[별지 제3호] 물품공급 또는 기술지원협약서

ㅇ 사 업 명 : 노후 보안관제시스템 현행화 사업
ㅇ 발주기관 : 공정거래위원회
ㅇ 제조사 또는 공급사 : ㈜스패로우

제1조(목적) 이 협약은 **소스코드진단 솔루션** 1식에 대하여 발주기관은 발주자로서 제조사 또는 공급사는 특수한 능력·품질의 납품능력을 보유하거나 제조할 수 있는 제조사(또는 공급사)로서 위 사업의 낙찰자에게 물품공급 또는 기술지원을 원활히 제공토록 하는 것을 목적으로 한다.

제2조(사용 및 협약의 범위) ①이 협약은 위 사업의 물품공급 또는 기술지원에 한해 사용범위를 제한한다.

②위 물품 중 제조사 또는 공급사가 낙찰자에게 물품공급 또는 기술지원을 해야하는 범위는 규격서(시방서)에 반영된 특수한 능력·품질의 납품능력이 요구되는 부분으로 한다.

③제2항에 의한 특수한 능력·품질 등의 납품능력이 요구되는 범위에 대하여 이견이 있는 경우에는 발주기관의 해석 및 판단에 따른다.

제3조(협약금액) 제2조에 따른 제조사 또는 공급사의 물품공급 또는 기술지원 범위에 대한 협약금액은 특수능력·품질 부분의 비중 등을 고려하여 발주기관과 제조사 또는 공급사가 협의하는 금액 **(37,450,000원 VAT포함)**으로 한다.

제4조(물품공급 또는 기술지원확약서 발급) 위 사업의 낙찰자와 제조사 또는 공급사는 이 약정의 범위 및 공정한 거래질서 등에 반하지 아니하는 범위 내에서 물품공급 또는 기술지원을 하기로 협의하고, 제조사 또는 공급사는 물품공급 또는 기술지원확약서를 낙찰자에게 발급하여야 한다.

2024년 3월 6일

발주기관 : 공정거래위원회 (인)

제조사 또는 공급사 : 스패로우 (인)

규 격 서(시방서)

2024년 2월

공정거래위원회

○ 프로젝트명 : 노후 보안관제시스템 현행화 사업

○ 금　　액 : 37,450,000원(VAT 포함)

○ 목　　적 : 형상관리시스템에서 관리하는 소스에 대한 취약점 분석 및 SBOM에 대한 보안성 강화

○ 특정제품필요성 : 공정거래위원회 도입된 기존 소스코드 취약점 분석도구와 호환을 위해 Sparrow 도입 필요

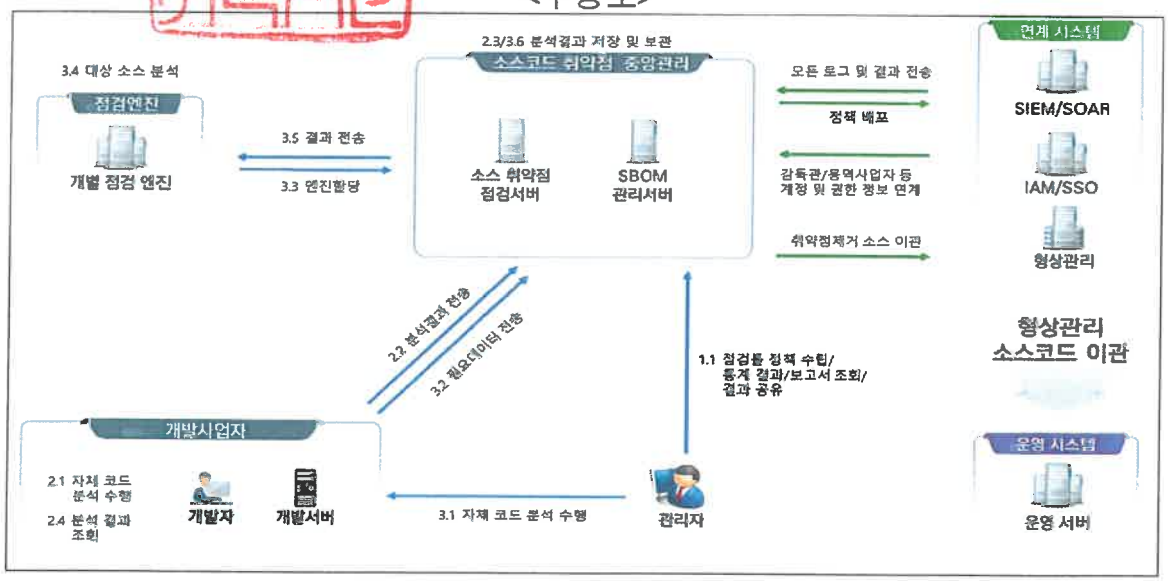
○ 대상시스템 :

