



제 433회 국회 (임시회)
제1차 기후에너지환경노동위원회

전기사업법 일부개정법률안 검 토 보 고

〈재생에너지 발전설비 보안기준 신설〉

■ 강승규의원 대표발의(의안번호 제2213062호)

2026. 3.

기후에너지환경노동위원회

수석전문위원 신항진

목 차

I . 제안경위	1
II . 제안이유 및 주요내용	1
III . 검토의견	2

I. 제안경위

1. 발 의 자 : 강승규의원 등 13인
2. 발의연월일 : 2025. 9. 17.
3. 회부연월일 : 2025. 9. 18.

II. 제안이유 및 주요내용

최근 재생에너지 기반 설비의 디지털 연계가 확대됨에 따라 국가안보와 전력계통 안정성을 동시에 고려한 대응의 필요성이 제기되고 있음. 특히 태양광 및 풍력발전소는 전력계통과 연계되어 원격으로 운영·제어되는 특성상, 제어시스템과 인버터 통신장치가 사이버공격에 노출될 경우 전력공급 안정성에 중대한 영향을 미칠 수 있음.

그러나, 현행법은 전력설비의 안전에 관한 일반적 관리 규정만 두고 있을 뿐, 재생에너지 발전설비 제어시스템 및 인버터 통신장치의 보안기준을 명시적으로 규정하고 있지 않아 법적 근거에 기반한 체계적 보안기준 마련이 미흡하다는 의견이 있음.

이에 재생에너지 발전설비의 제어시스템과 인버터 통신장치에 대한 보안기준을 법률에 명시하여, 사이버침해 예방과 대응 체계를 강화하고 전력계통의 안정성 및 국민의 에너지 안전을 확보하려는 것임(안 제67조의2 신설).

Ⅲ. 검토의견

개정안은 재생에너지 발전설비의 제어시스템과 인버터¹⁾ 통신장치에 대한 보안기준을 마련하여 전력계통의 안정성을 확보하려는 것으로, 구체적으로 보안 기준에 사이버 침해 대응 절차, 인증·암호화 기준, 특정 국가의 원격관리 차단²⁾ 등을 포함하도록 명시함(안 제67조의2 신설).

[개정안 조문대비표]

현 행	개 정 안
<신 설>	제67조의2(재생에너지 발전설비 제어시스템 등의 보안기준) ① 산업통상자원부장관은 재생에너지 발전설비의 제어시스템 전반과 인버터 통신장치의 안전한 운영을 위하여 보안기준을 마련하여야 한다. ② 제1항의 보안기준에는 다음 각 호의 사항을 포함하여야 한다. 1. 사이버침해 예방 및 대응 절차 2. 인증·암호화 등 통신보안 확보를 위한 기술적 기준 3. 보안취약점 점검 및 개선 주기

1) 인버터(Inverter): 태양광·풍력 등에서 발생하는 직류(DC) 전력을 전력계통에 공급 가능한 교류(AC) 전력으로 변환하는 장치로, 최근 원격 제어를 위한 통신 모듈이 탑재됨.

2) 특정 국가 원격관리 차단: 안보상 우려가 있는 특정 국가에서 제작된 소프트웨어의 백도어(Backdoor) 등을 통한 기술 탈취 및 제어권 장악 가능성을 원천 차단하려는 조치

현행	개정안
	4. <u>원격접속 통제, 접근권한 제한 및 특정 국가의 원격관리 차단 등 보안 조치</u> 5. <u>기타 전력계통의 안정적 운영을 위하여 필요한 사항</u> ③ <u>전기사업자는 재생에너지 발전설비를 보안기준에 적합하도록 유지하여야 한다.</u>

최근 국내 사업용 태양광 시장에서 외산(특히 중국산) 인버터의 점유율이 90%에 육박하며 전력망의 기술적 종속 우려가 심화되고 있음.

특히 2022년부터 네트워크 연결 기능을 보유한 인버터 보급이 본격화되면서, 해외 제조사의 무단 원격 접속에 의한 전력망 교란 위험이 안보적 쟁점으로 부상함.

