附件：

一、项目概述

项目名称	数据运营服务项目
项目内容	数据运营服务。具体要求详见招标需求。
预算金额	本项目预算金额 800 万元。超过预算的投标按无效投标处理。

二、项目招标需求

1　项目概述

1.1　背景和现状

1.1.1 背景

为落实市政府《上海市公共数据和一网通办管理办法》（沪府令 9 号）及市委办公厅、市政府办公厅《上海市加快推进数据治理促进公共数据应用实施方案》（沪委办〔2019〕8 号）、《松江区公共数据安全管理办法》（沪松府〔2021〕241 号）、《松江区公共数据管理办法》（沪松府〔2021〕242 号）等相关文件要求，更好地应对我区公共数据全生命周期管理工作中遇到的挑战，构建公共数据服务的生态系统，促进区域核心数据枢纽的建设，松江区政务服务中心自 2023 年起即启动了数据运营服务试点项目，并在总结试点经验基础上于 2024 年 8 月正式启动数据运营服务工作。

近年来，数据运营服务工作取得了一定成效，初步构建了区域级数据资源底座，支撑公共数据的全生命周期管理；完成了区领导交办的数字化六大会战之一的“数据上链”工作会战；按照“应编尽编”“应归尽归”的原则逐步覆盖各类公共服务数据；依托区大数据资源平台对接市级数据中台，连通了国家、市、区三级交换通道，推动各领域公共数据有效整合；探索专题库建设，有效支撑政务服务“一网通办”、城市运行“一网统管”、基层减负、经济运行等应用场景。

数据运营项目由松江区政务服务中心作为业主单位委托数据服务运营商负责整体项目实施，第三方监管机构负责对运营商的服务过程与产出执行监管。区政务服务中心是数据运营项目的总体负责方，整体负责数据运营项目的业务执行，制定并完善数据运营服务规范，分解项目周期工作目标，发起服务任务并对服务任务进行验收；数据服务运营商是数据运营项目的承接方，承接并组织服务和技

术力量执行区政务服务中心的数据运营服务，确保运营服务按时、按质、按量完成，并配合区政务服务中心及第三方监管机构的监督与考核工作；第三方监管机构是区政务服务中心委托的独立服务监督机构，负责对数据服务运营商在数据运营过程中的所有活动，包括由此产生的过程性或者结果性交付成果执行客观监督和评估评价，对监管过程中发现的问题提出整改建议，并追踪整改结果，另外协助完善服务目录以及相应的服务规范。

1.1.2 大数据资源平台现状

通过大数据资源平台（一期）和（二期在建）项目的建设，大数据资源平台基于数据基础底座能力，提供数据归集、数据资产管理、数据开发治理、数据共享等数据服务能力。组成部分包括：数据基础支撑子系统、数据协同管理子平台、数据赋能子平台、运营服务管理子平台、数据安全保障子平台以及政务大数据专区。

大数据资源平台在业务层面，当前支撑业务主要包括：“一网通办”、“一网统管”、“基层减负”、“经济运行”、各部门专题库业务应用等。

随着城市数字化转型工作的持续推进，为支撑经济数字化、生活数字化、治理数字化及满足国家相关法规要求，构建区域级核心数据枢纽和城市公共数字底座，大数据资源平台需要进一步丰富数据治理功能，增强数据中台共性能力，提升数据共享的时效性和便捷性，强化数据全过程监管和数据安全保障能力。

1.2 总体目标

根据区委、区政府全面推进城市数字化转型的要求，持续加强公共数据的归集、整合、应用、共享等工作，构建区域级核心数据枢纽和城市公共数字底座，建立建设运营一体化服务体系，推动数据资源要素化转型，支撑治理数字化、经济数字化和生活数字化，满足业务从面向部门业务人员需求到面向公众和企业需求的转变，强化公共数据安全管理，提高数字化治理水平，支撑实现城市整体数字化转型和国际数字之都建设。

具体目标包括：

（一）提升数据一体化运营服务管理，依托大数据资源平台数据统一集中管理能力，加强数据共享时效性、便捷性，探索构建数据授权运营的管理和监管能

力，满足分级分层分域管理的需要，形成与之匹配的数据安全运营能力，实现公共数据的全流程全链路安全监管，尤其是核心、重点数据，提高平台运行和安全保障服务。

（二）做好公共数据治理、分析应用等相关工作。**支撑公共数据上链工作，**完成职责目录、系统目录和数据目录编制的质量校核，配合各单位完成两两关联。在数据分级分类、元数据管理的基础上，完成数据信息系统盘点、数据标准、指标上链等工作。**配合开展公共数据“应编尽编”、“应归尽归”，**加强“数源目录”管理，落实“一数一源一标准”，推进应用场景备案管理，促进基于应用场景的便捷共享。**加强数据质量检查，提升数据质量，**完成全量入湖数据的质量检核，尤其是自然人、法人、空间地理数据等核心数据、重要数据的入库质量核验。探索建立区级数据质量检查规则库，落实数据资源全生命周期的质量检查和反馈，优化异议核实闭环管理机制，持续提高数据质量。**深化自然人、法人、空间地理综合库优化，**完成专题库建设和优化迭代的目标，进一步提升三大综合库以及专题库的应用成效，探索社会数据与公共数据融合治理。**支撑基层数据需求，**保障国家数据资源共享、直达及数据回流通道稳定可用，实现基层治理数据的统一汇聚和共享共用。**深化公共数据分析与应用，**围绕区委、区政府、区领导关心的内容开展专题分析；支撑公共数据授权运营社会化开发利用，以及其他各类区委区府重点工作的数据共享场景。

（三）更好地保障平台数据安全，通过多种专业安全服务方式，进一步提升区政务服务中心对非授权访问、敏感数据泄露及异常脚本爬取等行为的监测、检查、审计及防范能力，保障数据采集、数据使用、数据交换、数据共享、数据销毁等各环节的数据安全，强化安全管理落实，提升整体安全保障能力。

1.3 数据运营服务目录

数据运营服务目录及其单价的最高限价参见下表：

服务类型	序号	服务目录	单价（元）	计量说明	难度系数
基础服务类	1	数据采集接入	120 元/万条 90 元/幅	工作范围内，新增采集接入的工作项计量：1、涉及结构化数据采集接入按数据条数计量，单价为 120 元/万条； 2、涉及影像数据采集按幅计量，单价为 90 元/幅。	
	2	数据抽取服务	564 元/张 47 元/万坐标点 200000 元/年	工作范围内：1、对批数据的数据抽取的按数据表数计量，以张为计价单位，单价为 564 元/张； 2、对新增实时数据、流式数据、空间数据的抽取按坐标点计量，以万坐标点为计价单位，单价为 47 元/万坐标点； 3、对新增以数据高铁形式提供服务，按数据表数计量，200 张数据库表以内（包含 200 张），每年付费 20 万元，超出 200 张部分工作量按 1100 元/张数据库表计。	对批数据的抽取：1）费用以原有数据项处理费用为基数，按表格复杂度，取难度系数 N（N=0.5~1）确定单价，即 564*N 元； 2）0-1000 个计价单元（含 1000 个）按原始单价计算；1000-10000 个计价单元（包含 10000 个）按原始单价*80%；1 万个以上按原始单价*60%。 对新增实时数据、流式数据、空间数据的抽取：0-1000 个计价单元（含 1000 个）按原始单价计算；1000-10000 个计价单元（包含 10000 个）按原始单价*80%；1 万个以上按原始单价*60%。

	3	数据标签	300 元/个标签	工作范围内，对新增数据标签（包含数据字段标签、目录标签）的个数计量。	
	4	时空数据转换与处理	200 元/万点	工作范围内，对坐标转换、格式转换的时空数据加工按万点计量，单价为 200 元/万点。	
	5	对于历史数据的归档及销毁	550 元/张	工作范围内，对周期内销毁、归档的数据表数进行计量。	
	6	数据质量检查	90 元/个 60 元/张 5 元/万个 8000 元/万坐标点（内业）或 150000 元/万坐标点（外业）	工作范围内：1、对数据资产目录的质量检查，按照检查的目录个数计量，单价为 90 元/个； 2、对结构化数据表的质量检查，按照检查的数据表数计量，单价为 60 元/张； 3、对文件数据的质量检查，按照检查的数据文件个数计量，单价为 5 元/万个； 4、对空间地理数据的核实，分内业和外业质量检查，按照涉及的坐标点数计量，对内业核实，单价为 8000 元/万坐标点，对外业核实，单价为 150000 元/万坐标点。 5、若为新设计的数据质量检查规则，可附加设计费用（按规则个数计量，单价为 50 元/个）；基于新设计的数据质量规则检查出的问题数据进行修正处理，可附加修正费用（按修正处理的数据条数计量，单价为 50 元/条）。	针对结构化数据表的质量检查工作，结合工作复杂度，取难度系数 N（N=1～1.5），其中数据质量检查规则小于 5 种的，N=l；每增加一种规则难度系数增加 0.1，N 最高不超过 1.5。
	7	数据共享/开放/授权订阅服务	1000 元/组	工作范围内，数据共享、开放、社会化应用工作中所提供的一组完整服务接口数计量。	

	8	数据统计分析及报表服务	4000-5000 元/次	工作范围内，按需对各类需求进行数据统计分析，按涉及的统计次数计量。仅完成数据统计分析 4000 元/次，完成数据统计分析及报表服务 5000 元/次，同时按照工作难度，设置难度系数 N。	对数据统计分析服务按工作难度，取难度系数 N（N=1~3），对于仅涉及单领域数据的，N=1；每增加一个领域，N 增加 1；N 最高不超过 3。在单个专项任务中对于融合加工的程序个数进行控制，每个库中的数据融合加工程序个数最多记录 20 个（包括 20）；低于 20 个融合加工程序数，则按实结算。同一张统计报表的数据问题更正不再另外收费。开展报表数据更新的，数据自动更新不计费，数据手动更新每次乘以系数 M，（M=0.1~0.3）。统计报表未上线或未有有效调用量的不计费。
	9	数据挖掘建模	92000 元/个	工作范围内，按涉及的数据挖掘模型个数计量。	根据数据融合挖掘建模的难度，设置难度系数 N（N=1~3）。基于数学、统计学及相关学科及业务领域理论、规范及方法建立数据分析模型，应用于业务问题发现、数据规律研究和风险预警提示等工作，N=1；基于数据挖掘、人工智能等算法开展的数据分析建模服务，应用于综合性强、业务领域广、难度较高的数据分析场景，N=2～3。
	10	数据分类分级检查	1500 元/张表	工作范围内，按数据分级分类的检查数据表数计量。	

	11	数据加密、脱敏等控制	5 元/万条	工作范围内，按数据加密、脱敏等控制数据条数计量。	
	12	应用安全监测分析及威胁情报服务	280 元/台*年	工作范围内，按运营项目合同年内开展应用监测分析及威胁情报服务的台数计量。	
	13	应用安全检查评估服务	165 元/台*次	工作范围内，按运营项目合同年内开展检查评估的台数和次数计量。	
	14	应用安全基础管理服务	120 元/台*年	工作范围内，对于应用设备的管理的台数计量。	
	15	作业调度	45 元/个	工作范围内，按照新增作业调度的任务个数计量。	
应用服务类	16	数据开放运营接入服务	750000 元/年	工作范围内，基于数据开放和数据授权运营服务对接的各类需求对接、梳理、需求分析，相关工作整体年度计费。	
	17	公共数据上链服务	50000 元/个	工作范围内，按照公共数据上链服务单位的个数计量。 使用该目录时，不可使用数据质量检查、数据质量规则设计及异常处置服务目录。	根据上链单位的工作规模大小，设置难度系数 N（N=0.5-1）。
	18	主（专）题数据库建设	250000 元/个	工作范围内，按建设主（专）题库的个数计量。按工作内容，设置难度系数 N。使用该目录时，不可使用数据采集接入、数据抽取服务、数据标签、时空数据转换与处理、数据质量检查、数据质量规则设计及异常处置服务目录、数据共享/开放/授权订阅服务、数据统计分析及报表服务、数据挖掘建模、对于历史数据的归档及销毁服务目录。	按照业务目标的复杂度、涉及领域的数量等因素，取难度系数 N（N=1、2、3)。

	19	数据可视化展现工作	92500 元/个主题域	工作范围内，按大屏展现的主题域个数或中屏（小屏）模块数计量。 同时对大中小屏设置难度系数 N。	可视化大屏服务，以主题域个数为计费单元，确定计费基数：92500 元/主题域；中屏及小屏（含 H5 页面），同等情况下工作量分别按难度系数 N（N=0.1~0.2）折算。
	20	公共数据社会化应用服务	100000 元/个	工作范围内，按照公共数据社会化应用的场景个数计量。按工作的复杂度，设置难度系数 N。使用该目录时，不可使用数据采集接入服务、统计服务、数据分类分级检查目录。	按工作的复杂度，取难度系数 N（N=0.5～2.5）确定单价，其中难度系数评估涉及的数据级别相关联。 难度系数 0.5 按照数据分级标准，场景规划所使用数据分级等级小于等于 2 级，且有可参考的已评估成熟案例。 难度系数 1 按照数据分级标准，场景规划所使用数据分级等级为 1 级，且没有可参考的已评估成熟案例。 难度系数 2 按照数据分级标准，场景规划所使用数据分级等级为 2 级，且没有可参考的已评估成熟案例。 难度系数 2.5 按照数据分级标准，场景规划所使用数据分级等级为 2 级的案例（如涉及个人敏感信息或者由于场景的重要性、场景特殊性及紧急性案例）。
	21	数据共享/开放/授权运营服务	1000000 元/年	工作范围内，在数据共享开放和数据授权运营服务过程中，依托数据异议核实等工作机制进行的数据质量问题的跟踪、解答和处理，相关工作整体年度计费。	

