附件3

全省农信互联网信息系统网络安全监测

服务需求及技术要求

一、项目概况

为有效应对全省行社自建互联网系统数量多、风险高、管控不足、频繁被监管部门通报漏洞的复杂局面，自主、全面、持续检查和发现全省互联网系统安全风险，做到风险漏洞的持续监测、自主发现、快速预警、及时整改，拟开展全省农信互联网系统网络安全监测服务项目。

二、服务需求

**1、项目目标**

该项目通过采购全省农信互联网信息系统网络安全监测服务，自主、全面、持续监测全省农信互联网信息系统的网络安全风险，做到早预警、早监测、早整改。

**2、服务范围**

贵州省农村信用社联合社以及贵州辖内各信用联社、农商银行。

1. **服务内容**

3.1互联网资产测绘和管理

提供基于互联网的全网资产测绘平台服务，全天候对互联网IT资产、移动资产、数据资产等维度进行资产测绘、梳理并明确归属，从外部攻击者视角挖掘潜在可被利用的攻击风险，解决互联网资产维度广、攻击路径发现难、安全运营成本高等问题，实现对招标人互联网网络空间资产的全面测绘。通过资产测绘平台测绘及人工甄别，持续对贵州农信全省行社互联网系统资产进行收集、识别、管理、监控，形成完整的、准确的、动态的互联网信息资产台账。该项服务至少应包含但不限于以下内容：

3.1.1 应提供互联网资产测绘平台的3年使用许可和技术支持。

3.1.2 平台应支持持续性探测全球IPv4、IPv6地址，做到实时感知全球网络空间中各类资产并发现安全风险。支持互联网资产暴露面维度包括IT资产(域名、IP、端口、网站、指纹、主机漏洞、应用漏洞、弱口令、高危端口、管理后台等)、移动资产、数据资产等，通过定期持续化监测资产风险变化情况，掌握招标人在外部暴露面全貌及变化动态。

3.1.3在合同服务期内，投标人通过资产测绘平台及人工甄别，对招标人暴漏在互联网上的资产进行发现与测绘，充分、全面、详细的梳理招标人辖下各法人机构的互联网域名、互联网IP与端口、开放的高危端口、APP、微信小程序、微信公众号、web页面、H5页面等资产，以各法人单位为维度输出互联网资产清单。每季度开展1次全面资产测绘，输出4次完整的互联网资产清单。通过相应平台工具进行互联网资产管理，开展互联网资产实时变更监控，及时发现招标人互联网资产的变动，使招标人掌握本机构实时互联网资产信息，每月输出互联网资产变更清单，输出12次互联网资产变更清单。

3.1.4在资产及应用发现的基础上，招标人对招标人互联网网站应用进行安全监测，提供网站漏洞扫描、网页篡改监测、网页挂马监测、黑词/暗链监测、可用性监测、未知资产监测等安全云监测，持续挖掘网站风险，充分预警各类网站安全事件。

3.2 互联网系统漏洞监测扫描平台

在招标人本地化部署互联网系统漏洞监测扫描平台，提供3年软件授权和技术支持，采用7\*24h情报加主被动漏洞探测的方式，对全省行社互联网系统主机漏洞、应用漏洞、WEB漏洞、弱口令漏洞、数据泄露、网站挂马或篡改等进行监测预警，开展主机漏洞扫描、WEB漏洞扫描、弱口令扫描、自动化渗透等测试，为招标人提供攻击视角下的漏洞监测、扫描、挖掘能力，帮助梳理、自动发现资产漏洞，落实内部漏洞整改措施，实现资产从发现到风险处置的全流程管理，输出详细系统漏洞监测扫描报告。授权到期后，每年付费维保报价应低于该分项报价的10%。互联网系统漏洞监测扫描平台至少包含但不限于以下能力：

3.2.1 应支持个性化、定制化扫描策略，应支持周期性或定时自动扫描，应具备实时监测与预警功能，应支持通过漏洞情报赋能，利用POC插件进行全网检测，实现自动匹配预估受影响可疑资产，快速提升漏洞应急水平。

3.2.2 应可对主流的操作系统、服务、应用程序进行弱口令检测，自动识别存在的常见弱口令；可对web类资产进行应用漏洞检测，自动识别SQL注入、XSS跨站脚本、敏感信息泄露、CSRF跨站请求伪造、文件上传漏洞、目录便利漏洞等常见web应用漏洞；可通过对IP资产端口开展漏洞扫描，自动发现主机安全漏洞。