[최근 3년간 국내 사업용 태양광 인버터 제조국별 점유율 현황]

(단위: MW³⁾, %)

연도	국산 인버터	중국산 인버터	비중국산 외산	합계(점유율)
2022	418 (16.0%)	2,153 (82.5%)	39 (1.5%)	2,610 (100%)
2023	309 (12.6%)	2,131 (86.6%)	21 (0.8%)	2,461 (100%)
2024	299 (10.3%)	2,577 (89.2%)	12 (0.5%)	2,888 (100%)

*자료: 기후에너지환경부

위 데이터에 따르면 국산 인버터의 점유율은 3년 사이 약 6%p 하락한 반면 중국산 비중은 90%에 육박하며 매년 증가하는 추세로, 이는 국가 핵심 인프라인 전력망의 제어권이 특정 국가의 기술 생태계

3) MW(메가와트): 전력의 단위로, 1,000kW에 해당함

에 고도로 의존하고 있음을 시사함.

전력 제어 시스템은 사이버 공격 시 대규모 정전(Blackout)을 초래할 수 있는 국가 핵심 인프라임.

개정안은 보안기준을 법률에 명시함으로써 제조사별로 난립한 통신 규격과 보안 수준을 표준화하고, 특히 해외에 서버를 둔 외산 장비의 보안 취약성을 제도적으로 관리하여 에너지 안보를 강화할 수 있다는 점에서 입법 취지가 타당함.

다만 이러한 안보적 정당성에도 불구하고, 기존 전력망 보안 인프라와의 중복성, 타 법령(정보통신망법)과의 체계적 정합성, 그리고 특정 국가 배제에 따른 통상 마찰 가능성 등을 고려할 필요가 있는데, 구체적인 검토사항은 다음과 같음.

첫째, 물리적 차단 체계(RTU)⁴⁾와의 중복 및 실효성에 대한 검토가 필요함.

현재 90kW⁵⁾ 이상 재생에너지 설비는 전력 제어망 연계 시 RTU를 거치며, RS485⁶⁾ 시리얼 통신 방식을 적용하여 사이버 침해에 대응 중임.

90kW 이하 소규모 설비는 제어망과 분리되어 원격 제어가 불가능

4) RTU(Remote Terminal Unit): 원격 단말 장치. 계통운영시스템에서 전력설비를 원격 감시 및 제어하기 위해 발·변전소에 설치하는 통신 장비

5) 감시·출력제어 의무화 대상: 1,000kW 이상('20) → 100kW 이상('23.10) → 90kW 이상('25.1)으로 지속 확대됨

6) RS485: 로컬(현장) 연결 위주의 시리얼 통신 방식으로, 물리적으로 외부 인터넷망과 분리되어 침해 사고 위협에 대응함

한 구조임을 고려할 때, 추가적인 보안 기준 신설이 영세 사업자에게 불필요한 기기 교체 및 유지 비용을 지우는 중복 규제가 될 우려가 있음.

둘째, 타 법령과의 정합성 및 행정적 혼선 발생 가능성을 고려할 필요가 있음.

기후부는 통신장치 보안인증이 이미 「정보통신망법」 제48조의6⁷⁾에 따른 사물인터넷(IoT) 보안인증 제도로 운영되고 있음을 근거로 수용 곤란 의견을 제시하였음.

전기사업법상 별도 기준 수립 시, 동일 기기에 대해 소관 부처(기후부 및 과기정통부) 간 인증 기준이 상충하여 발생하는 행정적 불합리성과 현장의 혼선 등을 사전에 조정할 필요가 있을 것으로 보임.

셋째, 데이터 확보 부재 및 통상 마찰 발생 가능성을 고려할 필요가 있음.

7) 정보통신망법 제48조의6(정보통신망연결기기등에 관한 인증): 과학기술정보통신부 주관으로 사물인터넷(IoT) 기기 등의 정보보호 인증 기준과 절차를 규정함

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제48조의6(정보통신망연결기기등에 관한 인증) ① 과학기술정보통신부장관은 제4항에 따른 인증시험대행기관의 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.

