中，根据报道活动的重要程度和维护复杂性，派出相应数量的有经验的工程师提供现场技术支持。

2.3.6 其它运维要求

2.3.6.1 咨询与培训服务

提供运维过程中的技术咨询、评估和培训等服务，服务内容主要包括：

(1) 运维技术咨询：根据工作需要信息化运维管理人员提供运维技术咨询工作。

(2) 技术方案评估：根据工作需要信息化运维工作涉及的技术方案提出意见，并进行技术评估、指导。

(3) 业务培训：根据业务需要对信息化人员进行技术和运维管理方面培训，要求每年开展 4 期。

(4) 运维管理现状分析及改进建议报告：根据业务现状进行安全运维管理分析，并提出合理性建议及改进报告。

3. 项目整体要求及投标人要求

3.1 对投标人要求

3.1.1 投标人中标后，应负责完成从项目计划到进驻服务和日常管理全部有关文件、资料、记录、报告等文档，汇集成册并定期交付项目单位。

3.1.2 投标人需具有相关工作经验，能针对本项目实际情况制定详实、行之有效的服务方案和计划。

3.1.3 投标人应具有本次招标中所涉及硬件设备的日常巡检和管理能力，并确保在设备发生故障能及时、准确的判断问题，进行设备的维修或协调厂商及时排除故障；投标人应具有本次招标中所涉及所有软件的安装、调试和日常维护能力，当软件系统出现故障或因其它原因导致软件系统重新部署时，要能保证在短时间内解决故障和搭建新环境。

★3.1.4 投标人必须保证本项目中的服务团队成员在进行现场服务时，能够服从相关管理规定，当运维公司相关规定与市应急管理局规定冲突时，以市应急管理局相关管理规定为准。（投标人须按照招标文件第七章-商务技术文件格式-11-1 服务承诺的格式提供，否则**投标无效**）

3.1.5 投标人应针对本项目建立服务质量保证、考核和评价量化体系，并在投标书中应答。

3.1.6 在签订合同之后，甲方保留对本技术规格说明书提出补充要求和修改的权力，乙方应承诺予以配合。

3.1.7 本技术规格说明书中所使用的标准和规范如与投标人所执行的标准发生矛盾时，按较高标准执行。

3.2 对拟投入团队人员要求

投标人应认真组织好服务团队，做好工作计划并提出长期服务以的措施计划和承诺。

★投标人须提供每周 5*8 驻场服务、每周 7*24 应急响应及技术支持服务，要提供不少于 5 人的常驻场服务人员（包括 1 名驻地服务经理、4 名驻地工程师）。（投标人须按照招标文件第七章-商务技术文件格式-11-1 服务承诺的格式提供，否则予以废标）

驻地服务经理需具有信息化相关专业高级及以上职称并具有不少于 5 个与本项目需求类似的经验。

注：1、上述所有人员需相关证明材料，包括但不限于提交投标文件截止时间前 6 个月内任意 1 个月的社保记录证明及合同证明文件作为证明文件。

投标人需拥有强大的技术支持力量，稳定专业化的技术支持服务队伍，完善的技术支持服务体系。投标人需针对本项目组建一支专业化的服务团队，需提供

团队成员的名单、工作简历、认证证书复印件。

驻地服务经理负责带领运维团队管理驻地运维工作，需根据 IT 技术发展态势和信息化运维服务体系标准化的需要，提出具有战略性、前瞻性的业务咨询报告和运维评估报告，协助采购人不断提高信息化运维工作的效率和质量。服务经理需具有运维项目管理经验 5 年以上。

★投标人如果中标，实际安排运维技术人员必须与投标文件中的人员一致。如有个别人员调整，须有充分原因，并形成书面材料，得到采购人认可后方可调整。调整补充的服务人员，必须保证后续人员具有同等的资质和能力。（投标人须按照招标文件第七章-商务技术文件格式-11-1 服务承诺的格式提供，否则予以废标）

3.3 对运维工作要求

3.3.1 整体要求

★（1）国家法定节假日、重要会议、活动以及突发安全事件期间等，按采购人要求做好每周 7*24 驻地值守工作。每周 7*24 小时驻地值守期间应按照采购人要求进行巡检、运维维护和技术保障工作。（投标人须按照招标文件第七章-商务技术文件格式-11-1 服务承诺的格式提供，否则**投标无效**）

（2）工作汇报机制：

根据采购人要求，驻场人员需按时向市应急管理局提交日常巡检及维护记录、服务周报、服务月报、服务年报以及定期工作总结。

（3）服务方式要求：

现场值守服务、电话技术支持服务、电子邮件技术支持服务、远程管理服务、应急响应服务、技术培训服务并建立应急响应机制。

（4）应急服务：

中标人应建立应急响应机制，并严格按照要求实施，每季度配合信息化安全服务商实施一次“信息安全事件应急演练”及每年参加一次由指挥保障中心组织的“信息安全事件应急演练”。

（5）中标人应基于 ITIL 和 ITSS 的 IT 运维服务理念并结合市应急管理局的实际情况建立 IT 运维服务管理体系，设计服务流程，制定服务规范，并及时对服务进程进行记录。

