一、项目概况

项目名称：2025 年厅业务系统等级保护测评服务项目

预算金额：85.5 万元（最高限价 75 万元）。

对陕西省财政厅的业务信息系统开展等级保护测评工作，系统数量 15 个，等保级别三级。（在测评系统总数不变的情况下，甲方可根据实际工作需要自行调整测评系统）。

服务内容

（一）系统调研：在系统相关人员的协助下，对信息系统进行调研和梳理，了解系统当前信息系统资产现状。

（二）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信息系统中的相关资产进行测评项的检查、记录检查结果。

（三）分析整改：根据前述工作内容，分析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，可根据现场情况出具科学合理的整改建议及整改方案，配合采购单位安全整改工作。

（四）结论报告：根据前述工作内容，分析当前信息系统安全保护能力是否符合相应等级的安全要求，针对整改项进行再次测评,提供安全等级符合性测评服务，出具相关系统测评报告。

（五）配合验收：整理项目过程中所有相关的过程文档，提交系统相关资料。

三、项目技术标准及要求

（一）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《信息安全技术 网络安全等级保护基本要求》GB/T22239-2019 要求，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、安全运维管理等方面的内容，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。

（二）第一阶段：等级保护

信息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。

1.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。

2.备案：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》。

3.等级保护测评要求

供应商在测评过程中要求按照《计算机信息系统安全保护等级划分准则》(GB17859-1999)、《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。

测评指标：等级保护技术要求（三级）

安全层面	**安全控制点**	**测评指标**
安全物理环境	物理位置选择	a）机房和办公场地应选择在具有防震、防风和防雨等能力的建筑内；
		b）机房场地应避免设在建筑物的高层或地下室，否则应加强防水和防潮措施。
	物理访问控制	机房出入口应有专人值守，控制、鉴别和记录进入的人员。
	防盗窃和防破坏	a）应将设备或主要部件进行固定，并设置明显的不易除去的标记；
		b）应将通信线缆铺设在隐蔽安全处；
	防雷击	应将各类机柜、设施和设备等通过接地系统安全接地。
	防火	a）机房应设置火灾自动消防系统，自动检测火情、自动报警，并自动灭火；
		b）机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料；

安全 层面	安全 控制点	测评指标
	防水和防潮	a）应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；
		b）应采取措施防止机房内水蒸气结露和地下积水的转移与渗透。
	防静电	应采用防静电地板或地面并采用必要的接地防静电措施。
	温湿度控制	应设置温湿度自动调节设施，使机房温、湿度的变化在设备运行所允许的范围之内。
	电力供应	a）应在机房供电线路上配置稳压器和过电压防护设备；
		b）应提供短期的备用电力供应，至少满足主要设备在断电情况下的正常运行要求。
	电磁防护	电源线和通信线缆应隔离铺设，避免互相干扰。
安全通信网络	网络架构	a）应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址；
		b）应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离于段。
	通信传输	应采用校验技术保证通信过程中数据的完整性。
	可信验证	可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
安全区域边界	边界防护	应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。
	访问控制	a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；
		b）应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；
		c）应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许／拒绝数据包进出；

安全 层面	安全 控制点	测评指标
		d） 应能根据会状态话信息对进出数据流提供明确的允许/拒绝访问的能力；
	入侵防范	应在关键网络节点处监视网络攻击行为。
	恶意代码防范	应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。
	安全审计	a）应在网络边界、重要网络节点处进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；
		b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；
		c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。
	可信验证	可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
安全计算环境	身份鉴别	a)应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；
		b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；
		c)当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。
	访问控制	a）应对登录的用户分配账户和权限；
		b）应重命名或删除默认账户，修改默认账户的默认口令；
		c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；
		d）应授予管理用户所需的最小权限，实现管理用户的权限分离。

安全 层面	安全 控制点	测评指标
	安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；
		b)审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；
		c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。
	入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；
		b)应关闭不需要的系统服务、默认共享和高危端口；
		c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；
		d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；
		e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞；
	恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。
	可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
	数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。
	数据和备份恢复	a）应提供重要数据的本地数据备份与恢复功能；
		b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。
	剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。
	个人信息保护	a）应仅采集和保存业务必需的用户个人信息；

