采购需求

一、项目概况

陕西省卫生健康监督中心信息系统安全等级保护备案采购项目

二、服务要求

（一）服务内容

1、项目概况：对我单位 4 个系统进行网络安全等级保护测评及备案工作。（详见附件一）

2、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。

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信息系统中的相关资产进行测评项的检查、记录检查结果。

4、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。

5、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。

6、对我单位相关人员进行网络安全的培训。

7、配合验收：整理项目过程中所有相关的过程文档，提交系统相关人员。

附件一：

信息系统等级保护测评工作系统名称

序号	名称	等保等级	备注
1	省卫生监督综合业务平台信息系统	三级	
2	中心网站信息系统	二级	
3	食品企业标准备案管理系统	二级	
4	医疗机构放射人员培训系统	二级	

说明：在测评系统总数不变情况下，甲方可根据实际工作需要，自行调整测评系统。

（二）项目技术标准及要求

1. 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,最终出具《信息系统安全等级测评报告》。

2. 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、安全管理中心测评，以及安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理测评十个安全类别进行安全测评

（1）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。测评指标如下：

第三级测评指标表

测评指标			
技术管理	**安全类**	**安全控制点数量**	**测评项数量**

测评指标						
		S	A	G	小计	
安全技术要求	安全物理环境	1	1	8	10	22
	安全通信网络	1	0	3	3	8
	安全区域边界	1	0	5	6	20
	安全计算环境	8	1	2	11	34
	安全管理中心	0	0	4	4	12
安全管理要求	安全管理制度	0	0	4	4	7
	安全管理机构	0	0	5	5	14
	安全管理人员	0	0	5	4	12
	安全建设管理	0	0	10	10	34
	安全运维管理	0	0	14	14	48
					71	211

第三级测评指标要求项表

安全类	安全控制点	测评项数
安全物理环境	物理位置的选择（G3）	2
	物理访问控制（G3）	1
	防盗窃和防破坏（G3）	3
	防雷击（G3）	2
	防火（G3）	3
	防水和防潮（G3）	3
	防静电（G3）	2
	温湿度控制（G3）	1
	电力供应（A3）	3

安全类	安全控制点	测评项数
	电磁防护（S3）	2
安全通信网络	网络架构（G3）	5
	通信传输（G3）	2
	可信验证（S3）	1
安全区域边界	边界防护（G3）	4
	访问控制（G3）	5
	入侵防范（G3）	4
	可信验证（S3）	1
	恶意代码防范（G3）	2
	安全审计（G3）	4
安全计算环境	身份鉴别（S3）	4
	访问控制（S3）	7
	安全审计（G3）	4
	可信验证（S3）	1
	入侵防范（G3）	6
	恶意代码防范（G3）	1
	数据完整性（S3）	2
	数据保密性（S3）	2
	数据备份恢复（A3）	3
	剩余信息保护（S3）	2
	个人信息保护（S3）	2
安全管理中心	系统管理（G3）	2
	审计管理（G3）	2

安全类	安全控制点	测评项数
	安全管理（G3）	2
	集中管控（G3）	6
安全管理制度	安全策略（G3）	1
	管理制度（G3）	3
	制定和发布（G3）	2
	评审和修订（G3）	1
安全管理机构	岗位设置（G3）	3
	人员配备（G3）	2
	授权和审批（G3）	3
	沟通和合作（G3）	3
	审核和检查（G3）	3
安全管理人员	人员录用（G3）	3
	人员离岗（G3）	2
	安全意识教育和培训（G3）	3
	外部人员访问管理（G3）	4
安全建设管理	定级和备案（G3）	4
	安全方案设计（G3）	3
	产品采购和使用（G3）	3
	自行软件开发（G3）	7
	外包软件开发（G3）	3
	工程实施（G3）	3
	测试验收（G3）	2
	系统交付（G3）	3

