第三章 磋商项目技术、服务、商务及其他要求

（注：带“★”的参数需求为实质性要求，供应商必须响应并满足的参数需求，采购人、采购代理机构应当根据项目实际需求合理设定，并明确具体要求。带“▲”号条款为允许负偏离的参数需求，若未响应或者不满足，将在综合评审中予以扣分处理。）

3.1、采购项目概况

成都蓉北商圈发展服务局拟采购等级保护测评服务、商用密码应用安全性评估、软件测试及监理服务一项。

3.2、服务内容及服务要求

3.2.1 服务内容

采购包 1：
采购包预算金额（元）: 286,300.00
采购包最高限价（元）: 266,500.00

序号	标的名称	数量	标的金额（元）	计量单位	所属行业	是否涉及核心产品	是否涉及采购进口产品	是否涉及采购节能产品	是否涉及采购环境标志产品
1	等级保护测评服务、商用密码应用安全性评估、软件测试及监理服务	1.00	266,500.00	项	软件和信息技术服务业	否	否	否	否

3.2.2 服务要求

采购包 1：

标的名称：等级保护测评服务、商用密码应用安全性评估、软件测试及监理服务

参数性质	序号	技术参数与性能指标
★	1	（一）等级保护测评服务

		1.项目需求 根据等级保护测评的工作要求，测评范围覆盖安全管理中心、安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理制度，以及云计算安全、移动互联安全、物联网安全、工控制系统安全等扩展方面的要求。 具体服务内容包括： （1）协助业主单位进行信息系统的信息安全等级定级和备案工作。 （2）差距测评，至少包括： 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、安全管理中心方面的安全测评。 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、安全系统建设和安全系统运维五个方面的安全测评。 形成问题汇总及整改意见报告。依据测评结果，对等级测评结果进行汇总统计（测评项符合情况及比例、单元测评结果符合情况比例以及整体测评结果）；通过对信息系统基本安全保护状态的分析给出初步测评结论。根据测评结果制定《系统等级保护测评问题汇总及整改意见报告》，列出被测信息系统中存在的主要问题以、整改意见。 （3）协助完成整改

工作。依据整改方案，为安全整改的各项工作提供技术咨询服务。

（4）等级测评，包括：

按照等级保护相关标准对系统从安全技术、安全管理等方面进行等级测评工作。

编制测评报告，制定并提交《网络安全等级测评报告》，报告需提交公安机关有关部门备案，且能满足合规性要求。

2.服务内容指标

三级系统通用指标要求

分类	子类	基本要求
安全物理环境	物理位置选择	a）机房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顶层或地下室，否则应加强防水和防潮措施。
	物理访问控制	机房出入口应配置电子门禁系统，控制、鉴别和记录进入的人员。
	防盗窃和防	a）应将设备或主要部件进行固定，并设置明显的不易

				破坏	除去的标识; b）应将通信线缆铺设在隐蔽安全处。 c）应设置机房防盗报警系统或设置有专人值守的视频监控系统。
				防雷击	a）应将各类机柜、设施和设备等通过接地系统安全接地。 b）应采取措施防止感应雷，例如设置防雷保安器或过压保护装置等。
				防火	a）机房应设置火灾自动消防系统，能够自动检测火情、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; c）应对机房划分区域进行管理，区域和区域之

					间设置隔离防火措施。
				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; c）应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警。
				防静电	a）应采用防静电地板或地面并采用必要的接地防静电措施; b）应采取措施防止静电的产生，例如采用静电消除器、佩戴防静电手环等。
				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	a）应在机房供电线路上配置稳压

				应	器和过电压防护设备; b) 应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求; c）应设置冗余或并行的电力电缆线路为计算机系统供电。
				电磁防护	a) 电源线和通信线缆应隔离铺设，避免互相干扰; b）应对关键设备实施电磁屏蔽。
			安全通信网络	网络架构	a) 应保证网络设备的业务处理能力满足业务高峰期需要; b) 应保证网络各个部分的带宽满足业务高峰期需要; c) 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; d) 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手段; e) 应提供通信线路、关键网络设备和关键计算设备的硬件冗余，保证系统的可用性。
				通信传输	a) 应采用校验技术或密码技术保证通信过程中数据的完整性; b) 应采用密码技术保证通信过程中数据的保密性。
				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，应用程序的关键执行环节进行动态可信验证，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	a）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; b）应能够对非授权设备私自联到内部网络的行为进行检查或限制; c）应能够对内部用户非授权联到外部网络的行为进行检查或限制; d）应限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络。
				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; d) 应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力; e) 应对进出网络的数据流实现基于应用协议和应用内容的访问控制。	
				入侵防范	a) 应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为; b) 应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为; c) 应采取技术措施对	

					网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析; d) 当检测到攻击行为时，记录攻击源IP、攻击类型、攻击目标、攻击时间，在发生严重入侵事件时应提供报警。
				恶意代码和垃圾邮件防范	a) 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; b) 应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件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； d）应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。	
				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，并在应用程序的关键执行环节进行动态可信验证，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； d）应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技	

					术至少应使用密码技术来实现。
				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； e）应由授权主体配置访问控制策略，访间控制策略规定主体对客体的访问规则； f）访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级； g）应对重要主体和客体设置安全标记，并控

					制主体对有安全标记信息资源的访问。
				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； d）应对审计进程进行保护，防止未经授权的中断。
				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; f) 应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。	
				恶意代码防范	应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并	

					将其有效阻断。
				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，并在应用程序的关键执行环节进行动态可信验证，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	a）应采用校验技术保证重要数据在传输过程中的完整性，包括鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息； b）应采用校验技术或密码技术保证重要数据在存储过程中的完整

