# 河北省电子口岸信息安全等级保护测评项目比选文件

2020 年 6 月

## 一、投标人资质要求

*1、具备省级及以上信息安全等级保护工作协调领导小组办公室颁发的《信息安全等级保护测评机构推荐证书》。

*2、投标人应当具有满足等级测评工作的专业技术人员和管理人员，其中**信息安全高级测评师不低于 1 人（可从“中国信息安全等级保护网 www.djbh.net”-“测评机构”中查询，并提供相关截图）。**

*3、本项目的投标最高限价为 200,000 元（大写：人民币贰拾万元整）。投标人报价不得超过上述投标最高限价，否则按无效投标处理。付款方式：中标人每年出具合格三级等保测评报告后 30 日内，招标人支付中标总价款的三分之一。

*4、服务期：2020 年至 2022 年信息安全等级保护测评工作（每年 1 次三级等级保护测评，共 3 次）。

**以上资质带“*”的条款为必须满足项。**

## 二、技术要求

### 1、项目概况

2017 年 6 月 1 日起，《网络安全法》正式实施，其中，第 21 条明确规定，“国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改”。相关的文件均要求重要信息系统需尽快开展等级保护相关工作，以增加系统安全的规范性和有效性，提高用户的安全意识，增强网络的抗攻击的能力，保证被测系统正常运转。

本项目主要针对本单位的商务诚信系统的运行环境、应用架构、网络结构、安全控制、运行维护、操作规程、信息安全保障体系等各个环节做一次全面的评测分析。通过评测，分析定位信息系统安全风险和薄弱环节，制定信息系统安全风险管理策略，健全信息安全管理和保障体系，完善规章制度和操作流程。

### 2、特别说明

本招标文件中的所有内容仅供投标人了解本项目实施的要求所用，所有权属于招标方，未经许可，投标人不得以任何形式将有关的内容透露给任何第三方，同时，投标人同意采取有效措施，保证其接触本文件的人员不得对外披露和散布本文件涉及的有关信息和内容。

**3、测评目的**

本招标的宗旨在于通过对被测系统物理环境、网络设备、服务器群以及应用软件系统实施等级保护测评，明确该系统的安全建设现状，找出存在的安全风险，分析安全建设差距，提出安全整改建议，并以此为基础，进一步制定安全建设整改方案，完善保护措施，使该系统满足我国关于等级保护相应级别的具体要求。

**4、参照标准**

中标人应依据国家等级保护相关标准开展工作，依据标准包括但不限于如下国家标准：

- 《计算机信息系统安全保护等级划分准则》（GB17859-1999）
- 《信息系统安全保护等级定级指南》（GB/T 22240-2008）
- 《信息系统安全等级保护实施指南》（GB/T 25058-2010 ）
- 《信息系统安全等级保护基本要求》（GB/T 22239-2008）
- 《信息系统安全等级保护测评要求》（GB/T 28448-2012）
- 《信息系统安全等级保护测评过程指南》（GB/T 28449-2012）
- 《信息技术安全技术信息安全管理体系要求》（GB/T22080-2008）
- 《计算机信息系统安全等级保护通用技术要求》（GAT 390-2002）
- 《信息安全技术信息系统安全管理要求》（GB/T 20269-2006）
- 《信息系统安全工程管理要求》（GB/T20282-2006）
- 《信息系统等级保护安全设计技术要求》（GB/T 25070-2010 ）
- 《信息安全技术信息安全风险评估规范》（GB/T 20984-2007）

## 5、测评内容与流程

### 5.1 信息系统备案

协助招标方按照《信息安全等级保护备案实施细则》（公信安[2007]1360 号）文件要求完成定级、备案材料的整理及在公安机关相关部门备案工作。

### 5.2 初次测评

检查被测系统现状，参照《信息系统安全等级保护基本要求》（GB/T 22239-2008）从物理安全、网络安全、主机安全、应用安全、数据安全和安全管理等层面进行差距分析，依据《信息系统等级保护安全设计技术要求》（GB/T 25070-2010 ），对系统进行初次安全评估。

