

# 第三章 用户需求

## C包需求书

### 1、项目名称

项目名称：东方市社管平台公安分平台（东方市立体化治安防控（三期））项目（第2次）

### 2、项目背景

通过委托专业的网络安全等级保护测评服务机构，对招标人的信息系统安全保护等级进行需求分析，并协助招标人完成等保备案相关事宜。依据《信息安全技术网络安全等级保护基本要求》(GBT22239-2019)、《网络安全等级保护测评要求》(GBT28448-2019)，对信息系统的安全物理环境、安全通信网络、安全区域网络、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理等进行合规性检查，分析信息系统与网络安全保护等级要求之间的差距，并出具《网络安全等级保护测评报告》及提出具有针对性的整改意见。

### 3、项目工期和地点

项目实施工期：签订合同后 60 个日历天内交付测评报告，地点：用户指定。

### 4、项目需求

#### 4.1 测评内容

1、对招标人的信息系统进行摸底、分析和梳理，提出详细的测评方案及完成系统定级、备案工作。

2、逐一对信息系统进行安全等级保护测评，测评的内容包括但不限于以下内容：

(1) 安全技术测评：包括安全物理环境、安全通信网络、安全区域边界、安全计算环境和安全管理中心五个方面的安全测评；

(2) 安全管理测评：包括安全管理制度、安全管理机构、安全管理人员、安全建设管理和安全运维管理五个方面的安全测评。

3、完成测评工作后，出具符合等保主管部门要求的网络安全保护等级测评报告，提出整改意见。

#### 4.2 项目输出(包括但不限于以下内容)

- (1) 网络安全等级保护定级相关文件和报告；
- (2) 网络安全等级保护测评报告；

#### 4.3 测评对象描述

序号	被测系统名称	安全等级	被测系统描述
1	东方市立体化治安防控三期（卡口）	二级	该系统含 IVS3000 和东方市公安局大数据融合应用平台两个应用系统。IVS3000 是华为 CloudIVS 3000，支持视频调看、转发、回看、云台控制、视频上墙等视频管理基本功能、智能分析；东方市公安局大数据融合应用平台主要是东方市公安局大数据融合应用系统实现了对人脸、行人、汽车、三轮车、二轮车等目标的信息查询检索、智能化研判分析、轨迹追踪、多维布控等实战应用

#### 4.4 测评服务步骤

网络等级保护测评过程需按照《信息安全技术 网络安全等级保护测评过程指南》开展工作，等级测评过程分为四个基本测评活动：测评准备活动、方案编制活动、现场测评活动、分析及报告编制活动。测评双方之间的沟通与洽谈应贯穿整个等级测评过程。

##### 4.4.1 测评准备活动

测评准备工作包括编制项目启动、信息收集和分析、工具和表单准备。

详细要求见下表：

项目内容	工作内容	成果输出
项目启动	1. 组建测评项目组	向招标人提交 《项目计划书》 《提供资料清单》
	2. 编制《项目计划书》	
	3. 确定测评委托单位应提供的资料	
信息收集分	定级报告及整改方案分析	《系统基本情况分析报

析	1. 整理调查表单	告》
	2. 发放调查表单给测评委托单位	
	3. 协助测评委托单位填写调查表	
	4. 收回调查结果	
	5. 分析调查	
工具和表单 准备	1. 调试测评工具	确定测评工具（测评工具清单）《现场测评授权书》《测评结果记录表》《文档交接单》
	2. 模拟被测系统搭建测评环境	
	3. 模拟测评	
	4. 准备打印表单	

#### 4.4.2 方案编制活动

方案编制活动包括测评对象确定、测评指标确定、测试工具接入点确定、测评内容确定、测评指导书开发及测评方案编制等六项主要任务。

详细要求见下表：

工作内容	工作详细任务	输出成果
一、测评对象确认	识别被测系统等级 识别被测系统的整体结构 识别被测系统的边界 识别被测系统的网络区域 识别被测系统的重要节点和业务应用 确定测评对象	《测评方案》的测评对象部分
二、测评指标确定	识别被测系统业务信息和系统服务安全保护等级 选择对应等级的安全要求作为测评指标 就高原则调整多个定级对象共用的某些物理安全或管理安全测评指标	《测评方案》的测评指标部分
三、工具测试点确定	确定工具测试的测评对象 选择测试路径 确定测试工具的接入点	《测评方案》的测试工具接入点部分
四、测试	识别每个测评对象的测评指标	《测评方案》

内容确定	识别每个测评对象对应的每个测试指标的测试方法	的单项测评实施和系统测评实施部分
五、测评指导书开发	从已有的测评指导书中选择与测评对象对应的手册	《测评方案》的测评实施手册部分
	针对没有现成测评指导书的测评对象,开发新的测评指导书	
六、测评方案编制	描述测评项目基本情况和工作依据	向招标人提交《测评方案》
	描述被测系统的整体结构、边界和网络区域	
	描述被测系统的重要节点和业务应用	
	描述测评指标	
	描述测评对象	
	描述测评内容和方法	

