**南通市人社业务协同平台建设项目需求**

**一、项目背景**

（一）建设现状

省人社厅积极贯彻落实党中央国务院对社会保险省级统筹的要求，建设了数据全省集中、部门信息共享、流程统一规范、服务方便快捷、业务实时监控的人社一体化信息系统。按照省人社厅要求，2021年8月南通市全区域成功切换至省一体化系统。

2022年，建立了人社数据回流库。人社系统数据回流工作是从业务、服务、监管和决策等视角出发，全面深入数据资源挖掘、分析、应用和展现，促进各地市人社业务应用创新服务能力的一项重要工作，有利于进一步提升各地市人社局各科室（部门）的服务、监管、运维、决策水平，助力人社数字化转型及服务提升。

（二）存在的问题

目前南通人社数据目前外接渠道为南通市大数据局、中国银行、交通银行、招商银行、江苏银行等部门，存在问题如下：

1.对外交换数据量较大，无有效的接口安全访问管理

对上述部门对接转发省协同平台接口83个（人员基本信息、参保信息、缴费信息）所有对接数据均完全提供给第三方使用，无有效的管理控制，相关数据可能被多次转发、篡改造成严重的数据安全事故。

2.数据权限无控制

目前接口对接数据，无有效的数据权限控制，易造成严重的数据安全隐患。

3.无访问次数限制

目前所有导出数据均全部开放，没有针对不同接口、不同渠道进行访问次数限制。

4.无熔断机制

5.无访问审计及日志

没有记录各个请求的访问次数、访问日志，无法获取各个渠道的访问整体情况。

6.数据请求没有签名

目前针对请求报文体，没有对数据进行签名机制，容易产生被篡改、更换等漏洞和隐患。

7.重要数据没有加密

返回包含敏感数据时，报文体没有采用加密的手段，造成数据会被偷窥、泄露现象。

8.没有采用HTTPS加密

目前全部基于HTTP请求，没有采用HTTPS加密，不符合省人社数据安全规定。

9.缺乏有效数据展示

目前所有数据是碎片化式的，无数据展示，数据集中，无法直观看出问题数据等。

（三）项目建设的必要性和可行性

（1）项目建设的必要性

2022年5月20日，省人社厅印发《江苏省人社一体化信息平台共享交互体系升级方案》通知，要求各地需抓紧梳理本地应用与省人社一体化信息平台的各类交互点，对未按照相关安全规范要求设计的程序，制订整改计划和实施方案，完善已纳入管理的交互基本信息，做好接口的熔断限流等安全措施，确保交互平台的安全高效运行。

为进一步优化人社服务，优化发展环境，推进南通人社局的信息化环境建设，努力营造优质高效、便捷畅通的办事环境，落实省厅信息中心下发的关于《江苏省人社一体化信息平台共享交互体系升级方案》通知，做好与省人社一体化信息平台内外各类共享交互的管理工作，结合南通市人社局实际情况，整合现有服务资源，建立南通人社业务协同平台，切实与省人社一体化信息平台做各类数据交互，方便省人社一体化信息平台与本地信息化服务平台关联对接，同时利用协同平台与南通本地数据需求方进行接口对接，使信息中心能够统筹管理、高效服务。通过本项目建设整合南通人社及相关各部门的信息资源，促进信息资源共享，以此为契机，继续提升人社业务经办和公共服务水平，推动信息资源共享的建设和应用，对共享数据进行深层加工、利用，为政府决策提供快捷、可靠依据。

（2）项目建设的可行性

1.政策可行性

（1）《人力资源和社会保障事业发展“十四五”规划》

（2）《江苏省“十四五”人力资源和社会保障发展规划》（苏人社发〔2021〕67号）

（3）《江苏省人力资源社会保障一体化信息平台建设方案》（苏人社发[2019]181号)