	22	安全基线配置管理服务	250000 元/个子系统	此项目录，适用范围仅为大数据资源平台以及一体化综合运营平台。工作范围内，按系统个数计量。 按系统复杂度，设置难度系数 N。同时，系统数量达 20 个及以上，在总费用基础上乘以调整系数 0.8；系统数量达 50 个及以上，在总费用基础上乘以调整系数 0.6。	按系统复杂度，乘以难度系数 N (N=l～3), 系统主机≤50 台，N=1；系统主机≥150 台，N=3；其他 N 为主机数量除以 50 的值做为难度系数获得。
	23	综合运营保障服务	120000 元/个系统（数据服务）/年	工作范围内，按纳入运营监控服务的系统个数或数据服务个数计量。按工作复杂度，设置难度系数 N。	按工作复杂度，乘以难度系数 N (N=l～3)。以系统作为对象的，系统主机≤50 台，N=1，每增加 50 台主机数，难度系数增加 1，系统主机≥150 台，N=3。以数据服务作为对象的，当数据服务实际并发量≤500tps 时，N=1，每增加 500tps 难度系数增加 1，实际并发量≥1500tps，N=3。 若当年系统发生重保服务，难度系统（N）在原有基础上增加 0.25。全年由于重保服务发生费用 50 万元封顶。
	24	数据安全风险评估、安全审核服务	22 元/万条	此项目录，适用范围仅为大数据资源平台以及一体化综合运营平台。 工作范围内，针对运营项目合同年内开展数据安全评估、审核的工作，按数据条数计量。	
	25	应用安全渗透测试服务	30000 元/次	工作范围内，针对运营项目合同年内开展渗透测试的定期检查，按开展检查评估的台数和次数计量，按单个系统计费，单价 3 万/次(20 个页面以内)计算。按渗透测试的页面数量，设置难度系数 N。	针对运营项目合同年内开展渗透测试的定期检查，按渗透测试的页面数量，取难度系数 N(N=1～3)。

	26	安全审计服务	30000 元/个系统	此项目录，适用范围仅为大数据资源平台以及一体化综合运营平台。 工作范围内，按对开展安全审计的信息系统个数计量。 按系统复杂度，设置难度系数 N。同时，系统数量达 20 个及以上，在总费用基础上乘以系数 0.8；监控系统数量达 50 个及以上，在总费用基础上乘以系数 0.6。	按系统复杂度，乘以难度系数 N（N=1~3），系统主机≥50 台，N=1；系统主机≥150 台，N=3；其他 N 为主机数量除以 50 的值做为难度系数获得。
	27	系统功能符合性评估和测评服务	20000 元/次	此项目录，适用范围仅为大数据资源平台以及一体化综合运营平台。工作范围内，对子系统进行软件功能测试、等保测评、密码测评、安全评估、数据安全风险评估次数，分别进行计量。 按照评估和测评服务的复杂性，设置难度系数 N。同时，监控系统数量达 20 个及以上，在总费用基础上乘以调整系数 0.8；监控系统数量达 50 个及以上，在总费用基础上乘以调整系数 0.6。	按照评估和测评服务的复杂性，乘以难度系数 N（N=1~3），系统主机≥50 台，N=1；系统主机≥150 台，N=3；其他 N 为主机数量除以 50 的值做为难度系数获得。

1.4 招标范围

投标人中标后承担为期一年的数据运营服务。具体包括以下范围：

（一）基础类服务

以数据的生命周期管理为基础，针对数据管理服务工序类服务，主要以数据和系统为对象进行服务计量。数据采集接入、数据抽取服务、数据标签、时空数据转换与处理、对于历史数据的归档及销毁、数据质量检查、数据共享/开放/授权订阅服务、数据统计分析及报表服务、数据挖掘建模、数据分类分级检查、数据加密、脱敏等控制、应用安全监测分析及威胁情报服务、应用安全检查评估服务、应用安全基础管理服务、作业调度。

（二）应用类服务

以重点数据工作为基础，一揽子承接需求对接、数据治理、质量检查、数据安全等工作，以整体投入进行服务计量。包括数据开放运营接入服务、公共数据上链服务、主（专）题数据库建设、数据可视化展现工作、公共数据社会化应用服务、数据共享/开放/授权运营服务、安全基线配置管理服务、综合运营保障服务、数据安全风险评估、安全审核服务、应用安全渗透测试服务、安全审计服务、系统功能符合性评估和测评服务。

1.5 服务期限和地点

服务期限：自合同签订后 12 个月

服务地点：松江区政务服务中心

2 项目技术需求

2.1 各服务项的具体要求

以下为各服务目录及交付物的具体要求，服务规范将根据项目实际情况定期进行更新，倘若存在冲突，则参照最新版本的服务规范予以实施。

2.1.1 基础服务类

2.1.1.1 数据采集接入

- **服务要求**

实施支撑中心业务需求的数据接入工作，并保障接入数据的实时性、有效性

和完整性。数据采集接入工作包括数据编目和数据接入两部分，数据编目首先要对需要采集接入的数据进行业务理解和数据理解，然后再按照编目规范标准在编目系统中进行编目；数据接入工作包括协议适配、接口开发、数据清洗、资源挂载、数据对账以及质量检核等，将数据通过 ETL 汇集到中心数据湖。

- **交付成果和标准**

输出物	输出物标准
数据资源目录	目录符合编目规范、数据采集标准、符合系统的数据质量检查规则。
数据资源编目变更记录	附相关记录。
采集数据日志	日志包含但不限于以下字段：库表位置、运行状态、实际数量等。

2.1.1.2 数据抽取服务

- **服务要求**

对新增数据资源的抽取服务，按照编目规范标准在编目系统中完成编目。按照应用需求进行集中统一服务，根据抽取数据对象的不同数据属性、不同业务领域、不同授权场景从源数据库抽取数据到指定目标库中，并完成数据清洗加工、数据质量前置基础性评估和处理工作；对有实时数据共享需求的任务，依托区大数据资源平台提供源系统相关数据的编目、实时接入工作，并根据共享的具体场景提供数据接入的实时监控。实施日常数据抽取任务维护，保障各信息系统的数据及时准确地汇聚，对问题抽取任务进行处置调整。

- **交付成果和标准**

输出物	输出物标准
抽取流程设计	符合数据运营工作实际需求，符合数据抽取相关规范和数据对账方案。
抽取流程变更记录	附相关记录。
优化分析报告（如有）	符合优化分析报告模板。
抽取数据日志	日志包含但不限于以下信息：库表位置、运行状态、和数据对账记录等。
月总结报告	月汇总报告内容至少包含下述绩效指标： 及时率=要求的时间内抽取次数/计划抽取次数、 准确率=入湖数据量/源头数据量

2.1.1.3 数据标签

- **服务要求**

根据数据内容分类分级标准、数据标识的需求场景、需要标识的数据业务分类、需要标识的数据安全分类、需标注的数据范围，实施对结构化数据、文本数据、音频数据、视频数据、流媒体等格式进行内容释义，对数据内容进行分类分级管理，以挖掘数据资产价值，提升数据资产复用性和数据管理精细化程度。

- **交付成果和标准**

输出物	输出物标准
数据标签规则	规则符合数据分级以及相关重点工作的要求。
数据标签日志/记录	日志包含但不限于以下字段，含标签内容、数量等。

2.1.1.4 时空数据转换与处理

- **服务要求**

根据时空数据的坐标转换、格式转换等需求，对时空数据的坐标、格式进行转换服务工作，为业务需求提供专业化的时空数据需求。

- **交付成果和标准**

输出物	输出物标准
时空数据转换与处理流程设计	符合数据运营工作实际需求,符合数据转换处理相关规范和数据对账方案。
时空数据转换与处理工作记录	附相关记录材料。
优化分析报告（如有）	符合优化分析报告模板，附相关记录材料。
时空数据转换与处理数据日志	日志包含但不限于以下信息：库表位置、运行状态、和数据对账记录等。
总结报告	总结报告应体现服务需求来源、需求完成情况、服务工作总结等内容。

2.1.1.5 对于历史数据的归档及销毁

- **服务要求**

针对数据运营服务的要求，开展日常数据归档、恢复、销毁等工作的服务。该服务需要做到针对不同数据使用场景下的各类数据按需、配置化、全覆盖的服务要求，同时需要支撑该服务的可逆性和可视化需求。

- **交付成果和标准**

输出物	输出物标准
归档/销毁方案	符合归档或者销毁的运营需求。
归档/销毁执行日志	包含库表位置、运行状态、实际数量等。
数据归档/销毁服务报	报告期内各业务系统使用数据归档情况、数据销毁情

告	况。

2.1.1.6 数据质量检查

- **服务要求**

结合业务需求或数据质量管理要求，设计新的数据质量规则，并完成质量规则对应数据表的质量检查工作，并对检查出的非数据管理过程中的技术因素引起的问题数据，进行修正处理，不断提升数据质量。

对数据资产目录的质量检查工作，包括编目的内容、字段信息的完整性、有效性等质量检查，并就问题编目进行沟通对接、调整修改；对采集的数据、融合治理后的结构化数据，结合已有数据质量规则进行数据质量检查工作；对共享、开放的文件数据开展检查工作，包括文件可下载性检查、文件内容的查看、文件与编目的关联性检查等，并处置异常数据文件；对空间地理类新增数据开展核实工作，包括地名地址信息、门牌信息、坐标信息等真实有效性核实确认，并在综合库、基础库、专题库中进行更新。

- **交付成果和标准**

输出物	**输出物标准**
质量规则设计及变更记录	符合数据运营工作实际需求，符合数据标准和公共数据模型设计规范。
数据质量检查日志	日志包括但不限于以下字段：库表名称、检查规则、实际检测数量、异常数据量等。
异常数据清单	异常数据清单，包含数据信息和判定异常原因，附相关记录材料。
数据质量报告	符合数据质量报告模板。
综合数据质量评价报告	符合综合质量检查评价报告模板，附相关记录材料。
异常数据修复方案（如有）	符合方案模板要求，附相关记录材料。
异常数据处置及修复测试报告（如有）	测试报告，二次验证通过后的记录材料。
外业核查记录（如有）	符合外业核查要求的原始记录和确认记录

2.1.1.7 数据共享/开放/授权订阅服务

- **服务要求**

在数据共享、开放、社会化应用工作中所提供的一组完整服务接口的服务数，原则上服务主要针对数据集对外提供一组多种类型的接口服务，并根据不同用户

角色的需求开展满足不同 SLA 的数据共享需求；提供的一组多种类型的接口服务包括但不限于样例数据接口、Json、Xml；同时满足数据安全的工作要求。

- **交付成果和标准**

输出物	输出物标准
需求文档	接口清单、委办自定义入参出参，在文档模板里明确使用场景 文件订阅方式，需包含具体文件类型及规格说明、共享方式等信息，如果约定文件命名规则，必须在本文档中表述清楚；
数据模型设计（如有）	API 接口设计或库表落地数据模型设计，需包含库表说明，业务逻辑，推送方案； 文件订阅方式可以无数据模型设计文档；
接口开发代码	提供接口开发代码清单或截图
接口测试报告(含 API 接口列表)	测试报告需包括参数名称、类型、取值范围，附相关记录材料；API 接口符合业务需求和性能要求 文件订阅方式不涉及到接口，可以无测试报告
作业上线记录	需包含上线时间、共享频率、共享内容等记录； 文件订阅方式不涉及上线，可以无作业上线记录
共享记录	提供需求方调用或验证记录、数据库表落地验证记录、文件交付记录或 FTP 落地记录等，可截屏记录

2.1.1.8 数据统计分析及报表服务

- **服务要求**

开展数据统计分析服务，按需对各类数据进行统计分析，包括但不限于数据比对、分类筛选汇总、描述性统计、时间序列分析、多元统计分析等工作；同一个统计任务的数据修正及补充不再另外收费。基于完成项目中各类需求的数据统计分析部分定制场景开发，按需对各类数据统计后生成数据报表服务。

- **交付成果和标准**

输出物	输出物标准
需求文档	提供服务模板的需求文档。
模型设计文档	要求符合数据运营工作实际需求，符合数据标准和公共数据模型设计规范。
测试文档	符合测试报告模板，如实记录测试过程和缺陷。
指标设计文档（如有）	指标定义描述规范，指标间的设计逻辑和关系表述清晰
模型说明文档	模型表述包含必要的代码说明，内容清晰完整，

	符合模板要求
分析报告（如有）	报告内容和形式应满足个性化需求和管理目标要素，素材详实严谨，不限定模板，以获得正式交付对象的确认为标准
结果表及使用说明	内容完整，与需求和设计文档一致，符合模板
融合加工程序执行记录	系统获取的真实执行记录，与共享、治理业务需求一致

2.1.1.9 数据挖掘建模

- **服务要求**

基于数学、统计学等学科，数据挖掘、人工智能等算法，及业务领域理论、规范及方法开展数据分析建模服务，应用于业务问题发现、数据规律研究和风险预警提示等工作。在相关数据分析场景建立数据分析模型，并输出专题分析报告等相关成果。

- **交付成果和标准**

输出物	**输出物标准**
需求文档	提供符合模板的需求文档。
模型设计文档	提供含指标设计的设计文档，要求符合数据运营工作实际需求，符合数据标准和公共数据模型设计规范。
测试文档	符合测试报告模板，如实记录测试过程和缺陷。
指标设计文档（如有）	符合需求和模板，与模型设计文档保持一致
模型说明文档	提供符合数据运营工作实际需求，符合模型验证基本要求
分析报告	如有应用建模的分析工作，需提供符合模板的分析报告，获得正式交付对象的确认。

2.1.1.10 数据分类分级检查

- **服务要求**

结合数据分级分类的管理要求，以及分级分类标准、技术指南等规范，制定数据分级分类检查方案，并对各类型数据进行分类分级检查，提升数据安全的管理能力和管理水平，便于规避数据运营过程中的数据安全风险。