					性，包括鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息。
				数据保密性	a）应采用密码技术保证重要数据在传输过程中的保密性，包括鉴别数据、重要业务数据和重要个人信息； b）应采用密码技术保证重要数据在存储过程中的保密性，包括鉴别数据、重要业务数据和重要个人信息。
				数据备份恢复	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； c） 应提供

					重要数据处理系统的热冗余，保证系统的高可用性。
				剩余信息保护	a）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; b）应保证存有敏感数据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; 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	a）应对安全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管理操作，并对这些操作进行审

					计； b）应通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等。	
				集中管控	a）应划分出特定的管理区域，对分布在网络中的安全设备或安全组件进行管控； b）应能够建立一条安全的信息传输路径，对网络中的安全设备或安全组件进行管理； c）应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测； d）应对分散在各个设备上的审计数据进行收集汇总和集中分析，并保证审计记录	

					的留存时间符合法律法规要求; e）应对安全策路、恶意代码、补丁升级等安全相关事项进行集中管理; f）应能对网络中发生的各类安全事件进行识别、报警和分析。
			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主要管理内容建立安全管理制度; b）应对管理人员或操作人员执行的日常管理操作建立操作规程; c）应形成由安全策略、管理制度、操作规程、记录表单等构成的

					全面的安全管理制度体系。
				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）应成立指导和管理网络安全工作的委员会或领导小组，其最高领导由单位主管领导担任或授权; b）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; c）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。
				人员配备	a）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; b）应配备专职安全管理员，不可兼任。
				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建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度; c）应定期审查审批事项，及时更新需授权和

					审批的项目、审批部门和审批人等信息。
				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	a）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； b）应定期进行全面安全检查，检查内容包括

					现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等; c）应制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报。
			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，对其所具有的技术技能进行考核; c）应与被录用人员签署保密协议，与关键岗位人员签署岗位责任协议。
				人员离岗	a）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; b）应办理严格的调离手续，并承诺调离后的保密义务后方可离开。
				安全意识教育和培训	a）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; b）应针对不同岗位制定不同的培训计划，对安全基础知识、岗位操作规程等进行培训; c）应定期对不同岗位的人员进行技能考核。
				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; c）外部人员离场后应及时清除其所有的访问权限; d）获得系统访问授权的外部人员应签署保密协议，不得进行非授权操作，不得复制和泄露任何敏感信息。	
			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及与其他级别保护对象的关系进行安全整体规划和安全方案设计，设计内容应包含密码技术相关内容，并形成配套文件; c）应组织相关部门和有关安全专家对安全整体规划及其配套文件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; c）应预先对产品进行选型测试，确定产品的候选范围，并定期审定和更新候选产品名单。	
				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）应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则; c）应制定代码编写安全规范，要求开发人员参照规范编写代码; d）应具备软件设计的相关文档和使用指南，并对文档使用进行控制; e）应保证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; f）应对程序资源库的修改、更新、发布进行授权和批准，并严格进行版本控制; g）应保证开发人员为专职人员、开发人员的开发活动受到控制、监视和审查。
				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; c）应保证开发单位提供软件源代码，并审查软件中可能存在的后门和隐蔽信道。
				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; c）应通过第三方工程监理控制项目的实施过程。
				测试验收	a）应制订测试验收方案，并依据测试验收方案实施测试验收，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，安全测试报告应包含密码应用安全性测试相关内容。
				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	a）应定期

				级测评	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; c）应定期监督、评审和审核服务供应商提供的服务，并对其变更服务内容加以控制。
			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）应建立机房安全管理制度，对有关物理访问、物品带进出和环境安全等方面的管理作出规定; 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	a）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; b）应根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施; c）应对信息分类与标识方法作出规定，并对信

					息的使用、传输和存储等进行规范化管理。
				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; 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; c）信息处理设备应经过审批才能带离机房或办公地点，含有存储介质的设备带出工作环境时其中重要数据应加密; d）含有存储介质的设备在报废或重用前，应进行完全清除或被安全覆盖，保证该设备上的敏感数据和授权软件无法被恢复重用。	
				漏洞和风险管理	a）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; b）应定期开展安全测评，形成安全测评报告，采取措施应对发现的安全问题。	

				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; f）应指定专门的部门或人员对日志、监测和报警数据等进行分析、统计，及时发现可疑行为; g）应严格控制变更性运维，经过审批后才可改变连接、安装系统组件或调整配置参数，操作过程中应保留不可更改的审计日志，操作结束后应同步更新配置信息库; h）应严格控制运维工具的使用，经过审批后才可接入进行操作，操作过程中应保留不可更改的审计日志，操作结束后应删除工具中的敏感数据; i）应严格控制远程运维的开通，经过审批后才	

					可开通远程运维接口或通道，操作过程中应保留不可更改的审计日志，操作结束后立即关闭接口或通道; j）应保证所有与外部的连接均得到授权和批准，应定期检查违反规定无线上网及其他违反网络安全策略的行为。
				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）应定期验证防范恶意代码攻击的技术措施的有效性。
				配置管理	a）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; b）应将基本配置信息改变纳入变更范畴，实施对配置信息改变的控制，并及时更新基本配置信息库。
				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	a）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; b）应建立变更的申报和审批控制程序，依据程序控制所有的变更，记录变更实施过程; c）应建立中止变更并从失败变更中恢复的程

