2024年网络安全等级保护测评服务

采购需求

## 采购标的需实现的功能或者目标，以及为落实政府采购政策需满足的要求。

为深入贯彻落实《中华人民共和国网络安全法》《教育系统党委（党组）网络安全责任落实情况考核评价办法》《关键信息基础设施安全保护条例》《教育部办公厅关于组织开展部属单位信息安全等级保护工作的通知》（教技厅函〔2015〕68号）、《信息安全等级保护管理办法》（公通字[2007]43号）、《关于推动信息安全等级保护测评体系建设和开展等级测评工作的通知》（公信安[2010]303号）、陕西省信息安全等级保护工作联系会议办公室颁发的《关于印发<陕西省信息安全等级保护安全建设整改工作指导意见>的通知》（陕等保办[2011]2号）等相关要求，进一步提高西安交通大学网络信息系统安全保障能力和防护水平，学校委托测评机构按照国家有关规定和标准规范要求对学校网络信息系统展开等级保护测评，并协助完成网络信息系统的安全建议整改，使网络信息安全防护能力达到信息安全等级保护相关要求，并取得符合主管部门要求的安全等级保护测评报告。

### 采购标的需实现的功能或者目标

本项目负责完成采购方**2024年度网络安全等级保护测评任务及相关售后服务**，网络安全等级保护测评任务包括网络（信息）系统定级、备案、测评和分析整改等服务内容，含**第3级保护系统8个**和**第2级保护系统15个，共计23个系统**。售后服务包括**网络安全事件处置和安全运维、系统渗透测试、重要时期网络安全保障、网络安全攻防演练和网络安全培训（含从业资格认证培训）**。

本项目分三个服务标段，具体如下：

**标段一：含6个三级系统和3个二级系统测评及相关售后服务。**

**标段二：含1个三级系统和6个二级系统测评及相关售后服务。**

**标段三：含1个三级系统和6个二级系统测评及相关售后服务。**

#### 网络安全等级保护测评服务

**各标段**的网络安全等级保护测评服务内容如下：

（1）**系统调研**：在采购方相关人员的协助下，对相关网络（信息）系统进行调研和梳理，全面了解采购方当前网络资产现状，编制测评规划。

（2）**定级备案**：根据系统调研实际情况，按现行的网络（信息）系统定级指南及相关法律法规文件要求，完成对本项目相关需完成备案系统的定级备案工作。

（3）**现场测评**：根据国家等级测评的相关标准及已编制的相关等级保护测评指导书对网络（信息）系统中的相关资产进行测评项的检查、记录检查过程和结果。

（4）**分析整改**：根据前述工作内容，分析网络（信息）系统安全情况与等级保护基本要求的差距，提供差异化测评服务，并进行风险分析，根据现场情况出具科学合理的整改建议，并协助采购方进行整改，直至网络（信息）系统安全保护能力达到信息安全等级保护相关要求。

（5）**测评报告**：根据前述工作内容，分析当前网络（信息）系统安全保护能力是否符合相应等级的安全要求，出具相关网络（信息）系统符合信息安全等级保护要求的测评报告。

（6）**项目验收**：整理项目过程中所有相关的过程文档，提交采购方相关人员，并在采购方的安排下完成项目验收。

#### 售后服务

##### 标段一的售后服务内容如下：

（1）**网络安全事件处置和安全运维**：根据采购方实际需求，协助完成各类网络安全事件的处置工作，包含通报文档撰写、处置过程技术支持和处置结果的统计等，同时协助用户完成校园网络安全的运维工作。

（2）**系统渗透测试**：针对新上线系统以及现有信息系统按客户需要开展安全检测（基于人工渗透性安全测试）查找系统可能存在的安全漏洞，结合黑白盒方式进行漏洞挖掘，协助进行安全漏洞的整改与复测。

（3）**重要时期网络安全保障**：负责在重大节假日或活动前期开展专项安全问题排查工作，开展安全加固，提前修复安全问题。在重大节假日或活动期间，提供安全技术支持，保障客户相关网站及重要信息系统的安全稳定运行，避免出现信息系统被非法篡改、挂马等安全事件发生，根据预设应急响应流程进行安全事件处置，最大限度地减少安全事件造成的损害，降低应急处置的风险。提供已发生安全事件的事中、事后的取证、分析及提供解决方案等服务。