- **交付成果和标准**

输出物	**输出物标准**
数据分类分级检查方案	符合分类分级工作实际需求，符合数据分类分级标准规范。

数据分类分级检查报告	覆盖全部检查对象，符合分类分级标准规范要求的数据分类分级检查报告。

2.1.1.11 数据加密、脱敏等控制

- **服务要求**

数据安全控制服务是针对数据汇集、数据构建、数据开发、数据开放、数据共享、后台运维等数据流转场景，提升数据防护能力的建设，在满足业务需求正常开展的前提下，最大限度的对敏感数据进行保护，防止敏感数据泄露事件的发生，通过数据安全控制服务进行持续保障数据安全控制相应的应用系统安全、稳定运行。该服务需要做到针对不同数据使用场景下配置化、全覆盖的服务要求，同时需要支撑该服务的灵活性和操作友好性需求。

- **交付成果和标准**

输出物	输出物标准
安全控制配置化规则	规则应当符合数据加密、脱敏工作要求。
安全控制执行日志	包含安全控制策略、控制记录数等信息。
数据安全控制服务报告（如有）	包含脱敏、加密、加水印后安全控制服务的分析报告

2.1.1.12 应用安全监测分析及威胁情报服务

- **服务要求**

针对应用实时开展网络流量收集、分析、展示和预警，按要求提供使用统计报告，以满足对整体网络安全监控保障需要。该服务需要对应用安全监测分析服务中所需要提供的从流量接入、分析、场景事件到告警与交付输出的整个过程，达到流量实时监控与安全事件第一时间响应的目标。

收集威胁情报，以辅助识别外部威胁、确认攻击源头、预警安全威胁、发现未知风险等。需要提供的从安全社区公布、分析、威胁确认到告警与交付输出的整个过程，达到安全威胁情报监控分析与第一时间上报响应的目标。

- **交付成果和标准**

输出物	输出物标准
《安全监测分析日报》	包含值班时间、值班地点、值班人员、平台防护情况、平台攻击源 top 摘要、可能出现的攻击成功的安全事件。
《安全监测分析月报》	包含分析事件、告警 top 摘要、受攻击站点 top 摘要、攻击者 top 摘要、当月安全事件汇总。

《需求确认与跟踪列表》	对服务过程中产生的需求进行分析与执行，并对执行完成情况进行跟踪及说明。
《安全攻击事件汇总》	包含大量攻击事件、明显攻击事件、攻击成功的安全事件。
《安全监测在线报告》	对大屏实时展现的内容进行报告拉取、编辑汇总。
《安全监控告警处置类单据》	安全事件均录入平台工单系统可根据平台记录情况记录安全事件闭环结果，包含事件发生时间、发现人员、事件描述、处置时间、处置人员。
《模型设计与评估报告》	符合模型设计与评估报告模板。
《安全监测分析专项工作报告》	符合安全监测分析专项工作报告模板。

2.1.1.13 应用安全检查评估服务

- **服务要求**

按照《信息安全等级保护管理办法》、《关键信息基础设施安全保护条例》等法律法规、技术标准和招标方的信息安全、维护管理要求，对信息系统定期开展安全风险评估，准确及时有效识别系统脆弱性，确保漏洞隐患整改闭环，并按照要求开展应急演练，降低数据运营所涉及服务的安全风险，提高相关系统及服务的抗攻击能力，以满足防止相关数据泄露或者被窃取、篡改以及制定网络安全事件应急预案的要求。

- **交付成果和标准**

输出物	输出物标准
应用安全检查评估服务申请单	包含本次安全检查评估的对象范围、时间要求、评估方式（脆弱性检查或应急演练）。
安全脆弱性检查报告	包含本次脆弱性检查所使用的工具、对象、漏洞清单（漏洞漏报率小于 1~3%）以及漏洞整改建议。
安全脆弱项处置类单据	符合安全脆弱项处置类单据模板。
应急预案和应急演练记录	包含应急预案、应急演练的过程记录和需整改的问题清单。

2.1.1.14 应用安全基础管理服务

- **服务要求**

应用安全基础管理服务提供的整改需求接入、安全复测、问题跟踪与交付输出的整个过程，以满足整体应用安全管理需要的目标。结合安全基础管理服务的需要，在规定时间节点上，周期性组织应用安全基础管理工作，以满足防止网络数据被窃取、篡改和安全事件管理的要求。

- **交付成果和标准**

输出物	输出物标准
安全问题整改需求清单	包含应用对象、问题来源、问题描述、发生时间、复测时间要求。
安全整改验证处置类单据	记录安全问题整改过程，符合安全整改验证处置类单据模板。
安全问题跟踪表	包含应用对象、问题来源、问题描述、发生时间、复测时间、复测结果、复测人员。
安全基础管理工作报告	包含复测结果以及未整改完成项的整改建议。

2.1.1.15 作业调度

- **服务要求**

为了能够满足中心及各委办局对于数据及时性和稳定性的要求，通过作业调度工具对日常数据加工、数据开放、数据分发等作业的调度管理进行监控，对中断、失败、卡死、执行时间过长的作业进行问题分析、定位、处理和记录，并通过事后的分析，明确问题缘由，及时修复，以便后续能够避免同类问题发生。

作业调度服务工作内容包含但不限于：日常数据加工、数据开放、数据分发作业的调度管理，检查是否及时完成，对于中断作业进行处置。

- **交付成果和标准**

输出物	输出物标准
作业监控数据汇总报告（含异常作业分析）	作业监控数据汇总报告，包含但不限于作业运行情况、作业异常分析等。
月总结报告	符合运维报告模板，并包含以下绩效指标： 作业规模数据及变化记录（作业映射到目录数）、 作业可用率=（月实际及时完成作业量/每月计划执行作业量） 故障处理及时率 附相关记录材料。

2.1.2 应用服务类

2.1.2.1 数据开放运营接入服务

- **服务要求**

在支撑数据开放及数据社会化应用过程中，对各栏目和各主题的需求对接、

需求分析、咨询反馈的服务。

- **交付成果和标准**

输出物	输出物标准
内容发布记录	符合内容发布记录模板。
运营策划方案（如有）	符合数据运营需求附相关记录材料。
运营统计报告	包含运营数据统计相关数据。
问题回复记录	符合问题回复记录模板，并包括回复数量，回复及时率，用户满意度，附相关记录材料。
需求审核记录	包含需求审核数量及需求审核结果。
需求审核记录	包含需求审核数量及需求审核结果。

2.1.2.2 公共数据上链服务

- **服务要求**

在支撑各单位公共数据上链过程中，对于职责目录、系统目录、数据目录三目录编制的完成情况，以及三目录挂载关联情况进行逐一审核；按照新一年度的重点工作任务，制定工作方案并开展数据标准的上链、应用场景备案的逐一审核，并在过程中对各单位开展相关工作进行技术支撑。

使用该目录时，不可使用数据质量检查、数据质量规则设计及异常处置服务目录。

- **交付成果和标准**

输出物	输出物标准
公共数据上链目录	目录符合整体编目规范、数据采集标准、符合系统的数据质量检查规则。
公共数据上链方案	符合智能合约、应用场景备案的需求。
公共数据上链总结报告	公共数据上链总结报告，包含但不限于上链数据目录、数据清单、数据质量标准、数据异常分析等。

2.1.2.3 主（专）题数据库建设

- **服务要求**

根据数据库建设需求，对主题库建设，按照某一主题或业务领域，将相关的基础数据进行收集、整理、归类和存储的过程，以形成专业的知识库。主要包括主题的选择、数据的收集、整理和存储，其主要目的是为用户提供特定主题下的专业知识和研究素材。对专题库建设，根据特定专题或业务需求，对基础数据进行二次加工和整合形成的数据库，以满足特定专题分析的需求，包括对专题需求

分析、数据收集、清洗、治理、质量控制和更新维护等工作。

使用该目录时，不可使用数据采集接入、数据抽取服务、数据标签、时空数据转换与处理、数据质量检查、数据质量规则设计及异常处置服务目录、数据共享/开放/授权订阅服务、数据统计分析及报表服务、数据挖掘建模、对于历史数据的归档及销毁服务目录。

- **交付成果和标准**

输出物	输出物标准
主（专）题数据库需求书	提供经确认的需求文档
主（专）题数据库设计文档	提供含指标设计的设计文档，要求符合数据运营工作实际需求，符合主（专）题数据库设计规范。
测试文档	符合测试报告模板，如实记录测试过程和缺陷。
主（专）题数据库说明文档	提供符合数据运营工作实际需求，符合主（专）题数据库建设基本要求

2.1.2.4 数据可视化展现工作

- **服务要求**

可视化展现服务主要以需求调研明确大屏展示要求，通过系统设计与实施实现，将中心在公共数据治理、应用或安全方面的建设情况及成果借助图形化手段更加直观、清晰、全面的展现出来。为中心在公共数据治理、应用或安全方面决策上提供支撑及辅助判断，起到业务监控、风险预警的作用。

- **交付成果和标准**

输出物	输出物标准
需求文档	需求文档符合模板要求，经过需求方确认。
点线设计图	符合实际需求和设计规范，包括度量页面数量。
高保真设计图	根据需求说明书和点线设计图设计出高保真设计图，符合设计规范。
数据指标设计文档	符合指标设计文档模板。
数据库设计文档	符合数据库设计文档模板。
接口设计文档	符合接口设计文档模板。
相关代码	符合代码规范，测试通过。
测试文档	测试过程和缺陷记录完整，符合测试报告模板。
可视化交付物（含 url）	可视化交付物部署并正常运行。

2.1.2.5 公共数据社会化应用服务

- **服务要求**

在推进公共数据社会化应用过程中，围绕公共数据社会化应用场景的咨询管理、场景评估、数据支撑、产品或服务发布评估，其中场景规划评估包括社会伦理风险、技术安全风险、法律合规风险等评估，满足“一场景一授权”工作要求，对社会化应用场景中每个数据服务和产品的每次发布，进行发布前审核工作，包括但不限于以数据分级分类标准为依据，确保服务实现与方案涉及的一致性、与场景规划符合度。同时落实推进社会化应用场景的主体、场景内容、服务调用日志、授权凭证等管理要素上链等工作。

使用该目录时，不可使用数据采集接入服务、统计服务、数据分类分级检查目录。

- **交付成果和标准**

输出物	输出物标准
公共数据社会化应用方案	按照公共数据社会化应用的场景，编写公共数据社会化应用方案，包括应用场景的主体、场景内容、所需数据支撑、数据分类分级标准及评估情况、拟发布的产品或服务等。
公共数据社会化应用评估报告	包括社会伦理风险、技术安全风险、法律合规风险等评估。
公共数据应用日志	日志包含但不限于服务调用日志、授权凭证等。

2.1.2.6 数据共享/开放/授权运营服务

- **服务要求**

该目录用于在数据共享、开放和数据社会化应用服务过程中，对于委办用户的应答响应、报障、需求对接、数据异议核实等工作事项进行跟踪、解答和处理。

- **交付成果和标准**

输出物	输出物标准
内容发布记录	符合内容发布记录模板。
运营策划方案（如有）	符合数据运营需求。
运营统计报告	包含运营数据统计相关数据。
问题回复记录	符合问题回复记录模板，并包括回复数量，回复及时率，用户满意度。
知识库补充记录	符合知识库补充记录模板。
需求审核记录	包含需求审核数量及需求审核结果。
需求审核记录	包含需求审核数量及需求审核结果。

2.1.2.7 安全基线配置管理服务

- **服务要求**

根据中心业务管理和运行、安全管理的需要，结合《信息安全等级保护管理办法》、《关键信息基础设施安全保护条例》等法律法规、技术标准和招标方的维护管理要求，以网络信息安全、数据安全、安全稳定高效业务运行为服务目标，对区大数据资源平台开展基线巡检、备份执行与管理和配置执行、验证与管理工作，对平台服务连续性、可靠性和安全性相关的服务器、操作系统、中间件、网络策略、数据库、应用系统、安全策略（含账号和权限）、业务配置等进行服务。

- **交付成果和标准**

输出物	输出物标准
巡检台账	巡检对象范围包括：操作系统基础架构信息、数据库集群信息及应用子系统相关重要进程等内容。巡检台账包含巡检记录，含巡检对象，巡检对象正常值范围，以及巡检采集值信息等内容，以及进行巡检的时间和操作人员信息。
平台月度巡检工作计划	包含日期、任务名称、运维值班人员、早晚班及运维值班组长。
巡检表单	呈现本次巡检结果，包括巡检时间、巡检人员、巡检小结、异常情况汇总和分析
配置申请表	申请资源、申请人、申请时间。
配置管理台账	申请配置类型（资源、系统、JDBC），计划配置时间，申请配置内容

2.1.2.8 综合运营保障服务

- **服务要求**

为保障数据服务的安全性、可靠性、稳定性和连续性，通过综合运营模式，以保障业务安全为服务目标，对所涉及的支撑系统开展 7*24 小时的运营和安全监测、预警值守监控，及时发现并处置影响业务可用性的安全问题，并对问题通过线上工单流转进行持续追踪，确保问题工单及时有效闭环，对重大安全问题开展专项运营故障分析，提出整改及优化建议，整改完成后组织开展应急安全演练方式进行检验，实现 PDCA 循环以运营方式提升业务安全保障能力。

提供 7*24 小时的运营和安全监测、预警值守服务模式，提前预警问题项，实现早发现，早响应，为早解决铸造基石，提升资源利用率，保障应用系统、数据中心、终端设备、服务器及存储设备、网络及安全设备、运维服务台等的高效、

稳定运行。

针对在应用安全重点保障期间，对风险进行分析，制定并执行相应的安全保障方案，从技术、管理、人员等方面提出安全保障要求，确保信息系统的保密性、完整性和可用性，降低安全风险到可接受的程度，以满足对应用安全重保需要。

