武汉市城乡建设局网络安全等级保护测评
采购要求

一、项目概况

1、项目名称：武汉市城乡建设局网络安全等级保护测评。

2、项目工期：合同签订后180日内完成等保测评。

3、采购内容：

（1）信息系统基本情况：

序号	系统名称	拟定测评等级
1	武汉市智慧建管一体化服务平台	三级
2	武汉市建筑工人实名制管理系统	三级
3	武汉市城乡建设局工程项目审批系统	三级
4	武汉市建筑工程质量监督管理系统	二级
5	武汉市市民热线工作服务平台市城建局用户端	二级

（2）专家评审：由采购人组织，中标人承担专家评审费用。

（3）等级保护测评工作：根据以上信息系统基本情况，开展等级保护测评工作。

4、采购预算总额：29万元。

二、项目实施遵循标准、规范

《中华人民共和国计算机信息系统安全保护条例》国务院[1994]147号

《计算机信息系统安全保护等级划分准则》(GB17859-1999)

《关于加强信息安全保障工作的意见》中办发[2003]27号

《关于信息安全等级保护工作的实施意见》（公通字66号）

《信息安全等级保护管理办法》公通字[2007]43号

《关于加强国家电子政务工程建设项目信息安全风险评估工作的通知》（发改高技[2008]2071 号）

《信息安全技术网络安全等级保护基本要求》(GB/T 22239-2019)

《信息安全技术网络安全等级保护定级指南》（GBT 22240-2020）

《信息安全技术网络安全等级保护测评要求》(GB/T 28448-2019)

《信息安全技术网络安全等级保护安全设计技术要求》（GB/T 25070-2019）

《信息安全技术信息系统物理安全技术要求》(GB/T 21052-2007)

《信息安全技术信息系统安全等级保护实施指南》（GB/T 25058-2010）

《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/T20270-2006)

《信息安全技术操作系统安全技术要求》(GB/T20272-2006)

《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安全技术要求》（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 信息安全管理实用规则》（GB/T 19716-2005 ）

《信息技术 安全技术 信息技术安全性评估准则》(GB/T 18336.1--2001)

《信息安全技术 信息安全风险评估规范》（GB/T 20984-2007）

三、项目需求

按照《信息安全技术网络安全等级保护基本要求》(GB/T 22239-2019)、《信息安全技术网络安全等级保护测评要求》(GB/T 28448-2019)、《信息安全技术网络安全等级保护安全设计技术要求》（GB/T 25070-2019）、《信息安全技术信息安全风

险评估规范（GB/T 20984-2007）的条款要求，逐一对武汉市建筑工人实名制管理系统进行安全保护等级测评，开展信息系统等级保护测评工作，测评目标为武汉市建筑工人实名制管理系统。测评范围为项目目标所涉及的机房基础设施、网络环境、主机层面、应用层、数据库层及相关安全辅助设备与管理制度。服务目标为项目目标最终通过公安部门及相关部门的等级保护检查要求。

3.1 定级备案

依据《信息安全技术网络安全等级保护定级指南》(GA/T 1389-2017)以及相关标准对本次需要定级的信息系统进行定级、备案材料的编写，并协助取得监管机构颁发的《信息系统安全等级保护备案证明》。定级、备案材料需包含但不限于如下材料：

1、信息系统安全等级保护备案表

2、信息系统安全等级保护定级报告

3、附件（信息系统安全等级保护备案表表四附件）

（1）附件一：系统网络拓扑图以及详细说明

（2）附件二：系统安全组织机构及管理制度

（3）附件三：系统安全保护设施设计实施方案或改建实施方案

（4）附件四：系统使用的安全产品清单及认证、销售许可证明

（5）附件五：专家评审情况

（6）附件六：上级主管部门审批意见

3.2 等级保护测评

依据《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》、《GB/T 28448-2019 信息安全技术网络安全等级保护测评要求》、《GB/T 25070-2019 信息安

