青岛西海岸新区大数据公共服务平台信息安全风险评估与软件评测服务采购项目采购需求

1.项目说明

1.1 供应商中标后直至验收止，未经采购人同意，中标供应商不得以任何形式和理由转包或者分包；如出现上述情形，采购人向政府采购监督部门提出申请并经批准后，可取消其中标资格，并与其立即解除合同，由此引起的经济损失全部由中标供应商承担。

1.2 本章规定的各项技术规格若涉及到品牌、型号等，并不表明该标的被指定，而是仅供供应商做技术性的参考，供应商所投报的产品（服务）只要性能达到或超过采购文件要求（或没有重大偏离），都将被视为对采购文件作出了实质性响应。

1.3 采购文件中带“★”条款和第五章全部合同条款为实质性条款，供应商必须按照采购文件的要求做出实质性响应，否则投标无效。

1.4 除采购人拟采购进口产品通过政府采购监督部门审核外，供应商不得提供直接进口或者委托进口产品（包括已进入中国境内的进口产品）；否则，按无效投标处理。

1.5 带“※”标注的产品为供应商开标时需提供的样品，中标后供应商送至采购人指定地点封存。供应商提交的样品与投标文件不一致的，由供应商承担相关法律责任。

1.6 带“●”标注的产品为核心产品。

2.技术规格、数量、服务标准等要求

一、信息安全风险评估

1.1.服务目标

风险评估目的是分析大数据公共服务平台信息系统的安全状况，全面了解和掌握该系统面临的信息安全威胁和风险，明确采取何种有效措施，降低威胁事件发生的可能性或者其所造成的影响，减少信息系统的脆弱性，从而将风险降低到可接受的水平；可以定期了解信息系统的安全防护水平并为以后安全规划建设的提出提供依据和参考，综合平衡考虑安全风险与成本代价，为网络与信息系统进行风险管理奠定基石，帮助客户在降低风险、承受风险、转移风险等方面做出正确的选择。

风险评估阶段作为安全咨询服务中的重要组成部分，其为后续信息安全测评标准差距分析、整改提供的数据支撑。

1.2.服务依据

GB/T 20984-2007 《信息安全技术信息安全风险评估规范等管理规范和技术标准》

公安部、国家保密局、国际密码管理局、国务院信息化工作办公室联合转发的《关于信息安全等级保护工作的实施意见》（公通字[2004]66 号）；

公安部、国家保密局、国家密码管理局、国务院信息化工作办公室制定的《信息安全等级保护管理办法》（公通字 [2007]43 号）。

《信息安全技术信息系统通用安全技术要求》（GB/T20271-2006）

《信息安全技术网络基础安全技术要求》（GB/T 20270-2006）

《信息安全技术操作系统安全技术要求》（GB/T 20272-2006）

《信息安全技术数据库管理系统安全技术要求》（GB/T20273-2006）

《信息安全技术服务器技术要求》（GB/T 21028-2007）

《信息安全技术终端计算机系统安全等级技术要求》（GA/T 671-2006）

《信息安全技术信息系统安全管理要求》（GB/T20269-2006）

《信息安全技术信息系统安全工程管理要求》（GB/T20282-2006）

GB/T 18336-2001 信息技术 安全技术 信息技术 安全性评估准则

1.3.服务内容

本次项目风险评估内容包括但不限于：信息系统识别、资产识别、脆弱性识别、漏洞扫描、威胁识别、风险分析管理体系评估等，并撰写安全风险评估报告。

①系统识别描述

系统识别是风险评估实施的基础性工作，是进行相应加固的依据系统识别的工作主要包括：

识别信息系统的物理环境、网络拓扑结构和硬件设备的部署情况，在此基础上明确信息系统的边界，即确定对象及其范围；

识别信息系统处理的信息资产的类型，划分信息资产在保密性、完整性、可用性和保存周期等方面的等级；

对收集的信息进行整理、分析，形成对信息系统的总体描述文件。内容包括：系统概述、系统边界描述、网络拓扑、设备部署、支撑的业务应用种类和特性、处理的信息资产、用户范围和用户类型、信息系统的技术框架等。

②信息系统划分

依据系统识别描述的结果，按照信息系统的业务应用及组织管理、业务类型、物理区域等要素，将信息系统进行合理分解，划分出相对独立的应用系统，并在信息系统总体描述文

件中增加信息系统划分的相关内容。

③脆弱性识别描述

从安全技术和安全策略两个方面进行脆弱性评估，找到资产或资产组中可能被威胁和利用的弱点，包括物理环境、组织机构、人员、硬件、软件及通讯设施等各个方面，降低或者规避可能被各种安全威胁利用来侵害一个组织机构内的有关资产及这些资产所支持的信息系统。