- **交付成果和标准**

输出物	输出物标准
综合运营保障实施方案	需在其中明确综合运营保障服务工作要求及流程机制、相关部门工作职责和内容和要求。
值守服务和监测预警记录	提供值守工作记录及监测预警记录
综合运营保障处置单	服务商需对所保障各业务系统问题项第一时间响应，并对问题通过线上工单流转进行持续追踪处置，并收集记录处置结果。
综合运营保障总结报告	需要记录保障期间工作实施情况，需要对所有检测到的安全事件以及告警进行统计。要求做到对中高级告警 100%及时处理，并在报告中完整体现。

2.1.2.9 数据安全风险评估、安全审核服务

- **服务要求**

数据安全风险评估服务是指针定期开展存储分布、应用场景和安全策略评估，深入分析数据安全风险，对所发现问题闭环管理，并构建数据安全数据评估服务技术合规评测体系。

数据安全审核服务是针对数据开展过程中的日志进行审计、账户权限审计和访问行为分析等工作，深入分析数据资源平台在数据处理过程中的安全风险，对所发现问题进行闭环管理。

- **交付成果和标准**

输出物	输出物标准
《数据安全风险评估服务评估报告》	包含本次数据安全风险评估服务所使用的对象、存储分布、应用场景和安全策略评估以及深入分析数据资源数据存储过程安全风险。
《数据安全风险评估服务问题列表》	包含本次数据安全风险评估服务需整改的问题清单。
《数据安全风险评估服务问题整改单》	记录需要整改问题的发现、整改、二次验证以及确认全生命周期的文档。
审核日志	包含但不限于审核规则、审核内容、审核数量、审核结果。

审核报告	审核报告应当符合数据安全工作要求。
审核规则及变更	应当符合数据安全工作要求。

2.1.2.10 应用安全渗透测试服务

- **服务要求**

按照《信息安全等级保护管理办法》、《关键信息基础设施安全保护条例》等法律法规、技术标准和中心安全管理要求，对应用系统开展安全渗透测试服务，发现系统最脆弱的环节，采用可控制、非破坏性质的方法和手段发现目标和系统设备中存在的弱点，并提供安全加固意见以提升系统的安全性。

- **交付成果和标准**

输出物	输出物标准
《渗透测试报告》	包含本次测试系统检查所使用的工具、对象、漏洞清单（漏洞漏报率小于 1~3%）以及漏洞整改建议。
《应用系统漏洞汇总表》	包含各系统的渗透测试漏洞汇总，漏洞分类情况及修复建议。
《回归测试报告》	根据之前渗透测试发现的漏洞进行二次验证，检验是否完成所有漏洞的修复，符合回归测试报告模板。
《应用系统与映射主机对应清单表》	包含本次渗透测试服务中应用系统所对应的所有应用主机清单，便于后续的核算。
《安全脆弱项处置类单据》	包含发现的漏洞名称、类型潜在威胁及当前处置情况并及时下发。
《渗透测试专项总结报告》	包含本次渗透测试发现的所有漏洞清单及相关明细。

2.1.2.11 安全审计服务

- **服务要求**

按照《信息安全等级保护管理办法》、《关键信息基础设施安全保护条例》等法律法规、技术标准和中心安全管理要求，对应用系统开展综合安全审计评估，涵盖主机审计、网络审计、数据库审计、运维审计、业务审计、源代码审计等内容，发现系统性风险并进行分析预警。

- **交付成果和标准**

输出物	输出物标准
代码审计报告	根据 GB/T 39412-2020《信息安全技术代码安全审计规范》出具相应的报告
安全审计报告	包括但不限于所辖服务器主机操作系统、网络区域、应用平台软件、数据库、应用系统和网页等审计内容和审计结果。

安全整改方案和整改验证报告	根据审计报告发现的问题输出整改方案、验证整改方案的可行性并组织整改并提供整改后验证证明。

2.1.2.12 系统功能符合性评估和测评服务

- **服务要求**

根据中心业务开展和安全管理需要，结合《信息安全等级保护管理办法》、《关键信息基础设施安全保护条例》等法律法规规定以及主管单位的管理和技术标准要求，针对大数据资源平台，开展系统功能、安全及密码方面符合性测评。

- **交付成果和标准**

输出物	输出物标准
评估报告	符合国家、地方法律法规规定以及相关技术标准要求。
测试报告	符合招标方业务开展和安全管理需要。

2.2 重点工作目标

其中 2025-2026 年重点工作目标如下：

2.2.1 大数据资源平台运营

依托数据底座和大数据资源平台，夯实平台的服务能力和安全保障能力，深化数据资源一体化和目录一体化工作，完善数据归集、加工、共享、开放、应用、安全、存储、归档等各环节的规范统一和协调管理，统筹协调好目录和数据资产管理，完善数据安全管理制度文件，同步优化业务和管理流程，提升用户体验。

夯实大数据资源平台基础服务。依托统一数据底座和目录链能力，构建数据管理架构，支撑综合性公共数据共享交换、治理、专题库建设。推动新技术应用，通过隐私计算、区块链等技术，探索公共数据开发利用的安全可信环境，支撑数据的安全高效流通。

支撑数据标签、数据分析、数据可视化等服务。探索数据标签库建设，汇总和处理多个数据源的海量标签数据。通过配置规则将零散的、基础的用户数据和指标汇总为系统的用户画像数据。优化数据治理分析，提供数据接入、数据处理、数据资源目录、数据服务等基于中心提供的数据底座基础之上的独立资源池和共性化的服务，探索委办开展数据一级治理工作，实现行业和专业属性的数据治理、加工和应用，以数据资产服务化方式支撑委办多元业务场景建设，支撑委办的业

务运营。

完善大数据资源平台级联服务。支撑区大数据资源平台与市大数据资源平台的级联对接工作，强化平台协同联动聚焦数据互联互通，赋能基层治理。配合数据上链工作，拓展公共数据属地返还承接能力，提高数据共享精准化、便捷化水平，为基层减负增能、创新政府管理和服务提供支撑。

完善大数据资源平台的权限认证体系和授权体系管理。探索“数据可用不可见”，依托大数据资源平台数据资产管理能力，确保数据不被篡改，数据全程可溯，进一步完善数据共享互信关系。

完善授权运营管理。支撑公共数据社会化开发利用，探索授权运营主体管理、应用场景管理等服务能力建设。依托大数据资源平台资源目录管理能力，完善对资源目录、样例数据、样本数据以及生产数据等资源的出湖管理。

支撑数据运营管理等项目管理的要求。以信息化手段实现数据运营项目的过程合理、客观留痕，通过运营服务管理子平台实现需求单、服务单、工单等数据运营管理单元在发放、执行、验收过程中的线上化管理。实现统一需求、统一报障，实现中心数据治理全流程的管理，实现运营的集中化管控，辅助运营决策，形成覆盖全生命周期的整个运营流程，满足实际运营管理的需要，同时通过文件管理和过程管理，对服务单相关过程材料、验收材料做到统一管理，并保证整体项目的进度有序进行、按时交付。

保障大数据资源平台服务连续性及高可靠性。建立大数据资源平台的运营管理指标体系，进一步保障平台运行稳定性、高效性。保证核心服务和核心系统7*24 小时连续服务，减少系统计划内和计划外停机。在系统出现故障时能及时响应，实现核心应用的快速恢复，以保障关键数据和业务系统的运行稳定性和可持续访问性。配合平台运维，运维对象包含但不限于大数据资源平台相关的网络、主机、前置机集群、数据库、服务组件、应用系统以及数据归集任务、数据治理任务、对外共享服务等一系列数据服务。

保障大数据资源平台安全。维持平台安全可靠，避免出现病毒感染、黑客入侵、数据泄露等重大网络安全事故，实现平台安全问题可查可控。结合不同的安全视角（攻击者和防护者）来对平台进行全方位的安全检查，从而实时了解平台最新的安全状态，对潜在的安全风险及时干预和处置，对违规操作行为及时溯源

和追究，在风险尚未扩大的情况下就进行控制。同时结合定期的实操性演练，发现并及时修改紧急情况下处置流程中存在的缺陷和不足，检验平台各团队应急保障能力、对应急响应工作的了解程度和实际操作技能，从而最大程度上保障平台的安全稳定运行。依托数据安全保障子平台，综合应用安全能力，通过合理的安全策略和技术手段，为平台数据安全性和完整性提供能力支撑。依托运营服务管理子平台，建立对数据服务的全链路全方位的监控能力，以便运维团队能及时发现故障和隐患、更精准定位问题、更准确研判故障影响范围、缩短故障处置周期、及时恢复业务。

2.2.2 数据治理、共享及分析

1. 依托数据上链，优化数据治理体系

（1）提升数据目录质量

支撑包含但不限于政府、党委、人大、政协、政法等党政机关及事业单位数据上链。根据单位“三定”职责、权责清单及办事指南编制的职责目录和系统目录，校核所对应数据目录的准确性、完整性和一致性。根据需求配合各部门归集数据并完成融合治理，进一步厘清数据资源、数据模型等与数据目录的关联情况。

支撑国有企业等社会组织的数据上链工作，为数据要素流通提供高质量的数据目录索引服务。

加强数据目录分类标签和安全分级管理，结合数据目录标签，加强数据资源分类管理。

（2）公共数据上链常态化运营

支撑根据职责调整与变更、因项目建设或升级改造引起的系统调整以及应用场景数据需求需要等原因，目录链上目录的动态调整，做好数据目录版本更新、数据归档以及新老数据资源替换等工作。

配合市区两级事项库更新，加强“数源目录”校核，加强权威数据的管理。

（3）数据执行标准管理

落实数源目录“一数一源一标准”要求，推广“数源目录”在重要应用场景和高频共享场景中的应用，支撑数据共享和应用数源目录调整，保障供给高质量的数据应用和服务。探索自然人、法人、空间地理数据入库质量核验，将自然人证件号码、法人统一社会信用代码、空间地理区划信息和地名地址信息作为归集

入库的必备要素。

（4）数据供需管理

基于需求部门的应用场景，推动便捷共享，实现公共数据的高效、有序共享，落实数据授权、访问和服务调用日志管理。基于公共数据便捷共享应用场景清单，落实数据使用要求和安全管理责任。聚焦高频共享目录、“数源目录”和权威数据资源，推动数据标准全覆盖，探索公共数据质量规则库建设。

响应对国家政务数据资源的共享申请和使用，支撑区内应用场景建设。实现基层治理数据的统一汇聚和共享共用，解决基层数据获取难、不准确、时效性不高等问题。

2.深化源头治理，提升数据质量

探索建立数据质量检查规则库，落实数据资源全生命周期的质量检查和反馈，配合源头数据数据质量检查。优化公共数据异议核实的运营保障，提升运营效率和质量。优化数据治理评价指标体系，形成出具数据运营区级分报告的功能。

依托数据标准全覆盖工作，建立基于场景的数据质量管理机制，形成从源头数据对账、日常质量监督、关键环节质量评测以及应用服务抽检各环节的数据质量手段，全面加强数据质量工作，进一步提升数据质量水平。

3.做实分类分级，加强数据安全

深化公共数据运营安全管理体系设计，细化数据流转过程中各方安全责任，加强访问权限控制。结合主管单位要求和数据流通需求，加强数据全生命周期防护，落实资源平台安全保护举措。依托中心共性安全能力，开展敏感数据安全动态监控能力的接入，落实数据安全风险闭环管理流程。定期开展数据安全风险评估自查，确保安全管理有效实施。落实数据安全指标与安全可视化展示能力建设，实现数据安全工作“可量化、可评估”。

4.深化三大综合库应用，深化建设共性数据能力

持续加强上链目录中自然人、法人和空间地理等共性业务对象数据的融合治理和复用，强化自然人、法人、空间地理综合库应用。

(1) 自然人综合库

完成回流人房数据校验并加以优化，提高数据的准确性、时效性，赋能实有人口动态管理。探索建设“一人一档”数据查询服务。完善自然人属地返还数据

安全保障，探索自然人数据去标识化处理，加强个人信息保护。

(2) 法人综合库

探索建设“一企一档”，扩充法人综合库基础数据与监管类数据。建设数据服务或者应用，支撑“云间码”“重点企业服务包”等重点应用建设。探索建立法人数据标签、涉企知识图谱等查询服务能力。

(3) 空间地理综合库

探索建设空间地理数据资源目录，更好地支撑基础空间信息和核心业务图层的数据归集。支撑空间数据标准化，完成空间数据业务校验规则设置，并加入日常检验检查。完成梳理业务类、空间类标签，增加门牌标签信息。

5.孵化数据应用，促进数据开发利用

支撑授权运营重点应用场景建设所需要的数据治理，立足经济发展、社会民生重点领域，拓展数据利用范围，建立可视化看板。深化实验室工作，依托大数据资源平台，以孵化上线数据产品、提升社会化服务能力为目标，推动大数据创新实验室建设落地。

3 运营服务管理要求

3.1 总体要求

中标人应当根据服务任务要求组织服务团队，在理解、落实采购方运营管理和安全管理等相关制度和规范的基础上细化服务需求，形成服务实施方案，统筹实施任务管理，保质、保量完成服务交付；并在服务期间做好进度和质量控制，对运营服务实施的全过程进行安全管理。中标人应当在数据运营服务工作过程中，满足以下重点工作要求，保质保量完成工作。

一是在人员团队配置方面，在数量、资质、工作内容、驻场要求、能力优化支撑上均满足招标要求。应当满足采购方对于运营服务团队的要求，配备项目经理、运营管理团队、需求响应与分析团队、资深专家团队、服务单交付团队、客户响应团队，其中，团队人员数量、人员资质、人员社保缴纳情况、服务单交付团队的工作经验应当满足服务单交付要求。中标人确认的项目运营服务团队人员及数量，明确的驻场人员，应当与投标文件承诺一致，未经采购方书面批准不得随意调换或撤离，若自行更换或撤离，按照合同违约处理。中标人应具备提供

