政务数据安全风险评估与内控研究课题

技术服务需求

**一、项目概况**

本项目为政务数据安全风险评估与内控研究课题的技术服务项目。当前我省市场监管领域存在数据量大、覆盖面广、结构多样、关联关系复杂等特点，且其中涉及大量工作秘密、个人隐私数据等敏感数据。特别是在信息系统建设过程中，承建单位和第三方服务单位现场驻点人员数量多、变动快、管理难等问题较为突出，传统的网络安全防护手段不足以解决当前面临的数据安全问题，急需加强数据安全风险评估和内控管理。

本项目从福建省市场监管政务数据敏感发现入手,旨在实现数据从云端到终端的全过程闭环管控，实现对敏感数据自动扫描发现和敏感资产快速分级分类，有效提升数据安全内控管理水平。

**二、技术和服务要求**

**（一）服务内容**

1、识别福建省市场监管相关系统云端及终端敏感信息分布和不当存储，监控对敏感信息的使用并进行实时保护，制定多维度敏感数据分布地图。

（1）支持ORACLE、SQL SERVER、Hive、OceanBase、TIDB、MySQL、Odps、PgSQL、Mongodb等主流的关系型数据库、数据仓库、大数据平台、云数据库。

（2）支持上海热璞、武汉达梦、南大通用、巨杉等主流的中国国产数据库。

（3）具备敏感数据探测能力，自动发现敏感资产，系统内置的敏感数据类型。

（4）内置针对符合特征的敏感数据发现规则。

（5）支持敏感发现结果列表展示，包括表名、列名、敏感类型、数据抽样示例等，支持对发现结果进行校正。

（6）支持基于列的业务类型，设置脱敏策略，实现相同的业务类型同时设置脱敏策略。

（7）从表格、表格列、SCHEMA等维度归类敏感数据资产，形成多维度敏感数据分布地图。

2、零信任框架下动态异构网络的建模、表示与挖掘。

（1）研究福建省市场监管跨部门、跨业务、跨区域的系统数据流动安全性评估与预测方法。

（2）针对传播模型、因果关系、规则和常识、共现关系等关系，构建数据关系模型。

3、基于多元空间属性异质图（MS-AHG）的动态身份体系构建。

（1）对接触核心敏感数据的人员的权限进行细化与鉴权，建立包括账号、密码、IP地址、机器指纹、数字证书、应用程序、登陆时间等多维度的身份准入机制。

（2）支持身份的多因素认证，至少应支持应用程序名、IP地址、主机名、操作系统账户、数据库用户、数字证书、身份敏感标签、日期、时间、时间域、身份类别、有效时间、应用用户名、终端IP等因素的任意组合，系统根据多维身份管理策略，自动判别登录主体的合法性。

（3）对于不合规的用户访问予以阻断与预警，同时能够根据实际情况进行临时访问动态授权，阻断撞库、高频登录等异常行为。

（4）支持僵尸账号检测，对僵尸账号进行锁定，防止僵尸账号造成数据泄露。

（5）基于用户身份与数据资产关联关系，利用元知识指导单空间的异质网络构建和多元空间交融构建，通过刻画具有不同含义和对应不同数据源空间的个属性异质图，以及构建多元空间之间交互的属性异质图集合，实现多元空间属性异质图的构建。

（6）建立福建省市场监管动态身份体系，整个流动网络处于一个动态实时调整的状态中,从而实现对敏感数据精准性、差异化的安全防护，同时通过身份体系可将用户行为全过程留痕可追溯。

4、跨空间突发风险数据流传播主动监控与预测。

（1）构建福建省市场监管突发异常数据流动检测体系。

（2）生成跨空间异构数据流动图谱，构建“数据主体-数据关系-行为”的多层复杂网络，充分挖掘网络上的相关信息并进行相关分析，实现对突发异常数据流动行为的实时监控和预测。

（3）支持特权用户访问控制。

（4）根据应用程序名、IP地址、主机名、操作系统账户、数据库账户、数据库实例名、时间、U盾等实现敏感数据访问控制。

（5）限制过程、函数、包等对象访问敏感数据。

（6）视图中调用敏感数据管控。

（7）对访问身份设置敏感标签。

（8）限定、设置特定JOB作业访问敏感。

（9）支持策略中心全部策略、系统配置、资产配置（资产列表信息、数据源部署模式、数据源分组信息、敏感资产信息等）等进行备份与恢复。

（10）支持日报、月报、周报等生成，导出格式支持PDF/word。

5、“云端+终端”全过程数据安全闭环管控模型构建。

（1）具备政务云部署、监测能力。

（2）具备针对不同终端人员采用不同的安全权限进行访问能力，终端类型包括运维和开发终端、业务办理终端等。

（3）支持对终端信任应用保护策略，信任验证机制支持通过识别程序名、程序签名及安全标签（程序哈希值）三种方式对应用进行保护。

（4）具备对终端设备的扫描、监测、检测能力，能够针对设定的规则定期、不定期扫描、监测、检测终端设备上不当存储的敏感数据，并进行告警、锁定等操作。

（5）具备云端+终端联动功能，当云端检测引擎报告一个策略违规时，终端系统将执行“自动”响应规则。响应规则条件是基于检测匹配条件来触发操作，条件定义了系统触发响应规则操作的方式和时间，并提供了多种确定传入事件优先级的方式，以便进行重点补救并采取适当的响应。