通过对系统现状的分析和梳理，发现系统现有安全措施与等级保护基本要求的差距，提出安全整改建议，以指导后续安全整改工作。

测评内容：

**物理环境测评：**包括位置、访问控制、防盗窃防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电磁防护等内容。

**网络系统测评：**包括网络架构、网络访问控制、网络安全审计、边界完整性检查、网络入侵防范、网络恶意代码防范、网络设备防护等内容。

**主机与数据库测评：**身份鉴别、访问控制、安全审计、剩余信息保护、入侵防范、恶意代码防范、资源控制等内容。

**应用系统测评：**包括应用系统身份鉴别、应用系统访问控制、应用系统安全审计、剩余信息保护、通信完整性、通信保密性、抗抵赖、软件容错、资源控制等内容。

**数据及备份恢复测评：**包括数据完整性、数据保密性、备份和恢复等内容。

**安全管理测评：**涵盖管理制度、管理机构、人员管理、系统建设管理、系统运维管理等方面。

### 5.3 等保整改

协助招标方按照《信息安全等级保护管理办法》（公通字[2007]43 号）、《关于开展信息系统等级保护安全建设整改工作的指导意见》（公信安[2009]1429 号）等有关管理规范和技术标准，制定安全管理制度、落实安全责任，建议安全技术设施，落实安全技术措施。

通过安全建设整改，确保信息系统通过相应级别的安全等级评测。

协助招标方完成整改。

### 5.4 二次测评

此阶段是等级测评完整实施阶段，通过对整改后的系统进一步分析和梳理，并按照《信息系统安全等级测评报告模版（试行）》（公信安[2009]1487）编写等级测评报告。

## 6、测评对象

本系统测评的测评对象包括以下几类：

1．主机房（包括其环境、设备和设施等）和部分辅机房，应将放置了服务于信息系统的局部（包括整体）或对信息系统的局部（包括整体）安全性起重要

作用的设备、设施的辅机房选取作为测评对象；

2．办公场地；

3．整个系统的网络拓扑结构；

4．安全设备，包括防火墙、入侵检测设备和防病毒网关等；

5．边界网络设（可能会包含安全设备），包括路由器、防火墙、认证网关和边界接入设备（如楼层交换机）等；

6．对整个信息系统或其局部的安全性起作用的网络互联设备，如核心交换机、汇聚层交换机、路由器等；

7．存储被测系统重要数据的介质的存放环境；

8．承载被测系统主要业务或数据的服务器（包括其操作系统和数据库）；

9．管理终端和主要业务应用系统终端；

10．能够完成被测系统不同业务使命的业务应用系统；

11．业务备份系统；

12．信息安全主管人员、各方面的负责人员、具体负责安全管理的当事人、业务负责人；

13．涉及到信息系统安全的所有管理制度和记录。

## 7、咨询服务

在验收合格后一年内为招标方提供信息系统安全咨询服务，涵盖系统建设、运维、管理等相关的安全问题，提供信息安全检查咨询和整改建议等技术支持服务。

## 8、安全意识和技能培训

针对技术人员、管理层提供不同类型的信息安全培训，培训内容包括网络安全基础知识、等保测评知识交流、网络安全法知识普及、安全常识培训、安全意识培训。

为招标方完成信息安全培训不少于2次/年。

# 三、测评应满足的原则

本次安全保护等级保护测评实施方案设计与具体实施应满足以下原则：

（1）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人的行为，否则招标人

有权追究投标人的责任。

（2）规范性原则：投标人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。

（3）可控性原则：测评服务的进度要跟上进度表的安排，保证招标人对于测评工作的可控性。

（4）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。

**（5）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的正常运行、业务的正常开展产生任何影响，保证现有系统 24 小时的不间断、稳定、安全运行。**

（6）非高峰期原则：漏洞扫描及渗透测试时间，应尽量安排在夜间或法定节假日期间，制定切实可行的测试实施细则；对意外导致的宕机等，应提供应急保障方案，切实保证关键系统能正常工作。

投标人应严格依照上述原则和国家等级保护相关标准开展项目实施工作。

## 四、交付物

工作计划、流程、内容、及成果交付，严格遵循相关文件，根据实际情况，开展信息系统的等级测评，测评报告内容及格式严格遵照《信息系统安全等级测评报告模版》（2015 年版）撰写。