大型专业培训服务的能力，能够根据数据运营服务的特点制定培训方案并提供培训，使相关人员在培训后能够独立开展工作。中标人提供的培训课程应涵盖数据治理、数据共享和开放、数据安全以及大数据资源平台等的系统使用、配置维护、运营管理等内容，以满足采购方以及各委办局相关管理人员和操作人员的实际需求。同时，中标人应定期或不定期地组织各类外包服务人员的相关培训，以保证各类外包服务人员能够有效地理解和掌握运营服务相关的各类技术要求和管理要求。中标人应每季度征集各部门的培训需求，并根据培训需求提出相应的培训计划，报采购方同意后实施。中标人应安排具有相关认证的专业培训讲师授课，并提供全套培训教材、课件、讲义和培训课程计划表，所有资料均应提供中文版资料。投标人应在投标文件中提供详细的培训方案，列明相应的培训课程内容、人数和时间安排等。

二是在服务质量和时效性方面，按时响应并按时保质保量完成各项工作任务。中标人应当在 2 个工作日内组织人力、物力资源响应采购方的服务单需求，并在 5 个工作日内下达服务单的工作需求，包含但不限于按照服务单的要求细化工作需求的工作计划、完善服务单的业务方案和技术方案、明确交付绩效目标并启动开展服务单的实施工作。在服务单实施期间，中标方应做好进度和质量控制，对服务单实施的全过程进行安全管理。为保证服务响应效率，中标人运营服务团队应常驻采购方外包服务场地并服从采购方的管理。中标方应按双方确认的时间节点保质保量交付服务单的工作成果。为保障服务质量和数据质量，中标人应当做好全流程监控管理，并开展对账。

三是高度配合采购方，做好合同与协议管理备案、第三方监管要求响应、人员与场地管理、合规合理留痕等相关工作。在**合同与协议管理备案方面，**中标人由于数据运营服务的需要，与任何其他一方签订的合同，应当及时向采购方备案。中标人在服务期内每年通过签署补充协议对当周期内的数据运营服务绩效目标、SLA 服务要求、用户满意率目标以及服务目录细则予以确认和约定。在**配合第三方监管机构工作**方面，中标人应当在数据运营服务的工作要求下，无条件并及时配合数据运营服务第三方监管机构完成包括数据质量检核、数据质量攻防、安全审核、安全评估、飞行检查在内的数据质量、安全、人员场地相关工作内容。**在工作量合规合理留痕方面，**中标人在开展数据运营服务的过程中，应当

配备线上系统与后台技术能力实现工作量的线上合理合规留痕，确保公正客观，并在工作开展的过程中，做好相关管理平台的维护工作，保证与服务任务状态与实际工作相符合。按照数据运营服务目录和服务任务的考核标准在系统如实、及时留痕，客观展现工作内容和工作量，以便满足包括日常监督管理、服务任务验收等工作的需要。

四是在制度方面，在服务质量考核、资金管理、费用结算等方面建立符合采购方要求的制度体系。中标人在履行运营服务的过程中，应当遵循本市及采购方各类法律法规、制度规范的要求，因违反规定等原因造成的一切损失和责任由中标人承担。严格遵守采购方数据运营相关管理规范和管理办法的要求，若违反相关规定，按照合同违约处理。中标人应当按照采购方的要求，按照数据运营工作的需要，配套相适应的企业内部管理规范，并对不符合管理要求的已有企业内部制度规范进行整改，建立健全包括但不限于“人员考核管理办法”“数据运营服务项目供应商管理办法”“数据运营服务项目供应商选择（POC）管理办法”等内部制度体系。在**服务质量考核方面**建立相关管理制度，对各项服务明确考核指标和考核内容，对服务过程、服务交付物、数据质量等方面开展服务质量考核，开展全过程管理。在**资金管理方面**建立相关管理制度，根据“先用后付，按需响应，按时结算”的工作要求和工作原则开展资金管理，建立相适应的企业内部资金管理和商务体系，以适应数据运营的工作要求。在**费用结算方面**建立并落实相关管理制度，应当按照采购方的结算频率，在收到结算款后及时与供应商开展结算，如发生已查证的与供应商拖欠结算款等事件，按照合同违约处理。相关管理规范和制度必须在经采购方审核通过后发布，并向采购方备案。

五是在知识产权方面，满足合法合规要求。运营服务过程中涉及的所有数据及资产的拥有权及使用权均属于采购方，未经采购方许可，中标人无权对其进行支配。所有与数据相关的设备维修、报废等处理需经采购方同意，并在监管下进行。若发现中标人未经许可对数据进行支配，采购方将对中标人采取惩罚措施并追究其法律责任。除非事先书面申明并经采购方认可，中标人交付的软件、代码、模型、图纸、文档等是知识产权及使用权均归采购方所有；如交付成果涉及第三方知识产权，中标人应事先获得合法授权并保证采购方具有长期的合法使用权。

六是在安全管理方面，满足各类安全要求。中标人应制订运营安全管理方案，承担运营服务过程中环境安全、人员安全、信息安全、数据合规使用等相关各类安全责任。未经采购方书面授权，中标人不得实施漏洞探测、渗透性测试等活动，禁止上传木马、执行高危 payload 等可能影响系统运行的操作。在安全工作中，1）中标人应当坚持主动预防、迅速高效的原则，紧密结合实际情况，精心编制并持续完善应急预案，按需组织实施应急演练。2）必须提供 7*24 小时全天候应急响应服务。3）依据故障时间及故障范围划分故障级别，并根据六级故障分别落实不同的故障响应措施，当发生 B2 级及以上故障后，立即响应，故障(发现+预判+传报)时间 5 分钟，业务恢复历时 10 分钟，故障处理历时 2 小时；当发生 C+级故障后，5 分钟内响应，故障(发现+预判+传报)时间 30 分钟，故障处理历时 4 小时；当发生 C 级故障后，5 分钟内响应，故障(发现+预判+传报)时间 60 分钟，故障处理历时 48 小时。4）如发生故障，服务提供方应严格按照制定的应急预案中故障处理流程实施故障排除操作。5）当故障排除操作全部完成后，服务提供方应向采购方提交故障报告，经采购方验证通过后签字确认并归档保存，同时组织更新相关文档。6）如遇有重大事件（包括汛期、节假日、政治军事活动等），服务提供方应科学编制安全保障方案，并根据采购方需要提供现场保障服务。（注：特别重大故障（一级）A1：用户无法正常使用服务或者业务应用超过 60 分钟；重大故障（二级）A2：用户无法正常使用服务或者业务应用超过 30 分钟且低于 60 分钟（含）；较大故障（三级）B1：用户无法正常使用服务或者业务应用超过 10 分钟且低于 30 分钟（含）；一般故障（四级）B2：用户无法正常使用服务或者业务应用小于 10 分钟（含）；未产生批量投诉，无社会影响度 C+级：1.服务性能下降，引发用户体验下降；2.系统、中间件、网络冗余保护功能丧失，处于无保护运行状态；3.非核心业务接口故障，丢失辅助业务功能，不影响核心服务；C 级：1.常规的软、硬件故障，未触发业务功能受损，未导致业务的冗余保护功能丧失；2.常规的容量、性能故障，未触发业务功能受损，未导致业务的冗余保护功能丧失；3.其它故障）

七是承担数据运营相关文档材料、人员场地管理等工作。积极并准确响应采购方的需求，并做好转化。编制服务要素单、业务方案、技术方案等文档材料，

并做好需求单、服务单、工单的线上流程合理、客观管理。严格执行中心场地管理以及人员管理的要求，做好云桌面的管理、人员账号管理。

八是做好结算管理，与核心供应商和非核心供应商形成数据运营的良好生态体系。根据采购方与中标人的付款方式和付款节点，中标人应当及时向核心供应商进行预支付，作为预付服务费用于抵扣核心供应商将来实际发生的服务费。面向非核心供应商，中标人应当对已完成的服务单进行季度结算，结算费用为该服务单总费用的 60%，在结算完成以后应当及时向采购方进行报备。优化服务管理模式，深入落实数据运营机制，在支撑好重点工作建设的同时，维护好数据运营的生态圈，构建良好的数据运营生态体系。

九是“以成效为导向”做好服务单的分类管理，明确管理内容和目标。中标人应当对服务单做好分类管理，服务单类型包括但不限于数据采购服务、一级数据治理、二级数据治理等。其中，数据采购服务是由中标人直接采购数据服务，以支撑数据运营工作的需要。一级数据治理服务于委办局本身，开展源端数据治理，一般偏向于满足单部门、单领域、单行业的数据治理需求。二级数据治理服务于区领导、全区，开展多行业、多领域数据的融合治理，一般偏向于全区通用性的数据治理需要。中标人应当明确每项数据运营服务工作与数据服务商的工作边界、管理工作内容、预期工作成效、与数据服务商的结算机制等。原则上，一级数据治理代运营应当以数据运营实际工作内容为主，以管理性工作为辅。中标人应当根据服务单类型进一步明确运营商和服务商工作内容以及管理要求。

十是承担主体责任，承担经济损失。中标人应当在服务周期内做好数据质量和服务质量的保障，避免故障的发生。若发生故障，应按照相关故障处理的时长要求、流程标准等做好处置。在服务周期内，由于中标人直接或间接引起经济损失的，全部由中标人承担经济损失。

3.2 响应时间要求

3.2.1 需求响应时间

采购方提出服务单需求后，中标人应在 7 个工作日内向采购方提交该服务单的服务团队、实施计划和相应的实施方案，全面响应采购方的服务需求。

投标人应根据不同的运营服务任务要求，提出相应的运营服务方案，包括但不仅限于处理流程、响应时间、管理体制、服务人员和工具配备等。

3.2.2 应急服务响应时间

1、中标人应坚持主动预防、迅速高效的原则，紧密结合实际情况，精心编制并持续完善应急预案，按需组织实施应急演练。

2、中标人必须提供 7*24 小时全天候应急响应服务。

3、依据故障时间及故障范围划分故障级别，故障级别分为六级，依次为：

特别重大故障（一级）A1：用户无法正常使用业务应用服务超过 60 分钟；

重大故障（二级）A2：用户无法正常使用业务应用服务超过 30 分钟且低于 60 分钟（含）；

较大故障（三级）B1：用户无法正常使用应用服务超过 10 分钟且低于 30 分钟（含）；

一般故障（四级）B2：用户无法正常使用应用服务小于 10 分钟（含）；

未产生批量投诉，无社会影响度 C+级：1.服务性能下降，引发用户体验下降；2.系统、中间件、网络冗余保护功能丧失，处于无保护运行状态；3.非核心业务接口故障，丢失辅助业务功能，不影响核心服务；

C 级：1.常规的软、硬件故障，未触发业务功能受损，未导致业务的冗余保护功能丧失；2.常规的容量、性能故障，未触发业务功能受损，未导致业务的冗余保护功能丧失；3.其它故障；

当：

a、发生 B2 级及以上故障后，立即响应，故障(发现+预判+传报)时间 5 分钟，业务恢复历时 10 分钟，故障处理历时 2 小时

b、发生 C+级故障后，5 分钟内响应，故障(发现+预判+传报)时间 30 分钟，故障处理历时 4 小时

c、发 C 级故障后，5 分钟内响应，故障(发现+预判+传报)时间 60 分钟，故障处理历时 48 小时

4、如发生故障，服务提供方应严格按照制定的应急预案中故障处理流程实施故障排除操作。

5、当故障排除操作全部完成后，服务提供方应向采购方提交故障报告，经采购方验证通过后签字确认并归档保存，同时组织更新相关文档。

6、如遇有重大事件（包括汛期、节假日、政治军事活动等），服务提供方应科学编制安全保障方案，并根据采购方需要提供现场保障服务。

中标人应有专门的数据记录方式，记录和整理采购方的各类故障及技术分析处置结果、技术咨询问题及答复等。

投标人应提供相应的响应方案，包括 7*24 小时的故障接受渠道、处置流程、响应时间、服务人员和工具配备等。

3.2.3 重点保障服务

系统升级、迁移、割接：开展业务系统或相关软硬件的升级、迁移、割接等工作前，中标人应制定完善的操作实施方案，采取适当的措施降低对业务系统的影响。对于可能影响业务系统的各类操作，应全面评估其操作影响，至少提前 3 天通知采购方，经相关业务部门同意后方可实施，且实施时中标人应提供 7*24 小时的驻场值守服务。

系统中断：由于系统维护或其他原因需要计划性地中断系统时，应提前至少 72 小时通知采购方，经采购方同意后方可实施，且实施时中标人应提供 7*24 小时的驻场值守服务。

重大活动、节假日保障：针对重大活动、重要节假期及其他重要时期应提供重点保障服务，需提前制定强化重点保障措施，确保业务骨干、管理人员到场并提前制订预案，确保公共数据生产工作安全、稳定运行，涉及数据运营相关的信息安全提供重点保障。

应急演练：应根据采购方应急预案要求进行针对性应急演练，每年组织至少 2 次应急演练。中标人应制订应急演练方案，经采购方同意实施，且实施时中标人应提供 7*24 小时的驻场值守服务。

其他重点保障服务：当系统频繁出现故障、或需要提高系统维护等级等情况下，应采购方要求，中标人应提供 7*24 小时的驻场值守服务。

以上工作所产生的费用都由中标人承担。

3.3 服务团队要求

中标人应为松江区数据运营单独建立管理组织，配置相应团队。

3.4.1 服务团队配置要求

中标人配置的服务团队具体要求如下表：

中标人应当选派在项目服务方面富有经验的团队人员负责该项目，项目团队应配置对应的人员，团队应至少配备 35 人，其中驻场至少 21 人。其中，项目经理 1 人、业务需求团队 3 人、实施执行团队 17 人，咨询规划团队按需驻场。