（4）**网络安全攻防演练**：作为红方参加采购方举行的网络安全攻防演练活动，旨在发现蓝方的网络系统防御能力的薄弱点，并协助蓝方提升网络系统的整体防御水平。

（5）**网络安全培训**：根据采购方实际需求，完成对在职员工包括政策、安全意识培训和安全技术能力培训；为采购方的网络安全专业技术人员提供网络安全从业资格认证培训，资格证书必需为教育部认可的，如CISP（注册信息安全专业人员认证）和CISAW（信息安全保障人员认证）；为采购方完成网络安全宣传视频制作提供支持。

##### 标段二和标段三的售后服务内容如下：

（1）**系统渗透测试**：针对新上线系统以及现有信息系统按客户需要开展安全检测（基于人工渗透性安全测试）查找系统可能存在的安全漏洞，结合黑白盒方式进行漏洞挖掘，协助进行安全漏洞的整改与复测。

（2）**网络安全应急响应**：负责采购方的日常网络安全事件的应急需求响应，组织快速应对网络安全事件，根据预设应急响应流程进行安全事件处置，最大限度地减少安全事件造成的损害，降低应急处置的风险。提供已发生安全事件的事中、事后的取证、分析及提供解决方案等服务。

（3）**网络安全攻防演练**：作为红方参加采购方举行的网络安全攻防演练活动，旨在发现蓝方的网络系统防御能力的薄弱点，并协助蓝方提升网络系统的整体防御水平。

（4）**网络安全培训**：根据采购方实际需求，完成对在职员工包括政策、安全意识培训和安全技术能力培训；为采购方的网络安全专业技术人员提供网络安全从业资格认证培训，资格证书必需为教育部认可的，如CISP（注册信息安全专业人员认证）和CISAW（信息安全保障人员认证）；为采购方完成网络安全宣传视频制作提供支持。

### 为落实政府采购政策需满足的要求

根据《政府采购促进中小企业发展管理办法》（财库【2020】46号）规定，本项目采购标的为中小型企业制造、承建或承接的，投标人应提供办法规定的《中小企业声明函》，否则不得享受相关中小企业扶持政策。投标人应对提交的中小企业声明函的真实性负责，提交的中小企业声明函不真实的，应承担相应的法律责任。

本项目采购标的对应的《中小企业划型标准规定》所属行业为：**软件和信息技术服务业**。

## 采购标的需执行的国家相关标准、行业标准、地方标准或者其他标准、规范：

采购项目中所含的投标产品及制造商应符合国家有关部门规定的相应技术、计量、节能、安全和环保法规及标准，如国家有关部门对投标产品或其制造商有强制性规定或要求的，投标产品或其制造商必须符合相应规定或要求，投标人须提供相关证明文件的复印件。