#### 4.4.3 现场测评活动

现场测评活动通过与测评委托单位进行沟通和协调,为现场测评的顺利开展打下良好基础,然后依据测评方案实施现场测评工作,将测评方案和测评工具等具体落实到现场测评活动中。现场测评工作应取得分析与报告编制活动所需的、足够的证据和资料。

现场测评活动包括现场测评准备、现场测评和结果记录、结果确认和资料归还三项主要任务。

详细要求见下表:

工作内容	工作详细任务	输出
1. 现场测评准备	现场测评授权书签署	会议记录、确认的授权委托书、更新后的测评计划和测评方案
	召开现场测评启动会	
	双方确认测评方案	
	双方确认配合人员、环境等资源	
	确认信息系统已经备份	
	测评方案、结构记录表格等	

	资料更新	
2. 现场测评和结构记录	依据测评指导书实施测评	访谈结果：技术安全和管理安全测评的测评结果记录或录音 文档审查结果：管理安全测评的测评结果记录 配置检查结果：技术安全测评的网络、主机、应用测评结果记录表格 工具测试结果：技术安全测评的网络、主机、应用测评结果记录，工具测试完成后的电子输出记录，备份的测试结果文件 实地察看结果：技术安全测评结果记录 测评结果确认：现场核查中发现的问题 汇总、证据和证据源记录、被测单位的书面认可文件
	记录测评获取的证据、资料等信息	
	汇总测评记录，如果需要，实施补充测评	
3. 结果确认和资料归还	召开现场测评结束会	
	测评委托单位确认测评过程中获取的证据和资料的正确性，并签字认可	
	测评人员归还借阅的各种资料	

#### 4.4.4 报告分析及编制活动

在现场测评工作结束后，应对现场测评获得的测评结果（或称测评证据）进行汇总分析，形成等级测评结论，并编制测评报告。

测评人员在初步判定单元测评结果后，还需进行整体测评，经过整体测评后，有的单元测评结果可能会有所变化，需进一步修订单元测评结果，而后进行风险分析和评价，形成等级测评结论。分析与报告编制活动包括单项测评结果判定、单元测评结果判定、整体测评、风险分析、等级测评结论形成及测评报告编制六项主要任务。

详细要求见下表：

工作内容	工作详细任务	工作依据（模版）
1. 单项测评结果判定	分析测评项所对抗威胁的存在情况	等级测评报告的单项测评结果部分
	分析单个测评项是否有多方面的要求内容，依据“优势证据”法选择优势证据，并将优势证据与预期测评结果相比较	

	综合判定单个测评项的测评结果	
2. 单元测评结果判定	汇总每个测评对象在每个测评单元的单项测评结果	等级测评报告的单项测评结果汇总分析部分
	判定每个测评对象的单元测评结果	
3. 整体测评	分析不符合和部分符合的测评项与其他测评项（包括单元内、层面间、区域间）之间的关联关系及对结果的影响情况	等级测评报告的系统整体测评分析部分
	分析被测系统整体结构的安全性对结果的影响情况	
4. 风险分析	整体测评后的单项测评结果再次汇总	等级测评报告的风险分析部分
	分析部分符合项或不符合项所产生的安全问题被威胁利用的可能性	
	分析威胁利用安全问题后造成的影响程度	
	为被测系统面临的风险进行赋值	
	评价风险分析结果	
5. 等级测评结论形成	统计再次汇总后的单项测评结果为部分符合和不符合项的项数	等级测评报告的等级测评结论部分
	形成等级测评结论	
6. 测评报告编制	概述测评项目情况	等级测评报告 提交 招标人
	描述被测系统情况	
	描述测评范围和方法	
	描述整体测评情况	
	汇总测评结果	
	描述风险情况	
	给出等级测评结论和整改建议	

## 5、项目服务要求

### 5.1. 项目实施要求

项目实施过程中，投标人应遵循国家标准、行业标准。

---

在项目实施中投标人须做到：

1. 提供完整的系统实施方案和项目实施管理办法；
2. 提供详细的项目实施方案和计划进度说明书；
3. 项目实施完成后提供可靠的后期技术服务工作；
4. 严格按照双方确定的计划进度保质保量完成工作；
5. 规范项目实施过程中的文档管理。

## 5.2. 项目验收要求

中标人必须提供给业主详细的项目验收方案。

### 5.2.1 验收组织

成立由业主、中标人以及其他有关人员组成的验收小组，负责对项目进行全面的验收。

### 5.2.2 验收标准

- 标准化：项目验收最关键的指标，应确保测评过程符合国家标准规范；
- 系统稳定性：在测评过程中应确保软硬件环境的稳定性、运行正常；
- 系统文档：验收文档是否齐全、规范、准确、详细；
- 系统可操作性：交付成果清晰、通俗易懂。

## 5.3. 售后服务要求

对于现状测评过程中发现的安全问题，投标人应先出具问题汇总报告，并给招标人预留三十天的整改时间，整改完成后投标人提供一次全面问题复查，并出具网络安全等级保护测评报告。同时招标针对本次测评范围内的问题提供一年期的远程技术咨询服务。