投标人应提交完整的服务团队成员名单（包括所属团队、岗位、姓名、年龄、学历、职称、工作年限、手机号等）。服务团队中驻场成员应提供最近 3 个月中任意 1 个月的社保证明以及资质证明材料。驻场期间投标方应按照采购方关于办公地点进出人员管理要求和工作环境管理要求驻场服务。

最低人员要求如下表所示：

组别	职责	人员要求	人数要求	驻场要求
项目经理	负责项目总体实施，包括项目管理、治理任务实施进度管理、过程管理和验收管理、运营安全管理、人员场地管理等： 负责撰写项目计划书及其他相关文字材料； 负责项目现场需求调研、实施部署及项目管理工作，对项目需求、质量、进度、风险等进行有效管理； 负责落实项目范围，制定项目实施计划、项目进度管理、质量管理、成本管理、资源管理、风险管理等； 项目进展中协调与配备项目运行所需的资源，并根据考核结果进行相应的调整，对项目的最终验收负责； 高度配合采购方，做好合同与协议管理备案、第三方监管要求响应、人员与场地管理、工作量的客观、合规合理线上留痕等相关工作。	高级工程师或以上职称，具有 5 年以上相关工作经验，曾参与过类似重大项目。	1	驻场
咨询规划	深入了解数据运营服务业务需求，深度剖析的业	组长要求： 拥有大型数据平台建	3	可远程支撑，必要

	务需求，包括： 通过访谈、问卷调查、现场观察等方式收集客户需求信息；识别数据运营服务管理和实施的业务痛点和潜在需求。提供具备专业性的信息化规划建议。 制定具备专业性的数据运营服务总体规划，制定涵盖项目整体的规划以及实施策略，明确数据运营服务实施方案，包括：确定各项数据运营服务目标和范围；制定运营服务战略和规划；选择合适的运营服务方案和技术路线。 制定和完善运营服务的标准规范，设计运营服务流程、服务标准、形成具体规范要求。	设，或跨行业、跨领域数据治理、分析应用、数据安全管理的工作经验。拥有政府数据治理工作的优先考虑，在领域具有5年及以上工作经验的优先考虑，在工作领域有突出成就和研究成果的优先考虑。 组员要求： 1、本科或以上学历且具有3年以上相关工作经验，曾参与过类似重大项目。 2、熟悉Hadooop Storm Spark Flink Hive Hbase Kafka等常用大数据技术架构，熟悉大数据平台架构系统的搭建、开发、优化；熟悉数据加工、清洗、处理等开发以及相关数据管理技术问题的解决； 3、掌握应用系统设计思想，熟悉微服务架构并具有实战经验； 4、熟悉Linux、Unix系统环境下的操作及性能调优原理；掌握分布式系统原理，对存储、计算、消息队列、集群管理中的一项或多项有深入的理解和认识； 5、具备扎实的技术基础，有坚实的代编码功底和技术研究能力。熟悉大数据生态圈技术，对离线计算、内存计算和流式计算，消息中间件均有深刻理解，不限于		时驻场服务

		Spark、Storm、Flink等；熟悉网络基础知识，深入理解Linux，TCP/IP，防火墙和其他安全技术。		
业务需求	与数据运营服务需求方进行紧密沟通，明晰业务需求与期望。将业务需求精确转化为详尽的功能需求，形成项目需求规格说明书（SRS），如业务方案等。对需求进行合理的优先级排序与管理。积极参与需求评审，力保需求的精准性与完整性。 负责项目实施过程中的沟通和协调，包括：定期与需求方进行沟通，确保数据运营服务任务进展符合预期；协调项目团队成员之间的工作；解决实施过程中的问题；对服务任务成效进行管理和把控。	组长要求： 具有相应领域资质或能力水平证书且具有3年以上相关工作经验。 组员要求： 1、懂IT基本技术原理，了解应用系统设计思想，熟悉数据治理概念并具有实战经验； 2、有责任心，具备较强解决问题的能力，有良好的沟通能力和团队精神； 3、具有优秀的逻辑思维能力，并具有需求判断、引导、控制能力； 4、1年以上需求分析相关工作经验，有数据分析经验优先。	5	驻场人数要求至少3人
实施执行	负责数据运营服务任务实施工作，包括明确技术路径，设计服务任务流程、相关编码和配置工作、承担测试工作，确保运营服务的质量与稳定性。 负责项目实施过程中的问题反馈，支撑数据运营服务过程中各类问题的有效解决。 负责实施过程中按照运营服务工作的规范要求，编制运营服务各个工作环节的交付文档，并做好工作过程留痕。	组长要求： 高级工程师或以上职称，具有5年以上相关工作经验，曾参与过类似重大项目。 组员要求： 1、大专或以上学历且具有2年以上相关工作经验，曾参与过类似重大项目； 2、具备实施数据运营服务所需的技术知识和技能，包括编程、系统配置等技术实施能力； 3、在设计服务任务流程和进行编码配置	21	驻场人数至少17人以上

		时，对细节有高度的关注力和准确性； 4、能够执行测试工作，确保服务的稳定性和性能符合预期；能够编写清晰、准确的实施文档，为项目提供详细的记录和参考。		

3.4.2 服务团队管理要求

中标人应保证服务团队的稳定，其中驻场人员每月驻场考勤记录天数应不低于月工作日总数的 80%，人员变更须经采购方同意且人员变更数不得超过总数的 30%。

中标人应遵照采购方相关要求，实施对服务外包人员的监督管理工作，履行对进场外包服务人员的培训、指导和现场管理责任，落实服务商及现场服务人员签订《保密承诺》，确保进场服务人员的知晓、认可采购方的各项管理流程制度及工作规范并在服务过程中严格遵守。

驻场服务人员在驻场办公地点工作期间应遵守采购方的出入管理、行为规范、安全管理、出勤管理等相关规定，中标人按规定实施考核评估工作。

中标人应根据采购方相关绩效考核管理要求单独制订并执行运营服务团队人员的绩效考核办法，按照“一人一岗、一人一表、效率优先、兼顾公平”的原则每月对运营服务团队的所有人员进行考核，并将考核结论报采购方进行终评。人员考核内容应覆盖服务人员完成的日常工作、专项工作、安全保密工作、服务质量、能力水平和行为规范等，且适应采购方对服务人员的具体要求。中标人应建立相应的考核激励机制，对于考核结果优秀的人员予以表扬与奖励；对于考核不合格的人员应通过培训或调岗等方式提升其适岗能力，经采购方认可后方可回原岗位工作。

若驻场服务人员因违反保密义务、工作规范或有其他重大违规行为而被要求退场的，不得再次使用。若因能力上不符合要求，而被要求退场的外包人员则两年内不再使用。

3.4 第三方监管要求

采购方根据工作需要委托第三方监管机构或专家对中标人提供的运营服务工作量、工作内容和完成质量等进行审核、评估或验收，对运营服务过程中发生的质量问题、重大事故进行责任边界判定。中标人应积极配合第三方监管机构和专家的工作，遵从相关指令和要求并认可相关审核评估结论。

3.5 服务质量评估及违约责任

3.5.1 服务质量评估

采购方将委托第三方监管机构对中标人的数据运营服务进行服务质量评估，评估结果作为服务费结算的重要依据。

3.5.1.1 服务交付质量评估

服务交付质量评估主要针对中标人完成交付的每个服务单进行评估，以交付质量评估结果确定服务单的质量系数。交付质量评估内容主要包括服务响应、服务交付、服务过程管理和服务满意度等方面，交付质量评估分值满分为 100 分。采购方根据服务单交付质量评估分值按下表确定对应的服务单质量系数：

交付质量评估分值	等级	质量系数
≥90 分	A	1
≥80 分，<90 分	B	0.95
≥70 分，<80 分	C	0.9
≥60 分，<70 分	D	0.85
<60 分	E	应先进行整改，整改后评估分值≥60 分时质量系数为 0.8；整改后评估仍不合格的，质量系数为 0。

服务交付质量评估的评分标准如下：

指标分类	指标权重	评价指标	应达要求	评分标准
服务单发放与计划	10	服务单三要素规范性和完整性	提交的三要素材料应格式规范、内容完整，经评审一次性通过。	每发生 1 次评审未通过的，扣 2 分，扣完为止。
		需求满足情况	提交的三要素完全响应并满足服务	未满足服务需求的，每项扣 1 分，扣完为止（需求如发生变更，以客户认可的最终版本为准）。

			需求的不扣分。	
		实施计划合理性	提交的实施团队组织保障和计划合理可行、满足服务任务需求的不扣分。	实施团队组织保障不合理扣 2 分、计划不合理或不满足需求的扣 2 分。
服务任务交付	35	考核指标达标率	考核指标达标率应达 100%。	根据服务任务考核指标项的完成比率评分，即得分=10*完成的指标项数量/全部指标项数量
		绩效目标完成度	绩效目标完成率应达 100%	①绩效目标完成度＜60%的为 0 分；②绩效目标完成度≥60%的，得分=10*绩效目标完成度
		交付质量	服务单的交付符合质量要求。	①由第三方监管机构、测评机构或内部核查人员发现的架构合理性、设计遗漏、程序缺陷、用户体验、数据质量、代码质量等问题，每发现 1 项扣 1 分，扣完为止； ②被使用单位发现并查证的有责质量问题，每次扣 2 分，扣完为止； ③被使用单位发现并查证的有责其他交付物使用问题，每次扣 2 分，扣完为止； ④由第三方监管机构、测评机构或内部安全核查人员发现的安全隐患，每 1 个隐患扣 1 分，扣完为止； ⑤被上级单位或主管单位发现存在安全隐患，每 1 个隐患扣 5 分，扣完为止； ⑥服务任务交付验收未通过的，每发生 1 次扣 5 分，扣完为止； ⑦要求整改的问题未按时完成整改的，每项每延迟一周扣 1 分，扣完为止。
		交付时效	服务单按期交付完成。	服务任务按时完成交付不扣分；每延期 1 周扣 2 分，扣完为止；
服务过程管理	40	人力资源投入	满足服务任务人员要求且保持团队稳定。	①未经批准，实际投入人员与报送人员名单不符的，每发现 1 人扣 2 分； ②未经批准，团队重要成员擅自

				脱岗或未达到考勤率要求的，每发现 1 人次扣 2 分； ③未按照要求及时更替技术能力与岗位不相符的人员，并投入技术能力与岗位相符的人员，每出现一次扣 2 分； ④团队成员流失率或更替率每超 10%扣 2 分（中心要求的更替将另行评估）。
		人员行为规范	团队人员完全遵守各类制度规范。	①第三方监管机构飞行检查发现团队成员违反外包服务管理要求的，每发现 1 次扣 1 分，扣完为止； ②其他各类内部、外部检查中发现并通报团队成员违反相关规定的，每发现 1 次扣 2 分，扣完为止。
		服务沟通	服务沟通及时顺畅、各类报告材料满足要求。	①关键责任人在重要项目会议缺席，每发现一次扣 1 分，扣完为止； ②服务周报、月报或其他必要材料缺失、拖延或内容不完整，每被投诉 1 次扣 1 分，扣完为止； ③团队人员沟通态度问题，每被投诉 1 次扣 1 分，扣完为止。
		问题解决	对各类事件、故障和问题及时响应并处置解决，在平台运行服务中告警事件和报障事件及时进行处置且消除影响。	紧急事件、重要事件、故障和问题按要求及时解决，每出现一起事件同时未能按期解决的，扣 5 分，扣完为止。
		安全生产	有效落实系统漏洞扫描、渗透测试、代码审计等信息系统安全自查工作，并对出现的安全风险事件及时制定整	每被发现一例扣 1 分；每延迟一周，扣 3 分；高风险漏洞修复时限为 1 周，其他修复时限为 2 周。

			改方案并予以修复。	
		文档及备案管理	服务任务按相关服务要素单以及服务规范要求完成响应文档，同时运营商与服务商的相关材料在中心备案。	①所提交文档在内容、格式等方面不符合要求的，每发生 1 次扣 2 分，扣完为止；每份文档每延期提交 1 周扣 2 分，扣完为止 ②相关要求材料未向中心备案的，每发生 1 次扣 2 分，扣完为止。
服务满意度	15	服务满意度	满意度≥80 分	①满意度＜60 分的，扣 10 分； ②满意度≥60、＜80 分的，扣 6 分； ③满意度≥80 分的，不扣分。
		有责投诉	在服务周期内不收到投诉或通报的	①中心、各委办单位或第三方监管机构的有责投诉，受到投诉 1 次扣 2 分，受到投诉 2 次及以上该大项不得分； ②上级单位或第三方单位通报存在严重问题的，以及出现被安全主管单位、上级单位、中心安全管理部门、第三方测评机构或审计的系统安全评估和检查中发现或通报的安全问题的，每发生一次扣 2 分。
其他加分扣分项	/	重大责任事故		①产生严重不良社会影响或者被业务、行业主管单位及领导通报的重大责任事故，扣 50 分； ②发生严重数据泄露事件，扣 50 分；发生较大数据泄露事件，扣 20 分； ③受到安全攻击致使业务受到严重影响的扣 50 分，受到安全攻击致使业务受到较大影响的扣 20 分。

	/	重点保障服务		能提供重要事件或重点时刻及时保障服务的，每发生 1 次，加 1 分,最多加 5 分
	/	专业培训服务		应业主方要求提供专业培训服务，每次加 1 分，最多加 5 分；
	/	高水平规划方案		应业主方要求提供高水平规划方案，经评审通过每个方案加 1-2 分，最多加 5 分。
合计:100 分			含加分、扣分的总分最高为 100 分	