6、数据安全风险评估及内控管理系统研发

根据研究内容，配合开展福建省市场监管数据安全风险评估及内控管理系统原型机的研发、部署和实战检验。

**（二）服务要求**

**1、实施服务要求**

投标人应提供项目实施的项目人员及组织机构、实施策略、实施计划、项目保障措施、质量控制措施、系统测试、验收、交付物等。

（1）项目人员及组织机构

投标人应成立合理的组织机构，建立健全保障项目顺利实施的各项管理制度和质量保证体系，安排足够的高素质人才参加项目的建设。在项目机构中应明确各岗位的职责、任职资格，确保工程顺利实施。

为保障技术服务质量，中标人在项目实施期间须组建现场服务团点，派驻至少3名技术人员提供5\*8小时驻点技术服务，驻点人员须为中标人正式员工，且具有数据库、数据安全等相关领域的实施经验。

（2）项目实施策略

投标人应从项目实施范围及内容、项目实施准备、需求调研与确认、实施方案制定、项目实施管理办法、沟通管理等方面制定实施策略。

（3）项目实施计划

投标人应在项目总体进度要求时间内就本项目提供项目实施计划及日程安排。

（4）项目保障措施

为保障项目实施过程顺利完成，投标人应从项目管理措施（技术管理、进度管理、知识库管理）、项目质量管理、质量保障体系、风险管理方面进行项目保障。

（5）项目质量控制

为保障项目交付质量，投标人应从项目质量控制方法、项目质量控制内容、项目控制标准等方面进行项目质量保障。

**2、售后服务要求**

（1）中标人提供1年免费质保服务，质保期从项目验收合格之日起开始计算。

（2）中标人在质保期内提供7\*24小时的服务响应，并在2小时内做出明确响应和安排。如需现场服务的，中标人应派遣具有解决故障能力的工程师在4小时内到达现场。

（3）中标人对系统软件服务时不影响原有应用系统的正常运行和效率，不涉及对原有应用系统重新设计。对系统软件的更新及升级时，未经采购人同意，不改变针对本项目定制的功能。

**3、项目交付成果**

（1）本项目所涉及的与运行版本一致的所有完整安装程序及技术资料。

（2）软件产品和设计成果需完整安装在采购人指定的服务器上，并保障系统运行稳定、访问正常。

（3）技术资料文档，参照软件文档管理指南（GB/T16680-1996 、 GB/T8567-2006）提供相应文档，至少包括软件使用及维护等方面的文档资料。

（4）技术文档内容应满足有关应用软件文档编制规范标准要求。提供的文档和资料均应以纸张和光盘为载体，文件格式为Word文档或其他可视化、未加密的文件。

（5）投标人应在投标文件中提供需求调研、测试阶段、实施阶段、运行阶段、项目管理的全部交付成果的清单。

**4、项目工期要求**

中标人应在合同签订后6个月内完成本项目的所有技术服务内容及验收工作。

**5、项目验收要求**

（1）中标人所提供的技术服务成果应满足“第三章 二、技术和服务要求”中的所有要求，若有一项不满足的，不予验收。

（2）中标人所提供的产品及其配套使用的相关软件，必须是正版的、合法的。软件按采购人验收标准（符合国家、行业或地方标准）、竞争性谈判文件、响应文件、合同等有关内容进行验收。

**6、培训要求**

（1）中标人必须在应用软件安装、调试、定制开发过程中现场提供分别针对系统管理人员、应用管理人员的培训。

（2）中标人的培训教员应是项目组成人员并具有扎实的理论基础知识及实际工作经验，必须具备熟练的中文会话和书写能力。

（3）中标人必须为所有受训人员提供培训教材，所有的资料必须是中文书写。

（4）所有培训应是免费的。

**7、**保密要求

（1）中标人应当对合同的内容、因履行合同或在合同期间知悉的或收到的采购人的财务、技术、产品、数据信息或其他工作上的文件资料、工作内容等予以保密，不得向合同以外的任何第三方披露。

（2）中标人进入采购人工作区域的工作人员需严格履行保密义务。

（3）中标人需了解有关保密法律法规，知悉应当承担的保密义务和法律责伍，并庄重承诺：

（a）认真遵守国家保密法律、法规和规章制度，履行保密义务；

（b）不提供虚假个人信息，自愿接受保密审查；

（c）不违规记录、存储、复制国家秘密信息，不违规留存国家秘密载体；

（d）不以任何方式泄露所接触和知悉的国家秘密；

（e）未经采购人审查批准，不擅自发表涉及未公开工作内容的文章、著述；

（f）若违反保密承诺，自愿承担有关法律后果。

（4）中标人违反本条约定泄露采购人的涉密信息的，应承担相应的法律责任，造成采购人损失的，中标人应当依法承担赔偿责任。

（5）本条款不因合同届满或解除而失效。

**8、其他要求**

（1）本项目不允许中标人以任何名义和理由进行转包，如有发现，采购人有权单方中止合同，且中标人必须赔偿由此给采购人带来的一切损失。

（2）本招标文件要求项目履行期间所发生的一切费用均包含在投标总价中。对于采购人提出的技术实现方式、手段和要求，中标人必须无条件服从并完成有关工作，不再另计开发费用。

（3）采购人在授予合同及项目实施过程中有权根据实际需求对本招标文件的服务内容进行部分调整。