# 中国环境监测总站

# 全国污染源监测信息管理与共享系统

# 维护服务方案

# 项目服务要求

**2021年 6 月**

## 项目背景

“全国重点污染源监测数据管理与信息公开能力建设”项目，于2015年立项，2016年完成了项目的硬件配置、软件开发与集成，2017年组织开展了试运行，2017年底系统正式上线使用并确定系统名称为“全国污染源监测数据管理与共享系统”。

“全国污染源监测数据管理与共享系统”用于采集全国已发放排污许可证企业的自行监测信息以及各地开展的执法监测信息。系统主要包括数据采集子系统、排放标准管理子系统、监测业务管理子系统、数据查询与分析子系统、移动app子系统以及数据交换共享平台。在企业自行监测方面，本系统与“全国排污许可证管理信息系统”互联互通、数据共享，系统用户为发放排污许可证的企业、全国各级环保部门以及第三方机构等。按照生态环境部要求，根据排污许可证发放进度逐步推进自行监测数据联网，企业在发放排污许可证后3个月内需在本系统录入自行监测信息，完成数据联网。另外，各级环保部门需在完成监督性监测后5个工作日内登陆本系统录入监督性监测信息，完成数据联网。

2021年，为继续保障系统运行正常，自行监测以及监督性监测数据联网工作顺利开展，需要对系统环境提供程序更新、系统功能和性能优化、系统稳定运行保障、系统安全保障以及数据安全保障等方面的运维服务。

## 项目目标

### 总体目标

对全国污染源监测信息管理与共享系统开展运行维护技术服务，在系统运行、数据安全、用户使用帮助和程序优化改进等方面进行保障，确保系统正常运行，从而保证联网和应用工作顺利开展，支撑环境管理。

在系统使用方面，保障系统支撑全国约37万家已发证企业在线填报自行监测方案信息和监测结果信息，支撑全国3000多个环保管理部门用户审核监测方案，查询分析监测结果。

### 具体目标

（1）根据业务需求对程序进行更新，针对软件程序运行过程中出现的各种问题进行定位、修复和更新。

（2）针对软件功能应用方面，在非程序BUG导致的问题影响到业务工作的情况下，进行必要地修改和完善。

（3）保障系统的安全，定期升级系统软件的基础程序包，更新相关防护软件，防止病毒、黑客入侵。

（4）防范应急突发事件，针对各类应急事件制定预案并定期进行演练。

（5）保障系统数据的安全，做好数据的备份工作，并定期进行数据恢复演练。

（6）优化程序和网络性能，保障大量用户（系统设计时使用用户为重点排污单位，预计为2万家。目前已接入近12万用户，最终增加到约37万）使用时，系统能够稳定运行。

## 运维地点

北苑大酒店901（中国环境监测总站提供的运维场所）。

## 运维服务范围和需求

### 服务对象

生态环境部级、省级、市级、县级共四级环保管理部门用户，中国环境监测总站以及各省、市、县级环境监测机构用户，已核发排污许可证企业用户，共约37万。

### 基础环境

 为保障系统的安全，系统采用了应用服务器部署在互联网端，数据库服务器部署在环保专网，应用服务器通过vpn接入专网访问数据库服务器的跨网段部署方式。

 本项目涉及的硬件清单如下：

| **服务器类型** | **数量** |
| --- | --- |
| I类数据库服务器 | 2 |
| 信息发布应用服务器 | 4 |
| 缓存服务器 | 2 |
| 企业填报应用服务器 | 4 |
| 前置交换服务器 | 2 |
| web应用服务器 | 2 |
| 视频服务器 | 1 |
| 流媒体服务器 | 1 |
| 视频图形工作站 | 2 |
| 网管服务器 | 1 |
| 网络与数据库审计服务器 | 1 |
| 入侵防御服务器 | 1 |
| NAS存储 | 1 |
| 安全区防火墙 | 3 |
| 数据区防火墙 | 2 |

### 服务内容

4.3.1 乙方提供运行维护服务至2022年2月28日。

4.3.2 提供全年法定节假日外7\*24小时的系统运行保障。系统出现故障时，确保1小时内响应。一般故障当天解决，当天更新系统。复杂故障组织专题小组，三天内解决并更新系统。