					序，明确过程控制方法和人员职责，必要时对恢复过程进行演练。
				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）应制定安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) 应在安全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; d)对造成系统中断和造成信息泄漏的重大安全事件应采用不同的处理程序和报告程序。	
				应急预案管理	a)应规定统一的应急预案框架，包括启动预案的条件、应急组织构成、应急资源保障、事后教育和培训等内容; b) 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; c)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; d）应定期对原有的应急预案重新评估，修订完善。
				外包运维管理	a）应确保外包运维服务商的选择符合国家的有关规定; b）应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容; c）应保证选择的外包运维服务商在技术和管理方面均应具有按照等级保护要求开展安全运维工作的能力，并将能力要求在签订的协议中明确; d）应在与外包运维服务商签订的协议中明确所有相关的安全要求，如可能涉及对敏感信息的访问、处理、存储要

				求，对 IT 基础设施中断服务的应急保障要求等。

3. 完成项目所需提交的文档清单

在本项目完成后，服务方须提供以下文档资料：

3.1《信息系统安全问题汇总及整改建议》

3.2《网络安全等级保护等级测评报告》及过程资料

4. 安全要求

成交供应商在项目实施过程中，必须遵守以下技术原则：

4.1 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采购方的行为，否则采购方有权追究供应商的责任。

4.2 标准性原则：测评方案的设计与实施应依据国家等级保护的相关标准进行。

4.3 规范性原则：供应商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，测评出具的报告须符合公安部颁布的《信息系统安全等级测评报告模板》。

		4.4 可控性原则：等保测评服务的进度要按照文件 的要求，保证采购方对于测评工作的可控性。 4.5 整体性原则：等保测评服务的范围和内容应当整体全面，包括国家等级保护相关要求测评要求涉及的各个层面。 4.6 安全性原则：等保测评服务工作应不得影响系统和网络的正常运行；测评工作不得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。 4.7.测评机构资质及人员要求： 从事信息系统检测评估相关工作人员无违法记录。 工作人员仅限于中华人民共和国境内的中国公民，且无犯罪记录。 测评期间需遵守被测单位相关管理规定，禁止利用测评工作从事危害被测单位利益、安全的活动。
★	2	**（二）商用密码应用安全性评估** **服务任务** 被评估对象的商用密码应用安全性评估服务内容如下: 1、密码应用总体要求测评 1.1 密码算法合规性测评 系统中使用的密码算法是否符合法律、法规

		的规定和密码相关国家标准、行业标准的有关要求。 1.2 密码技术合规性测评 系统中使用的密码技术是否遵循密码相关国家标准和行业标准。 1.3 密码产品合规性测评系统中使用的密码产品与密码模块是否通过国家密码管理部门核准。 1.4 密码服务合规性测评系统中使用的密码服务是否通过国家密码管理部门许可。 2、密码应用技术要求测评 2.1 物理和环境安全测评 2.1.1 是否使用密码技术的真实性服务来保护物理访问控制身份鉴别信息，保证重要区域进入人员身份的真实性； 2.1.2 是否使用密码技术的完整性服务来保证电子门禁系统进出记录的完整性； 2.1.3 是否使用密码技术的完整性服务来保证视频监控音像记录的完整性。 2.2 网络和通信安全测评 2.2.1 是否在通信前基于密码技术对通信双方进行身份认证,使用密码技术的机密性和真实性服务来实现防截获、防假冒和防重用,保证传输过程中鉴别信息的机密性和网络设备实体身

		份的真实性； 2.2.2 是否使用密码技术的完整性服务来保证网络边界和系统资源访问控制信息的完整性； 2.2.3 是否采用密码技术保证通信过程中数据的完整性； 2.2.4 是否采用密码技术保证通信过程中敏感信息字段或整个报文的机密性； 2.2.5 是否采用密码技术建立一条安全的信息传输通道，对网络中的安全设备或安全组件进行集中管理。 2.3 设备和计算安全测评 2.3.1 是否使用密码技术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； 2.3.2 在远程管理时，是否使用密码技术的机密性服务来实现鉴别信息的防窃听； 2.3.3 是否使用密码技术的完整性服务来保证系统资源访问控制信息的完整性； 2.3.4 是否使用密码技术的完整性服务来保证重要信息资源敏感标记的完整性； 2.3.5 是否采用可信计算技术建立从系统到应用的信任链，实现系统运行过程中重要程序或文件完整性保护； 2.3.6 是否使用密

		码技术的完整性服务来对日志记录进行完整性保护。 2.4 应用和数据安全测评 2.4.1 是否使用密码技术对登录的用户进行身份标识和鉴别，实现身份鉴别信息的防截获、防假冒和防重用，保证应用系统用户身份的真实性； 2.4.2 是否使用密码技术的完整性服务来保证业务应用系统访问控制策略、数据库表访问控制信息和重要信息资源敏感标记等信息的完整性； 2.4.3 是否采用密码技术保证重要数据在传输过程中的机密性，包括鉴别数据、重要业务数据和重要用户信息； 2.4.4 是否采用密码技术保证重要数据在存储过程中的机密性，包括鉴别数据、重要业务数据和重要用户信息； 2.4.5 是否采用密码技术保证重要数据在传输过程中的完整性，包括鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要用户信息； 2.4.6 是否采用密码技术保证重要数据在存储过程中的完整性，包括鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要用户信息、重要可执行程序；

