2025년 디지털인프라(SW) 진단 및 개선 사업 수요기업(기관) 모집 공고

과학기술정보통신부는 사회 전반의 안전 확보를 위하여 국민 안전과 밀접한 민간 및 공공시스템(SW)을 대상으로 SW안전 진단을 수행하고 개선방안을 지원하고 있습니다.

이에 정보통신산업진흥원, 한국인터넷진흥원 및 한국정보통신기술협회에서 진단 수요기업 및 공공기관을 모집하오니 관심 있는 기업 및 공공기관의 적극적인 참여를 바랍니다.

2025년 3월 4일

과학기술정보통신부장관
정보통신산업진흥원장
한국인터넷진흥원장
한국정보통신기술협회장

1 사업개요

□ 추진목적

○ 교통, 재난관리, 환경 등 국민 생활·안전과 밀접한 인프라의 SW 오작동 문제 등을 사전 진단 및 개선 지원함으로써 잠재적인 SW안전* 위협 요소를 미리 점검하고 안전사고 방지에 기여

* SW안전 : SW의 내부적인 오작동 및 안전 기능(위험발생 방지 기능) 미비 등으로 인하여 발생 가능한 사고 피해(생명, 신체 등)나 위험에 충분한 대비가 되어 있는 상태

□ 지원대상

○ 교통, 재난관리, 대민서비스 등 국민 생활·안전과 밀접한 분야*의 SW를 개발, 운영하거나 유지보수하는 민간기업 또는 공공기관

* 지원분야 例 : 자동차, 철도, 항공, 도로, 항만·해상, 에너지, 보건의료, 환경·식용수, 재난관리, 치안방범, 사회·생활안전, 대민서비스 등

※ SW 공급망 보안성 영역은 민간기업만 신청 가능

□ 지원내용

○ 진단영역 및 항목

진단영역	진단항목	주요내용	모집 규모*	수행 기관
시스템(SW) 안전성	안전기능	시스템 장애 등에 대비한 위험분석 및 안전 요구사항 도출, 표준 GAP 분석, 안전 설계 등 진단 및 개선 지원	13건 내외	TTA
	SW품질	SW 기능 테스트를 통해 SW 동작 정확성, 데이터 정합성, 예외처리 등 SW품질 안전성 진단 및 개선 지원	18건 내외	
	소스코드	소스코드 정적분석 도구를 이용하여 소스코드 잠재 결함, 복잡도 등 (품질)진단 및 개선 지원	20건 내외	
운영기반 안전성	DBMS	DBMS 서버의 성능(용량, SQL 응답시간 등), 구조(인덱스 등), 장애 대응(이중화, 백업 등) 진단 및 개선 지원	12건 내외	
	WEB/WAS	WEB/WAS 서버의 운영상태, 세션관리, 구성 및 설정 최적화 등 진단 및 개선지원	10건 내외	
	구조	시스템/서버의 서비스 구동 상태, 자원 및 구성, 이중화, 용량 등 안정적 운영 기반 진단 및 개선지원		
프로세스 안전성	구축체계	시스템 구축 단계(분석·설계·구현·테스트)별 프로젝트 관리, SW개발, SW안전개발, 지원영역 진단 및 개선지원	25건	NIPA
	유지관리 및 운영	SW유지관리, 시스템운영, SW안전유지보수 영역 진단 및 개선지원		
SW 공급망 보안성		국내 SW 정적진단(보안), 동적진단(보안), SBOM 생성 및 분석, 보안체계(SW&개발환경) 진단 및 기술지원	10건	KISA

※ 진단항목별 세부 지원 내용은 '[첨부1] 항목별 세부 진단 내용' 참고

※ 모집규모는 **SW안전 신규진단 및 재진단 건수를 합산한 규모**이며 진단 신청, 선정결과 등에 따라 일부 변경될 수 있음**(조기마감 가능)**

※ **'SW 공급망 보안성' 항목을 신청**하는 경우에는 해당 지원영역과 중복되는 **'SW품질', '소스코드', '구축체계', '유지관리 및 운영' 항목에 중복 신청 불가**

(예시1) 개발중인 A시스템 '안전기능', 'SW품질', '소스코드' 희망
⇒ 모두 신청 가능 + **'구축체계' 필수**

(예시2) 운영중인 B시스템 'SW품질', 'DBMS', 'SW 공급망 보안성' 희망
⇒ 'DBMS', 'SW 공급망 보안성' 신청 가능 / **'SW품질' 신청 불가**