4.3.3 对发现的问题进行修复

因为业务需求变化，采集信息不全，以及外部系统传递数据不规范等原因导致的系统不能正常运行的问题进行修复，包括：

（1） 企业基础信息采集不全，补充采集监管级别，名录类别，监督性监管单位等信息。与名录库数据进行匹配，同步名录类别。与许可证平台对接，获取发证日期。

（2） 修改所有企业自行监测相关基础信息数据结构以及对应的程序对象，增加同步时间和同步来源。清理和修复已有未正确写入这两项信息的数据。

（3） 加入对行政区划数据的匹配。清查许可证导的数据行政区划有问题的数据，重新进行匹配以正常展示信息。

（4） 增加企业最新发布数据表，利用现有数据计算出最新发布数据后导入新建的数据表；

（5） 解决对许可证导入的方案信息，在排放标准数据格式不规范，排口编码不一致，排放设施编码与本平台冲突等方面存在的问题。整理和修复已有的错误数据；

4.3.4 对地方平台与本项目平台的对接，提供接口对接和数据上行下行的技术支持。

（1） 为自建平台的省份提供数据接口的联调。

（2） 定期清理地方平台传递上来的脏数据。

（3） 为自建省平台提供数据校验页面。

4.3.5 提供每天三次的系统运行监控，掌握各服务器运行状态，保障系统的稳定运行。

4.3.6 每周对系统运行的软件支撑环境进行升级检查，若有更新，则实施更新操作。

4.3.7 每个月进行一次应急演练，保证系统出现不同应急事件时，能及时有效地应对。

4.3.8 每天对数据库进行备份，每月进行一次恢复演练，保证数据备份的可靠性。

4.3.9 登记各类问题、事件、程序调整优化等事项，以及事项的处理过程及处理结果，并形成相关文档。

### 项目实施要求

4.4.1 进度要求

项目服务周期为合同签订之日至2022年2月28日。

系统问题修复方面要求发现问题当天修改，当天更新。对于修改用时超过一天，乙方应向甲方汇报并给出合理的修改计划。

系统优化方面要求在需求明确后根据具体的需求制定合理的计划。

乙方应根据服务内容制定详细的项目实施计划和实施方案，明确各项工作任务的执行策略、进度安排。进度计划按照服务内容、时间进行结构化分解，确定项目的重大节点和里程碑，提出有效的节点控制办法，保证项目的整体时间进度要求。

4.4.2 办公场地要求

运维服务方需提供满足运维团队提供系统服务需求的办公场地，并提供相关的办公基础设施，保证运维人员能在15分钟内赶到用户现场。

4.4.3 运维团队要求

需提供固定的运维团队，中标方需提供至少8名专职驻场人员，保证系统正常运行、用户使用技术支持、功能优化需求调研、软硬件和安全运维等日常工作。

4.4.4 技术要求

运维过程中对系统进行优化和调整时，新增功能应保证与现有平台技术的兼容性，优先考虑使用与现有平台相同的技术，确保系统采用技术的一致性，以便于后期维护。

现有系统采用J2EE体系架构，使用的技术主要有：

1、系统框架spring mvc，bootstrap

2、前端展示echarts，jsp，Ajax，jquery

3、数据库访问mybatis

4、移动端html5、andrio api，ios api

4.4.5 信息网络安全

 本项目涉及的安全包括应用安全和数据安全，应通过与运维人员签订安全协议，进行安全保密培训，加强系统的用户名密码管理，对设备、系统、业务应用的登录进行管理，定期对操作系统、业务系统及数据库系统等软件进行补丁更新，漏洞修复等安全加固措施。

4.4.6 应急保障

制定应急预案，并进行定期演练的目的是确保系统发生故障或面对意外灾难时，相关服务能在最短时间内得以恢复运行，最大限度地保证业务的连续性，将损失降低到最小程度。

乙方需了解甲方业务需求和服务质量要求，确定应急恢复计划的范围与目标，协助用户方设计提供系统应急恢复方案，以保证用户方业务的持续性与可用性。双方需充分沟通与讨论以完成应急恢复方案的设计。

应急恢复方案设计完成以后，双方共同参与，完成至少每年一次的应急方案的测试预演，以确定是否满足业务需要和达到设定的恢复目标。

本项目的应急措施应充分考虑到以下几种情况：

1、黑客攻击时的紧急处置措施

2、病毒安全紧急处置措施

3、业务系统遭受破坏性攻击的紧急处置措施

4、数据库安全紧急处置措施

5、广域网外部线路中断紧急处置措施

6、设备安全紧急处置措施

7、运维人员不在岗的紧急处置措施

4.4.7 系统配置变更发布管理

参照ITSS服务标准，具体要求如下：

1）建立运维档案库，包括运维工作中涉及到的所有资料，并实施配置管理流程，做到各类资料可回溯性。

配置库：软、硬件，组件，任务计划清单及变更历史资料。

根据变更、发布流程，维护管理软件更新的版本信息

2）规范变更流程，可保证由变更引起的对IT环境的影响降到最小，提高IT系统和服务的质量，为业务的快速发展提供更优质的IT服务，并且可以有效地实施其他相关管理流程，如发布流程、配置管理等。

3）通过建立、监控和维护发布管理信息，提供系统更新准确性、安全性和可追溯性保障。

### 运维服务产出报告

承建方必须每日做日常巡检记录；每月提交运维月报；如有运维变更，需提交运维重大变更申请表；如有硬件维修申请，需要提交硬件维修申请表；如有应急事件，需要提交应急响应服务记录；如有问题，需要提交问题记录。