项目实施验收前应提交真实可靠、客观公正的评估文档，文档应包括但不限于以下内容：

1)测评方案；

2)安全建设整改建议；

3)协助完成整改；

4)等级测评报告；

5)公安相关部门出具的信息系统安全等级保护备案证明；

6)协助完成信息安全培训。

## 五、评分标准

| 评审内容 | 分值标准 | 评审标准 |
| --- | --- | --- |

| | | |
|---|---|---|
| 商务部分（共 40 分） | 投标报价（20 分） | 以所有有效投标报价的最低价为评标基准价。投标有效报价与评标基准价一致得满分，投标有效报价每高于评标基准价一个百分点的扣 1 分。 |
| | 商务标响应情况（10 分） | 不能实质性满足采购文件重要商务条款要求的为无效投标。在满足招标文件重要商务条款的基础上，对投标人商务条款响应程度进行综合比较评价：<br>第一档，响应全面，描述完备、细致，完全满足 且部分优于采购需求，得 7-10 分；<br>第二档，响应较全面、细致，满足采购需求，得 4-6 分；<br>第三档，基本响应采购需求，但有缺陷或部分一般指标不满足需求，得 0-3 分。 |
| | 相似业绩（10 分） | 近三年内，每具备 1 个 10 万以上同类业绩，得 2 分，此项最高得 10 分;<br>**注明:**.1.以与最终用户签订的合同原件为准； |
| 技术部分（共 60 分） | 测评方案（15 分） | 熟悉用户网络以及安全现状，方案设计详细合理，安全性、扩展性强，能够按照标书要求编制针对项目的设计方案及提供技术支持服务方案，根据投标人提供的测评方案设计及测评技术指标、参数的可行性、先进性、实用性、合理性、扩展性等方面情况，由评委分三个档次在 1-20 分之间打分。<br>第一档：对本项目针对性强，技术方案先进、合理、完整，思路清晰，有完整、准确的网络拓扑图和连接图，符合国家及行业相关标准和规范，能完全满足招标人要求，得 12-15 分。<br>第二档：对本项目针对性较强，技术方案先进、合理，有完整、准确的网络拓扑图和连接图，符合国家及行业相关标准和规范，基本满足招标人要求，得 7-11 分。<br>第三档：对本项目针对性较弱，技术方案基本合理、基本符合相关标准和规范，但在满足招标人要求方面欠缺，思路欠清晰。无完整、准确的网络拓扑图和连接图。得 1-6 分。 |
| | 整改及方案（15 分） | 熟悉用户网络现状，方案设计先进完整，性能优越，能够协助完成整改得 12-15 分；<br>方案设计合理准确，性能满足招标文件要求，，能够协助完成整改得 7-11 分；<br>方案不够完整，性能基本满足招标文件要求的，能够协助完成整改得 1-6 分。<br>不能协助完成整改得 0 分。 |
| | 培训（10 分） | 按照项目实施的时间、人员、培训安排的优劣进行分档打分，培训内容包括网络安全基础知识、等保测评知识交流、网络安全法知识普及、安全常识培训、安全意识培训：<br>第一档，实施时间、人员和培训计划及培训内容方面安排合理可行，实施培训次数大于等于 2 次，得 9-10 分； |

| | | |
|---|---|---|
| | | 第二档，实施时间、人员和培训计划及培训内容方面安排合理可行，但有不足之处，实施培训次数大于等于 2 次，得 6-8 分；<br>第三档，实施时间、人员和培训计划及培训内容方面安排有缺陷，实施培训次数大于等于 2 次，得 3-5 分。<br>第四档，实施培训次数小于 2 次，得 0 分。 |
| | 售后服务承诺（10 分） | 第一档能够主动的提供技术支持和维护、及时相应故障服务的，得 9-10 分；<br>第二档能够主动的提供技术支持和维护、相应故障服务不及时的，得 7-8 分；<br>第三档不能够主动的提供技术支持和维护、相应故障服务不及时的，得 5-6 分。 |
| | 项目人员配置（10 分） | 1、 项目组测评师均具备测评资格证书，满足得 3 分，不满足得 0 分。<br>2、 项目组成员具备三年及以上测评经验的测评师，满足加 4 分。<br>3、 项目组渗透工程师具备 CISP-PTE（注册渗透测试工程师）证书加 3 分。 |

## 六、比选应答文件

比选应答文件应包括下列内容：

（1）营业执照；

（2）法定代表人（单位负责人）身份证明或授权委托书；

（3）等保测评推荐证书；

（4）登记测评案例；

（5）公司情况介绍；

（6）报价函；

（7）测评方案；

（8）整改方案；

（9）培训方案；

（10）售后服务方案；

（11）项目人员配置；

（12）其他规定的资料；