○ 진단 프로그램

① 시스템(SW) · 운영기반 · 프로세스 안전성 진단 영역

진단프로그램	SW안전 신규진단	SW안전 재진단
지원대상	국민 생활·안전과 밀접한 민간·공공 시스템(SW)	**'20~'24년 내 진단완료**한 민간·공공 시스템(SW)
기업당 최대 지원건수	**최대 5개** 진단항목 * 프로세스 안전성 영역 중 진단항목 1개 진단 必	**최대 2개** 진단항목 * 기진단완료한 진단항목에 한해 지원가능
진단기간	최대 15일	
모집규모	88건 내외	10건 내외
	총 98건	

※ SW안전 신규진단(시스템 및 운영기반 안전성 영역 대상) 중 현재 개발 중인 시스템의 경우, '구축체계' 항목 진단 必, 운영 및 유지관리 중인 시스템인 경우, '유지관리 및 운영' 항목 진단 必

※ 기진단완료 시스템의 변경이 과도하게 이루어진 경우, 재진단 신청 시 수행기관에서 신규진단으로 조정 가능

※ 진단 수행여건 등에 따라 진단 수행기관에서 진단항목 조정 가능

② SW 공급망 보안성 진단 영역

진단프로그램	SW 공급망 보안성 진단
진단대상	국민 생활·안전과 밀접한 **민간 시스템(SW)** ※ 기업당 1개 시스템(SW)에 한함
진단내용	**정적진단, 동적진단, SBOM 생성 및 분석, 보안체계 진단**
진단기간	최대 15일
모집규모	총 10건

□ 진단 혜택

○ **(서비스연계)** 소프트웨어 확인 및 검증시험(V&V) 비용 할인 (10%, 최대 100만원까지)

* 진단 완료 후 1년 이내 TTA 분당시험소 계약 건에 대해 10% 할인(개별 건 합산 최대 100만원까지, V&V 신청 시 진단 담당자에게 연락 필요)

※ 위의 **진단 혜택은 시스템(SW) 안전성, 운영기반 안전성, 프로세스 안전성 영역의 항목을 진단을 완료**한 경우에 한함

2 추진일정 및 신청방법

□ 추진일정

절차	주요내용	일정
모집공고 및 신청접수	· 과기정통부, NIPA, KISA, TTA 홈페이지 등을 통한 공모 · 신청서 접수 및 확인	(1차) 3.4.~3.21. (2차) 3.22.~4.25. (3차) 4.26.~6.16.
대상선정 및 선정결과 안내	· 평가 및 심의위원회를 통한 진단대상 최종 확정 · 선정 결과 개별 안내	(1차) 4월 초 (2차) 5월 초 (3차) 6월 말
진단 및 개선지원	· 진단방법, 일정 등 세부사항 협의 · 대상SW 분석, 진단 및 개선지원 · 진단 결과서 제공	4~11월

※ 세부 추진 일정은 진행 상황에 따라 변경될 수 있으며, **조기마감 가능**

※ **'SW 공급망 보안성'** 진단 영역은 **6월부터 진단 가능**

- **다수 시스템(SW) 신청 시 시스템별로 신청서를 작성하여 제출해야 함**
- **SW 공급망 보안성 영역 단독 신청 시 별도 사이트에서 신청서 작성하여 제출 필요**
- **진단 결과 및 진단 대상 SW의 중요 정보에 대하여 보안을 유지함**
  (진단 결과서는 수요기업(기관)에만 제공)

□ 신청방법

○ 시스템별 ‘진단 신청서’ 작성하여 이메일 접수

- 진단 영역 복수 신청 시, ‘TTA SW시스템안전센터’로 접수 요망

진단영역	접수처	문의처
시스템(SW) 및 운영기반 안전성	system.safety @tta.or.kr	TTA SW시스템안전센터 - 조한석 책임(010-5110-7542)
프로세스 안전성	sjhan@nipa.kr	NIPA SW안전팀 - 한상진 책임(043-931-5385)
SW 공급망 보안성 (단독 신청 시)	KISA 보호나라 신청페이지 * 시스템 주소 별도 추가 예정	KISA 디지털정부보호팀 - 오세영 책임(061-820-1159)