- 보안관제시스템
  - Sparrow SAST v5.6 E Major Upgrade (통합)
  - Sparrow SCA v1.6, 1 Server (조달)
  - Sparrow SCA v1.6, 5 User (조달)

○ 도입시기 : 협의 후 결정

○ 기술지원내용

<구성도>



- 로그 및 정책관리는 업무망에서 관리 및 접근
- 망간 연계는 망연계 방식을 준수하여야 함
  - 연계 원칙은 단방향 통신, 파일전송 방식임

- IAM과 연계하여 사용자 및 권한 관리되어야 함
- 모든 로그 및 분석자료는 SOAR에 제공하여야 함
- SOAR에서 정책(롤, 기능 등)배포를 연계하여야 함
- 사용자에게 필요한 정보에 대해 알림 기능을 제공하여야 함
- SAST 솔루션은 국내용 CC인증 EAL2 이상, GS 인증(1등급)을 획득한 제품, SCA 솔루션은 GS인증(1등급)을 획득한 제품
- 영구 사용 가능 라이선스
- 전자정부 표준 프레임워크 3.0 호환성 인증을 획득한 제품
- 분석 용량(소스코드량)에 따른 제한이 없어야 함.
- 분석 필수언어 : C, C++, C#, Pro-C, JAVA, JSP, JavaScript, HTML, XML, SQL, PHP, ABAP, ASP.NET, VB.NET, VBS, Android-JAVA, Object-C, Swift, Python, Kotlin, React 등 다양한 언어 지원
- 지원 프레임워크 : 전자정부 표준 프레임워크, Spring Framework, IBATIS, MYBATIS, Struts2, Tmax Proframe, Vue.js, Node.js, 투비소프트 플랫폼(MiPlatform, XPlatform, Nexacro), BANCS 프레임워크, JSTL 라이브러리, MVC구조 분석 지원
- 행정안전부 소프트웨어 보안취약점 기준 49개 항목, 국정원 8대 보안취약점 항목, 전자금융감독규정, PCI-DSS, 주요 정보통신 기반시설 등의 항목 검출 지원 단면/양면/다면, 확대/축소 보기
- 다양한 방식의 정적분석 기법 제공 (Data Flow, Control Flow, Semantic, Configuration 등)
- 연관관계 분석을 제공해야 함
- 관리자가 중앙에서 점검정책 관리 및 배포가 가능해야 함
- 형상 관리 이관 제어시 기준 설정이 가능하여야 함
- 사용자가 시큐어코딩과 형상관리를 별도 관리하지 않도록 UI를 제공하여야 함
- 소스코드 중 함수에 대한 정의 및 관리 기능 제공
- 소스코드와 바이너리에 포함된 오픈소스 S/W이 보안 취약점을 진단하고 라이선스 식별 및 위반사항에 대한 점검이 제공되어야 함
- 소프트웨어 자재명세서 SBOM(Software Bill of Material)을 다양한 형식(SPDX, CyclonDX, SWID, NIS SBOM)으로 산출 가능해야 함
- 기도입된 시큐어코딩시스템(차세대사건처리시스템)에서 통합관리 필요