		2.4.7 是否使用密码技术的完整性服务来实现对日志记录完整性的保护； 2.4.8 是否采用密码技术对重要应用程序的加载和卸载进行安全控制。
★	3	**（三）软件测试** 服务内容 1、编写项目测试方案，对项目测试内容进行阐述，并提出项目对应的测试通过准则，及测试实施计划 2、对项目进行系统测评，测评内容主要包括：系统软件的功能测试、性能（效率）测试、可靠性测试、可移植性测试、易用性测试、维护性测试、用户产品说明测试、文档集测试。在完成项目系统测试后出具项目《测评报告》。 具体测试内容如下： （1）功能测试 在系统正式运行环境中，采用手工验证的方式，对系统中的主要功能点进行测试。检测在当前硬件、软件环境下，系统的各功能点的正确性和可用性，验证各项主要功能是否满足需求和用户使用的要求。 （2）性能（效率）测试 性能（效率）测试将采用自动化测试工具通过编写测试用例，模拟综合业务情况下用户并发性操作系统时，系统性能是否达到要求。

		（3）可靠性测试 应保证软件产品在规定的时间内以及规定的环境条件下，完成规定功能的能力。可靠性测试应包括以下 3 方面：成熟性、容错性、易恢复性。 （4）易用性测试 考察评定软件的易学易用性，各个功能是否易于完成，软件界面是否友好等方面进行测试，对该系统的易用性测试应包括以下 3 个方面：易理解性、易学性、易操作性。 （5）可移植性测试 应检测软件产品从一种环境迁移到另外一种环境的能力。可移植性测试应包括以下 4 个方面：适应性、易安装性、共存性、易替换性。 （6）维护性测试 应检测软件开发工作是否严格按照软件工程的要求，遵循特定的软件标准或规范进行开发。保证软件的文档和源程序易于理解和修改，可维护性测试应包括以下 4 个方面：易分析性、易改变性、稳定性、易测试性。 （7）产品说明测试 参照需求说明，检查产品功能说明书描述的产品将要实现的功能是否已经完整、准确、一致、合理的描述了产品的功能，并确保这些功能是可测试的。 （8）文档集测试 依据国家标准，按照系统文档的内容执行系统操作，验证文档的正确

		性、完整性和一致性，检测文档内容是否覆盖了系统的所有功能，检测文档描述内容与系统实际是否保持一致，检查文档内容是否条理清晰、结构合理、容易理解，检查文档内容语言表述和表现形式是否符合规范，主要包括以下 5 个方面：完整性、正确性、一致性、易理解性、易浏览性。 项目实施过程及完成后，供应商应向采购人提交包含以下的文档： 《项目测评报告》。 《项目测试用例及记录》。
★	4	**（四）监理** 监理服务内容： 1、质量控制 建议采购人和承建单位充分考虑目标系统和现有系统的兼容性和可操作性；正确理解采购方的需求，及时发现承建方对需求理解不恰当的地方，并作正确解释；审核承建单位提交的设计方案，对有明显错误或不当的设计，及时提出改进意见，必要时召开专家评审会议。 和采购人共同审核承建单位提交的阶段性测试验收方案报审表。 2、进度控制 审核承建单位提交的阶段进度计划报审表；审核承建单位提交的阶段计划报审表；根据承建单位提交的阶段计划，确定阶段性进度监督、控制的措施和方法，作为监理

		细则的内容。 3、投资控制 依据招投标文件、承建合同，审核项目计划、设计方案中所说明的建设目标、范围、内容、产品和服务，对可能的投资变化，向采购人提出监理意见；控制设计变更，变更应由三方达成共识，并做备忘录。 4、合同管理 及时处理采购人或承建单位合同变更的申请，协助保持合同、协议及其附件内容的实效性、一致性；及时对合同的变更做备忘录。 5、信息管理 对设计阶段三方共同参与的过程和活动做项目建设备忘录，并由三方签字确认；妥善保管项目设计阶段的文档；对项目建设中各方提出保密要求的信息实施保密。 6、协调 与采购人、承建单位确定设计阶段的协调形式和方法，如监理例会和专题会议等，并在项目过程中执行；协调采购人调动适当的资源，配合承建单位完成设计前期的调研工作；对设计阶段出现的变更提出监理意见，协调采购人和承建单位达成一致；对协调结果做备忘录，并经三方签认。 7、监理成果 监理成果要求包括：方案评审报告、技术评审报告、监理规划、开工令、复工令、停工令、项目款

		支付证书、监理周报、会议纪要、监理月报、实施文档类监理审核意见、监理工作联系函、监理通知单、项目备忘录、设施设备验货台账、设备加电检查记录、专项项目监理报告、监理总报告。
	5	**（一）等级保护测评服务** **技术标准和规范** 1《中华人民共和国计算机信息系统安全保护条例》(国务院令 147 号) 2《信息安全等级保护管理办法》 3《计算机信息系统安全保护等级划分准则》（GB17859） 4《信息安全技术网络安全等级保护定级指南》（GB/T22240） 5《信息安全技术网络安全等级保护基本要求》（GB/T22239） 6《信息安全技术网络安全等级保护测评要求》（GB/T28448） 7《信息安全技术网络安全等级保护测评过程指南》（GB/T28449） 本文中所有国家标准如有最新标准以最新为准。
	6	**（二）商用密码应用安全**

		性评估 **1.服务总体目标** 严格按照《中华人民共和国密码法》、《商用密码管理条例》、GM/T0054《信息系统密码应用基本要求》、《信息系统密码测评要求（试行）》、《商用密码应用安全性评估测评过程指南（试行）》、《商用密码应用安全性评估测评作业指导书（试行）》、《商用密码应用安全性评估测评工作使用需求说明（试行）》和相关国家标准和密码行业标准，高质量完成信息系统的密码应用安全性评估工作。 **2.密码应用技术要求测评** 对密钥的生成、存储、分发、导入、导出、使用、备份、恢复、归档、销毁等环节进行管理和策略制定的全过程进行测评： 2.1 密钥生成测评 密钥生成使用的随机数是否符合《GM/T 0005 随机性监测规范》的要求，密钥是否在符合《GM/T 0028 密码模块安全技术要求》的密码模块中产生；密钥是否在密码模块内部产生，不得以明文方式出现在密码模块之外；是否具备检查和剔除弱密钥的能力。 2.2 密钥存储测评 密钥是否加密存储，