安全 层面	安全 控制点	测评指标
		b）应禁止未授权访问和非法使用用户个人信息。
安全管理中心	系统管理	a）应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计；
		b）应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。
	审计管理	a）应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计；
		b）应通过审计管理员对审计记录应进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。
安全管理制度	安全策略	应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等。
	管理制度	a)应对安全管理活动中的各类管理内容建立安全管理制度；
		b)应对要求管理人员或操作人员执行的日常管理操作建立操作规程。
	制定和发布	a)应指定或授权专门的部门或人员负责安全管理制度的制定。
		b)安全管理制度应通过正式、有效的方式发布，并进行版本控制。
	评审和修订	应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。
安全管理机构	岗位设置	a)应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责；
		b)应设立系统管理员、审计管理员和安全管理员等岗位，并定义部门及各个工作岗位的职责。

安全 层面	安全 控制点	测评指标
	人员配备	应配备一定数量的系统管理员、审计管理员和安全管理员等。
	授权和审批	a)应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等；
		b)应针对系统变更、重要操作、物理访问和系统接入等事项执行审批过程。
	沟通和合作	a)应加强各类管理人员 、组织内部机构和网络安全管理部门之间的合作与沟通,定期召开协调会议，共同协作处理网络安全问题；
		b)应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通；
		c)应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。
	审核和检查	应定期进行常规安全检查,检查内容包括系统日常运行、系统漏洞和数据备份等情况。
安全管理人员	人员录用	a)应指定或授权专门的部门或人员负责人员录用；
		b)应对被录用人员的身份、安全背景、专业资格或资质等进行审查。
	人员离岗	应及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备。
	安全意识教育和培训	应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施。
	外部人员访问管理	a)应在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案。
		b)应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案；

安全 层面	安全 控制点	测评指标
		c)外部人员离场后应及时清除其所有的访问权限。
安全建设管理	定级和备案	a)应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由；
		b)应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定；
		c)应保证定级结果经过相关部门的批准；
		d)应将备案材料报主管部门和相应公安机关备案。
	安全方案设计	a)应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施；
		b)应根据保护对象的安全保护等级进行安全方案设计；
		c)应组织相关部门和有关安全专家对安全方案的合理性和正确性进行论证和审定，经过批准后才能正式实施。
	产品采购和使用	a)应确保网络安全产品采购和使用符合国家的有关规定；
		b)应确保密码产品与服务的采购和使用符合国家密码管理主管部门的要求。
	自行软件开发	a）应将开发环境与实际运行环境物理分开，测试数据和测试结果受到控制；
		b)应在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测。
	外包软件开发	a）应在软件交付前检测其中可能存在的恶意代码；
		b）应保证开发单位提供软件设计文档和使用指南。
	工程实施	a） 应指定或授权专门的部门或人员负责工程实施过程的管理；
		b）应制定安全工程实施方案控制工程实施过程。
	测试验收	a）应制定测试验收方案，并依据测试验收方案实施测试验收，

安全 层面	安全 控制点	测评指标
		形成测试验收报告；
		b)应进行上线前的安全性测试，并出具安全测试报告。
	系统交付	a)应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；
		b)应对负责运行维护的技术人员进行相应的技能培训；
		c)应提供建设过程文档和运行维护文档。
	等级测评	a)应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改；
		b)应在发生重大变更或级别发生变化时进行等级测评；
		c)应确保测评机构的选择符合国家有关规定。
	服务供应商选择	a)应确保服务供应商的选择符合国家的有关规定；
		b)应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务。
安全运维管理	环境管理	a)应指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理；
		b)应对机房的安全管理做出规定，包括物理访问、物品进出和环境安全等；
		c)应不在重要区域接待来访人员，不随意放置含有敏感信息的纸档文件和移动介质等。
	资产管理	应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容。
安全运维管理	介质管理	a)应将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点；

安全 层面	安全 控制点	测评指标
		b)应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录。
	设备维护管理	a)应对各种设备(包括备份和冗余设备)、线路等指定专门的部门或人员定期进行维护管理；
		b)应对配套设施、软硬件维护管理做出规定，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等。
	漏洞和风险管理	应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补。
	网络和系统安全管理	a)应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限；
		b)应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制；
		c)应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定；
		d)应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等；
		e)应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容。
	恶意代码防范管理	a)应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等；
		b)应对恶意代码防范要求做出规定，包括防恶意代码软件的授权使用、恶意代码库升级、恶意代码的定期查杀等；