(6) 在《项本项目实施团队主要人员简历表》中需清晰说明相应服务人员在该项目中的职责及所具备的响应技术技能及工作经验。

(7) 中标人需依据与采购人签订的保密协议，由中标人保证对于其员工所接触过的采购人信息数据内容，将采取合理、必要的步骤（包括但不限于与员工签订保密协议），来要求中标人及其员工不透露或者以其它方式提供给第三方。

(8) 中标人要在进场一个月内完成信息化维护的交接工作。

3.3.2 运维质量指标及验收标准

3.3.2.1 各类运维服务的质量指标通常包括但不限于：

(1) IT 基础设施和应用系统运维服务。

(2) 监控类服务：异常报告及时率、异常漏报率。

(3) 日常维护类服务：维护作业计划的及时完成率、故障隐患发现率、异常主动发现率、故障服务请求及时满足率、业务服务请求及时满足率、问题解决率等。

(4) 维修保障类服务：服务响应及时率、到达现场及时率、故障修复及时率。

(5) 网络接入服务：平均响应时间、问题解决比率等。

(6) 内容信息服务：响应及时率、完成率等。

(7) 综合管理服务：平均响应时间、问题解决比率等。

(8) 通过集中运维服务体系的建设和，实现以用户为中心的、安全稳固的、质量成本最优的每周 5*8 小时 IT 运维服务，从而保障应急业务运作的安全稳定。

3.3.2.2 要求：

(1) IT 系统安全、稳定：

●重大安全事故次数为 0（其中重大安全事故指因人为操作失误或破坏等原因，导致网络与信息系统出现业务中断、系统破坏、数据破坏、信息失窃或泄密等故障，从而造成不利政治影响和经济损失等。）

●面向预算单位的财政核心 IT 系统稳定运行率 \geq 99.9%

●重大 IT 运行事故次数为 0（其中重大 IT 运行事故指大面积网络瘫痪、技术保障失误、业务系统运行较长时间中断等。）

(2) 优质服务：

●IT 服务入口统一，规范标准

- 用户对系统的满意度 $\geq 95\%$
- IT 需求客户满意度 $\geq 95\%$
- IT 服务投诉趋向于 0

3.3.3 本项目基本服务级别（SLA）要求

指标	目标值（标杆值）
IT 系统稳定运行率（%）	$\geq 96\%$
其中 OA、局网站系统、应急值守系统	$\geq 96\%$
应急移动指挥通信系统	$\geq 96\%$
其他辅助系统	$\geq 93\%$
重大 IT 运行事故（次）	0
重大 IT 安全事件（次）	0
计算机终端可用性	$\geq 95\%$
IT 服务客户满意度	$\geq 95\%$
IT 服务投诉（个）	$\leq 5\%$

3.3.4 运维工具要求

目前在用的运维管理工具主要有电子政务运维支撑平台。电子政务运维支撑平台部署与使用、服务台建设工作推进、流程管理优化、知识库系统建立、应急预案管理完善等，进一步健全了采购人信息化运维体系。

投标人本次投标应该负责投放以上类似运维服务支撑系统（使用成本包含在投标总价中，不另行计费）。

3.4 运维连续性要求

中标单位要确保招标工作开展前与中标后运维工作的连续性，确保运维服务内容和质量不间断。

3.5 对相关文档的要求

（1）中标单位应向采购人提供运维过程中的各种文档资料，以便采购人能掌握相关配置及设备、应用运行状况。

（2）中标单位应以周为单位向采购人提供运维周报，内容应包含运维范围内的所有工作情况等。

（3）中标单位应以月、年为单位向用户提供运维月报和年报，内容包含运维范围内的所有工作情况、运维过程中重大事件、运维流程及网络和其它环境的改进建议等。

3.6 技术支持与服务

3.6.1 技术后援支持

为保证机房设备及应用每周 7*24 小时稳定运行，投标人需为运维工作提供专业的技术团队。一旦出现故障，投标人需按照故障响应和处理时间标准开展应急保障工作。

故障响应时间：根据市应急管理局运维分级管理，工作时间内重要类系统响应时间标准为 10 分钟、一般类系统响应时间标准为 20 分钟；由于非工作时间内，人员需从局外到达，因此非工作时间相应标准如下：重要类系统响应时间标准为 2 小时、一般类系统响应时间标准为 3 小时。

故障处理时间：根据运维分级管理，工作时间内重要类系统故障处理时间标准为 1.5 小时、一般类系统故障处理时间标准为 3 小时；由于非工作时间内，人员需从局外到达，或发生运维事件转移时，第三方厂商需临时安排人员进行处置，因此非工作时间相应标准如下：重要类系统故障处理时间标准为 3 小时、一般类系统故障处理时间标准为 4 小时（注：故障处理时间不包含响应时间）。

3.7 知识产权要求

投标人应能保证所提供的所有产品和服务涉及到的知识产权是合法取得，并享有完整的知识产权，不会因为投标人或采购人投入本项目的使用而被责令停止使用、追偿或要求赔偿损失，如出现此情况，一切经济和法律責任均由投标人承担。除投标服务本身归属于投标人或制造商所拥有的知识产权外，因本项目建设期间所产生的所有的知识产权均归采购人所有。