		并采取严格的安全防护措施，防止密钥被非法获取；密钥加密密钥是否存储在符合《GM/T 0028 密码模块安全技术要求》的二级及以上密码模块中。 2.3 密钥分发测评 密钥分发是否采取身份鉴别、数据完整性、数据机密性等安全措施，是否能够抗截取、假冒、篡改、重放等攻击，保证密钥的安全性。 2.4 密钥导入与导出测评 是否采取安全措施，防止密钥导入导出时被非法获取或篡改，并保证密钥的正确性。 2.5 密钥使用测评 密钥是否明确用途，并按用途正确使用；对于公钥密码体制，在使用公钥之前是否对其进行验证；是否有安全措施防止密钥的泄露和替换；密钥泄露时，是否停止使用，并启动相应的应急处理和响应措施。是否按照密钥更换周期要求更换密钥；是否采取有效的安全措施，保证密钥更换时的安全性。 2.6 密钥备份与恢复测评 是否制定明确的密钥备份策略，采用安全可靠的密钥备份恢复机制，对密钥进行备份或恢复； 密钥备份或恢复是否进行记录，并生成审计信息；审计信息包括备份或恢复的主体、备份或恢复的时间等。

		2.7 密钥归档测评 是否采取有效的安全措施，保证归档密钥的安全性和正确性；归档密钥只能用于解密该密钥加密的历史信息或验证该密钥签名的历史信息；密钥归档是否进行记录，并生成审计信息；审计信息包括归档的密钥、归档的时间等；归档密钥是否进行数据备份，并采用有效的安全保护措施。 2.8 密钥销毁测评 是否具有在紧急情况下销毁密钥的措施。 **3.密钥管理测评** 3.1 制度测评 3.1.1 是否制定密码安全管理制度及操作规范、安全操作规范。密码安全管理制度是否包括密码建设、运维、人员、设备、密钥等密码管理相关内容； 3.1.2 是否定期对密码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； 3.1.3 是否明确相关管理制度发布流程。 3.2 人员测评 3.2.1 是否了解并遵守密码相关法律法规； 3.2.2 是否能够正确使用商用密码产品； 3.2.3 是否根据相关密码管理政策、数据安全保密政策，结合组织实际情况，设置密钥管理人员、安全审计人员、密码

		操作人员等关键岗位；建立相应岗位责任制度，明确相关人员在安全系统中的职责和权限，对关键岗位建立多人共管机制；密钥管理、安全审计、密码操作人员职责，互相制约互相监督，相关设备与系统的管理和使用账号不得多人共用； 3.2.4 是否建立人员考核制度，定期进行岗位人员考核，建立健全奖惩制度； 3.2.5 是否建立人员培训制度，对于涉及密码的操作和管理以及密钥管理人员进行专门培训； 3.2.6 是否建立关键岗位人员保密制度和调离制度，签订保密合同，承担保密义务。 3.3 实施测评 3.3.1 规划测评 系统规划阶段，责任单位是否依据密码相关标准，制定密码应用方案，组织专家进行评审，评审意见作为项目规划立项的重要材料。 3.3.2 建设测评 是否按照国家相关标准，制定实施方案，方案内容是否包括但不少于信息系统概述、安全需求分析、商用密码系统设计方案、商用密码产品清单（包括产品资质、功能及性能列表和产品生产单位等）、商用密码系统安全管理与维护策略、商用密码系统实施计划等；是否选用的经国家密码

管理部门核准的密码产品、许可的密码服务。

3.3.3 运行测评

系统投入运行前，是否经密码测评机构进行安全性评估，评估通过方可投入正式运行；信息系统投入运行后，责任单位每年是否委托密码测评机构开展密码应用安全性评估，并根据评估意见进行整改；有重大安全隐患的，是否停止系统运行，制定整改方案，整改完成并通过评估后方可投入运行。

3.4 应急测评

3.4.1 是否制定应急预案，做好应急资源准备，当事件发生时，按照应急预案结合实际情况及时处置；

3.4.2 事件发生后，是否及时向信息系统的上级主管部门进行报告；

3.4.3 事件处置完成后，是否及时向同级的密码主管部门报告事件发生情况及处置情况。

4.测评指标

4.1 总体测评指标

4.1.1 密码算法测评

测评单元	**测评指标**
密码算法	信息系统中使用的密码算法应当符合法律、法规

			合规性检测	的规定和密码相关国家标准、行业标准的有关要求。

4.1.2 密码技术测评

测评单元	测评指标
密码技术合规性检查	信息系统中使用的密码技术应遵循密码相关国家标准和行业标准。

4.1.3 密码产品测评

测评单元	测评指标
密码产品合规性检查	信息系统中使用的密码产品与密码模块应通过国家密码管理部门核准。

4.1.4 密码服务测评

测评单元	测评指标

			密码服务合规性检查	信息系统中使用的密码服务应通过国家密码管理部门许可。

4.2密码技术应用测评指标

4.2.1物理与环境安全测评

测评单元	测评指标
身份鉴别	应使用密码技术的真实性功能保护物理访问控制身份鉴别信息，保证重要区域进入人员身份的真实性。
电子门禁记录数据完整性	应使用密码技术的完整性功能来保证电子门禁系统进出记录的完整性。
视频记录数据	应使用密码技术的完整性功能来保证视频监控音像记录的完整性。