(예시1) ‘DBMS’, ‘WEB/WAS’ + ‘구축체계’ 신청
⇒ TTA SW시스템안전센터로 신청

(예시2) ‘구조’ + ‘SW 공급망 보안성’ 신청
⇒ TTA SW시스템안전센터로 신청

(예시3) ‘SW 공급망 보안성’ 단독 신청
⇒ KISA 보호나라 신청페이지로 신청

3 선정방법 및 유의사항

□ 선정기준 및 방법

(1) 시스템(SW) · 운영기반 · 프로세스 안전성

① SW안전 신규진단

○ 외부전문가로 구성된 평가위원회를 개최하여 신청서 기반으로 평가항목에 따라 **평가 후 심의위원회**를 통해 **최종 확정**

- **진단항목별 평가점수 70점 이상**인 시스템(SW) 중에서 **고득점 순**으로 선정

평가항목	배점	내용
진단 필요성	30점	· 신청 배경 및 목적이 명료하고 본 사업 취지에 부합하는지 여부 · SW오작동, 장애발생 등에 따른 진단의 필요성 및 시급성
안전 연관성	35점	· 국민의 안전(생명, 신체, 환경, 재산 등)과의 밀접 여부 · SW오작동, 장애발생 등에 따른 사회 혼란, 행정마비 등 대국민 파급효과 및 범위
진단결과 활용 및 개선의지	20점	· 진단 결과를 반영한 시스템 개선의지 및 결과 활용 방안의 구체성
진단 수행 여건	15점	· 진단 환경, 산출물 제공, 인터뷰 등 원활한 진단을 위해 필요한 지원의 가능 여부 및 적절성

* 평가점수 산출은 위원별 평가점수 중 최고·최저점수를 제외한 나머지 평가점수를 산술 평균하며 소수점 둘째자리 이하 반올림하여 소수점 첫째자리까지 산정
* 서면평가를 원칙으로 하나 평가상황 등에 따라 변경될 수 있음

② SW안전 재진단

○ 외부전문가로 구성된 평가위원회를 개최하여 신청서 기반으로 평가항목에 따라 **평가 후 심의위원회**를 통해 **최종 확정**

- **진단항목별 평가점수 70점 이상**인 시스템(SW) 중에서 **고득점 순**으로 선정

평가항목	배점	내용
진단 필요성 (시급성)	40점	· 재진단 신청 배경 및 목적이 본 사업 취지에 부합하는지 여부 · 기존 진단 완료 이후 발생하는 문제점의 시급성
개선의지	40점	· 진단 결과의 반영 정도(%) 및 반영 노력 정도 · 재진단 이후 결과 활용 방안의 구체성
진단 수행 여건	20점	· 진단 환경, 산출물 제공, 인터뷰 등 원활한 진단을 위해 필요한 지원의 가능 여부 및 적절성

* 평가점수 산출은 위원별 평가점수 중 최고·최저점수를 제외한 나머지 평가점수를 산술 평균하며 소수점 둘째자리 이하 반올림하여 소수점 첫째자리까지 산정
* 서면평가를 원칙으로 하나 평가상황 등에 따라 변경될 수 있음

(2) SW 공급망 보안성

○ 기업당 1개 시스템(SW)에 대한 4개 항목* 전체 진단 가능 여부를 확인 후 기업 담당자 사전 인터뷰 및 KISA 내부 검토를 통해 최종 확정
* 4개 항목 : SW 정적진단, 동적진단, SBOM 생성 및 분석, SW 개발환경 진단

□ 유의사항

○ 신청서 내용이 누락 또는 잘못 기재된 경우 평가 대상에서 제외될 수 있으며, 허위, 모방, 도용 등으로 밝혀질 경우, 선정 취소 등 제재조치를 받을 수 있음

○ 선정평가 결과는 신청서에 기재된 담당자의 연락처를 통해 개별 통보하며, 평가 점수는 원칙적으로 공개하지 않음

○ 진단 대상 기업(기관)은 진단 완료 후 2년간 성과조사(취약점 관리율 등)에 적극적으로 응하여야 되며, 우수사례 등에 대해 일부 내용을 공개할 수 있음

[첨부1] 항목별 세부 진단내용

○ 시스템(SW) 안전성 및 운영기반 안전성(수행기관: TTA)

진단영역	진단항목	세부 진단내용
시스템(SW) 안전성	SW품질	- 대상SW(또는 주요 기능/모듈) 중점적 테스트 및 결함 검출 - 예외/이상상황 시나리오 테스트 및 개선사항 검출 - 오조작 유발 사용자 인터페이스 안전성 테스트 및 개선 방법 지원
	소스코드	- 소스코드 품질 룰셋* 기반 위반사항(잠재 결함) 검출 - 소스코드 메트릭** 측정 * 예) MISRA-C/C++, 전자정부표준프레임워크 코딩규칙, Microsoft C# ** 예) Cyclomatic Complexity, Number of Call Level, Comments ※ 코드품질/안전성 룰셋을 기반으로 진단. 보안 룰셋 적용은 추가협의 필요
	안전기능	- 위험분석, TARA(Threat Analysis and Risk Assessment) 분석 - 위험 대비 SW 안전 기능 요구사항 도출 - 안전 요구사항 대비 설계 분석 및 안전성 개선방안 지원 - 안전 표준 기반 갭(GAP) 분석 및 개선방안 지원 - 안전 산출물 작성 및 문서화 지원
운영 기반 안전성	DBMS	- DB와 관련 문제점, 이슈 집중 진단 및 개선지원 - DB파라미터, 테이블, 인덱스, 테이블스페이스 등 진단 및 개선방법 제시 - SQL 성능 분석(응답시간, Top-N SQL 등) 및 적절성 점검 - DB이중화, DB백업 및 복구 등 구성 적절성 진단 등
	WEB/WAS	- WEB/WAS 관련 문제점, 이슈 집중적으로 진단 및 개선 - 파라미터 설정(WEB/WAS, JAVA, 커널 등) 진단 및 개선지원 - 운영 상태/로그(Heap Dump, Error log 등) 분석 및 개선방법 제시 - WEB/WAS 이중화 적절성, 모니터링 적절성 진단 등
	구조	- 시스템/서버의 자원, 구성 관련 문제점, 이슈 집중 진단 및 개선지원 - 주요 자원 사용량(CPU, Memory, Disk, Page Fault 등) 적절성 확인 - 운영체제 에러 로그, 파라미터 및 패치 설정 상태 등 점검 - 기본 이중화 상태, 동기화 구성 상태 등 점검

