**附件1**

灰盒测试工具（IAST）技术及服务要求

一、服务内容

（一）中标方应完成灰盒测试工具服务器本地部署。按招标方要求，通过定制化开发，以插件形式完成与招标方DevOps平台的对接。

（二）中标方应按招标方要求批量完成所需测试环境的插桩工作。

（三）中标方完成验收工作后，应提供一年的维保服务。

二、总体要求

（一）本项目所涉及的产品技术服务须由产品厂商专家技术团队完成。其中系统部署调试等重要工作须由产品厂商总体负责。项目的具体实施方式由招标方根据项目建设需要动态调整。

（二）拟派实施工程师应具有3年及以上灰盒测试工具部署及维护经验。同时，近三年参与过2家及以上金融机构项目实施案例。

（三）中标方的项目成员须根据招标方的计划安排全职参与项目的建设，在建设过程中，若中标方项目组成员未能达到招标方要求，招标方有权要求中标方更换项目人员，由此造成的项目延误由中标方承担责任。

（四）中标方须与招标方签署安全保密协议，在未经招标方许可前，服务商及其服务人员均不得向第三方透露与招标方有关的信息系统、数据资料、管理制度、人员安排等相关信息，也不得利用本项目服务期间获取的招标方各类信息进行相关宣传、交流活动。

（五）服务过程中产生的一切数据、文档、软件程序源代码所有权归招标方所有。

（六）产品无license授权限制，插桩数不限。

三、功能需求

供应商提供的灰盒测试工具应符合以下要求：

（一）基础功能

1.项目管理：支持不同部门/项目组进行数据权限隔离，部门/项目组层级下以不同子系统、版本进行漏洞管理。

2.漏洞描述：漏洞描述一般包括漏洞名称、漏洞等级、漏洞状态、漏洞类型、漏洞发现模式、漏洞发现时间、漏洞地址、漏洞判断依据（漏洞触发的HTTP信息或者数据流信息）、漏洞详细描述、漏洞修复方案、数据流完整信息、请求完整信息。

3.漏洞利用展示：针对检测出来的漏洞，可进行漏洞利用操作（例如窃取数据、执行命令、读取敏感文件、反弹shell等）展示漏洞的危害细节。

4.漏洞复测：针对检测出来的安全漏洞，可进行漏洞回归测试以验证漏洞的排查和修复情况。

5.漏洞修复建议：针对不同开发语言、不同漏洞类型提供详细的代码修复示例。

6.漏洞操作：漏洞处理支持批量操作，包括但不限于批量添加漏洞审计信息、批量漏洞修改状态等操作。

7.漏洞查询：支持以不同部门/项目组、子系统、版本、漏洞类型、漏洞等级、漏洞状态、漏洞发现时间、漏洞地址等信息进行查询漏洞，并支持查询结果导出至附件。

8.漏洞自定义：支持修改漏洞默认的等级、描述信息、修复方案等信息。

9.漏洞导出：支持以常见格式（XML/JSON/EXCEL/WORD/PDF）进行漏洞导出，生成报告可自定义报告名称、logo等信息，以贵州农信实际需求为准。

10.漏洞继承功能：对于同一子系统的不同版本，上一版本审计的漏洞信息在后续版本中重复出现时可自动继承上一版本漏洞审计信息。

11.报告合并：对于不同扫描节点的扫描测试结果，支持漏洞报告以子系统和版本维度进行漏洞报告合并。

12.API功能：对接所需功能模块、页面均提供API调用方式支持。

13用户认证：支持本地用户、LDAP等认证方式。

14.权限管理：支持以本地用户、LDAP导入用户进行新建用户，并以部门/项目组、子系统为维度树状进行权限管理。

15.角色管理：支持自定义角色功能（例如自定义超级管理员、部门管理员、普通用户等不同角色进行管理）。

（二）系统架构

1.产品功能架构:通常包括管理后台、Agent插桩、流量代理、扫描引擎等组件。管理后台包括不限于项目管理、漏洞管理、部署实现管理、扫描策略管理、扫描引擎管理、系统管理等功能；Agent插桩可独立部署在被测应用服务器上，进行安全漏洞检测及漏洞上报；流量代理可获取功能测试的流量信息；扫描引擎可在流量模式时根据扫描规则进行安全漏洞扫描。

2.Agent部署:提供不同语言/不同容器的Agent下载功能以及部署指引，Agent部署支持命令行方式部署。

3.Agent注册:支持以自动化、批量形式进行Agent注册。

4.Agent更新:支持配置热更新、版本在线更新等方式进行更新。

5.Agent监控:支持监控Agent状态信息，包括连接状态、版本、注册子系统等信息。

6.Agent性能熔断机制:支持配置（例如服务器内存资源或cpu资源使用率达到80%）主动关闭Agent运行（停止Agent运行进程）、以及手动远程触发启停Agent运行的功能。