（4）《江苏省人社一体化信息平台共享交互体系升级方案》

依照省一体化平台建设要求，结合南通人社数字化转型等各项创新政策措施，南通市人社局通过建设业务协同平台，将省一体化接口服务和本地接口服务进行整合封装，由平台统一管控并对外提供服务，供外联单位调用，并根据本地公共服务的实际功能需要，依托本地“回流库”进行接口的开发对接。

2.技术可行性

本项目按照“金保二期”工程标准、省一体化平台实施规范进行建设，技术能够满足管理、监督及服务的各项要求，并具有较强的可扩展性和兼容性。“金保二期”工程、省一体化平台实施规范形成了完备的业务、应用、技术、数据及网络的技术应用指导规范，制订了详细的发展规划和科学的方法论，为提供了标准体系指导规范。因此，技术可行性较强。

3.外部条件可行性

南通市人力资源和社会保障局具有完善的信息化管理体系和完整的队伍，领导高度重视，需求描述明确，能够为系统的应用开发提供有力保证。因此，外部条件可行性较强。

**二、****项目内容**

**（一）建设目标**

**1.构建统一的南通人社一体化共享交互体系**

南通人社一体化信息平台项目建成以来，实现了省人社与南通人社之间的纵向协同，以及南通人社与南通各委办局之间的横向协同，目前人社一体化数据交互需求仍在日益增多，亟需建立一套完整的人社一体化共享交互体系，使目前已有的和所有后续新增的交互场景都在人社一体化共享交互体系中有明确的位置并遵循相应的标准规范，确保达到安全可控的目标。

**2.实现所有的南通人社一体化交互业务受控**

南通人社一体化信息平台由于上线时间要求紧以及接口的特殊性原因，已上线的共享交互服务并未全部纳入平台监管,可能导致遗漏了部分接口服务或长期未对相关应用进行维护。一旦服务由于某些业务调用量爆发增长，或报错发生阻塞，无法迅速定位问题，同时服务使用的框架型漏洞爆发或被攻击时也无法及时进行补丁更新升级，错过最佳的应急响应时间。所以本次升级方案将梳理南通一体化信息平台所有对外数据交互场景，将场景与管理平台形成映射关系，将各场景全部共享交互服务统一纳入平台管理，实现交互业务的全面受控。

**3.针对南通人社一体化业务协同平台全面升级**

为实现南通人社一体化数据交换的全面受控，需要针对承担数据交换的平台能力进行全面升级，制定接口纳入后针对高并发压力、个人敏感信息保护、第三方不可调整接口的管理、原平台不支持协议无法纳入的接口服务、针对接口提供后外部单位二次转发的控制的解决方案，并依照方案对相应的平台完成升级改造，改造完成后进行充分测试后将对应服务纳入平台进行管理。

**4.南通人社一体化平台的交互体系标准**

南通人社一体化平台按照江苏省数据交换标准进行开发，满足省厅的接口管理规范要求，从接口的需求、审批、定义、测试、发布的全流程管理。

**5.构建南通人社数据仓库**

依托省一体化平台回流库与南通本地金保系统库，建设数字人社交换数据库（南通人社数仓），结合部省技术规范要求，建立南通人社数据治理标准。通过对业务特点、业务数据、用户行为等数据进行多维分析，抽取服务对象的特征，形成个人、单位、银行等服务对象的个人标签、画像平台，推动人社业务发展提高，提高数字经济服务业务、服务经济发展的能力。促进行业数据与人工智能算法深度融合，辅助领导决策、业务经办、服务优化，实现决策科学化、管理精准化、服务人本化。