④漏洞扫描描述

使用成熟的安全检测产品、软件、硬件设备完成指定内容的扫描并出具相应报告，内容如下：

查找网络结构、服务器主机、数据和用户账号/口令等安全对象存在的安全风险、漏洞和威胁；

查找操作系统本身的不安全因素，主要包括身份认证、访问控制、系统漏洞、端口、操作系统的安全配置等存在的问题；

检测网络信息的安全性，包括网络层身份认证，网络资源的访问控制，数据传输的保密与完整性、远程接入、路由系统的安全等；

评估应用系统（含软、硬件）、接口和数据信息的安全性，包括：数据库软件、Web 服务等。

⑤威胁识别描述

对系统主机采用可控制的、非破坏性质的攻击性测试，发现最严重的安全漏洞；

调查了解信息泄漏问题，包括主机网络、端口、操作系统类型、应用服务、账号、配置信息等；

查找系统远程漏洞，分析目标系统中的漏洞分布及形成原因；

⑥风险分析描述

结合现有部署的网络以及安全产品分析和评估信息系统的安全策略、资产管理、物理和环境安全、访问控制、通讯与运维管理、系统开发和维护、业务连续性计划、安全控制、安全执行等内容。

分析和评估整个网络在安全控制、安全使用等方面存在的问题；

⑦管理体系评估描述

通过管理体系审核、管理问卷调查、安全顾问访谈、安全策略分析、安全审计等方式开展安全管理体系评估分析，包括信息安全组织、安全策略、人力资源管理、系统开发和维护、

资产管理、物理和环境安全、访问控制、通讯与运维管理、业务连续性计划、安全事件管理、应急预案等多个方面。

管理体系审核是通过对现有的安全管理体系进行审核，了解现有管理体系文档与安全管理体系等相关国家和行业标准的符合情况。安全管理体系的文档包括现有的安全管理策略文档、制度文档、流程文档、方案文档、规范文档、应急计划、业务连续性计划等。

1.4.交付成果

a.《信息安全风险评估测评报告》

b.《信息安全风险评估测评过程文档》

二、软件评测

2.1.服务目标

软件验收测评：依据软件测评方案及国家有关软件质量检测标准，开展大数据公共服务平台软件验收测评工作，依据项目招投标书、建设方案、商务合同及项目开发过程资料，设计完善项目各个系统的软件测评方案，并对项目所属系统实现的功能、性能、安全性等进行符合性验证，及时准确报告测评期间发现的问题，并进行问题确认及修复验证，实现对软件质量的提升。

2.2.服务依据

GB/T 25000.51-2016《 软件工程 软件产品质量要求和评价（SQuaRE）商业现货（COTS）软件产品的质量要求和测试细则》

GB/T 15532-2008《计算机软件测试规范》

GB/T 16260.1-2006《软件工程 产品质量 第1部分：质量模型》

GB/T 16260.2-2006《软件工程 产品质量 第2部分：外部度量》

GB/T 18905.1-2002《软件工程 产品评价 第1部分：概述》

GB/T 18905.1-2002《软件工程 产品评价 第1部分：策划和管理》

GB/T 18905.5-2002《软件工程 产品评价 第5部分：评价者用的过程》

GB/T 8567-2006 《计算机软件文档编制规范》

GB/T 11457-2006 《信息技术 软件工程术语》

《信息安全技术 信息系统通用安全技术要求》（GB/T20271-2006）；

《信息安全技术 服务器技术要求》（GB/T 21028-2007）；

《信息安全技术 信息系统安全管理要求》（GB/T20269-2006）；

《信息安全技术 信息系统安全工程管理要求》（GB/T20282-2006）；

《信息技术 安全技术 信息技术安全性评估准则 第 2 部分：安全功能要求》（GB/T 18336.2-2008）

《信息技术 安全技术 信息技术安全性评估准则 第 3 部分 安全保证要求》（GB/T 18336.3-2008）

GB/T 18336-2001 信息技术 安全技术 信息技术 安全性评估准则。

2.3.服务内容

验收测评服务单位应依据项目的建设目标及国家相关软件质量检测标准，认真执行测试方案，发现各系统潜在的质量缺陷，以便进行及时修复，从而提升各系统的质量，为系统上线后稳定、高效运行奠定好的基础。最终形成符合国家相关标准的软件验收测试报告，为整个项目验收提供客观依据，并对测试中发现的问题，对整改情况进行回归测试。