			完整性	
			密码模块实现	宜采用符合《GM/T 0028 密码模块安全要求》的三级以上密码模块或通过国家密码管理部门核准的硬件密码产品实现密码运算和密钥管理。

4.2.2网络与通信安全测评

	测评单元	**测评指标**
	身份鉴别	应在通信前基于密码技术对通信双方进行验证或证明，使用密码技术的机密性和真实性功能来实现防截获、假冒和重放，保证传输过程中鉴别信息的机密性和网络设备实体身份的真实性。
	访问控制信息完整	应使用密码技术的完整性来保证网络边界和系统资源访问控制信息的完整性。

			性	
			通信数据完整性	应采用密码技术保证通信过程中数据的完整性。
			通信数据机密性	采用密码技术保证通信过程中敏感信息字段或整个报文的机密性。
			集中管理通道安全	应采用密码技术建立一条安全的信息传输通道，对网络中的安全设备或安全组件进行集中管理。
			密码模块实现	宜采用符合《GM/T 0028 密码模块安全要求》的二级以上密码模块或通过国家密码管理部门核准的硬件密码产品实现密码运算和密钥管理。

4.2.3 设备和计算安全测评

测评单元	**测评指标**
身份鉴	应使用密码技术对登录的用户进行身份标

			别	识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度并要求定期更换。
			远程管理身份鉴别信息机密性	在远程管理时，应使用密码技术的机密性功能来实现鉴别信息的防窃听。
			访问控制信息完整性	应使用密码技术的完整性功能来保证系统资源访问控制信息的完整性。
			敏感标记的完整性	应使用密码技术的完整性功能来保证重要信息资源敏感标记的完整性。
			重要程序或文件完	应采用可信计算技术建立从系统到应用的信任链，实现系统运行过程中重要程序或文件完整性保护。

			整性	
			日志记录完整性	应使用密码技术的完整性功能对日志进行完整性保护。
			密码模块实现	宜采用符合《GM/T 0028密码模块安全要求》的三级及以上密码模块或通过国家密码管理部门核准的硬件密码产品实现密码运算和密钥管理。

4.2.4应用和数据安全测评

测评单元	**测评指标**
身份鉴别	应使用密码技术对登录的用户进行身份标识和鉴别，实现身份鉴别信息的防截获、防假冒和防重用，保证应用系统用户身份的真实性。
访问控制	应使用密码技术的完整性功能来保证业务应用系统访问控制策略、数据库访问控制

				信息和重要信息资源敏感标记的完整性。
			数据传输机密性	应采用密码技术保证重要数据在传输过程中的机密性，包括鉴别数据、重要业务数据和重要用户信息。
			数据存储机密性	应采用密码技术保证重要数据在存储过程中的机密性，包括鉴别数据、重要业务数据、重要用户信息和重要可执行程序。
			数据传输完整性	应采用密码技术保证重要数据在传输过程中的完整性，包括鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要用户信息。
			数据存储完整性	应采用密码技术保证重要数据在存储过程中的完整性，包括鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据、重要用户信息和重要可执行

				程序。
			日志记录完整性	应使用密码技术的完整性功能对日志进行完整性保护。
			重要程序或文件完整性	应采用密码技术对重要应用程序的加载和卸载进行安全控制。
			密码模块实现	宜采用符合《GM/T 0028 密码模块安全要求》的三级及以上密码模块或通过国家密码管理部门核准的硬件密码产品实现密码运算和密钥管理

4.3 密钥管理测评指标

4.3.1 密钥生成

测评单元	**测评指标**
密钥生成	密钥生成使用的随机数应符合《GM/T 0005 随机性检测规范》要求，密钥应在符合《GM/T 0005 随机性检测规

				范》的密码模块中产生；密钥应在密码模块内部产生，不得以明文方式出现在密码模块之外；应具备检查和剔除弱密钥的能力。不适用时需标识。

4.3.2 密钥存储

测评单元	测评指标
密钥存储	密钥应加密存储，并采取严格的安全防护措施，防止密钥被非法获取；密钥加密密钥应存储在符合《GM/T 0028 密码模块安全要求》的二级及以上密码模块中。不适用时需标识。

4.3.3 密钥分发

测评单元	测评指标
密钥分发	密钥分发应采取身份鉴别、数据完整性、数据机密性等安全措

				施，应能抗截取、假冒、篡改、重放等攻击，保证密钥的安全性。不适用时需标识。

4.3.4 密钥导入与导出

测评单元	测评指标
密钥导入与导出	应采取安全措施，防止密钥导入导出时被非法获取或篡改，并保证密钥的正确性。不适用时需标识。

4.3.5 密钥使用

测评单元	测评指标
密钥使用	密钥应明确用途，并按用途正确使用；对于公钥密码体制，在使用公钥之前应对其进行验证；应有安全措施防止密钥的泄露和替换，密钥泄露时，应停止使用，并启动相应的应急处理和响

				应措施。应按照密钥更换周期要求更换密钥；应采取有效的安全措施，保证密钥更换时的安全性。不适用时需标识。

4.3.6 密钥备份与恢复

测评单元	测评指标
密钥备份与恢复	应制定明确的密钥备份策略，采用安全可靠的密钥备份恢复机制，对密钥进行备份或恢复；密钥备份或恢复应进行记录，并生成审计信息；审计信息包括备份或恢复的本体、备份或恢复的时间等。不适用时需标识。