安全类	安全控制点	测评项数
	等级测评（G3）	3
	服务供应商管理（G3）	3
安全运维管理	环境管理（G3）	3
	资产管理（G3）	3
	介质管理（G3）	2
	设备维护管理（G3）	4
	漏洞和风险管理（G3）	2
	网络与系统安全管理（G3）	10
	恶意代码防范管理（G3）	2
	配置管理（G3）	2
	密码管理（G3）	2
	变更管理（G3）	3
	备份与恢复管理（G3）	3
	安全事件处置（G3）	4
	应急预案管理（G3）	4
	外包运维管理（G3）	4

第二级系统测评指标

测评指标						
技术管理	安全类	安全控制点数量				测评项数量
		S	A	G	小计	
安全技术要求	安全物理环境	1	1	8	10	15
	安全通信网络	1	0	3	3	4
	安全区域边界	1	0	5	6	11

测评指标						
	安全计算环境	7	1	2	10	23
	安全管理中心	0	0	2	2	4
安全管理要求	**安全管理制度**	0	0	4	4	6
	安全管理机构	0	0	5	5	9
	安全管理人员	0	0	4	4	7
	安全建设管理	0	0	10	10	25
	安全运维管理	0	0	14	14	31
					68	135

第二级测评指标要求项表

安全要求	安全分类	安全子类	测评要求项数
安全通用要求	安全物理环境	物理位置选择	2
		物理访问控制	1
		防盗窃和防破坏	2
		防雷击	1
		防火	2
		防水和防潮	2
		防静电	1
		温湿度控制	1
		电力供应	2
		电磁防护	1
	安全通信网络	网络架构	2
		通信传输	1
		可信验证	1

	安全区域边界	边界防护	1
		访问控制	4
		入侵防范	1
		恶意代码	1
		安全审计	3
		可信验证	1
	安全计算环境	身份鉴别	3
		访问控制	4
		安全审计	3
		入侵防范	5
		恶意代码防范	1
		可信验证	1
		数据完整性	1
		数据备份恢复	2
		剩余信息保护	1
		个人信息保护	2
	安全管理中心	系统管理	2
		审计管理	2
	安全管理制度	安全策略	1
		管理制度	2
		制定和发布	2
		评审和修订	1
	安全管理机构	岗位设置	2
		人员配备	1

		沟通和合作	3
		审核和检查	1
	安全管理人员	人员录用	2
		人员离岗	1
		安全意识教育和培训	1
		外部人员访问管理	3
	安全建设管理	系统和备案	4
		安全方案设计	3
		产品采购和使用	2
		自行软件开发	2
		外包软件开发	2
		工程实施	2
		测试验收	2
		系统交付	3
		等级测评	3
		服务供应商选择	2
	安全运维管理	环境管理	3
		资产管理	1
		介质管理	2
		设备维护管理	2
		漏洞和风险管理	1
		网络和系统安全管理	5
		恶意代码防范管理	3
		配置管理	1

		密码管理	2
		变更管理	1
		备份与恢复管理	3
		安全事件处置	3
		应急预案管理	2
		外包运管理	2
		移动应用软件开发	2

3. 第二阶段：建设整改咨询

根据测评结果内容，分析信息系统安全情况与等级保护基本要求的差距，并进行风险分析，尚易安华出具科学合理的整改建议及整改方案，配合中国电信西安分公司进行安全整改方案制定和信息安全整改工作。