服务商在提供测评服务过程必须按照国家现行信息安全技术相关的技术标准规范开展网络安全等级保护测评服务工作。相关标准如下：

**《信息安全技术 网络安全等级保护定级指南》（GB/T 22240-2020）、**

**《信息安全技术 网络安全等级保护实施指南》（GB/T25058-2019）、**

**《信息安全技术 网络安全等级保护基本要求》（GB/T22239-2019）、**

**《信息安全技术 网络安全等级保护测评要求》（GB/T28448-2019）、**

**《信息安全技术 网络安全等级保护测评过程指南》（GB/T28449-2018）。**

## 采购标的概况

（一）采购项目名称： **2024年网络安全等级保护测评服务** 。

（二）采购数量及计量单位： **网络安全等级保护测评1次和相关的售后服务** 。

（三）最高限价：标段一限价人民币 **45万** 元，标段二限价人民币 **24万** 元，标段三限价人民币 **24万** 元。

（四）交付时间：合同签订后**45**天内。

（五）交付地点： 西安交通大学 。

（六）付款进度安排： **标段验收合格后一次性付标段合同全款** 。

## 采购标的需满足的质量、安全、技术规格、物理特性等要求：

### 总体要求

根据国家《信息安全等级保护管理办法》(公通字[2007]43号)与《网络安全等级保护定级指南》（GB/T 22240-2020）及网络安全等级保护技术指标要求，完成网络（信息）系统定级、备案和测评等工作。网络安全等级测评工作须覆盖安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管等方面的内容，并根据现场实际情况完成风险分析工作,最终为完善等级保护安全防护体系提供指导依据。网络安全售后服务工作包括网络安全事件处置和安全运维、系统渗透测试、重要时期网络安全保障、网络安全巡检和网络安全从业资格认证培训。

### 定级备案及评测指标

网络安全等级保护工作共分为五步，分别是：“定级、备案、建设整改、等级测评、监督检查”。该项目主要完成系统的安全测评工作，依据安全技术和安全管理两个方面的测评要求，分别从安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理十个安全类别进行安全测评。

#### 定级要求

该项工作开展的主要依据是《网络安全等级保护定级指南》（GB/T 22240-2020）确定系统等级。

服务商应完成本项目标段中**未完成（或需变更）网络安全保护等级定级的网络（信息）系统的定级工作**。

#### 备案

网络（信息）系统的安全保护等级确定后，二级以上（含二级）信息系统的运营使用单位或主管部门应到属地公安机关办理备案手续。按照国家政策要求，跨省或者全国统一联网运行的信息系统在各地运行、应用的分支系统，向当地设区的市级以上公安机关备案。该项目系统应向归属地网络安全监察支队申请重要信息系统备案。完成备案的信息系统，将获得公安机关颁发的《**信息系统安全等级保护备案证明**》。

服务商须协助采购方完成本项目标段**未获取或需变更的网络（信息）系统安全等级保护备案证明的获取或更换**。

#### 等级保护测评要求

服务商在测评过程中要求按照《信息安全技术 网络安全等级保护定级指南》（GB/T 22240-2020）、《信息安全技术 网络安全等级保护实施指南》（GB/T25058-2019）、《信息安全技术 网络安全等级保护基本要求》（GB/T22239-2019）、《信息安全技术 网络安全等级保护测评要求》（GB/T28448-2019）、《信息安全技术 网络安全等级保护测评过程指南》（GB/T28449-2018）等相关的标准规范开展等级测评工作，对系统的安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理共10个层面进行安全等级保护测评。

服务商须按信息安全技术相关技术规范要求，完成本项目标段中**所有网络（信息）系统的测评服务****，并出具符合信息系统安全等级保护要求的测评报告。**

### 售后服务

#### 标段一售后服务包含如下内容：

##### 网络安全事件处置和安全运维

标段服务商必须安排**1名计算机相关专业人员**在采购方进行每周5天\*8小时的驻场运维服务，协助完成采购方各类网络安全事件的处置工作和网络安全运维工作，包含网络安全通报文档撰写、处置过程技术支持、处置结果的统计和安全应急以及安全制度建设，同时协助用户完成校园网络安全的运维工作，具体工作由采购方根据实际需求而定。**驻场运维服务期为一年整**，时间从人员正式驻场算起。

##### 系统渗透测试

渗透测试是通过模拟恶意黑客的攻击方法，来评估计算机信息系统是否安全的一种评估方法。这个过程包括对系统的任何弱点、技术缺陷或漏洞的主动分析，通常该分析是从一个攻击者可能存在的位置来进行的，并且从这个位置有条件主动利用安全漏洞。

标段服务商须按照国家和地方法规以及相关标准完成**不少于5个第2级保护系统的渗透测试服务**。所有渗透测试服务必须提供相关系统的渗透测试报告。服务商须协助完成发现问题的整改并完成整改后的复测直至漏洞完全修复。

成果文档（最终交付成果包括但不限于以下内容）：

**《系统渗透测试报告》。**

##### 重要时期网络安全保障

标段服务商负责在重大节假日或活动前期对西安交通大学网络安全开展专项安全问题排查工作，开展安全加固，提前修复安全问题。在重大节假日或活动期间，提供安全技术支持，保障客户相关网站及重要信息系统的安全稳定运行，避免出现信息系统被非法篡改、挂马等安全事件发生，根据预设应急响应流程进行安全事件处置，最大限度地减少安全事件造成的损害，降低应急处置的风险。提供已发生安全事件的事中、事后的取证、分析及提供解决方案等服务；**重保服务每年不少于2次。**