4.3.7 密钥归档

测评单元	测评指标
密钥	应采取有效的安全措施，

			归档	保证归档密钥的安全性和正确性；归档密钥只能用于解密该密钥加密的历史信息或验证该密钥签名的历史信息；密钥归档应进行记录，并生成审计信息；审计信息包括归档的密钥、归档的时间等；归档密钥应进行数据备份，并采用有效的安全保护措施。不适用时需标识。

4.3.8 密钥销毁

测评单元	测评指标
密钥销毁	应具有在紧急情况下销毁密钥的措施。不适用时需标识。

4.4 安全管理测评指标

测评单元	测评指标
制度	应制定密码安全管理制度及操作规范、安全操作规范。密码

				安全管理制度应包括密码建设、运维、人员、设备、密钥等密码管理相关内容。
				应定期对密码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。
				应明确相关管理制度发布流程。
			人员	应了解并遵守商用密码相关法律法规。
				应能够正确使用商用密码产品。
				应根据相关密码管理政策、数据安全保密政策，结合组织实际情况，设置密钥管理人员、安全审计人员、密码操作人员等关键岗位；建立相应岗位责任制度，明确相关人员在安全系统中的职责和权限，对关键岗位建立多人共管机制；密钥管理、安全审计、密码操作人员职责应建立多人共管制度，互相制约互相监

					督，相关设备与系统的管理和使用账号不得多人公用。	
					应建立人员考核制度，定期进行岗位人员考核，建立健全奖惩制度。	
					应建立人员培训制度，对于涉及密码的操作和管理以及密钥管理人员进行专门培训。	
					应建立关键岗位人员保密制度和调离制度，签订保密合同，承担保密义务。	
				实施	规划	信息系统规划阶段，责任单位应依据密码有关标准，制定密码应用建设方案，组织专家进行评审。评审意见作为项目规划立项的重要材料。
					建设	应按照国家相关标准，制定实施方案，方案内容应包括但不少于信息系统概述、安全需求分析、商用

					密码系统设计方案、商用密码产品清单（包括产品资质、功能及性能列表和产品生产单位等）、商用密码系统安全管理与维护策略、商用密码系统实施计划等。	
					应选用的经国家密码管理部门核准的密码产品、许可的密码服务。	
				运行	信息系统投入运行前，应经密评机构进行安全性评估，评估通过方可投入正式运行。	
					信息系统投入运行后，责任单位每年应委托密码测评机构开展密码应用安全性评估，并根据评估意见进行	

<table>
<tr><td></td><td></td><td></td><td></td><td></td><td>整改；有重大安全隐患的，应停止系统运行，制定整改方案，整改完成并通过评估后方可投入运行。</td></tr>
<tr><td></td><td></td><td></td><td>应急</td><td></td><td>制定应急预案，做好应急资源准备，当事件发生时，按照应急预案结合实际情况及时处置。</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td>事件发生后，应及时向信息系统的上级主管部门和同级的密码主管部门进行报告。</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td>事件处置完成后，应及时向同级的密码主管部门报告事件发生情况及处置情况。</td></tr>
<tr><td></td><td></td><td></td><td>成果</td><td></td><td>出具《商用密码应用安全性评估报告》</td></tr>
<tr><td></td><td>7</td><td colspan="4">（三）软件测试

1.项目概述

为掌握信息系统的安全状况、排查系统功能隐患和薄弱环节、明确信息系统建设整改需求，发现存在的隐患，查找信息系统运行使用过程中存在的不足，及时改进，保证信息系统安全、稳定的运行，全面提升信息系统</td></tr>
</table>

		整体稳定性。 **2.技术和服务要求：** 2.1 测试依据 2.1.1、GB/T 25000.51《系统与软件工程系统与软件质量要求和评价（SQuaRE） 第51部分：就绪可用软件产品（RUSP)的质量要求和测试细则》； 2.1.2、《计算机软件测试规范》（GB/T 15532）； 2.1.3、GB/T 8567《计算机软件文档编制规范》； 2.1.4、GB/T 29831.1/2/3《系统与软件功能性》（第1部分：指标体系、第2部分：度量方法、第3部分：测试方法）。
	8	**（四）监理** 1.主要依据： 1.1建设方与监理方的监理服务合同； 1.2建设方与承建方的承建合同； 1.3本项目采购文件、响应文件； 1.4监理服务合同、建设合同； 1.5本项工程规划设计方案； 1.6本项工程的实施方案； 1.7GB 50174《数据中心设计规范》； 1.8GB/T 8567《计算机软件文档编制规范》； 1.9.GB/T 19668.1信息技术服务监理第1

		部分：总则； 1.10.GB/T 19668.2 信息技术服务监理第 2 部分：基础设施工程监理规范； 1.11.GB/T 19668.3 信息技术服务监理第 3 部分：运行维护监理规范； 1.12.GB/T 19668.4 信息技术服务监理第 4 部分：信息安全监理规范； 1.13.GB/T 19668.5 信息技术服务监理第 5 部分：软件工程监理规范； 1.14 GB/T 19668.6 信息技术服务监理第 6 部分：应用系统数据中心工程监理规范； 1.15.国家发改委第 55 号令《国家电子政务工程建设项目管理暂行办法》

3.2.3 人员配置要求

采购包 1：
按需求配置

3.2.4 设施设备要求

采购包 1：
按需求配置

3.2.5 其他要求

采购包 1：
1.供应商为本项目提供技术服务方案：包含①测评指标、②被测系统网络拓扑及资产清单、③被测系统密码应用现状分析、④风险告知及规避对策、⑤人员安排及时间进度安排、⑥安全物理环