**5.1通过平台实现多厂商共建模式**

为了构建标准统一、多数据源的大数据资源体系，数据资产可能需要由多家厂商共同建设。多厂商共建数据中台的目标在于促进数据资产的高效管理和利用。通过数据中台，不同厂商可以共同使用、开发其中的数据资产，并统一遵循约定的标准和管理实践，从而确保数据资产的一致性和可靠性。 数据中台的标准构建有以下几个主要方面： 1. 标准制定与协商：多厂商共建数据中台需要通过协商和共识来制定统一的标准和规范。这些标准可以涵盖数据格式、数据安全、数据接口、权限管理等方面，以便所有厂商都能够按照同一套标准进行数据管理。 2. 架构集成与接口对接：为实现多厂商数据资产的联合管理，数据中台需要提供统一架构集成和接口对接功能。不同厂商可以根据标准规范使用并开发数据资产平台上的数据。 3. 统一管理与监控：数据中台可以提供统一的管理和监控功能，方便对数据资产进行集中管理，并管理多厂商的协同开发使用。这包括数据质量监控、数据生命周期管理、数据访问控制等功能，以确保数据的可靠性和合规性。 多厂商共建数据中台的目标是通过统一的标准和管理实践，促进各厂商之间的数据资产共享与协同管理。这样，无论是数据的一致性、安全性还是可靠性，都能得到有效的保障，从而为多厂商合作提供更加稳定和高效的数据基础。同时为了解决多厂商共同使用数据中台互相影响的问题，并实现统一标准和统一管理，数据中台采取了以下措施：

1.项目管理功能：通过项目管理功能，数据中台能够将各个建设厂商的工作空间进行隔离。项目空间是数据资产管理服务平台管理数据源、作业和任务的基本单元。所有的开发工作都在项目空间中完成。

2.项目的创建和授权：在数据中台的管理中心，通过选择项目管理组件并点击项目管理菜单，可以进行项目的创建。项目的创建通常由建设方管理员或老平台系统管理员完成。系统管理员可以查看并管理所有的项目列表。创建项目后，需要将当前项目授权给相应的厂商角色。只有被授权的厂商角色的人员才能进入该项目进行开发。

3.用户权限管理和项目授权：在管理中心的用户管理模块中，进入用户权限管理系统，点击资源权限管理，并选择业务角色维护。右侧选择项目授权，并选择对应的厂商角色。在关联项目列表下，可以新增授权项目。这样，被授权的厂商角色包含的数据源可以被项目使用。

4.数据开发和作业开发：在数据资产管理服务平台的数据开发模块中，可以进入作业开发模块。不同的脚本或作业流程可以切换至不同的项目空间进行开发。这样，多个厂商可以在数据中台上共同建设，并通过项目管理功能实现工作空间的隔离，避免相互影响。

通过以上措施，数据中台支持多厂商共建并实现统一标准和统一管理。各个厂商可以根据授权的权限，在指定的项目中进行数据开发和作业开发工作。



**6.人社数字能力输出体系**

依托南通人社数仓、人社标签体系，精准运算分析形成企业、个人基础信息模型、企业、个人征缴数据模型、企业监察仲裁数据模型、惠企政策模型等，既满足人社对金融行业的服务又对人社数据的保障。

依据公共服务、社会保险、就业创业、社保卡、劳动关系、人才人事、公安户籍数据、工商法人数据、教育学历数据、民政婚姻/低保、医保学生参保、乡村振兴、残联、退役军人、地税征缴数据、卫计委和银行贷款数据等标签数，对个人自然属性、社会保障卡信息、教育情况、参保情况、就业情况和职业偏好，单位招聘情况、社保征缴情况、企业用工情况、监察、仲裁案件、政策享受情况和风险指数检测预警进行指标分析，并且列举个人身份标签和企业身份标签。对数字标签体系标签总数进行分析累计，并对个人标签、单位标签、高校标签和银行标签的标签数量、数据总量和标签详细情况进行分析。

**7.运营中心**

（1）数据交换监控

数据交换监控大屏是对任务最近执行的数据交换情况的管理与跟踪，提供系统运行的整体概览，包括当前系统最新任务运行状态的汇总，数据交换任务持续时间等信息。同时提供对数据集成任务的操作，包括任务的运行、状态展现（完成、错误终止、运行中、警告、异常终止）、排队情况、执行方式（自动、手动）等信息，以及按时间维度进行任务的排行展示等功能。