③ 과학기술정보통신부장관은 정보보호인증을 받은 자가 다음 각 호의 어느 하나에 해당하는 경우에는 그 정보보호인증을 취소할 수 있다. 다만, 제1호에 해당하는 경우에는 그 정보보호인증을 취소하여야 한다.

1. 거짓이나 그 밖의 부정한 방법으로 정보보호인증을 받은 경우

2. 제2항에 따른 인증기준에 미달하게 된 경우

④ 과학기술정보통신부장관은 정보통신망연결기기등이 제2항에 따른 인증기준에 적합한지 여부를 확인하는 시험을 효율적으로 수행하기 위하여 필요한 경우에는 대통령령으로 정하는 지정기준을 충족하는 기관을 인증시험대행기관으로 지정할 수 있다.

현재 해외 제조사들이 영업 비밀을 사유로 서버 위치 및 원격 접속 구조를 비공개하고 있어 기후부 차원에서도 구체적인 보안 취약점 점검에 한계를 보이고 있음.

이는 제조사가 기술 정보를 독점하는 반면 규제 기관은 세부 제어 메커니즘을 파악하지 못해 정책을 정확히 설계하거나 감시하기 어려운 정보 비대칭 문제를 야기할 수 있음.

또한, '특정 국가 원격관리 차단' 규정은 WTO TBT⁸⁾ 협정이나 FTA상의 내국민 대우 원칙⁹⁾ 위반으로 해석되어 통상 마찰을 야기할 위험이 있으므로 해당 쟁점에 대해 산업통상부 등과도 협의가 필요할 것으로 보임.

기후에너지환경부는 정보통신망법 체계 내 관리가 타당하다는 이유로 개정안에 대해 수용 곤란 입장이나, 외산 인버터의 해외 서버 접속 문제를 해결하기 위해 태양광 경쟁입찰 시 국내 서버 유치를 유도하는 방안을 별도로 검토 중이라는 의견을 제시함.

그 밖에 국가정보원은 단순 기술 기준을 넘어 조달부터 폐기에 이르는 '공급망 보안'¹⁰⁾ 절차를 강화하는 방향으로 수정 보완할 필요가 있다는 입장임.

8) TBT(Technical Barriers to Trade): 무역에 관한 기술적 장벽 협정. 국가 간의 서로 다른 기술 규정이나 인증 절차 등이 무역의 장애가 되지 않도록 하는 협정

9) 내국민 대우 원칙(National Treatment): 조세나 법령 적용에 있어 외국인 및 외국 제품을 자국민이나 자국 제품보다 불리하게 대우해서는 안 된다는 국제 무역의 기본 원칙. 특정 국가 제품을 명시적으로 배제할 경우 이 원칙 위반으로 제소될 위험이 있음.

10) 공급망 보안(Supply Chain Security): 하드웨어 및 소프트웨어의 설계, 제조, 유통 등 전 과정에서 발생할 수 있는 안보 위협을 관리하는 체계

한국전력공사는 공공 분야는 이미 국정원 가이드라인을 준수 중이나, 민간 영역의 인버터 보안은 관리 주체인 한국에너지공단과의 협의가 선행되어야 한다는 입장임.

한국전력거래소는 인버터를 IoT 기기로 분류하여 「정보통신망법」에 따른 보안인증을 의무화하는 것이 실무적으로 유효하다는 대안을 제시함.

그 밖에 미국(NERC CIP-013)¹¹⁾이나 EU(CRA)¹²⁾ 등 주요국은 이미 공급망 보안을 법제화하는 추세임.

문 의 처
02)6788-5537

11) NERC CIP-013: 북미전력계통신뢰도협회(NERC)가 제정한 핵심 인프라 보호 표준으로, 전력망 기자재 조달 시 공급망 보안 위험 관리 계획 수립을 의무화함

12) CRA(Cyber Resilience Act): 유럽연합 내 판매되는 디지털 요소 제품(인버터 등)에 대해 전생애주기 보안 및 취약점 관리를 의무화하는 법안