附件1

采购项目需求

开发安全管理平台及配套软件成分分析工具（SCA）

一、服务内容

（一）中标方应完成开发安全管理平台及软件成分分析工具服务器本地部署。按招标方要求，完成定制化功能开发。项目建设周期不超过12个月；

（二）中标方完成验收工作后，应提供一年的维保服务。

二、功能需求

（一）开发安全管理平台

1.平台基础

（1）产品功能架构

1）平台包括安全中心、策略中心、运维中心、安全需求设计中心、数据报表中心、待办事项等功能组件；

2）安全中心包括但不限于贵州农信源代码检测、灰盒测试、黑盒测试、软件成分分析等各个安全工具扫描结果详情查询、安全缺陷管理；

3）策略中心包括但不限于扫描策略管理、审核人配置、安全质量门禁配置、安全例外与豁免配置、系统授权；

4）运维中心包括但不限于流量监控、用户认证、角色管理、权限管理；

5）安全需求设计中心包括但不限于安全需求分析场景、安全设计与安全测试用例知识库；

6）数据报表中心按照贵州农信需求定制开发安全统计数据大屏展示，并提供相关报表管理功能；

7）待办事项可展示用户待办事项，内容包括但不限于待处理漏洞、待处理审批节点等贵州农信需要流转的办理事项。

（2）操作系统支持

支持贵州农信部署环境要求，例如Windows、linux、统信、麒麟等系统环境，支持物理机、云主机、虚拟机等部署环境。

（3）API功能

各个功能模块均支持对应API调用方式。

1. 系统可用性

平台各功能模块的请求、下载的并发、吞吐量需满足贵州农信的需求。

2.安全中心

（1）扫描结果详情

1）支持查看贵州农信各个安全工具的扫描结果详情，包括但不限于源代码扫描、组件扫描、黑盒扫描、灰盒扫描、APP扫描与加固、API检测等；

2）结果详情查询功能页面支持展示归属子机构/部门/职能组/人员，系统与版本信息，漏洞详情等信息；

3）漏洞详情信息包括：漏洞等级、漏洞状态、漏洞类型、漏洞来源、漏洞发现时间、漏洞发生代码文件/所在代码行、漏洞判断依据（漏洞触发的数据流信息）、漏洞详细描述、漏洞修复方案等；

**（2）安全缺陷管理**

1）扫描结果详情查询功能页面支持对漏洞进行批量操作，包括添加漏洞审计信息、漏洞修改状态、漏洞任务指派等；

2）漏洞批量审计操作有审批流程，即用户提交审计后，需要经过审批人审批（例如同意、驳回、征询等）后进入漏洞状态修改等环节；

3）平台支持用户在页面手工提交漏洞并上传测试报告或相关证明材料，提交内容包括数据来源，归属子机构/部门/职能组/人员，系统与版本信息，漏洞详情等。

（3）扫描报告导出

1）扫描结果详情查询功能页面支持以常见格式（例如WORD、EXCEL、PDF等）进行扫描报告导出；

2）扫描报告内容是否包括：系统与版本信息、系统归属公司/部门/职能组/人员、扫描时间、漏洞分布概述、漏洞详细描述等。

3.策略中心

（1）扫描策略管理

1）平台支持对贵州农信各个安全工具进行扫描策略管理，包括但不限于源代码扫描、组件扫描、黑盒扫描、灰盒扫描、APP扫描与加固等；

2）扫描策略管理功能需要支持对上述各个安全工具扫描策略进行新增、修改、禁用、等级调整操作，或管控漏洞黑/白名单，当高权限用户更新漏洞黑/白名单后，数据同步至对应工具的扫描结果详情页面以及流水线/版本安全质量门禁。