（2）数据资源目录监控

数据资源目录监控大屏主要对系统中的数据资源数据量的资产统计展示情况、数据资源目录的分布情况统计，以及资源数据的使用情况和资源更新情况的统计及浏览统计，以及Top n排行的详情数据的展示等内容信息。

（3）社保卡资金发放情况监控

展示社保卡资金各险种每月发放人数、金额等情况，供领导业务掌握社保卡资金收入支出等情况。

**三、建设规模**

1.目前现状：

a.目前南通人社数据通过库表共享和转发省协同平台接口两种方式与其他单位实现数据共享。库表共享包含：单位基本信息、人员基本信息、单位参保信息、人员参保信息、法人社保缴纳信息、自然人社保缴纳信息、单位欠费信息、工伤护理费待遇享受信息等共21项，通过定时任务执行方式，有时候执行失败导致共享失败，不能实时监控数据运行情况。

b.外部门申请数据共享需通过手工填单等方式申请权限，无操作留痕。

2.建成后成效：

a.能监控数据共享运行情况，及时发现问题并解决；

b.申请、审批、授权全流程系统留痕操作；

c.及时掌握社保卡资金发放情况，目前通过社保卡发放养老待遇、工伤待遇、失业待遇、养老代发及就业补助等，累计服务人数268万余人、累计发放金额32亿元。待遇进卡分为社保待遇、就业补贴、代发项目三大类，其中社保待遇展示了养老、失业、工伤等8项通过社保卡发放情况，就业补贴展示了创业贷款补贴、公共实训补贴、企业招聘奖励等11项通过社保卡发放情况，代发项目展示了事转企差额补贴、军转补贴、劳模津贴、国企职教幼教差额、离休干部春节慰问等5项通过社保卡发放指标数据、明细数据对大数据底座进行资产集成对接。

3.建设原则：

（1）全面受控原则

针对南通人社一体化涉及的所有交互场景全面纳入管控，同时针对服务交互的从发起到交互完成的全生命周期的身份认证、信息加密等进行全面管控。

（2）业务连续性原则

一体化共享交互体系的建设和升级，必须尽可能考虑减少业务活动的中断，尤其是关键业务过程免受主要故障的影响，并建立有效的灾备机制确保及时恢复。

（3）安全性原则

安全作为一体化数据交互体系的重要运行保障，必须尽可能考虑到鉴权认证、权限控制、加密解密、熔断控制、合规标准，从硬件、软件、网络等方面综合考虑，建立一整套的数据交互安全体系。要求采用国密算法对数据共享、传输等过程进行加密。