3.5.1.2 服务管理质量评估

服务管理质量评估主要针对中标人的运营服务管理水平进行月度评估，评估内容包括运营管理、现场管理、安全管理和服务满意度等方面。服务管理质量评估分值满分为 100 分。

服务管理质量评估评分标准如下：

指标分类	指标权重	**评价指标**	**应达要求**	**评分标准**
需求管理	4	需求响应及时性、准确性	建立完善的需求管理流程，快速响应编制需求管理计划，及时并准确落实专项团队响应包括临时任务需求在内的各项任务需求；并做好需求文档的更新和管理。	①每延期 1 周响应（或者完成）扣 2 分，扣完为止； ②未与中心沟通达成一致，擅自变更需求的，扣 2 分，扣完为止。
服务交付管理	20	服务交付及时率	严格管控任务进度，保障各项工作按计划执行、及时交付工作产物，按时、按要求完成服务单的最终交付。	①服务单交付每延期 1 周扣 2 分，扣完为止； ②需求响应每延期 1 周扣 1 分，扣完为止； ③中心交办的其他任务每延期 1 周扣 1 分，扣完为止； ④未按时配合第三方监管工作的每延迟 1 周扣 1 分，扣完为止；双方确认的计划调整不扣分。

		服务交付质量	服务单交付不出现质量问题，满足需求方要求，符合服务规范。	①服务单交付每发生一起不符合需求方要求的扣 2 分，扣完为止； ②服务单交付每发生一起不符合服务规范的扣 2 分，扣完为止； ③被使用单位发现并的除数据质量以外的其他有责交付物使用问题，每次扣 2 分； ④服务单交付验收未通过的，每次扣 5 分。
		数据质量	对湖内数据质量进行全覆盖管理，形成完整的数据质量管理规则和体系，不发生数据质量问题。同时，发生数据质量问题时，应当按照已约定的整改期限进行整改。	①未按照约定时间建立数据质量规则的、被发现数据质量检查规则覆盖不完整的，每发现 1 项，扣 2 分； ②每发生一起第三方检查发现的湖内数据质量问题时，扣 1 分； ③每发生一起第三方检查发现的湖内数据质量问题按照要求进行整改的，扣 2 分； ④被发现代码质量问题，每发现 1 项扣 2 分； ⑤被使用单位投诉数据质量问题，每次扣 3 分； ⑥以上问题应当按要求、按时完成整改，每项每延迟一周扣 2 分。
		数据安全	对湖内数据安全和交付物安全进行全覆盖管理。	①由第三方监管机构、测评机构或内部安全核查人员发现的数据安全隐患，每 1 个隐患扣 2 分； ②被上级单位或主管单位发现存在数据安全隐患，每 1 个隐患扣 5 分；
服务可用性及故障管理	20	服务可用性	服务可用性应达 99.99%，减少每个月计划外停服时间。	服务连续性不达 99.99%，若每月每降低 0.01%，则扣除权重的 1%，扣完为止。
		故障发生数	不发生故障	①运营商每发生一起 C 级故障扣 1 分，扣完为止； ②运营商每发生一起 C+级故障扣 2 分，扣完为止； ③运营商每发生一起 B2 级故障扣 4 分，扣完为止； ④运营商每发生一起 B1 级故障扣 6 分，扣完为止； ⑤运营商每发生一起 A2 级故障扣 8 分，扣完为止；

				⑥运营商每发生一起 A1 级故障扣 10 分，扣完为止。
		故障及时恢复数	运营商在数据服务（或者平台）出现故障，按时间要求及时恢复服务。	运营商的故障及时恢复时间未达到要求，每发生 1 起扣 5 分，扣完为止。
		故障上报数	严格按照故障上报规范按期上报、如实上报	每发生一起从迟报、错报、瞒报事件扣 4 分，扣完为止
		闭环管理	对于事件和问题执行有效的闭环管理，按要求形成整改方案查证原因并整改落实。形成 PDCA 闭环管理，不再发生此类故障或事件。	①每发生一次事件或者问题未按计划整改闭环的扣 1 分，扣完为止； ②由于同一个故障点导致的问题或发生同类型问题的，每再发生一次，扣 5 分，扣完为止。 ③整改方案延期提交的，每延期一周，扣 3 分，扣完为止。
安全管理	18	安全攻击事件及数据泄露事件	不发生安全事件	①受到安全攻击轻微影响业务运行扣 5 分；受到安全攻击但业务未受影响扣 1 分，扣完为止。 ②发生一般数据泄露事件，扣 5 分。具体的安全事件类型以中心或者安全第三方的通报及认定报告为准
		网络安全检查	顺利通过各项网络安全检查	①被上级单位、安全主管单位安全检查发现漏洞、风险、安全问题的，影响到中心安全检查结果的，每发生 1 次扣 5 分； ②倘若安全检查结果较差则扣 20-50 分 ③出现被中心安全管理部门、第三方测评机构或审计的系统安全评估和检查中发现或通报的安全问题的，每发生 1 次扣 2 分

		网络安全意识	做好网络安全培训，团队人员应明确知晓网络安全要求，具备网络安全意识。	①登录接口设置 123456、root 等这种极简单的弱口令、未设置锁屏、随意点开钓鱼邮件、未对重要系统进行安全漏洞扫描、编写没有对参数进行安全过滤的代码等等视为缺乏网络安全意识，每发现 1 例扣 1 分，扣完为止。 ②每月不定时进行访谈及安全问卷，如访谈过程中安全意识淡薄，考试不及格则扣 2 分，扣完为止
		安全生产	有效落实系统漏洞扫描、渗透测试、代码审计等信息系统安全自查工作，并对出现的安全风险事件及时制定整改方案并予以修复。	未能及时有效修复的每出现一例扣 0.5 分；高风险漏洞修复时限为 1 周，其他修复时限为 2 周。
制度管理	6	运营制度健全性	应按照招标要求、投标承诺、合同（以及附件）和中心相关制度要求建立运营管理制度：在运营工作上按照实际情况不断更新完善；服务规范应与服务目录保持同步更新。	①每缺失一项相关制度扣 2 分，扣完为止； ②每发现 1 项制度更新不及时扣 1 分，扣完为止； ③每发现 1 项因制度不完善造成执行困难的扣 1 分，扣完为止。
		运营制度执行有效性	严格执行运营制度，不发生违反制度的事件。	每发生一起违反运营制度的事件扣 2 分，扣完为止（除按照本考核体系已完成扣分的以外）。
人员管理	13	人员进退场管理	现场管理团队按照中心要求进行管理，严格执行中心管理制度	①人员进场、变更、退场等相关流程未按规定执行的，每发现 1 次扣 2 分，扣完为止； ②运营商应及时在系统上进行投入人员信息更新，如发现与现场投入人员不符的情况，每发现 1 次扣 1 分，扣完为止。

		人员现场管理与考勤	整体人员投入及出勤情况应符合投入计划和中心要求	①未严格执行考勤管理制度，每发现 1 次扣 1 分； ②未经批准，团队重要成员擅自脱岗或未达到考勤率要求的，每发现 1 人次扣 2 分； ③未按照要求及时更替技术能力与岗位不相符的人员，每出现 1 次扣 2 分； ④团队成员流失率或更替率每超 10%扣 2 分（中心要求的更替将另行评估）。
		办公秩序与人员行为管理	入驻人员严格遵守外包人员及供应商人员管理要求	①未佩戴胸卡者，每发现 1 次扣 1 分； ②未经批准，违规使用移动终端、移动介质或进行摄像拍照的，每发现 1 次扣 1 分； ③未经中心认可，擅自对场地设施进行变动（包括但不限于增加工位牌、增加摄像设施等），每发现 1 次扣 1 分； ④违反其他管理规定视情节严重程度每次扣 1-3 分。
		人员工作积极性和严肃性	服务沟通及时顺畅，满足要求；工作具有严肃性，按照已达成一致流程和工作机制、已发布的规章制度开展工作	①关键责任人在未经中心许可的情况下重要项目会议缺席，每发现 1 次扣 3 分； ②团队人员沟通态度或工作积极性问题，发生欺上瞒下，故意隐瞒，每被投诉 1 次扣 5 分。
运营生态管理	6	服务商管理与良性发展	建立项目服务商规范性管理体系，制定相应制度规范，保障在项目内供应商行为的规范性，构建数据运营良性发展生态体系。	①缺失重要管理制度，考核期内每发现 1 次扣 2 分； ②发生服务商对运营商的有责投诉，每发生 1 次扣 2 分。
		结算及备案管理	运营商按相关规范制度要求及时与服务商结算，运营商将服务商的相关材料按要求在中心备案。	①在结算过程中，因乙方原因造成延误结算的，每发现 1 次扣 1 分，扣完为止； ②违背相关规范制度要求实施结算的，每发现 1 次扣 3 分，扣完为止。 ③每发现一起材料未备案的扣 1

				分，扣完为止。
文档管理	8	文档提交完整率	安排团队积极配合并完成相关服务需求调研，形成服务要素单、业务方案和技术方案（按需）等文档，完整提交服务周报、月报以及其他必要材料；完整提供服务单验收材料。	提交的文档内容不完整、不规范的，每次扣 1 分；
		文档提交及时率	安排团队积极配合并完成相关服务需求调研，形成服务要素单、业务方案和技术方案（按需）等文档，且及时提交服务周报、月报以及其他必要材料。	未按时提交文档的，每发生 1 次扣 1 分，超过一周的，每延期一周追加扣 2 分；
投诉管理	5	投诉管理	不发生有责投诉，不被上级单位或第三方单位通报。	①中心各部门、各委办单位或第三方监管机构的有责投诉，受到投诉 1 次扣 2 分，受到投诉 2 次及以上该项不得分； ②上级单位或第三方单位通报存在安全问题或其他严重问题的，该项不得分。
其他	/	重大责任事故	不发生该类事故	①产生严重不良社会影响或者被业务、行业主管单位及领导通报的重大责任事故，扣 50 分； ②发生严重数据泄露事件，扣 50 分；发生较大数据泄露事件，扣 20 分； ③受到安全攻击致使业务受到严重影响的扣 50 分，受到安全攻击致使业务受到较大影响的扣 20 分。
		重点保障服务	/	能提供重要事件或重点时刻及时保障服务的，被中心或用户方正式表扬的，每发生 1 次，加 2 分，

				最多加 10 分。
		专业培训服务	/	应业主方要求提供专业培训服务，反馈满意的，每次加 3 分，最多加 15 分。
		高水平规划方案	/	应业主方要求提供经认可的高水平规划方案，经评审通过每个方案加 3-5 分，最多加 15 分。
合计：100 分			**含加分、扣分的总分最高为 100 分**	

3.5.2 违约金

★投标人应提供无条件响应本项违约责任要求的承诺函。

中标人每一个月度的服务管理质量评估分值应不低于 80 分，否则视为违约，处罚金额见处罚标准。

月度问题，在验收前完成整改的，可不扣违约金。

服务管理质量评估分值<60 分的视为中标人运营服务能力不合格，项目周期内连续 3 次或累计 4 次服务管理质量评估分值<60 分的，在扣除违约金基础上，采购方有权提出终止合同，责令中标人退出运营服务。

中标人在履行运营服务过程中出现重大事故时，由第三方监管机构界定责任边界和严重程度，采购方将依据事故严重程度计算重大事故违约金，并有权根据合同约定视中标人责任情况采取终止合同、将该中标人报财政部门备案、列入黑名单等措施。

重大事故违约金按以下方式确定：

序号	问题描述	罚款金额
1	因运营服务的人为失误导致服务中断	10 万元
2	依据本招标要求未能履行具体条款	20 万元
3	因运营服务的责任事故导致服务中断	20 万元
4	运营管理月度评分合格但得分 80 分以下	20 万元/次
5	因运营服务的责任事故导致数据丢失	50 万元
6	因运营服务的责任事故导致数据泄露	50 万元
7	因运营服务重大责任事故导致数据无法使用	100 万元
8	运营管理月度评分不合格的	100 万元/次
9	产生直接或间接财政经济损失	实际财政经济损失

3.6 服务交付质量评估和项目验收

在服务期内，采购方按先用后付、阶段评估、周期验收的方式对运营服务交付的数量和质量进行评估和验收。

（1）服务交付质量评估：原则上每 3 个月开展 1 次服务交付质量评估工作，对期间已完成交付的每 1 个服务单进行服务交付数量和质量的评估。根据中标人期间已完成实际交付的每 1 个服务单情况，经第三方监管机构审核和评估，明确各服务项有效完成数量、服务交付质量评估分值和质量系数，按照中标服务项单价计算服务费用（该服务单服务费=服务项单价×服务项使用量×质量系数）。

（2）内部验收：按需进行项目阶段性验收和 1 次内部总项目验收。采购方组织第三方监管机构、专家进行项目内部验收。

（3）最终验收：内部验收通过后，采购方将内部验收结果报主管部门进行审核。审核通过后即视为项目最终验收通过。

4 投标报价和付款方式

4.1 投标报价要求

投标人按数据运营服务内容逐项申报各服务项单价形成《投标报价明细》。

各投标人应详细了解项目实际应用要求、现状与各种可能产生影响的因素制定项目技术和实施方案，充分考虑在项目实施期限内各项工作所必须发生的各类费用及应承担的相关责任后进行报价，根据数据运营服务目录正确填写《投标报价明细》。一旦中标，《投标报价明细》的服务单价即为合同价结算依据。

本项目服务费应是投标人根据项目实际应用要求达到采购需求目标、完成项目所需的所有费用，包括提供数据运营服务所需劳务及各类成本，以及人员开支、系统测试、调校、试运转、培训等服务、有关保险费用、实施相关的措施费、制度流程规范研制费、资料整理编制费、财务费、利润、税金等费用，以及合同明示或暗示的所有责任、义务和一般风险，无论此等义务和风险是否在合同文件中详细指出。若招标文件提出的相关配置或要求中存在不合理或不完整的内容，投标人应在投标文件中进行补充和修正，所产生的费用应纳入到投标价中。服务过程中若发生类似知识产权、软件、专利费等费用，投标人应一并考虑并纳入到投标价中。