境、⑦安全通信网络、⑧安全区域边界、⑨安全计算环境、⑩安全管理中心、⑪安全管理制度、⑫安全管理机构、⑬安全管理人员、⑭安全系统建设及安全系统运维管理、⑮监理整体方案； 2.履约能力：具有类似项目业绩的实施案例。3.人员配置： 项目总测评师（1 人）具有以下有效证书：①具有网络安全等级测评师高级证书，②具有商用密码应用安全性评估人员能力合格证书，③具有信息系统监理证书，④具有软件测试工程师证书，⑤具有计算机技术与软件专业资格信息安全工程师，⑥具有国家重要信息系统保护人员证书（CIIP-A），⑦具有注册渗透测试工程师（CISP-PTE），⑧具有系统架构师（高级），⑨具有网络信息安全工程证书，⑩具有网络安全管理（I 级）。 项目经理（1 人）具有以下有效证书： ①具有信息安全等级测评师高级证书，②具有信息技术应用创新考试评价证书（信创规划管理师），③具有信息安全保障人员认证证书（CISAW）认证方向：风险管理（专业级），④具有网络工程师（高级），⑤具有软件性能测评师高级，⑥具有系统架构师（高级）⑦具有国家重要信息系统保护人员证书（CIIP-A）。 其他测评人员具有以下有效证书： ①具有商用密码应用安全性评估人员能力合格证书，②具有国家重要信息系统保护人员证书（CIIP-A），③具有信息系统监理师证书，④具有注册网络安全渗透评估专业人员，⑤具有网络信息安全工程证书，⑥具有网络安全技术（I 级），⑦具有注册渗透测试专家（CISP-PTS） 。4.质量体系：供应商通过质量体系认证，且认证范围包括“信息安全等级保护测试评估服务、商用密码应用安全性评估、软件测评”； 通过信息安全管理系统认证，且认证范围包括“信息安全等级保护测试评估服务、商用密码应用安全性评估、软件测评”；通过环境管理体系认证，且认证范围包括“信息安全等级保护测试评估服务、商用密码应用安全性评估、软件测评”；通过职业健康安全管理系统认证，且认证范围包括“信息安全等级保护测试评估服务、商用密码应用安全性评估、软件测评”

3.3、商务要求

3.3.1 服务期限

采购包 1：

自合同签订之日起 365 日

3.3.2 服务地点

采购包 1：

采购人指定地点

3.3.3 考核（验收）标准和方法

采购包 1：

按本竞争性磋商文件 2.6.5 履约验收方案执行

3.3.4 支付方式

采购包 1：
分期付款

3.3.5 支付约定

采购包 1： 付款条件说明： 合同签订后，成交供应商向采购人提供合法、等额、有效的发票后 ，达到付款条件起 12 日内，支付合同总金额的 40.00%。
采购包 1： 付款条件说明： 服务期限结束后出具全部成果报告，成交供应商向采购人提供合法、等额、有效的发票后 ，达到付款条件起 12 日内，支付合同总金额的 60.00%。

3.3.6 违约责任及解决争议的方法

采购包 1：
1、双方必须遵守本合同并执行合同中的各项规定，保证本合同的正常履行。 2、甲方无正当理由逾期付款的，除应及时付足款项外，应向乙方偿付应付而未付款总额万分之五/天的违约金；但累计违约金不得超过应付而未付款总额的 5%。 3、除考核办法约定的情形外，供应商提供的服务不符合本合同规定的，每出现一天违约（合同涉及“日期”和“天数”的，逾期一天或少一天视为一天），供应商须向采购人支付本合同总金额 5%的违约金并且按甲方要求进行整改，出现违约__3__次及以上或未按采购人要求整改的，采购人有权无条件解除本合同并根据实际情况要求供应商退还已收取的费用。 4、如因乙方工作人员在履行职务过程中的疏忽、失职、过错等故意或者过失原因给甲方造成损失或侵害，包括但不限于甲方本身的财产损失、由此而导致的甲方对任何第三方的法律责任等，乙方应支付合同总价万分之五/天的违约金，并承担全部的赔偿责任。 5、任何一方不得擅自变更、中止或者终止合同。若合同发生变更、中止或终止的，有过错的一方应当承担赔偿责任，双方都有过错的，各自承担相应的责任。 6、供应商保证本合同所涉产品的权利无瑕疵，包括所有权和知识产权等权利无瑕疵，不侵犯任何第三方的合法权益。如任何第三方经法院（或仲裁机构）裁决有权对上述产品主张权利，由供应商承担经济责任的，供应商除应向采购人返还已收款项及利息外，还应另按合同总价的 5%向采购人支付违约金并赔偿因此给采购人造成的一切损失，包括采购人因诉讼产生的律师费、诉讼费等费用。 7、如果供应商违反保密义务的，采购人有权解除本合同并要求供应商赔偿合同总金额 5%的违约金，供应商还应退还采购人已支付的全部款项。供应商及涉事人员还需承担相关的法律责任。 8、供应商偿付的违约金不足以弥补采购人损失的，还应按采购人损失尚未弥补的部分，支付赔偿金给采购人。9、合同签订后，若供应商存在违法违规行为的，采购人有权无条件解除本合同并要求供应商退还已经支付但尚未产生的费用。 10、如果合同双方在履行本合同过程中发生争议，双方首先应当采取协商的方式解决该争议，如果协商不成，双方同意选择向甲方所在地人民法院提起诉讼。11、对任何争议进行诉讼，除争议事项或争议事项所涉及的条款外，双方应继续履行本合同项下的其它义务。

3.4 其他要求

本项目全部商务要求及 3.4 其他要求均为实质性要求，供应商必须响应并满足所有要求，若不满足，响应文件做无效处理。