7.分布式部署:支持管理后台分布式部署，支持快速弹性扩缩。

8.高并发处理能力:支持对agent的高并发处理,流量模式扫描时支持高并发处理。

9.管理后台高可用:管理后台支持高可用部署。

11.扫描调度:流量模式扫描时支持集群组模式进行扫描调度。

12.扫描线程数配置:支持扫描线程数自定义配置。

13.扫描引擎监控:支持扫描引擎监控，监控信息包括扫描引擎信息、所在集群、扫描状态、心跳等信息。

（三）漏洞检测

1.产品功能架构:通常包括管理后台、Agent插桩、流量代理、扫描引擎等组件。管理后台包括不限于项目管理、漏洞管理、部署实现管理、扫描策略管理、扫描引擎管理、系统管理等功能；Agent插桩可独立部署在被测应用服务器上，进行安全漏洞检测及漏洞上报；流量代理可获取功能测试的流量信息；扫描引擎可在流量模式时根据扫描规则进行安全漏洞扫描。

2.Agent部署:提供不同语言/不同容器的Agent下载功能以及部署指引，Agent部署支持命令行方式部署。

3.Agent注册:支持以自动化、批量形式进行Agent注册。

4.Agent更新:支持配置热更新、版本在线更新等方式进行更新。

5.Agent监控:支持监控Agent状态信息，包括连接状态、版本、注册子系统等信息。

6.Agent性能熔断机制:支持配置（例如服务器内存资源或cpu资源使用率达到80%）主动关闭Agent运行（停止Agent运行进程）、以及手动远程触发启停Agent运行的功能。

7.分布式部署:支持管理后台分布式部署，支持快速弹性扩缩。

8.高并发处理能力:支持对agent的高并发处理,流量模式扫描时支持高并发处理。

9.管理后台高可用:管理后台支持高可用部署。

10.扫描调度:流量模式扫描时支持集群组模式进行扫描调度。

11.扫描线程数配置:支持扫描线程数自定义配置。

12.扫描引擎监控:支持扫描引擎监控，监控信息包括扫描引擎信息、所在集群、扫描状态、心跳等信息。

（四）其他

1.知识产权实力:中标方应具备产品软件著作权。

2.兼容性：与听云监控平台等基于字节码增强技术的监控平台相互兼容。

3.接入DevOps平台：负责插件定制化开发，通过插件形式接入招标方DevOps平台。同时，通过DevOps平台自动推送代理，完成大部分自动化插桩工作。

四、交付及验收要求

（一）项目规划及建设须符合国家网络安全法律法规，满足人民银行、银保监局监管要求等。且根据招标方项目建设安排限时完成系统安装、调试及系统适配等工作。

（二）项目交付物包括但不限于安装部署手册、用户说明书、运行维护手册、常用语言编码规范、工具规则配置基线、工具培训资料、配套制度规范等文件。

（三）在工具投产使用并稳定运行3个月后进行。验收内容包括：系统运行情况、系统配套文档等。中标人提交的验收内容和资料，应准确、真实、易读，如招标方对中标人所提交材料的完整性、准确性、规范性等存在异议，中标人须按要求重新整理后提交招标方。

（四）满足验收条件后，由中标方提出验收申请，招标方对提供的验收材料进行审核；审核通过后，招标方组织项目验收小组验收，届时中标方需有至少2人参加；验收时，现场给出验收结果。

五、维保服务要求

中标方须提供原产品厂商一年（或以上）维保服务，维保时间自项目竣工验收通过之日起计算，要求提供原厂针对本项目的授权原件及维保服务承诺书原件，并在维保期内提供规范化、高质量的维保服务，需提供以下维保服务：

1. 维护技术支持：根据招标方需求，中标方安排技术人进行长期驻场系统维护工作，一是负责日常的工具规则调优以及插桩工作；二是协助漏洞识别、误报漏洞确认、漏洞修复等工作；三是每月进行例行巡检，出具巡检报告并加盖公章，对巡检过程中出现的问题，中标人需配合整改优化。

2.漏洞库更新：中标方应定期（频率不低于每月一次）或在重大漏洞发布后及时更新漏洞库。

3.远程技术支持：招标方在遇到使用问题或系统一般问题时，乙方提供电话技术指导、邮件指导或现今通用的各种远程方式，做系统维护和技术支持工作，远程技术支持不限次数。

4.技术服务支持：当集群架构有所调整时原产品厂商需提供技术服务支持。必要时，原厂技术工程师须提前1天内到达现场，配合招标人做好规划实施。

5.升级服务：在原厂商提供升级与更新漏洞库等基础上，中标人还需免费提供系统版本更新、系统缺陷修复、必要的补丁更新等技术支持服务。

6.快速响应服务：系统出现故障不能正常工作时，招标人通过电话、邮件等方式通知后，中标人需在30分钟内通过远程诊断解决问题，如果通过电话、远程协助等方式无法使系统恢复正常，需在6小时内安排原厂技术工程师到现场进行故障定位及处置。

7.系统运行事故维护：维保系统出现故障导致单节点或整个集群故障时，具备快速重新搭建系统的能力，重新搭建时间需保证在24小时之内，如因系统版本缺陷问题导致，需及时提供系统补丁包，有必要时需提供其他稳定版本部署。

8.技术培训服务：为了更好的保障招标人系统安全稳定运行，维保服务期内中标人按需安排高级技术专家进行技术支持及培训交流工作，其中培训次数不得低于2次。