附件 2

服务质量考核标准

一、考核原则

本着以SLA和相关管理规范为考核依据，以运维的持续改进为最终目标的原则，对运维过程，运维结果进行考核。

二、考核方式

通过服务厂商自评，服务交付物质量评估和甲方评估三方面评估相结合的方法开展考核，服务厂商需对服务工作进行专题汇报。

三、考核内容与标准

指标	目标值（标杆值）
IT 系统稳定运行率（%）	≥96%
其中 OA、局网站系统、应急值守系统	≥96%
应急移动指挥通信系统	≥96%
其他辅助系统	≥93%
重大 IT 运行事故（次）	0
重大 IT 安全事件（次）	0
计算机终端可用性	≥95%
IT 服务客户满意度	≥95%
IT 服务投诉（个）	≤5%

附件3

安全保密协议

甲方：北京市应急指挥保障中心

乙方：太极计算机股份有限公司

住所：北京市朝阳区容达路7号

法定代表人：肖益

鉴于，甲、乙双方于2022年__月__日就运维过程中已经或将要知悉对方的相关保密信息，为了保护上述合作中涉及的保密信息，明确双方的权利义务，甲、乙双方在平等自愿、协调一致的基础上达成一下协议：

第一条 安全要求

一、乙方必须遵守甲方的各项规章制度，严格按照工作规范组织进行运维工作，制定切实可行的措施保障人员安全，设备安全，生产安全。

二、乙方必须制定合理的措施对运维人员进行管理和思想教育，加强保密意识，安全生产意识。

第二条 保密信息范围

本协议称的“保密信息”是指，双方在订立和履行合同过程中获得的下列信息，但不包括一方通过公众渠道可以获得的信息或经对方书面同意允许向第三方透露的信息：

一、工作秘密：一切与政府工作相关的信息资料或其他性质的资料，包括但不限于：政府业务数据、人员机构信息、财务资料等。

二、技术秘密：指甲方的计算机信息系统、网络架构、信息安全体系结构、软件、数据库系统、文档及技术指标等。

三、其他保密信息：包括但不限于运维过程中获取的有关数据、流程、分析成果；甲方的内部管理资料、财务资料；甲方其他项目的信息及有关政府行政机关规划、调整等尚未公开的资料。

上述保密信息的表现形式不限，无论是书面的、口头的、图形的或其他任何形式的信息。

第三条 安全保密期限

本协议约定的保密责任期为本合同服务期内。

第四条 保密义务人

本协议项下保密义务人为双方单位及双方涉密信息的员工。

第五条 保密义务

一、甲、乙双方保证对所获悉的对方保密信息按照下列规定进行保密，并在缺少相关保密条款约定时，应至少采取适用于对自己的保密信息同样的保护措施和审慎程度进行保密：

1. 仅将本协议项下保密信息使用于与运维工作有关的用途。
2. 除直接参与运维工作的人员之外，不得将保密信息透露给其他无关人员和任何第三方。
3. 不能将对方保密信息的全部或部分进行发布、传播、复制或仿造。
4. 双方均应告知并以适当的方式要求其直接参与运维工作的人员，按照本协议规定保守保密信息。如一方工作人员违反本协议规定，泄露对方保密信息的，该方应承担违约责任。
5. 任何一方不能利用获悉信息为自己或其他方开发信息、技术和产品、或与对方的产品进行竞争。

二、乙方保密义务

1. 未经对方书面许可并采取加密措施，不得擅自将载有保密信息的任何文档、图纸、资料、磁盘、胶片等介质，带离对方工作场所。
2. 对于用户数据和服务结果数据的保管、访问，乙方无关人员不能访问；必须访问的人员，乙方要进行严格的访问控制；管理用户数据的人员应由乙方严格筛选。
3. 对于甲方提供给乙方使用的任何资源，如网络、NOTES等，乙方都只能将其用于工作，而不能用于其他目的，特别是从事侵害甲方利益的活动。

第六条 保密信息的交回

一、运维工作终止后，双方应按照对方的要求对相关保密信息做相应处理，比如销毁或其他处理方式。

二、当一方以书面形式要求交回保密信息时，接受通知的一方应当立即交回所有的书面或其他有形的保密信息以及所有的描述和概括保密信息的文件。

三、未经对方书面许可，任何一方不得丢弃和自行处理保密信息。

第七条、违约责任

任何一方未履行本协议项下的任一条款均视为违约，违约方应按照守约方要求采取的有效的补偿措施，以防止泄密范围继续扩大，同时还应向守约方支付违约金为合同总金额的5%。

第八条、争议的解决

因履行本合同而发生的或与本合同有关的一切争议，双方应协商解决，协调不成的，双方同意提交北京仲裁委员会进行仲裁。

第九条、其他

本协议未尽事宜，甲、乙双方另行签订补充协议，补充协议与本协议具有同等法律效力。

甲方：北京市应急指挥保障中心

(签字)



任金周

2022年7月12日

乙方：太极计算机股份有限公司

(签字)



黄佳

2022年7月12日