包括但不限于以下安全事件的保障服务：

 应用服务瘫痪；

 网络阻塞、DDoS 攻击；

 服务器遭劫持；

 恶意入侵、黑客攻击；

 病毒爆发；

 内部安全事故。

为确保西安交通大学在重要保障时期的系统安全运行，**期间需提供不少于1人的保障人员**，要求工作经验丰富的技术专家和咨询专家，能够支持西安交通大学在重要时期保障工作的开展，并且在经验的积累和传递上能够形成知识库和安全保障案例供内部分享和使用。

要求重保前配合西安交通大学开展网络安全工作大检查，加大网站的安全扫描，多轮次交叉检测、渗透测试、排查整改漏洞隐患，现场安全加固、配合应急演练。

在重保期间成立应急小组一周工作时段12小时值守待命，非工作时段24小时远程支持，各类应急工具和处理突发事件预案到位。

接到西安交通大学安全事件应急处置请求后，在第一时间启动应急处置预案，组织对事件进行分析研判，提出应急处置方案，采取有关技术措施，并针对已入侵系统进行调查取证、灾难恢复等安全服务工作，协助西安交通大学信息中心快速有效完成对突发安全事件的应急处置，尽量减小网络攻击对西安交通大学信息中心所造成的风险损失。在应急响应的各项环节中，应符合《中华人民共和国突发事件应对法》《中华人民共和国网络安全法》等法律法规和《国家突发公共事件总体应急预案》《国家网络安全事件应急预案》等相关规定。

成果文档（最终交付成果包括但不限于以下内容）：

**《重要信息系统及网络安全保障服务方案》；**

**《重要信息系统及网络信息安全事件应急处置报告》。**

##### 网络安全攻防演练

标段服务商需要根据采购方的网络安全攻防演习需求，组建**不少于2人的**技术团队队伍，作为红方参加攻防演习活动，发现蓝方的网络系统防御能力的薄弱点报送采购方，并协助采购方提升网络系统的整体防御水平。

##### 网络安全培训

（1）政策、安全意识培训

对在职员工的网络安全知识进行宣传培训。内容包括：网络安全法知识普及、典型信息安全事件知识案例讲解、安全保密意识建立以及前沿信息安全技术知识培训等。标段服务商必须完成**不少于2个学时的网络安全相关内容培训**，内容贴合国家网络宣传周主题。培训方式可采用线上或线下形式。

（2）安全技术能力培训

对信息系统管理人员和专业网络安全技术人员的技能培训。包括针对安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理相关的检查方法进行培训。标段服务商必须完成**不少于2个学时的网络安全技能相关内容培训**。培训方式可采用线上或线下形式。

（3）从业资格认证培训

标段服务商为采购方的网络安全专业技术人员提供教育部认可的**网络安全从业资格认证培训**，**培训名额为2个**，培训资质包括但不限于以下认证内容。

CISP:注册信息安全专业人员认证

PMP:项目管理专业人员资格认证

CISAW:信息安全保障人员认证

ITSS:信息技术运行维护服务认证

CISP-PTE:注册信息安全专业人员渗透测试工程师

CISP-PTS:注册信息安全专业人员-渗透测试专家

NSATP-A:注册网络安全渗透评估专业人员

NSATP-D:注册网络安全专业防御人员

（4）网络安全视频制作

标段服务商为采购方的提供不少于1个的网络安全视频制作。网络安全视频内容4-5分钟，题材内容主要围绕网络安全思想意识、宣传教育等内容。视频形式包含实景拍摄、动画制作等。

#### 标段二和标段三售后服务包含如下服务项目：

##### 系统渗透测试

渗透测试是通过模拟恶意黑客的攻击方法，来评估计算机信息系统是否安全的一种评估方法。这个过程包括对系统的任何弱点、技术缺陷或漏洞的主动分析，通常该分析是从一个攻击者可能存在的位置来进行的，并且从这个位置有条件主动利用安全漏洞。

