

의안번호	2221546
의 퇴 인	이정헌의원
회 답 일	2026. 10. 2.
추 계 번호	26B4915

정보통신망 이용촉진 및 정보보호 등에 관한 법률 일부개정법률안

【비용추계서 미첨부 사유서】

I. 재정수반요인

연번	조·항(조제목)	주요내용	비고
1	안 제48조의6(정보통신망연결기기등에 관한 인증)	정보통신망연결기기등 중 침해사고가 발생하는 경우 국가안전보장에 지장을 초래하거나 사람의 생명·신체 또는 재산에 피해를 줄 우려가 큰 것으로서 대통령령으로 정하는 기기·설비·장비(이하 “고위험기기등”이라 한다)를 제조하거나 수입하는 자는 제1항에 따른 정보보호인증을 받아야 한다.(제3항 신설)	의무규정

II. 미첨부 근거 규정 및 상세 사유

1. 근거 규정

연번	조·항(조제목)	미첨부 근거 규정
1	안 제48조의6(정보통신망연결기기등에 관한 인증)	•제3호: 의안의 내용이 선언적·권고적인 형식으로 규정되는 등 기술적으로 추계가 어려운 경우

2. 상세 사유

- **현행법¹⁾은 과학기술정보통신부장관이 정보통신망연결기기등²⁾에 대하여 일정한 인증기준에 적합한 경우 정보보호인증을 할 수 있도록 하고 있음**
- 정보통신망연결기기등(IoT) 정보보호인증제도는 가전·교통·금융·스마트도시·의료·제조 및 생산·주택·통신 등 8대 분야의 기기·설비·장비(IoT)를 대상으로 데이터보호, 암호, SW보안, 업데이트 등 총 50개 항목에 대해 인증시험을 실시하여, 보안 위험 등급을 3개 등급(라이트, 베이직, 스탠다드)으로 구분하여 인증하는 제도로 과학기술정보통신부는 한국인터넷진흥원(KISA)에 정보보호인증제도를 위탁하여 운영 중에 있음

※ [참고자료] 정보통신망연결기기등 정보보호인증제도 개요

[표 1] 정보통신망연결기기등 품목 예시

구 분	품목 예시
주택	월패드, 디지털도어록, 도어센서, 무선호출기, 무선 온습도 센서, 스마트홈 모바일 앱 등
가전	로봇청소기, 냉장고, 홈 네트워크 카메라, IoT 통신 모듈, 대기전력자동차단 콘센트 등
스마트도시	전력측정기, 무선 소방 시스템, 실외공기질측정기, 스마트센서, 전기자동차 충전기 콘센트 등
의료	체외용 인슐린주입기, 블루투스 온도 센서, IoT 자동심장충격기 통합관리 시스템 등
제조 생산	IoT 센서데이터 전송장치, 신재생자료취득장치, 분산형전원 감시제어장치 등
통신	무선통신 단말기, IoT 리모컨, IoT 센서, 키오스크, 홈 CCTV 등
교통	차량번호 인식 시스템, 딥러닝 기반 영상 분석 장치, 스마트워치 앱 등
금융	카드단말기(POS), 키오스크 등

자료: 과학기술정보통신부

- 1) 제48조의6(정보통신망연결기기등에 관한 인증) ① 과학기술정보통신부장관은 제4항에 따른 인증시험대행 기관의 시험 결과 정보통신망연결기기등이 제2항에 따른 인증기준에 적합한 경우 정보보호인증을 할 수 있다.
② 과학기술정보통신부장관은 제1항에 따른 정보보호인증(이하 "정보보호인증"이라 한다)을 위하여 정보통신망의 안정성 및 정보의 신뢰성 확보 등에 관한 인증기준을 정하여 고시할 수 있다.
- 2) 제45조(정보통신망의 안정성 확보 등) ① 다음 각 호의 어느 하나에 해당하는 자는 정보통신서비스의 제공에 사용되는 정보통신망의 안정성 및 정보의 신뢰성을 확보하기 위한 보호조치를 하여야 한다.
2. 정보통신망에 연결되어 정보를 송·수신할 수 있는 기기·설비·장비 중 대통령령으로 정하는 기기·설비·장비(이하 "정보통신망연결기기등"이라 한다)를 제조하거나 수입하는 자

- 개정안은 정보통신망연결기기등 중 침해사고가 발생하는 경우 국가안전보장에 지장을 초래하거나 사람의 생명·신체 또는 재산에 피해를 줄 우려가 큰 기기·설비·장비(이하 “고위험기기등”)를 제조하거나 수입하는 자는 정보통신망연결기기등 정보보호인증을 의무적으로 받도록 하는 것으로, 정보보호 인증제도 운영 비용(인증신청 접수, 평가기관 배정, 인증위원회 개최, 사후관리 등) 증가 등의 추가재정소요가 발생할 수 있음