安全 层面	安全 控制点	测评指标
安全运维管理	恶意代码防范管理	c)应定期检查恶意代码库的升级情况，对截获的恶意代码进行及时分析处理。
	配置管理	应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等。
	密码管理	a)应遵循密码相关国家标准和行业标准；
		b)应使用国家密码管理主管部门认证核准的密码技术和产品。
	变更管理	应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审，审批后方可实施。
	备份与恢复管理	a)应识别需要定期备份的重要业务信息、系统数据及软件系统等；
		b)应规定备份信息的备份方式、备份频度、存储介质、保存期等；
		c)应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等。
	安全事件 处置	a)应及时向安全管理部门报告所发现的安全弱点和可疑事件；
		b)应制定全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等；
		c) 应在事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训。
	应急预案 管理	a)应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容；
		b)应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练。
	外包运维	a)应确保外包运维供应商的选择符合国家的有关规定；

安全 层面	安全 控制点	测评指标
	管理	b)应与选定的外包运维供应商签订相关的协议，明确约定外包运维的范围、工作内容。

（三）第二阶段：渗透测试

渗透测试是通过模拟恶意黑客的攻击方法，来对计算机网络的安全性进行检测评估的过程。对系统和网络进行非破坏性质的攻击性测试，尝试侵入系统，获取系统控制权并将入侵的过程和细节产生报告给陕西省财政厅，由此证实陕西省财政厅系统所存在的安全威胁和风险，及时提示开发人员修复安全漏洞，提醒安全管理员完善安全策略，提升系统安全防护能力。通过这种方法，可以发现系统面临和暴露的安全问题，同时渗透测试也是对安全措施有效性的重要验证。

（四）第三阶段：整改咨询及安全加固（不涉及硬件）

建设整改咨询工作以等级测评和渗透检测发现的安全问题为工作重点，编写《信息系统安全建设整改建议》；将信息系统的安全建设整改需求落实到可操作的安全技术和管理上，提出能够实现的技术参数或制度及其具体规范。之后在陕西省财政厅业务系统依据相关《信息系统安全建设整改建议》开展建设整改工作时，供应商将提供建设整改过程中的与建设整改相关的咨询服务。对信息系统安全整改建议进行确认，并依照建议，协助采购单位进行漏洞修复，补丁升级等非硬件层面的安全加固,制定可执行的安全整改方案和计划,然后协助采购单位分步实施安全整改工作。

（五）第四阶段：售后服务

售后服务供应商应向陕西省财政厅业务系统提供包括应急响应、安全监测、配合检查、电话支持、安全咨询等服务在内的安全维保服务。具体服务内容如下：

1.应急响应服务

针对本次项目，服务方提供7*24的常规应急响应及灾难恢复专家服务。在接到用户故障报修电话10分钟内响应。对客户信息网络应用系统突发的信息安全事件进行响应、处理、恢复、取证、跟踪、事后分析的方法及过程。

2.配合检查服务

供应商协助陕西省财政厅业务系统响应公安机关、单位内部以及第三方机构针对信息系统安全等级保护工作的检查工作。服务内容包括协助陕西省财政厅业务系统准备、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。

3.电话支持服务

服务期间解答陕西省财政厅业务系统在使用过程中遇到的问题,及时提出解决问题的建议和操作方法。电话响应时间不超过 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。

4.安全咨询服务

供应商为陕西省财政厅业务系统提供一年技术咨询服务,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，一旦接到用户的服务请求，技术服务工程师将立即开始提供服务，帮助客户解决信息安全相关技术问题，全面配合陕西省财政厅业务系统做好业务系统全保障工作。

四、其他要求

（一）测评人员要求：本项目的测评人员需具有 1 年或 1 年以上测评工作经验，项目经理和质量负责人必须具备丰富的安全服务经验及相关资质认证，并提供人员管理及配备方案，并确保人员稳定。如需更换测评人员，须由采购单位同意。

（二）**人员配备：**供应商必须为本项目成立本地化等级保护测评小组，由测评小组组长统一负责，测评小组组长具有一定的技术及管理知识和经验，能容易地与客户沟通，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。

（三）供应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。

（四）供应商应严格遵守采购方有关保密的相关规定，不得泄漏单位的任何机密。

五、交付内容

（一）《信息系统安全等级保护定级备案证明》

（二）《信息系统测评方案》

（三）《信息系统整改建议书》

（四）《信息系统渗透测试报告》

（五）《信息系统安全等级测评报告》