**四、具体建设明细**

包含但不限于以下内容：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 南通协同平台建设项目 | | | | | |
| 序号 | 建设内容（功能点） | | | | 备注 |
| 1 | 数据平台管理 | 统一门户 | 接入系统维护 | 支持接入系统新增、修改、删除和列表查询功能，并指定接入系统的集成方式是菜单级集成或系统级集成 |  |
| 菜单资源维护 | 支持菜单层级树形展示，菜单新增、修改、删除。绑定菜单和接入系统的关系。绑定菜单与URL资源关系。 |
| URL资源维护 | 支持URL资源的新增、修改、删除和列表查询功能。 |
| 用户信息查看 | 支持用户信息展示，密码修改功能。 |
| 登录登出 | 支持用户统一登录、统一登出。 |
| 权限管理 | 管理角色维护 | 支持分层级展示管理角色，对管理角色增删改操作。 支持指定管理角色可使用的菜单资源。 支持指定管理角色可分配的菜单资源。 支持指定管理角色可管理的组织机构。 支持指定管理角色可管理的业务角色。 支持为人员分配管理角色权限。 |
| 业务角色维护 | 支持查询展示业务角色，对业务角色增删改操作。 支持指定业务角色可使用的菜单。 支持为人员分配业务角色权限。 |
| 用户角色维护 | 支持以列表的方式查询展示用户信息 支持为用户分配关联管理角色 支持为用户分配关联业务角色 |
| 用户管理 | 用户信息维护 | 查询系统已经维护的用户信息 新增用户 修改选定的用户信息 删除选定的用户 |
| 组织机构信息维护 | 查询系统已经维护的组织结构信息 新增机构 修改选定的机构信息 删除选定的机构信息 维护机构关联的用户 |
| 数据源管理 | 数据源管理 | 1、支持数据源页面翻页展示 2、支持数据源增、删、改 3、支持数据源检索 4、支持数据源分组迁移 |
| 数据源种类兼容 | 数据库 | 1、支持关系数据库 2、支持数据源进行连通性测试 3、支持数据源连接池信息配置 |
| 文件系统 | 1、支持FTP、SFTP、HDFS等文件型数据源管理 2、支持数据源进行连通性测试 |
| 数据接口 | 1、支持Rest API、Soap API等接口数据源管理 2、支持数据源进行连通性测试 |
| 2 | 数据资产目录 | 目录管理 | 首页展示 | 所有部门用户可以通过门户主页查看资源目录信息，最新数据，最热数据，也可以通过关键字搜索信息。查看各资源总量数据。 |
| 目录集市 | 所有部门用户可以通过查询条件对数据进行筛选，查询结果在页面下方展示。查看数据详情，申请资源信息。不同的资源类型的信息详情内容不同。 |
| 目录管理 | 资源目录编目部门操作人员可以通过目录管理功能创建目录，并对目录未提交的目录进行修改、查看详情操作以及对目录信息列表进行检索操作。 |
| 所有目录 | 资源目录编目部门操作人员可以通过所有目录功能进行检索查询当前部门的所有目录，对当前部门已发布的目录进行变更升级及下架操作。 |
| 资源注册 | 资源申请查询 | 所有进行过目录资源申请部门的用户通过资源申请功能查询所有申请的目录资源，以及查看资源申请的审批流程及审批结果。 |
| 目录资源挂载 | 部门和信息中心的用户通过查询条件进行当前部门目录列表筛选，查看目录资源详情并可以对目录中已挂载的资源进行移除，对目录中未挂载的本部门资源进行挂载。 |
| 资源申请 | 目录发布审批 | 资源目录发布审批部门操作员登录系统通过查询条件筛选目录，并对申请列表中的目录进行审批操作，根据相关法律法规给出审批结果和审批意见。 |
| 目录资源挂载审批 | 目录资源挂载审批部门操作员登录系统通过查询条件筛选目录，并对申请列表中的目录资源挂载进行审批操作，根据相关法律法规给出审批结果和审批意见。 |
| 资源申请交换审批 | 目录资源交换审批部门，对申请的目录资源进行审批操作，一般交换审批分为三级审批，首先由资源申请部门进行审批，然后信息中心进行审批，最后由资源所属部门进行审批。 |