[표 2] 정보통신망연결기기등 정보보호인증 제도 관련 예산현황

(단위: 백만원)

	2022	2023	2024	2025	2026
세부 내역	·IoT 보안 시험인증 지원 595 ·컨설팅 및 교육 255 ·시험절차 및 기준 개발 400 ·인증위원회 운영 50	·IoT 보안 시험인증 지원 595 ·컨설팅 및 교육 255 ·시험절차 및 기준 개발 400 ·인증위원회 운영 50	·IoT 보안 시험인증 지원 595 ·컨설팅 및 교육 255 ·시험절차 및 기준 개발 300 ·인증위원회 운영 50	·IoT 보안 시험인증 지원 595 ·컨설팅 및 교육 205 ·시험절차 및 기준 개발 50 ·인증위원회 운영 28	·IoT 보안시험·인증 지원 ¹⁾ 595 ·IoT 보안인증컨설팅 및 교육 ²⁾ 176 ·제품별IoT 보안시험 절차및기준개발47 ·IoT 보안전문가검토 및 인증위원회 운영 20
계	1,300	1,300	1,200	878	838

주: 1) 중소기업의 정보보호인증시험 수수료 80% 국가 지원

2) 정보보호인증 신청인에 대한 기술 등 컨설팅 및 교육 실시

자료: 과학기술정보통신부

- 다만, 개정안에 따른 추가재정소요를 추계하기 위해서는 개정안에 따라 증가하는 인증대상의 수, 이에 따른 인증제도 운영비용 증가 규모 등에 대한 정보가 필요하나, 개정안은 정보보호인증 의무대상인 고위험기기등의 종류를 대통령령으로 정하도록 위임하고 있어, 현 시점에서 인증대상의 수 및 운영비용 증가 규모 등을 합리적으로 예측하는 데 한계가 있음

Ⅲ. 부대의견

☐ 없음

Ⅳ. 작성자

☐ 성명

국회예산정책처	분석관	과장
경제비용추계과	최동완	예승우

☐ 대표연락처

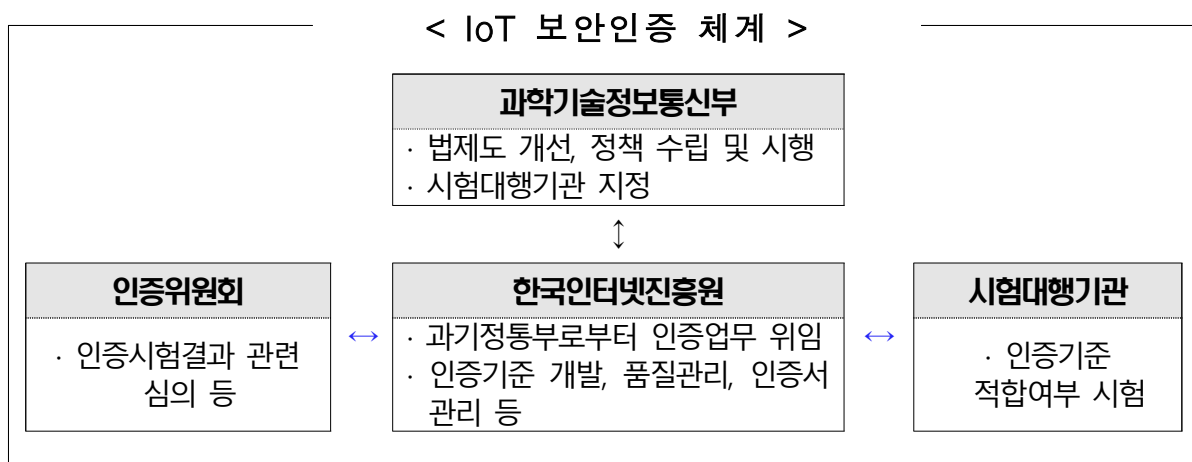
성명	전화번호	이메일 주소
최동완	02-6788-3746	dongwaniii@nabo.go.kr

[참고자료] 정보통신망연결기기등 정보보호인증제도 개요

(과학기술정보통신부 제출자료)

□ 개 요

- 국민의 실생활과 밀접한 IoT 제품에 대한 보안내재화를 촉진하고 안전성을 확보하기 위한 기본적 요건에 대한 기준을 마련하여 평가·인증
- ※ 법적근거 : 정보통신망법 제48조의 6(정보통신망연결기기등에 관한 인증)