标段服务商须按照国家和地方法规以及相关标准完成**不少于3个第2级保护系统的渗透测试服务**。所有渗透测试服务必须提供相关系统的渗透测试报告。服务商须协助完成发现问题的整改并完成整改后的复测直至漏洞完全修复。

成果文档（最终交付成果包括但不限于以下内容）：

**《系统渗透测试报告》。**

##### 网络安全应急响应

标段服务商在接到采购方的网络安全事件的应急处置需求，第一时间组织**不少于2人**的快速应对团队，对事件进行分析研判，提出应急处置方案，采取有关技术措施，并针对已入侵系统进行调查取证、灾难恢复等安全服务工作，协助采购方快速有效完成对突发安全事件的应急处置，尽量减小网络攻击造成的风险损失。**响应服务每年不少于4次。**

网络安全事件包括但不限于以下内容：

 应用服务瘫痪；

 网络阻塞、DDoS 攻击；

 服务器遭劫持；

 恶意入侵、黑客攻击；

 病毒爆发；

 内部安全事故。

在应急响应的各项环节中，应符合《中华人民共和国突发事件应对法》《中华人民共和国网络安全法》等法律法规和《国家突发公共事件总体应急预案》《国家网络安全事件应急预案》等相关规定。

成果文档（最终交付成果包括但不限于以下内容）：

**《网络信息安全事件应急处置报告》。**

##### 网络安全攻防演练

标段服务商需要根据采购方的网络安全攻防演习需求，组建**不少于2人**的技术团队队伍，作为红方参加攻防演习活动，发现蓝方的网络系统防御能力的薄弱点报送采购方，并协助采购方提升网络系统的整体防御水平。

##### 网络安全培训

（1）政策、安全意识培训

对在职员工的网络安全知识进行宣传培训。内容包括：网络安全法知识普及、典型信息安全事件知识案例讲解、安全保密意识建立以及前沿信息安全技术知识培训等。标段服务商必须完成**不少于2个学时的网络安全相关内容培训**，内容贴合国家网络宣传周主题。培训方式可采用线上或线下形式。

（2）安全技术能力培训

对信息系统管理人员和专业网络安全技术人员的技能培训。包括针对安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理相关的检查方法进行培训。标段服务商必须完成**不少于2个学时的网络安全技能相关内容培训**。培训方式可采用线上或线下形式。

（3）从业资格认证培训

标段服务商为采购方的网络安全专业技术人员提供教育部认可的**网络安全从业资格认证培训**，**培训名额为1个**，培训资质包括但不限于以下认证内容。

CISP:注册信息安全专业人员认证

PMP:项目管理专业人员资格认证

CISAW:信息安全保障人员认证

ITSS:信息技术运行维护服务认证

CISP-PTE:注册信息安全专业人员渗透测试工程师

CISP-PTS:注册信息安全专业人员-渗透测试专家

NSATP-A:注册网络安全渗透评估专业人员

NSATP-D:注册网络安全专业防御人员

### 其它安全保障

所有标段服务商还应提供的如下安全保障服务：

（1）配合检查服务

标段服务商必须免费协助采购方响应公安机关、教育主管部门以及第三方单位针对网络安全等级保护工作的检查工作。

服务内容包括协助我校准备和完善各类资料文档，配合检查过程中的答疑及技术支持及其他现场检查的响应。

（2）电话支持服务

标段服务商提供每周7\* 24小时不间断的电话支持服务，解答采购方在使用过程中遇到的问题，并及时提出解决问题的建议和操作方法。

电话响应时间小于10分钟，到达现场时间不超过2小时，解决问题不超过24小时。

（3）安全咨询服务

标段服务商须为采购方免费提供两年技术咨询服务，包括信息系统整改建设咨询服务以及其他相关安全咨询服务，一旦接到采购方的服务请求，技术工程师将立即开始提供服务，帮助采购方解决网络安全相关技术问题，全面配合采购方做好网络安全保障工作。