| 3 | 数据赋能 | 个人标签 | 自然特征 | 个人基本信息如姓名、身份证号码、性别、出生日期、年龄、民族等；户籍信息如户口性质、户籍所在地区划、常住地区划等；毕业生信息如学历、毕业院校等。 |
| 社会特征 | 就业、失业、失业待遇信息；就失业登记信息；个人就业信息；单位、个人参保信息；个人失业、失业待遇领取信息；就业困难人员认定信息；求职培训信息；创业大赛和创业项目信息等。 |
| 单位标签 | 自然特征: | 单位基本信息如单位名称、统一信用代码、所在地区划、单位类型、经济类型、单位所属行业、产业类别、隶属关系、单位性质等。 |
| 社会特征 | 单位从业人员信息、个人就业信息、招聘信息、政策享受信息等。 |
| 企业指标 | 社保信息 -征缴 | 企业近36个月社保缴存时间 |
| 企业近36个月社保缴费人数 |
| 企业近36个月社保缴费类别 |
| 企业近36个月社保缴费基数 |
| 企业社保缴存总数较上月下降20% |
| 企业社保缴存总数连续两个月下降 |
| 企业是否存在委托第三方代缴 |
| 社保信息 -欠缴 | 企业社保欠缴情况 |
| 企业连续两个月账户状态处于欠缴状态 |
| 企业缓/欠缴原因 |
| 企业缓/欠缴滞纳金类型 |
| 社保信息-工伤 | 企业工伤人员发生次数 |
| 就业信息 | 企业补贴类型 |
| 企业是否有补贴 |
| 信用数据 | 企业是否有过劳动仲裁案件 |
| 企业是否有过劳动监察案件 |
| 个人指标 | 基础信息 | 人员姓名 |  |
| 身份证号码 |  |
| 有效期 |  |
| 联系方式 - 手机号 |  |
| 是否三代社保卡 |  |
| 居住地址 |  |
| 居住地址更新时间 |  |
| 社保信息 | 个人近36个月社保缴费月份 |  |
| 个人近36个月社保缴费基数档位 |  |
| 个人近36个月社保缴费到账标记 |  |
| 个人近36个月社保缴费类型 |  |
| 个人近36个月社保缴费单位名称 |  |
| 个人近36个月缴费单位统一信用代码 |  |
| 个人社保账户首次缴费时间 |  |
| 个人最后一次单位开始缴费时间 |  |
| 个人最后一次单位连续缴存月份数 |  |
| 个人社保缴费状态 |  |
| 个人最近一次社保缴费日期 |  |
| 个人社保缴费单位名称 |  |
| 个人参保险种 |  |
|  |
| 岗位工种 |  |
| 个人过去36个月缴费单位个数 |  |
| 个人过去24个月缴费单位个数 |  |
| 个人过去12个月缴费单位个数 |  |
| 个人过去6个月缴费单位个数 |  |
| 人才信息 | 职称/专业 |  |
| 职称级别情况 |  |
| 技能级别情况 |  |
| 技能证书获取情况 |  |
| 就业信息 | 就业困难人员认定时间 |  |
| 就业困难人员认定类型 |  |
| 就业困难人员认定结果 |  |
| 就业状态 |  |
| 个人补贴类型 |  |
| 是否有个人补贴 |  |
| 4 | 运营中心 | 数据资产情况概览 | 实时展现各类数据资产信息，包括接口、库表等资产的数量、被订阅次数以及被调用次数。同时可以清楚了解当前接入外部各机构资产数量以及整合内部各业务条线资产数量。通过数据资产全景图，能够有效对人社信息资源进行全局管控，了解数据资产的来源、分布及使用情况，更好的协同各方组织开展数据工作，发挥更大的数据资产价值 | |  |
| 库表资源分析监控 | 展示当前已有库表资产数量、被使用次数、数据交换总量等信息。同时提供对库表资产使用热度排行、调用明细分析，方便管理者及时了解数据共享的效率和效果，为改进数据共享工作提供依据和支持。 | |  |
| 接口资源分析 | 接口资源分析从多种维度对接口资产应用情况进行分析，包括内外部调用量分析、接口资产调用热度分析，调用失败任务分析，实时调用情况分析等。有利于数据管理人员快速掌握接口资产的使用情况，调整接口资产共享策略。同时方便运维人快速跟踪资产使用情况，及时发现并处理相关问题。 | |  |
| 数据使用情况分析 | 通过对数据资产的使用部门、使用人员、使用数据的频率、方式以及应用场景的分析,以了解数据在支持决策制定和业务操作中的价值和作用。 | |  |