全技术网络安全等级保护安全设计技术要求》、《GB/T 28449-2018 信息安全技术网络安全等级保护测评过程指南》等标准的要求，对武汉市建筑工人实名制管理系统进行等级测评，出具符合格式要求的等级测评报告。服务目标为项目目标最终通过公安部门及监管部门的等级保护检查要求。

其中，系统网络安全等级保护测评范围应包含内容清单列举的所有信息系统所涉及的机房基础设施、网络环境、主机层、应用层、数据库层及相关安全辅助设备与管理制度，测评工作内容应包括安全技术测评和安全管理测评，至少包含以下内容：

3.2.1 安全技术测评

安全技术测评包括五个部分：分别是安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心。

1）安全物理环境

安全物理环境应至少包括：物理位置的选择、物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应和电磁防护等控制点。

2）安全通信网络

安全通信网络应至少包括：网络架构、通信传输、可信验证等控制点。

3）安全区域边界

安全区域边界应至少包括：边界防护、访问控制、入侵防范、恶意代码和垃圾邮件防范、安全审计等控制点。

4）安全计算环境

安全计算环境测评对象应至少包括：网络设备、安全设备、服务器设备、终端设备、应用系统和其他设备等；测评内容应至少包括：身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、可信验证、数据完整性、数据保密性、数据备份恢复、剩余信息保护、个人信息保护等控制点。

5）安全管理中心

安全管理中心应至少包括：系统管理、审计管理、安全管理等控制点。

3.2.2 安全管理测评

安全管理测评应包括五个部分：安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理。

1）安全管理制度

安全管理制度测评应至少包括：安全策略、管理制度、制定和发布、评审和修订控制点。

2）安全管理机构

安全管理机构测评应至少包括：岗位设置、人员配备、授权和审批、沟通和合作以及审核和检查等控制点。

3）安全管理人员

安全管理人员测评应至少包括：人员录用、人员离岗、安全意识教育和培训和外部人员访问管理等控制点。

4）安全建设管理

安全建设管理测评应至少包括：定级和备案、安全方案设计、产品采购和使用、自行软件开发、外包软件开发、工程实施、测试验收、系统交付、系统备案、等级测评、服务供应商管理等控制点。

5）安全运维管理

安全运维管理测评应至少包括：环境管理、资产管理、介质管理、设备维护管理、漏洞和风险管理、网络和系统安全管理、恶意代码防范管理、配置管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理、外包运维管理等控制点。

四、整体要求

4.1 测评实施原则

在项目实施过程中必须满足以下原则：

保密原则：对测评的过程数据和结果数据严格保密，未经授权不得泄露给任何单位和个人，不得利用此数据进行任何侵害招标方的行为。

标准性原则：测评方案的设计与实施应依据国家信息系统安全等级保护的相关标准进行。

规范性原则：投标方的工作中的过程和文档，具有很好的规范性，可以便于项目的跟踪和控制。

可控性原则：项目安排工作进度要跟上进度表的安排，保证工作的可控性。

最小影响原则：测评工作应尽可能小的影响系统和网络，并在可控范围内；测评工作不能对现有信息系统的正常运行、业务的正常开展产生任何影响。

整体性原则：测评的范围和内容应当整体全面，包括国家等级保护相关要求涉及的各个层面。

4.2 专用工具要求

本项目涉及工程实施和验收测试所需的工具，由投标方负责提供。用于网络安全等级保护测评的工具主要包括服务器安全测评工具、网络设备安全测评工具、终端计算机安全测评工具、网站等应用系统安全测评工具、端口扫描工具等。