□ 주요 내용

- (인증대상) 영 제36조의2(정보통신망연결기기등의 범위) 별표1의3*
- * 가전, 교통, 금융, 스마트도시, 의료, 제조 및 생산, 주택, 통신 등 8대 분야로 정의
- (인증기간) 인증서 3년
 - (시험항목) 식별·인증, 데이터보호, 암호, 소프트웨어보안, 업데이트, 네트워크 보안, 하드웨어보안 등 영역에 총 50개 항목
 - (인증유형) 3개 등급으로 구분(Lite, Basic, Standard)

□ 기대효과

- 융합산업 분야의 다양한 IoT 제품이 개발 단계부터 보안이 고려되어 개발됨에 따라, 안전한 제품이 국민들에게 제공
- 중소기업의 인증 부담을 경감하여 안전한 IoT 제품 수요를 창출

○ 인증기준

인증 영역	인증기준		설명	인증 유형		
				라 이 트	베 이 직	스 텝 단 위
식별 및 인증	1.1	안전한 인증정보 사용	초기 인증정보는 변경하거나 생성되어야 하고, 인증정보의 안전성을 검증해야 한다.	○	○	○
	1.2	사용자 인증 및 권한 관리	관리기능 또는 중요정보에 접근 시 사용자 인증 을 수행하고, 서비스 이용에 필요한 최소한의 권 한만을 부여해야 한다.	○	○	○
	1.3	비인가 상호인증 제한	다른 기기와 연결 또는 중요정보 전송 시 기기의 식별정보가 신뢰성이 있음을 확인하는 인증을 선행해야 한다.	-	○	○
	1.4	반복된 인증시도 제한	사용자 인증이 연속적으로 실패하면 반복된 인 증시도를 제한해야 한다.	○	○	○
	1.5	정보노출 방지	인증정보가 출력장치에 노출되지 않아야 하고, 인증실패 사유에 대한 피드백 정보가 제공되지 않아야 한다.	-	○	○
	1.6	안전한 세션 관리	세션 연결 이후 일정한 시간 동안 사용하지 않으면 해당 세션을 잠그거나 종료시켜야 하고, 재접속 시 세션 정보가 재사용되는 것을 방지해야 한다.	-	○	○
데이터 보호	2.1	전송 데이터 보호	중요정보 전송 시 기밀성 및 무결성이 보장되도 록 암호화해야 한다.	○	○	○
	2.2	저장 데이터 보호	중요정보는 소스코드에 하드코딩되지 않아야 하 고, 저장 시 암호화해야 한다.	○	○	○
	2.3	중요정보 저장 영역 보호강화	중요정보는 물리적 훼손 공격 등에 내성을 갖는 안전한 영역에 저장해야 한다.	-	-	R
	2.4	개인정보 법적 준거성	개인정보 수집 및 처리 시 개인정보 관련 법적 요구사항을 준수해야 한다.	-	○	○
	2.5	중요정보 완전삭제	중요정보는 복구가 불가능하도록 완전하게 삭제 할 수 있어야 한다.	-	○	○
암호	3.1	안전한 암호 알고리즘 사용	중요정보를 전송하거나 저장 시 안전한 암호 알 고리즘을 사용해야 한다.	○	○	○
	3.2	안전한 암호키 생성	기기별로 고유한 암호키를 생성해야 한다.	-	○	○
	3.3	안전한 암호키 관리	암호검증 모듈 등 안전성이 검증된 방식으로 암호 키를 관리해야 한다.	-	-	○
	3.4	안전한 난수 생성	난수 생성 시 난수성이 검증된 알고리즘을 이용해야 한다.	-	-	○
소프트 웨어 보안	4.1	시큐어 코딩	소스코드에 대한 보안약점이 존재하지 않도록 시큐어 코딩을 적용해야 한다.	-	○	○
	4.2	소스코드 난독화	소스코드 노출을 최소화하기 위해 난독화 기법 을 적용해야 한다.	-	○	○
	4.3	소프트웨어 보안기능 시험	소프트웨어 보안약점 및 보안기능을 시험하여 정상동작함을 확인해야 한다.	-	-	○
	4.4	알려진 취약점 조치	공개된 보안취약점이 있는지를 분석하고, 이에 대한 조치를 수행해야 한다.	○	○	○
	4.5	불필요한 기능 및	디버깅 · 시험용 코드 · 주석 등 운용에 불필요한	-	○	○