1）建设南通人社业务协同平台是实现业务系统之间服务治理与服务管理的产品。支持信息系统服务的统一管理，统一授权，加强数据的安全共享与交换。人社业务协同平台定位于横纵纬度的统一数据交换、统一服务授权、统一协同监控、统一协同管理。

横向协同上，满足内部电子政务服务和外部渠道接入服务的信息整合共享。

纵向协同上，实现省市之间达成数据交换管控。

建立南通市人社内部及对外各部门之间数据交换与共享的制度化与常态化，有效整合分散异构系统的信息资源，消除“信息孤岛”现象，为提高政府的信息化水平，灵活实现不同系统间的信息交换、信息共享与业务协同，加强信息资源管理创造通道和支撑条件。

2）充分运用省一体化平台回流数据，根据本地化业务需求、综合统计查询的需要、南通数据仓库标准化的建设需要以及满足综合部门数据共享交换的需要，结合部省技术规范要求，建立南通人社数据治理标准。

建立数据交换平台：数据交换平台部署在人社局内网，各部门的业务子系统实时为数据交换平台提供数据来源。

系统支持对标签的整体展示，支持标签的可视化配置管理，支持标签数据和标签应用情况的展示。

3）利用南通数据仓库和人社标签体系，通过大数据手段与人工智能的精准运算，形成人社数字能力输出。

4）构建数据管理平台

构建一个通用、开放、可持续发展的数据管理平台底座，将南通人社全系统的数据资产统一管理，实现数据资产的可见、可懂、可用和可运营，并将数据进行分级分类管理。

根据数据产生频率、数据产生方式、数据结构化特征、数据存储方式、数据质量要求等不同对数据进行分级分类管理，建立南通人社数据资产目录。根据业务数据应用领域，对公共数据资源目录中的数据数据产生来源、数据所属行业、数据应用领域、数据使用频率、数据共享属性、数据开放属性进行业务应用维度分类。

①数据供需平台

通过“供需管理”激发需求，能够保障数据需求方部门在发起需求时的标准规范。通过“中心审批”管理保障数据供需对接机制的规范；通过“部门审核管理”把控数据源头部门供给，支持数据目录和供需对接清单，实现数据共享的技术支撑。通过“验收管理”完善安全管理制度，保障数据供给和使用安全。通过“责任归集”和“负面清单”的管理机制和完善制度规范建设，同时能够强化部门责任，促进部门之间数据交换的合理性及时效性。

②数据资产目录

人社数据目录是面向数据资源开放共享、数据交换和数据分析等场景，为数据提供方与数据需求方之间搭建共享数据的统一平台，提供数据资源注册、发现、查询和获取的统一入口。通过数据目录的应用，实现数据资源共享发布、资源检索和下载订阅等相关功能，降低部门间沟通和系统对接的成本，提升数据资源利用率和应用价值。

③数据服务管理

可以将人社共享数据进行分类管理、如特定身份类、生物识别信息类、金融账户类、医疗健康类、行踪轨迹类、未成年个人信息类、身份鉴别信息类、敏感个人信息类，并且以Web页面快速封装成API接口，以API接口形式对外提供数据服务。通过实时统一的数据访问入口提供数据服务，一方面可以屏蔽共享异构数据的复杂性，同时也大幅降低了传统硬编码共享接口的工作量，显著缩短项目工期。

5）构建可视化监控平台

实时展示人社数据资产目录、人社数据共享交换以及社保卡资金收入支出情况。

**五、项目建设安全性要求**

**1.****最小化原则**

受保护的敏感信息只能在一定范围内被共享，履行工作职责和职能的安全主体，在法律和相关安全策略允许的前提下，为满足工作需要。仅被授予其访问信息的适当权限，称为最小化原则。敏感信息的。知情权一定要加以限制，是在“满足工作需要”前提下的一种限制性开放。可以将最小化原则细分为知所必须和用所必须的原则。

**2.分权制衡原则**

在信息系统中，对所有权限应该进行适当地划分，使每个授权主体只能拥有其中的一部分权限，使他们之间相互制约、相互监督，共同保证信息系统的安全。如果—个授权主体分配的权限过大，无人监督和制约，就隐含了“滥用权力”、“一言九鼎”的安全隐患。