4.3 安全管理要求

为做好全过程的安全保密工作，在等级保护测评前、中、后三个阶段都要做好安全保密工作。

(1)测评前

1）对实施人员要进行安全保密教育，制定安全保密措施；

2）签订安全保密协议。

(2)测评中

1）对被测单位的性质、机房物理位置、网络与系统、应用与服务、资料与数据、人员与管理等方面的信息进行严格的安全保密管理；

2）测评工具应经过严格测试和检验，确保不对被测评系统造成损失，工作结束后不驻留任何程序；

3）对被测单位信息系统的信息资产、发现的脆弱性和发生过的安全事件等威胁情况要控制知情范围；

4）对测评设备、介质进行严格的保密管理；

5）工作过程中对人员要实施封闭式集中管理；

6）对进场人员遵守被测单位的相关管理规定。

(3)测评后

1）认真清退各种文档、资料和数据并予以销毁，确保工作过程中敏感数据不被泄漏；

2）现场工作结束后，按被测单位的要求及时还原系统，确保系统中不遗留任何代码或可执行程序；

3）在其他风险测评任务或宣传材料中不涉及被测单位的秘密、敏感情况。

4.4 风险规避要求

项目开展工作涉及到单位重要信息系统和数据，在测评过程中必须加强安全保密管理与风险控制。

指定项目经理为专人负责网络安全测评过程中的安全保密管理工作，对测评活动、测评人员以及相关文档和数据进行安全保密管理，对重点设备的技术检测进行监督，对接入的检测设备进行控制。

等级测评人员需具备等级测评师证书或国家网络安全应用检测专业测评人员证书。项目实施人员需签订专项保密协议。

安全测评工作中可能出现的安全风险点，按照检测对象周密制定测评方法，根据被测评对象的不同采取相应的风险控制手段。不限于以下方法：

1）操作的申请和监护

在实施过程中必须遵守的相关操作章程，以防止敏感信息泄漏和确保及时处理意外事件。

2）操作时间控制

对测评直接影响系统工作时，尽可能避开敏感时期。

3）人员与数据管理

必须高度重视信息保密工作，加强资料管理，确保人员可靠、稳定和可控。测评与被测评单位之间应签署长期保密协议，测评人员与被测评单位之间也要有相应的约束和控制措施，按国家有关要求做好保密工作。

4）制定应急预案

根据测评范围界定的系统情况，在实施前制定应急预案。

5）关键业务系统风险控制

对影响较大的重要关键业务系统在无法搭建模拟环境情况下，原则上不采用测评工具，采用访谈、测评和简单测试的方式进行。

6）优化扫描策略

分类扫描:对不同的主机和设备类型执行不同的扫描会话，从而减少不必要的脆弱项目测试。针对扫描对象细化扫描策略：对不同类型的主机或设备，需要根据其上不同的应用和服务情况，有针对性地定制扫描策略选项。

7）数据备份与恢复

对业务系统和数据库主机，应对其上数据进行备份，防止测评过程中对设备与主机的损伤影响业务系统的正常运行。

8）厂商协作

厂商需要提供各应用系统的名称、版本、协议、开发语言、进程名和相应的端口号等信息，在测评之前，由三方共同分析测评对业务可能造成的风险，分析可能存在的问题。在测评过程中尽量规避这些风险。

4.5 其他要求

（1）供应商的技术方案中应有完备的保密管理、项目管理、质量管理等安全管理制度；

（2）投标人应详细描述本次信息系统安全等级保护测评的整体实施方案，包括项目概述、等级保护测评方案、测试过程中需使用测试设备清单、时间安排、阶段性文档提交等。

（3）投标人应详细描述测评人员的组成、资质及各自职责的划分。投标人应配置有测评资质的专业人员进行本次信息安全等级保护测评工作。

（4）本次信息系统安全等级保护测评实施过程中所使用到的各种工具软件（包括测试工具和报告编写工具）应符合国家相关要求，报告编写工具必有取得中关村测评联盟授权，经招标人确认后由投标人提供并在信息系统等级保护测评中使用。

（5）信息系统安全等级保护测评需要的运行环境（如场地、网络环境等）由招标人提供，投标人应详细描述需要的运行环境的具体要求。