①功能测评

测试各系统功能操作、业务流程操作、数据接口是否正确、准确，功能实现是否完整，以及与其他系统的交互是否有问题。测试时对软件的每个组成部分中的每项功能逐项进行测试。功能测试应覆盖系统软件中的所有功能点，对系统的功能进行业务、结构和技术等方面的分析，设计完善的测试用例。

②效率（性能）测评

性能测试包括负载和压力测试。通过负载测试，可以了解正常工作状态下，系统的工作情况和数据的交互过程；通过压力测试，可以了解系统在较大的负荷下的工作状态，为将来系统的工作情况做出预测，并找出系统中的性能瓶颈或性能弱点。

测试各业务系统的性能是否符合预期的要求，从而保证各系统快速稳定的运行。通过仿真模拟大量用户在一段时间内集中进行业务操作，以检验业务系统运营服务能力和运行支撑平台的资源利用情况，及时发现系统是否存在性能瓶颈，并针对测试过程发现的效率问题进行原因定位，提出优化解决建议。

③安全测评

主要验证软件的安全防护能力，发现软件在运行过程中，信息及数据的泄漏、重要数据的丢失、非法入侵、非法操作，定位安全漏洞和缺陷，并通过优化，解决软件的安全性问题，提升安全防护能力。安全性测试应包括以下内容：

1. 应用程序级别安全测试：应用安全测试验证系统的用户安全机制是否有效、权限管理是否严密，包括对数据或业务功能的访问等。

2. 系统安全漏洞测试：定位系统应用安全、代码安全、业务安全等方面安全漏洞，提

出系统安全加固解决意见。

④可靠性测评

测试各系统在各种异常条件下，如异常用户输入、异常操作、异常网络状态等情况，是否仍然可以稳定、可靠运行。主要是对软件在特定条件下维持其规定的性能级别的能力进行验证和测试，包括：

成熟性：验证软件为避免由软件中故障导致的失效的能力；

容错性：在软件出现故障或者违反其指定接口、操作模式的情况下，验证软件维持规定的性能级别的能力。

⑤易用性测评

对各系统的被理解、学习、使用和界面的一致性进行验证和测评。

易用性测试应检查软件以及软件执行过程中的界面、图形、文字、信息和标识是否容易理解，易用浏览，检查软件的输入、操作方式是否便捷、易用、易学，并验证软件和相关标识、行业要求、双方合同在易用性方面的符合性。

⑥维护性测评

对各系统的通用性、适应性、配置灵活性进行测试。

应验证软件提供的缺陷与失效原因诊断、修改、错误排除等方面的能力以及可扩展能力和相关标准、双方合同、行业要求的符合性。

⑦文档测评

对各系统相关文档的正确性、完整性、一致性、易浏览性的检查和验证。尤其是软件文档与程序之间的一致性验证。

⑧回归测试

回归测试：不仅针对发现的缺陷，还应根据更改和相应的影响域的分析说明，挑选、新增测试用例，确保问题消除并不引入新的缺陷。

2.4 交付成果 ：

（1）测试方案

依据招标单位系统建设要求及国家有关软件质量检测标准，制定切实可行的测试方案，测试方案需包括但不限于以下内容：被测对象整体业务、关键业务、技术架构分析，功能、性能、安全、可靠性、易用性、维护性、文档测试内容及测试方法，测试环境说明，项目风险分析，测试工作流程，测试计划，测试工具等。

（2）测试报告

中标单位应依据项目整体建设目标及国家相关软件质量检测标准，认真执行测试方案，形成符合国家相关标准的软件测试报告。测试报告应包含以下内容：

功能测试：对系统的功能进行业务、结构和技术等方面的分析，设计完善的测试用例，并完成测试用例的执行及执行结果的监控，报告测试发现的问题，提供功能测试报告。

性能测试：通过调查分析系统使用情况，建立性能测试模型，开发测试脚本，模拟系统使用场景，通过负载测试、压力测试等多种策略全面评估系统性能状况，并提交相关报告。

非功能测试：对系统的非功能性（可靠性、易用性、可维护性和安全性）进行业务、结构、技术分析，设计完善的测试用例，并完成测试用例的执行及执行结果的监控，报告测试发现的问题，提供相关非功能特性的测试报告。

文档测试： 中标单位应对测试期间提交的相关用户文档进行内容审查， 并及时报告所发现的问题，编制并提交详细的文档测试报告。

（3）缺陷报告

中标单位应对测试过程中发现的各类问题进行详细记录，并通过规范的缺陷管理工具管理测试过程发现问题，并最终形成完整的项目缺陷报告。

（4）修改建议

针对软件存在的缺陷，提出具体的修改建议，包括功能改进建议、性能优化建议、安全加固建议等。