所谓信息安全是“三分管理，七分技术”，在进行建设整改工作时一般建议先进行安全管理整改，再进行安全技术整改，有利于开展整改工作。

具体流程如下图所示：

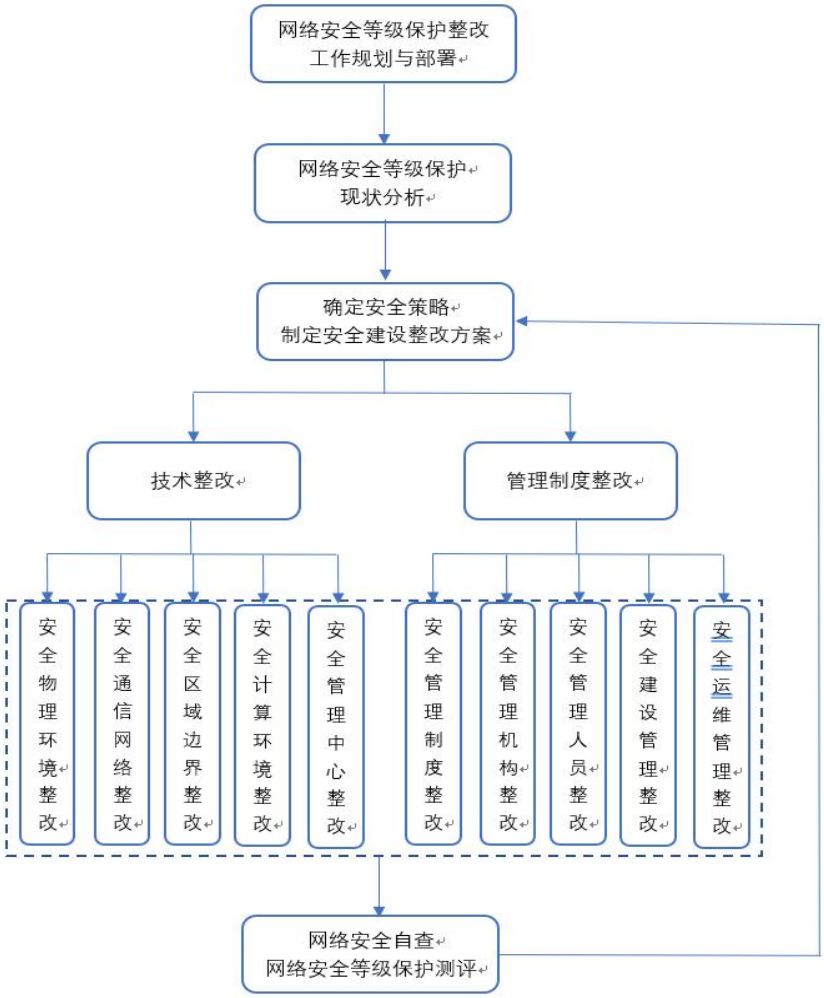

图 1：整改流程图

信息安全等级保护安全建设整改工作中，严格遵循国家有关规定和标准规范要求，坚持管理和技术并重的原则，将技术措施和管理措施有机结合，建立信息系统综合防护体系，提高信息系统整体安全保护能力。按照《基本要求》的相关要求，落实信息安全责任制，建立并落实各类安全管理制度，开展人员安全管理、系统建设管理和系统运维管理等工作，落实物理安全、网络安全、主机安全、应用安全和数据安全等安全保护技术措施，具体内容整改内容如下所示。

图 2：安全整改建设内容

根据信息系统定级时的业务信息安全等级和系统服务安全等级，以及信息系统安全保护现状确定信息系统的具体整改事项。根据现状测评工作中发现的安全问题，进行风险分析，发现其中的共性的安全技术问题和个性的信息安全需求，进而为技术整改提供有力的支撑。对于安全管理中存在的问题，提供安全管理体系建设的整改及相关咨询。

4. 第三阶段：售后服务

为期一年的售后服务工作中，供应商将向客户信息系统提供包括配合检查、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）配合检查服务

供应商免费协助客户信息系统响应公安机关、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。服务内容包括协助客户信息系统准备、

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。

（2）电话支持服务

每周 7 天/每天 24 小时不间断的电话支持服务，解答金融控股集团信息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 30 分钟，到达现场时间不超过 2 小时。

（三）服务团队要求

供应商项目团队不少于 8 人，其中至少包含 1 名高级测评师，3 名中级测评师和 4 名初级测评师。且供应商必须为本项目成立本地化等级保护测评小组团队，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。

（四）交付内容

1.《信息系统安全等级测评报告》；

2.《信息系统整改建议书》；

3.《信息系统渗透测试报告》。