4.2 投标报价服务项内容、最高限价

序号	服务类型	服务目录名称	计费单位	最高限价（元）
1	基础服务类	数据采集接入	万条	120
			幅	90
2		数据抽取服务	张	564
			万坐标点	47
			年（或张）	200000/1100
3		数据标签	个标签	300
4		时空数据转换与处理	万点	200
5		对于历史数据的归档及销毁	张	550
6		数据质量检查	个	90
			张	60
			万个	5
			万坐标点	8000/150000
7		数据共享/开放/授权订阅服务	组	1000
8		数据统计分析及报表服务	次	4000-5000
9		数据挖掘建模	个	92000
10		数据分类分级检查	张	1500
11		数据加密、脱敏等控制	万条	5
12		应用安全监测分析及威胁情报服务	台*年	280
13		应用安全检查评估服务	台*次	165
14		应用安全基础管理服务	台*年	120
15		作业调度	个	45
16	应用服务类	数据开放运营接入服务	年	750000
17		公共数据上链服务	个	50000
18		主（专）题数据库建设	个	250000
19		数据可视化展现工作	个	92500
20		公共数据社会化应用服务	个	100000
21		数据共享/开放/授权运营服务	年	1000000
22		安全基线配置管理服务	个子系统	250000
23		综合运营保障服务	个系统（数据服务）/年	120000
24		数据安全风险评估、安全审核服务	万条	22
25		应用安全渗透测试服务	次	30000
26		安全审计服务	个子系统	30000

27		系统功能符合性评估和测评服务	次	20000

4.3 过程及验收管理

（1）运营管理平台：应按照采购方要求提供在线运营管理平台，需满足数据服务运营商、第三方支撑单位和采购方等不同用户角色的使用要求，满足服务单发放流程、交付流程、阶段工作量结算、项目过程及验收管理的相关使用需求，相关文档应在运营管理平台进行流转和归档；

（2）月度报告：服务期内，每个月服务结束后，在次月 10 个工作日内，数据服务运营商应按照采购方要求提交月度报告至第三方支撑单位。数据服务运营商应配合第三方支撑单位，自提交报告 10 个工作日内完成月度报告内容修改，并协助第三方支撑单位将修改后的月度报告提交至采购方；未按时提交以上材料将扣除数据服务运营商月度服务费 3%；

（3）阶段工作量结算：在第 6 个月及第 9 个月设阶段工作量结算点。数据服务运营商应按照采购方要求，在阶段结算节点后的 10 个工作日内提交相关材料至第三方支撑单位，并根据第三方支撑单位意见及时修改完善；数据服务运营商应配合第三方支撑单位，自提交材料之日起的 15 个工作日内完成阶段结算材料内容修改，并协助第三方支撑单位将修改后的阶段结算材料提交至采购方；未按时提交以上材料将扣除数据服务运营商相应服务周期对应服务费 3%；

（4）项目验收：本项目周期完成后应发起项目验收。数据服务运营商应按照采购方要求，在项目工作结束后的 20 个工作日内提交相关材料至第三方支撑单位；数据服务运营商应配合第三方支撑单位，自提交材料之日起的 15 个工作日内完成项目结算材料内容修改，并协助第三方支撑单位将修改后的阶段结算材料提交至采购方；未按时提交以上材料将扣除数据服务运营商相应服务周期对应服务费 3%。

4.4 工作量结算

（1）阶段工作量结算相关材料，经采购方初审后提交上级主管部门进行审定。阶段工作量结算经上级主管部门审定后原则上不做修改，并作为后续付款依据。

（2）本项目周期工作量结算，应在阶段工作量结算的基础上，结合本项目

周期工作完成、绩效达成、服务质量及各类违约情况统筹后提交上级主管部门审定，审定结果作为最终项目付款依据。

4.5 付款方式

中标人中标本项目后，服务费用按以下方式支付：

（1）第一笔预付服务费：合同签订生效后且招标人收到中标人开具的等额发票后的 10 个工作日内，支付项目中标金额的 35%作为预付服务费用于抵扣将来实际发生的服务费。

（2）进度服务费：通过中心组织的本项目周期验收且招标人收到中标人开具的等额发票后的 10 个工作日内，支付项目中标金额的 35%进度服务费。

（3）服务费尾款：最终验收通过后，采购方根据上级主管部门依据本项目合同条款审定的本项目周期服务金额，扣除各类违约扣款后差额进行支付。

采购人根据本项目周期结算服务金额与已支付服务费（预付服务费+进度服务费）的情况与数据服务运营商进行结算。若已支付服务费＜本项目周期结算服务金额，采购人在收到上级主管部门审定的本项目周期服务金额和中标人开具等额发票后的 10 个工作日内支付服务费尾款。若已支付服务费≥本项目周期结算服务金额，则按财政管理规定做好后续结算处理。

5 其它

5.1 投标要求

（1）投标人需介绍自己公司的背景情况和资信状况。

（2）投标人需介绍自己公司在类似项目的成功案例。

（3）由中标人原因造成的工期延误，由中标人赔偿采购方的损失。

（4）本技术需求书视为保证系统运行所需的基本要求，如有遗漏，投标人应予以补充，否则一旦中标将认为中标人认同遗漏部分并免费提供。

（5）投标人确保其技术建议的可行性以及所提供软件的完整性，若出现由于投标人提供的软件不满足要求或其所提供的技术支持和服务不全面而导致系统功能无法实现或不能完全实现，由投标人无偿补足，并负全部责任。

（6）投标人应陈述其项目管理模式。

（7）投标人应该建立完善的技术服务保障体系，形成闭环管理。

5.2 知识产权要求

本运营服务中形成的知识产权（包含需求分析、系统设计、软件程序、核心技术、数据标准、接口规范、知识库、专有方法、模板、工具包、培训材料、专有数据、技术文档、服务模式、运作模式等，但不限于上述形式）归采购方所有。中标人向采购方交付的信息系统已享有知识产权的，中标人应事先申明并保证采购方在许可范围内合理使用。

本运营服务中形成的知识产权的申请权、所有权与利益（包括：专利权、商标权、著作权、商业秘密专有权等，但不限于上述权益的申请权）归采购方所有。未经采购方书面同意，中标人及其合作方不得以任何形式自行申请。

中标人不得以任何形式侵害本项目中形成的知识产权。未经采购方书面同意，中标人不得以任何形式提供或出售给其他单位使用。若发生侵害行为，中标人则全额赔付采购方本项目中标金额以及中标人通过侵害行为获得的全部收益。

没有采购方明示的书面同意，中标人不能作出关于本项目或者其条款的任何新闻公告、媒体宣传或其他形式的公开披露。

中标人提供的产品和服务等不得侵犯任何第三方的知识产权。若发生侵权行为，一切法律责任、后果及损失均由中标人承担，采购方不承担任何法律责任及后果，且保留追责权。

5.3 保密要求

中标人因履行本项目而知悉的所有数据、信息和资料（包括但不限于账号信息、图表、文字、计算过程、任何形式的文件、访谈记录、现场实测数据、采购方相关工作程序等）以及因履行本项目而形成的数据、信息和任何形式的工作成果，均是采购方要求保密的信息。未经采购方书面同意，中标人不得对外泄露采购方要求保密的信息，不得用于其他用途，否则中标人需承担由此引起的法律责任和经济责任，包括但不限于直接损失、间接损失、律师费、诉讼费/仲裁费、调查费、公证费等。

中标人对采购方提拱的临时使用账号要保密，不得公开，对组件开发的账号密码需进行加密，避免信息泄露，确保信息安全。未经采购方的同意不得利用采购方的网络及平台进行短信、彩信发送，否则产生的一切后果由中标人负责。

中标人应采取必要的有效措施保证其参与本项目的人员（包括中标人的聘用人员、借调人员、实习人员等）无论是在职或离职后，以及中标人的合作方无论是合作中或合作终止后，都能够履行本项目约定的保密义务。若中标人人员或合作方违反本条规定，中标人应承担连带责任。

中标人（含中标人参与本项目的人员及合作方）未经采购方书面许可，不得以任何形式自行使用或以任何方式向第三方披露、转让、授权、出售与本项目有关的技术成果、计算机软件、源代码、策划文档、技术诀窍、秘密信息、技术资料和其他文件。中标人不以实施项目为名，侵害本项目各参与单位的技术、商业秘密或者知识产权。

本招标需求书仅作为投标人投标依据，未经采购方书面许可，不可转发第三方或随意传播。

以上内容的保密期限自投标人知悉保密信息起至保密信息被合法公开之日止。

5.4 备份与恢复

1、服务提供方必须制定数据备份策略，按需备份关键数据。

2、服务提供方必须制定数据恢复策略，以便发生故障时及时恢复；（具体标准参见 3.2.2 应急服务响应时间）。

3、服务提供方必须根据实际情况制定相应灾难恢复策略，以便发生灾难时快速恢复。

5.5 退出机制要求

发生以下情况，启动退出机制：

- 服务期内，如中标人提出退出要求，需至少提前 6 个月向采购方提出退出申请，经批准后需提供 6 个月的延续服务。
- 服务期满后，若双方不再续约，中标人无条件免费配合各方完成服务交接工作，服务交接期一般延续 6 个月。
- 服务期内，若由于中标人服务能力不能满足约定要求，例如：考核分数<60 分，采购方有权终止合同，责令其退出，并由中标人向采购方支付违约金，见 3.5.2。

退出机制启动后，中标人无条件协助采购方完成数据运营相关系统的迁移和退出。从系统迁移出的数据，包括但不限于采购方移交给中标人的数据和资料，数据运营系统运行期间产生、收集的数据以及相关文档资料等，中标人不得自行保留，也不得以技术手段恢复相关数据和文档资料。

如果中标人丧失履约能力、发生资不抵债或进入破产程序，采购人可在任何时候以书面形式通知中标人终止本项目的执行而不给予中标人补偿。该终止本项目将不损害或影响采购人已经采取或将要采取任何行动或补救措施的权利。

如遇国家、行业管理部门等机构的有关标准和规定调整的，导致本项目内容须做相应调整时，双方应按照公平、合理的原则共同协商修改本项目对应的合同的相关条款。

三、商务要求：

类别	要求
投标有效期	开标后 90 天
合同履约期限	自合同签订后 12 个月
付款方式	（1）第一笔预付服务费：合同签订生效后且招标人收到中标人开具的等额发票后的 10 个工作日内，支付项目中标金额的 35%作为预付服务费用于抵扣将来实际发生的服务费。 （2）进度服务费：通过中心组织的本项目周期验收且招标人收到中标人开具的等额发票后的 10 个工作日内，支付项目中标金额的 35%进度服务费。 （3）服务费尾款：最终验收通过后，采购方根据上级主管部门依据本项目合同条款审定的本项目周期服务金额，扣除各类违约扣款后差额进行支付。 采购人根据本项目周期结算服务金额与已支付服务费（预付服务费+进度服务费）的情况与数据服务运营商进行结算。若已支付服务费＜本项目周期结算服务金额，采购人在收到上级主管部门审定的本项目周期服务金额和中标人开具等额发票后的 10 个工作日内支付服务费尾款。若已支

	付服务费≥本项目周期结算服务金额，则按财政管理规定做好后续结算处理。
转让与分包	（1）本项目合同不得转让； （2）本项目不得分包。

四、投标文件的编制要求

投标人应按照《投标人须知》的相关要求及电子采购平台电子招投标系统要求编制网上投标文件，其中投标文件应包括下列内容（不限于下列）：

商务投标文件由以下部分组成：

1. 《投标函》
2. 《开标一览表》
3. 《投标报价分类明细表》
4. 《资格性响应表》
5. 《符合性要求响应表》
6. 《商务要求响应表》
7. 《与评标有关的投标文件主要内容索引表》
8. 《法定代表人授权委托书》（含法定代表人身份证、被授权人身份证复印件，提供被授权代表人近3个月任意一个月的社保关系证明或退休返聘合同等证明劳动关系的文件）
9. 《投标人类似项目一览表》：

包括类似项目的有效合同复印件，其中合同复印件指包含合同金额的合同首页和有合同双方盖章的尾页，否则不算有效的类似项目业绩，评审时不予考虑。

10. 投标人基本情况简介
11. 投标人营业执照（或事业单位、社会团体法人证书）、税务登记证（若为多证合一的，仅需提供营业执照）符合要求。
12. 依法缴纳税收和社会保障资金、没有重大违法记录的声明：

具有依法缴纳税收和社会保障资金的良好记录、参加本次政府采购活动前3年内在经营活动中没有重大违法记录的声明函，截止至开标日成立不足3年的供应商可提供自成立以来无重大违法记录的声明。

13. 财务状况及税收、社会保障资金缴纳情况声明函。

14. 享受政府采购优惠政策的相关证明材料，包括：中小企业声明函、监狱企业证明文件、残疾人福利性单位声明函等（中标人为中小企业、残疾人福利性单位的，其声明函将随中标结果同时公告）。
15. 投标人质量管理和质量保证体系等方面的认证证书。

技术投标文件由以下部分组成：

1. 供应商应详细描述针对本项目的实施方案;
2. 项目需求理解;
3. 整体运营服务方案;
4. 文档管理、验收方案及培训;
5. 经费管理方案;
6. 突发应急响应能力;
7. 各项目团队主管人员要求;
8. 企业实力、及类似业绩;
9. 保密措施。
10. 其他必要的说明。例如，供应商对本项目的合理化建议等。
11. 按照《招标需求》要求提供的其他技术性资料以及供应商需要说明的其他事项。

以上各类投标文件格式详见招标文件第六章《投标文件有关格式》（格式自拟除外）。