**3.****安全隔离原则**

隔离和控制是实现信息安全的基本方法，而隔离是进行控制的基础。信息安全的一个基本策略就是将信息的主体与客体分离，按照一定的安全策略，在可控和安全的前提下实施主体对客体的访问。

在这些基本原则的基础上，在生产实践过程中还总结出的一些实施原则，他们是基本原则的具体体现和扩展。包括：整体保护原则、谁主管谁负责原则、适度保护的等级化原则、分域保护原则、动态保护原则、多级保护原则、深度保护原则和信息流向原则等。

**4.安全系统建设内容**

本项目的安全保障体系将在统一的安全策略指导下，充分利用和依托已有网络安全基础设施，通过建设安全技术体系、安全管理体系、安全服务体系，形成集防护、检测、响应、恢复于一体的安全保障体系，从而实现网络和通信安全、设备和计算安全、应用和数据安全，构建可信、可控、可管的安全体系。

**5.****网络安全设计**

应用系统安全将遵循《网络安全等级保护基本要求》(GB/T 22239-2019)中应用和数据安全的控制点，通过安全运维、安全防护、审计分析、安全制度四部分的部署加固，满足事前检测、事中防护、事后追溯的安全要求，结合安全服务对管理制度的完善，提供对重要信息系统起到一体化安全防护，保证了核心应用和重要数据的安全。满足三级等级保护对相关检测项目的要求。

**6.数据加密要求**

提供sm4国密加密算法对数据进行加解密，调用方拿到协同平台下发的密钥对参数进行sm4加密，然后把密文传输到协同平台，协同平台对密文用下发的密钥进行解密。

**7.国产化适配**

1）软硬件选型

（1）服务器

系统应可适配国产化基础平台，如鲲鹏服务器、龙芯服务器、飞腾服务器、申威服务器、海光服务器等。

（2）操作系统

系统可适配国产化基础平台操作系统，如中标麒麟、银河麒麟、统信UOS等。

（3）数据库

系统应可适配国产数据库，如达梦数据库、神通数据库、人大金仓数据库等。

（4）应用中间件

系统部署应用中间件可适配国产应用中间件平台，如东方通、金蝶等。

（5）终端及操作系统

系统使用所涉终端应可适配各类国产终端，如PC机、笔记本、移动终端等。

2）技术架构

应用系统应采用跨平台、可扩展、可移植、安全可靠的技术框架进行编程开发，尽量少采用组件、控件方式实现功能。不可采用单平台开发语言编程，避免系统重构、改造。

本系统采用数据开发技术可完全适配国产化基础平台。

本系统采用Springboot等Java技术架构开发，前端采用VueUI、Bootstrap等技术开发，可完全适配国产化基础平台。

**六、售后服务：**

1. 免费运维期为1年，自通过验收之日起计算。

2．免费运维期内，系统在使用过程中出现问题，中标方应当在1小时以内响应，一般故障须在2小时内解决，重大故障须在两天（自然日）内解决。

3.在系统上线运行后，中标供应商负责对采购人人员进行系统操作培训，培训方式须由采购人指定。

**七、其他要求**

1. 需配合业主完成等级保护三级测评、代码审计、渗透测试和漏洞扫描、安全加固、系统软件测评等工作。

2. 因本项目产生的开发成果(包括源代码、系统技术文档、软件、数据等)须完整交付给业主方，由业主方享有知识产权。未经业主方书面许可，中标方不得许可第三方阅读、使用或复制。

3. 中标方保证其开发成果及其开发过程不侵犯第三人的知识产权，如第三方以该产品侵犯知识产权为由提起诉讼，责任由中标方承担，并赔偿因此给业主方造成的损失。

**八、合同履行期限**：合同签订后六十个工作日内完成所有工作具备验收条件。

**九、付款方式：**合同签订后，采购人一个月内支付合同金额的50%；系统开发完毕经验收合格后，采购人一个月内支付剩余50%合同款。