		코드 제거	기능 및 코드는 제거되어야 한다.			
	4.6	안전한 소프트웨어 적용	최신 보안패치가 적용된 안전한 버전의 공개 · 상용 소프트웨어를 탑재해야 한다.	-	○	○
	4.7	감사기록	기기 운용 과정에서 발생한 보안이벤트에 대한 감사기록을 생성하고 안전하게 보호해야 한다.	-	-	○
업데이트 및 기술지원	5.1	모델명 및 제품정보 확인	기기 모델명 및 제품정보(소프트웨어 · 펌웨어)의 식별정보를 확인하기 위한 수단을 제공해야 한다.	○	○	○
	5.2	안전한 업데이트 수행	업데이트 수행 전에 업데이트 서버를 검증하고, 사용자 인가여부를 확인해야 한다.	○	○	○
	5.3	업데이트 파일의 안전성 보장	업데이트 파일이 비인가자에게 접근되지 못하게 하고, 위 · 변조 시 탐지할 수 있어야 한다.	-	○	○
	5.4	업데이트 실패 시 복구	업데이트 실패 시 안전한 상태인 기존 버전으로 복구할 수 있어야 한다.	-	-	○
	5.5	업데이트 기술 지원	제품보증기간 내에 소프트웨어 또는 펌웨어 업데이트가 불가능한 경우, 기술지원 서비스를 제공해야 한다.	-	-	○
	5.6	업데이트 정보 제공	사용자에게 업데이트 알림 등 정보를 제공하여야 한다.	-	○	○
	5.7	자동업데이트 기능 제공	최신 버전의 자동업데이트 기능을 제공해야 한다.	-	-	R
운영체제 및 네트워크 보안	6.1	안전한 운영체제 적용	운영체제는 최신의 보안패치가 적용되어야 하고, 기술지원을 지속적으로 할 수 있어야 한다.	-	○	○
	6.2	불필요한 계정 통제	불필요한 계정은 제거하거나 비활성화해야 한다.	-	○	○
	6.3	불필요한 서비스 및 포트 통제	불필요한 서비스 및 포트는 제거하거나 비활성화해야 한다.	-	○	○
	6.4	불필요한 네트워크 인터페이스 비활성화	불필요한 네트워크 인터페이스는 비활성화해야 한다.	-	○	○
	6.5	실행코드 및 설정파일 무결성 검증	실행코드 및 설정파일의 무결성을 검증하고, 검증 실패 시 안전한 상태로 복원하는 등 대응 기능이 제공되어야 한다.	-	-	○
	6.6	장애 시 시스템 복원	전력공급 중단, 통신 장애 등 예기치 않은 외부 요인에서 복구된 후 시스템의 서비스를 정상상태로 복원해야 한다.	-	-	○
	6.7	서비스 거부 공격 대응	서비스 거부 공격에 동작을 멈추거나 오작동하지 않아야 한다.	-	-	R
	6.8	운영체제 기능 보호	운영체제의 보안기능을 활성화하여 보안기능 우회를 차단해야 한다.	-	-	○
	6.9	접근권한 최소화	기능 및 서비스 운용에 필요한 최소한의 접근권한만 설정해야 한다.	-	-	○
	6.10	비인가 소프트웨어 설치 · 실행차단	인가되지 않은 소프트웨어가 설치되지 않도록 차단하거나 실행되지 않도록 제한해야 한다.	-	-	○
	6.11	원격접속 통제	접근통제, 인증, 보안채널 등이 적용된 환경에서 원격접속을 해야 한다.	-	○	○
	6.12	네트워크 트래픽 통제	허가되지 않은 네트워크 트래픽을 차단해야 한다.	-	○	○
하드웨어 보안	7.1	안전한 부팅 및 자체시험	안전한 하드웨어 부팅 절차를 제공해야 하고, 기기 구성요소에 대한 자체시험을 수행해야 한다.	-	-	○
	7.2	자체시험 실패 시 대응	자체시험 실패 오류메시지를 출력하고, 필요시 적절한 대응행동을 수행해야 한다.	-	-	○

7.3	하드웨어 장애 대응	시스템 장애가 발생한 경우, 사용자 또는 관리자에게 장애 발생에 대한 알림을 제공해야 한다.	-	-	○
7.4	무단 훼손 방어	하드웨어 무단 조작 공격에 대응하여 하드웨어 설계 보안을 적용해야 한다.	-	-	R
7.5	부채널 공격 대응	전력, 시간 등 부가정보를 악용하는 부채널 공격으로 중요정보가 외부에 노출되지 않아야 한다.	-	-	R
7.6	메모리 공격 대응	휘발성 메모리 공격에 대응하기 위해 메모리 보호 기법을 적용해야 한다.	-	-	R
7.7	비휘발성 메모리 보호	비휘발성 메모리에 저장되는 펌웨어를 판독할 수 없게 해야 한다.	-	-	R
7.8	외부 인터페이스 보호	불필요한 외부 인터페이스는 비활성화해야 하고, 필요 시 접근통제 기능을 지원해야 한다.	-	○	○
7.9	내부 인터페이스 보호	비인가 접근을 막기 위해 내부 인터페이스를 비활성화해야 한다.	○	○	○

※ ‘○’ 는 인증의 유형에 해당함을 의미하며, ‘R’ 은 권고사항으로 선택적으로 적용 가능