（2）用户角色管理

平台支持自定义用户角色功能（包括超级管理员、部门管理员、开发人员、测试人员、安全审计人员等等）不同角色进行管理。

（3）安全质量门禁配置

**平台支持以全局/部门维度设置安全质量门禁校验类型及阈值，例如需要完成需求分析且无风险等，相应数据应同步至蓝鲸DevOps流水线安全质量门禁插件。**

（4）系统授权

平台支持高权限用户对单个或批量的低权限用户进行单个或批量的系统的安全数据进行访问授权。

（5）安全例外与豁免配置

**1）平台支持用户在页面提交安全例外与豁免申请，经审核通过的数据应同步至对应工具扫描结果详情、流水线/版本安全质量门禁以及数据报表涉及的图表中；**

**2）平台支持高权限用户对单个或批量的系统进行安全例外与豁免配置，配置完成后应同步至对应工具扫描结果详情、流水线/版本安全质量门禁以及数据报表涉及的图表中；**

**3）安全例外与豁免配置适用场景包括但不限于无法进行安全扫描、不适用需求分析的版本/流水线。**

4.运维中心

（1）用户认证

平台支持本地用户、LDAP等认证、单点登录方式。

（2）权限管理

平台支持以本地用户、LDAP导入用户进行新建用户，并以公司/部门/职能组/员工、系统为维度树状进行权限管理。

（3）扫描监控

平台支持扫描引擎监控，监控信息包括但不限于扫描引擎信息、扫描状态、心跳等信息。

5.安全需求设计中心

（1）平台支持高权限用户通过页面新增、编辑、删除或导入固定格式的excel，对安全需求设计与安全测试用例知识库内容进行更新；

（2）平台支持高权限用户通过页面导出安全需求设计与安全测试用例知识库内容，导出格式为pdf、excel等贵州农信需求格式；

（3）支持安全需求分析、安全需求评审、安全设计、安全设计评审、安全编码、安全测试、安全验收以串联流程形式运转，并实现任务分配、处理、转派、知会、关闭等；

（4）支持安全需求文档、安全设计方案、测试案例、测试报告、各阶段评审报告文档导出等功能。

6.数据报表中心

平台支持对项目、职能组多维度的交付效能、安全工具的检测能力等进行可视化展示，例如展示应用系统版本数据、系统缺陷/风险情况、推广覆盖情况等。

7.待办事项

（1）平台支持展示用户当前待办事项；

（2）待办事项包括但不限于待修复漏洞、待审批事项等；

（3）新增的待办事项可通过黔农办公进行消息推送。

8.开发安全管理平台与DevOps平台数据交互

（1）DevOps平台承接项目管理，业务功能需求管理，制品库、代码库、组件库对接，编译、扫描、部署等流水线节点插件的支持，业务功能测试案例及测试缺陷管理。开发安全平台通过调取DevOps平台API接口，获取相关仓库配置信息、流水线状态信息等；

（2）开发安全管理平台与扫描工具进行对接，相关扫描信息、漏洞信息、安全配置数据由开发安全平台提供。同时，开发安全生命周期管理整个过程在开发安全管理平台实现，安全需求分析、安全需求评审、安全设计、安全设计评审、安全编码、安全测试、安全验收等相关数据由开发安全平台提供并开放相关API接口，**根据需要定制化开发蓝鲸DevOps平台插件，实现与蓝鲸DevOps平台数据交互。**

（3）安全扫描功能交互：

1）当DevOps平台的流水线执行到安全扫描插件节点时，需要返回扫描状态给开发安全平台；

2）当DevOps平台的流水线的安全扫描插件节点执行完毕后，开发安全平台需要返回扫描结果给DevOps平台的流水线；

3）当用户在开发安全平台完成安全漏洞审计操作后，需要返回漏洞状态给DevOps平台的流水线。

（4）安全门禁管控功能交互

1）开发安全平台需要返回扫描状态与结果到DevOps平台，由流水线上的安全门禁插件节点进行安全门禁校验；

2）DevOps平台的流水线上的安全门禁插件节点校验结果应返回开发安全平台；

3）当用户在开发安全平台完成安全漏洞审计操作后，需要返回漏洞状态给DevOps平台的安全门禁插件。

（5）安全豁免与安全例外功能交互：

当用户在开发安全平台完成安全豁免与安全例外审批流程后，需要返回状态给DevOps平台的流水线，以通过流水线；

1. 通过单点登录方式，实现DevOps平台与开发安全平台之间平滑跳转。

（二）软件成分分析工具

1.核心功能

（1）扫描引擎

本地化纯软件部署组件安全漏洞扫描工具，部署环境支持统信、麒麟等操作系统。

（2）IDE插件检测

1）支持本地化IDE插件使用组件安全漏洞扫描工具；

2）应尽可能支持开发工具中实时引用告警，在不能满足实时应用告警的情况下，至少支持插件推送检测等其他依赖平台的方式检测。

（3）支持扫描语言

支持主流编程语言的扫描，包括但不限于Java、Android、Python、C/C++、PHP、C#、HTML\JavaScript、Go、Objective-C、Swift。