3.2.3 应可支持常见应用漏洞的自动化渗透测试，可对渗透测试的信息收集、漏洞扫描、漏洞利用、权限提升、证据收集等步骤实现自动化处理。应在填入目标网络地址（IP+端口或URL链接等）后可直接进行自动测试评估，进行安全测试评估时应没有任务、IP限制，一次可对多个目标进行渗透测试。应可人工选择不同的渗透测试强度，避免影响被测业务系统的正常运行。应能设置和完成自动渗透测试工作流，能设定渗透测试工作流的自动执行计划。

3.2.4应可对漏洞风险进行安全管控，其中漏洞扫描的漏洞库数量不少于 20万条，覆盖CVE编号数量不低于 15万个。能对漏洞进行精确检查，各类安全检查项总数不低于50万个。支持漏洞详细信息展示，包括但不限于：CVE编号，CNNVD编号，原厂链接，漏洞风险，分类细节，漏洞发布时间，漏洞检测项修改时间，严重性分类等。

3.2.5 应可对已发现的漏洞，实现漏洞全生命周期管理，对漏洞状态和处置流程进行跟踪，如新增、遗留、减少、已加固、误报、待复测等，并能对漏洞状态分布、业务分布等进行统计，掌握信息系统漏洞整体状况。

3.3 互联网系统漏洞人工发现与处置

通过专业的安全服务工程师驻场服务对全省行社互联网系统进行信息资产人工确认、扫描报告人工甄别、手工渗透测试、手工漏洞探测、漏洞核实与报告整理、漏洞整改指导、漏洞复测等工作。

3.3.1 驻场人员主要工作内容

根据招标人安排，完全模拟黑客可能使用的攻击技术和漏洞发现技术，在不影响信息系统正常运行情况下，进行全面深入的手工渗透测试与漏洞探测， 及时发现存在的漏洞，出具详细漏洞报告。对常见漏洞或共性问题进行专项排查。对互联网系统漏洞监测扫描平台自动扫描结果进行人工甄别和验证，出具详细、客观、可读的扫描报告。对漏洞整改与系统加固提出有效方案。对修复后的漏洞进行复测并出具复测报告。管理、汇总和分析已发现漏洞。开展安全漏洞通告和重大安全事件通告等。

3.3.2 驻场人员数量及时间

专业安全人员2人，现场驻场1年。

3.3.3 驻场人员要求

驻场人员须专业能力突出、项目经验丰富，须至少具备PMP、CISP、CISSP、CISA、CISP-PTE、CISP-PTS、CISP-IRE、CISP-IRS、安全厂商专家认证、网络工程师、信息安全工程师、CNVD漏洞证明中的2项证书，须具有3年（含）以上相关工作经验。

1. **服务期限**

从合同签订之日起一年。

1. **服务团队**

投标人要组建专业能力突出、项目经验丰富的团队开展相应服务，在入场前要提前指定项目经理和项目人员，提交项目人员分工情况说明、个人简历、项目履历等相关材料工招标人审核。对不符合招标人要求的投标人项目人员和驻场人员，招标人随时可以提出人员更换要求。投标人不得随意更换项目经理和驻场人员，若因特殊情况确需更改项目经理和驻场人员的，应出具正式更换的函件并征得招标人同意。

1. **服务质量要求**

投标人应及时、有效、充分发现招标人互联网信息系统存在安全漏洞，若因投标人在服务过程中未及时发现招标人信息系统安全漏洞导致招标人被外部监管机构（如人行、银监、通管局、网信办、网安部门等）通报的，招标人有权按照通报数量和级别扣减应付款项：

1. 入场实施后3个月起算，到合同结束为止，招标人（含省联社及各分支机构）的互联网信息系统被外部监管机构通报中危漏洞的，每通报一个漏洞，扣减人民币一万元。
2. 入场实施后3个月起算，到合同结束为止，招标人（含省联社及各分支机构）被外部监管机构通报高危或严重漏洞的，每通报一个漏洞，扣减人民币两万元。

（3）因被外部通报而扣减的应付金额，不应超过合同总金额的30%。