### 保密责任与赔偿承诺

1．服务商保密承诺

（1）标段服务商必须签订保密协议，严格遵守采购方有关保密的相关规定，不得泄漏采购方的任何机密；

（2）标段服务商技术人员必须签订保密协议，在技术服务期间，标段服务商对接触到的有关采购方工作活动、商业活动、技术情报和技术资料等文件进行保密。

2．赔偿承诺与措施

（1）在测评服务期间，如果出现因服务商责任，未能在承诺时间内恢复业务运行，采购方有权请第三方进行解决处理，由此所产生的一切费用由标段服务商承担。

（2）测评服务期间，标段服务商不符合或达不到合同中要求的技术服务标准，采购方可以提前终止或解除合同。

### 其它要求

1．**资质要求：****投标人必须具有公安部第三研究所颁发的《网络安全等级测评与检测评估机构服务认证证书》。**

2．测评人员要求：标段服务商必须为本项目成立**本地化项目组**，**组长（项目经理）必须具有中级以上测评师资质**；由组长统一负责，组长具有一定的技术及管理知识和经验，能容易地与西安交通大学相关人员沟通，能很好的执行与完成测评工作，并根据适当情况增加测评人员。现场测评成员应**至少含1名高级测评师**，**中级及以上测评师不少于4人**，**参与人员不少于7人；现场测评人员不得少于5人**。参与本项目的测评师须提供投标截止日前半年中任一个月社保缴纳证明及网络安全等级保护网（www.djbh.net）查询（信息查询<机构人员-正文>）截图。

3．标段服务商应按等级保护测评要求制定测评过程中产生的文档，做到科学、规范、详尽、统一。

4．**投标中标：本次采购分为三个标段，三个标段可兼投，但同一投标人最终中标的标段数量不超过一个，按照标段一、标段二和标段三的顺序依次确定中标人。**

5．标段服务商中标后，**先付中标价10%的履约保证金再签订合同**，履约保证金于**项目标段验收合格并完成标段全部售后服务**后**无息退回**。

## 采购标的需满足的服务标准、期限、效率等要求

1. 质保期： 本项目标段**质保期为两年**。质保期满后，仍需提供专业维修服务，投标人在投标文件中需注明维修服务单项报价。
2. 服务响应时间：接到维修电话后4小时内给予明确答复，8小时内到达现场维修。维修人员到现场后若问题特殊无法现场修复的，供货方需在24小时内给出合理解决方案。

## 采购标的的履约验收标准

标段服务商在完成网络安全等级保护测评服务后向采购方交付满足本投标文件技术参数要求的验收文档。

|  |  |  |  |
| --- | --- | --- | --- |
| 现场的检验指标及方法 | | | |
| 序号 | 功能或指标 | 验收方式或测试方法 | 履约范围 |
| 1 | 测评报告 | 公司出具的《网络安全等级保护测评报告》原件 | 标段所有评测的信息系统 |
| 2 | 渗透测试报告 | 公司出具的《信息系统渗透测评报告》原件 | 标段所有三级系统 |
| 3 | 备案证明 | 公安局出具的《信息系统安全等级保护定级备案证明》原件 | 标段需要取证、换证的信息系统 |
| 4 | 项目完工报告 | 公司出具的《项目完工报告》原件 | 标段所有评测的信息系统 |
| 5 | 整改建议报告汇总 | 公司出具的《整改建议报告汇总》原件 | 标段所有评测的信息系统 |
| 6 | 渗透测试报告汇总 | 公司出具的《渗透测试报告汇总》原件 | 标段所有评测的信息系统 |
| 验收时是否需要供应商提供样品 | | 是□ | 否☑ |
| 验收时是否需供应商提供必要的其他设备 | | 是□ | 否☑ |
| 除现场验收外，需提供的其他验收要求 | | | |
| 除现场验收外，是□否☑需提供第三方检测报告 | | 对于检测机构的要求：国家正规检测机构，出具的检测报告由验收复核专家认可之后作为验收复核通过的主要依据。  对于检测执行标准的要求：各项检测项目标准以检测机构按照行业相关要求最新适用并执行的标准为准。 | |