* 위 진단항목 이외, 요청사항이 있을 경우 협의하여 진단 가능함

** 진단내용은 SW 규모 등에 따라 조정될 수 있음

○ 프로세스 안전성(수행기관: NIPA)

진단영역	진단 항목	세부 진단내용
프로세스 안전성	구축	· 프로젝트 관리 프로세스 - 프로젝트의 목표와 범위를 정의하고, 이를 달성하기 위한 계획의 수립 - 수립된 계획에 따라 프로젝트 수행 활동을 점검 및 통제 진단 - 협력업체 선정 및 관리 · 개발 프로세스 - 프로젝트 계획에 따라 고객 요구사항 추출, 분석, 설계, 구현 및 테스트 활동 수행 여부 및 산출물 검토 - 정의된 프로젝트 프로세스에 따라 작업산출물을 작성하고 유지하며, 변경사항 처리 절차와 관련사항 · 지원 프로세스 - 프로젝트의 프로세스가 프로젝트 전체 과정의 활동에 대해 적합성과 해당 작업산출물이 요구사항, 계획에 부합하는지 확인하고 검증 - 프로젝트 수행 중에 발생하는 작업산출물에 대한 단계별 추적 및 해당 산출물들의 무결성 - 프로젝트 개발 및 관리 활동의 효율적 지원을 위해 계획된 항목에 대한 데이터의 측정과 분석 · SW안전개발 프로세스 - SW안전 계획에 따라 고객 요구사항 추출, 분석, 설계, 구현 및 테스트 활동 수행 여부 및 산출물 검토 - SW위험원 분석 및 안전 무결성 등급 평가 수행 여부 및 산출물 검토
	유지관리 및 운영	· SW유지관리 프로세스 - 서비스 요청사항에 대한 식별, 영향 분석, 설계, 구현 및 테스트 활동 수행 - 성능측정, 가용성 분석, 용량분석 및 백업 절차 - 장애관리 및 형상관리 절차 여부 및 활동 수행 · 시스템운영 프로세스 - 운영유지보수 및 이관활동 점검 - 서비스 요청 처리절차 및 서비스 수준관리 활동 여부 및 절차 점검 · SW안전유지보수 - SW안전관련 운영 및 유지보수 계획 수립여부 점검 - SW안전관련 변경 및 배포활동에 관한 절차 점검

* 위 진단항목 이외, 기업 요청사항이 있을 경우, 협의하여 진단 가능함

** 진단내용은 SW 규모 등에 따라 조정될 수 있음

○ SW 공급망 보안성(수행기관: KISA)

진단영역	진단 항목	세부 진단내용
SW 공급망 보안성	정적진단	- 국내외 도구를 활용한 소스코드 시큐어코딩 적용 여부 * SW 진단 기준:『정보시스템 구축·운영 지침(별표 3)』 * 모바일 SW 진단 기준 :『모바일 전자정부 서비스 관리지침(별표 2, 3)』
	동적진단	- SW 개발보안·개발환경 진단이 필요한 기업에 방문하여 진단 및 기술지원 - 신청 서비스 대상 시나리오 기반 모의침투 테스트를 통해 보안취약점 도출
	SBOM 생성 및 분석	- 소스코드, 바이너리, 의존성 분석을 통해 구성요소를 식별할 수 있는 명세서인 SBOM 생성 - SBOM의 신뢰성 확보를 위해 정확성, 완전성 등의 유효성 검증 수행 - SW에 숨어있는 보안취약점을 탐지하고 분석을 통한 개선 조치 지원
	SW 개발환경	- SW 개발 단계별 보안 활동의 적절성 진단 및 개선 지원 - 개발 산출물 보안 적용 여부 진단 및 개선 지원 등