（4）漏洞检测类型

支持代码成分分析、**代码片段分析**、文本内容协议识别、容器镜像分析、**二进制制品分析**。

（5）自定义策略

1）支持自定义漏洞及协议的风险等级、描述信息、修复方案等信息；

2）支持配置组件版本黑、白名单。

（6）扫描方式

1）支持B/S方式提交代码至平台发起扫描请求（包括上传本地代码压缩包、SVN、Git、TFS等方式进行扫描）；

2）支持本地提取代码特征后提交至后端scanner进行分析；

3）支持持续集成系统扫描（包括Jenkins、GitLab-CI集成扫描）。

（7）检测模式

支持分别检测生产依赖、开发依赖，并支持参数指定。

（8）代码级差异识别

可识别出二次开发与官方组件的差异，具备代码级组件风险验证能力。

（9）API功能

验证工具的漏洞管理平台中各个功能模块，是否均提供对应API调用方式支持(发起扫描,扫描状态检查,扫描结果,结果详情,漏洞详情,License信息,组件库查询)。

2.基础功能

1. 漏洞详情

可查看漏洞详情，漏洞详情信息包括但不限于漏洞等级、漏洞状态、漏洞类型、漏洞发现时间、漏洞发生代码文件/所在代码行、漏洞判断依据（引用路径）。

1. 漏洞修复示例

1）支持针对不同开发语言、不同类型组件均分别提供最优或通用修复方案及漏洞缓解方案；

2）至少需要满足能提供通用的升级修复方案；

3）建议能提供无需业务代码变动或变动最小的最优升级修复方案，且提供组件升级带来的变动说明；

4）建议能提供无法进行升级修复时的缓解方案。

（3）知识库更新

验证平台是否支持以全量、增量的方式离线、在线更新知识库并提供详细准确的changelog。

（4）扫描报告导出

支持以常见格式（JSON、XML、EXCEL、PDF）进行漏洞导出；

支持以不同标准规范进行自定义报告导出。

（5）高并发高可用支持

1）架构上支持高可用高并发，以报告论证支持日均完成贵州农信需求数量级的扫描；

2）支持快速自动化弹性伸缩；

3）支持不受限制的多并发同时进行扫描分析作业。

（6）日志功能

支持查看和导出应用日志。

（7）组件库功能

支持全量组件库的精确及模糊搜索。

（8）组件准确性保证

1）支持组件识别的准确度展示；

2）支持准确度阈值设置；

3）对于知识库中暂不存在的版本，能识别组件名称但不匹配为知识库中的错误版本。

3.许可证风险治理功能

（1）支持扫描协议

支持主流开源协议类型的扫描，包括但不限于AGPL、GPL、MPL、CC、EPL、CDDL、Apache、BSD、MIT。

（2）开源许可证风险判断及定位

支持依据软件清单（BOM）扫描结果综合分析系统开源许可证风险，并给予风险定级及风险定位。

（3）多许可证风险交叉判断

1）支持对单一系统多开源许可证及因引用或依赖不同开源许可证引发的多许可证之间的传染、叠加、豁免规则；

2）有明确规则确定最终风险，同时规则可公开。

（4）公共开源社区项目许可风险提示知识库

验证工具是否支持对公开开源社区项目引入前做许可证适用场景风险提示的知识库。

三、总体要求

1.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。

2.拟派实施工程师应具有5年及以上开发安全实施经验。同时，近三年参与过1家及以上金融机构与此项目服务内容相关的实施案例。

3.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，驻场完成系统部署及功能定制化开发等工作不低于120人天，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。

4.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。

5.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。

四、交付及验收要求

1．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、国家金融监督管理总局监管要求等。且根据招标方项目建设安排限时完成系统安装、调试及定制化功能开发、测试、系统适配等工作。

2．项目交付物包括但不限于安装部署手册、平台功能白皮书、用户使用说明书、运行维护手册、常用语言编码规范、平台培训资料、配套制度规范等文件。

3．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。中标方提交的验收内容和资料，应准确、真实、易读，如招标方对中标方所提交材料的完整性、准确性、规范性等存在异议，中标方须按要求重新整理后提交招标方。

4．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.服务方式包括但不限于现场人员支持、现场咨询、现场排除故障、电话咨询、远程支持等。

2.维护技术支持：根据招标方需求，中标方进行不定期驻场系统维护工作（驻场时间不低于36人天），一是负责平台与扫描工具、DevOps平台、办公消息推送平台以及其他平台的交互功能调优；二是协助漏洞识别、误报漏洞确认、漏洞修复等工作；三是技术咨询、故障诊断和故障排除；四是每月进行例行巡检，对巡检过程中出现的问题，中标方需配合整改优化，出具月度工作报告。

3.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软件成分分析工具漏洞库。

4.升级服务：在原厂商提供升级与更新漏洞库等基础上，中标方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。

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

6.系统出现异常时，如果通过电话、远程协助等方式无法使系统恢复正常，或者招标方认为有必要的情况下，招标方有权要求中标方到达现场进行支持服务。系统故障级别由招标方确定，中标方根据故障级别提供相应的应急响应机制。