



제418회국회(정기회)
제 6 차 국 방 위 원 회

국방정보화 기반조성 및 국방정보자원관리에 관한 법률 일부개정법률안

검 토 보 고

〈국방 사이버보안 위험관리업무의 법적 근거 마련〉
■ 성일종의원 대표발의(의안번호 제2204097호)

2024. 11.

국 방 위 원 회

수석전문위원 오명호

목 차

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

I. 제안경위

1. 발 의 자: 성일종의원 등 10인
2. 발의연월일: 2024. 9. 19.
3. 회부연월일: 2024. 9. 20.

II. 제안이유 및 주요내용

초고속 네트워크 환경 기반과 기술의 혁신적 발전으로 사이버 위협이 다양해지고 복잡해짐에 따라 국방정보 및 국방정보시스템을 사이버 위협으로부터 안전하게 보호하기 위한 사이버보안 위협관리의 중요성이 증대되고 있는바, 국방 사이버보안 위협관리를 하기 위한 법적 근거를 명확히 하고, 이에 필요한 사항을 보완하려는 것임(안 제21조의2 신설).

Ⅲ. 검토의견

- 개정안은 국방부가 국방정보시스템 및 소프트웨어가 내장된 무기체계와 전력지원체계의 전 수명주기 관점에서 사이버보안 위협관리를 시행할 수 있는 법적 근거를 명확히 하려는 것임(안 제21조의2 신설).

현행	개정안
<신설>	제21조의2(국방 사이버보안 위협관리) ① 국방부장관은 「국군조직법」에 따른 국군의 부대와 기관이 활용하는 국방정보시스템 및 소프트웨어가 내장된 무기체계와 전력지원체계(「방위사업법」 제3조에 따른다)에 대해 소요기획부터 획득, 운영·유지, 폐기에 이르는 전 수명주기 관점에서 사이버보안 위협을 관리하기 위한 체계적 방안을 마련하여야 한다.
<신설>	② 국방정보시스템, 무기체계 및 전력지원체계의 소요제기, 획득, 운영·유지, 폐기를 수행하는 기관 또는 부대의 장은 제1항에 따라 사이버보안 위협관리를 수행하여야 한다.
<신설>	③ 제1항에 따른 사이버보안 위협관리의 구체적 방안 및 사이버보

	<u>안 위험관리 수행 기관 또는 부대 의 범위 등 필요한 사항은 국방부 장관이 정한다.</u>
--	---

□ 최근 사이버위협이 다양해지고 복잡해짐에 따라, 국방정보시스템 및 소프트웨어가 내장된 무기·전력지원체계를 사이버위협으로부터 안전하게 보호하기 위한 사이버보안 위험관리의 중요성이 증대되고 있음.

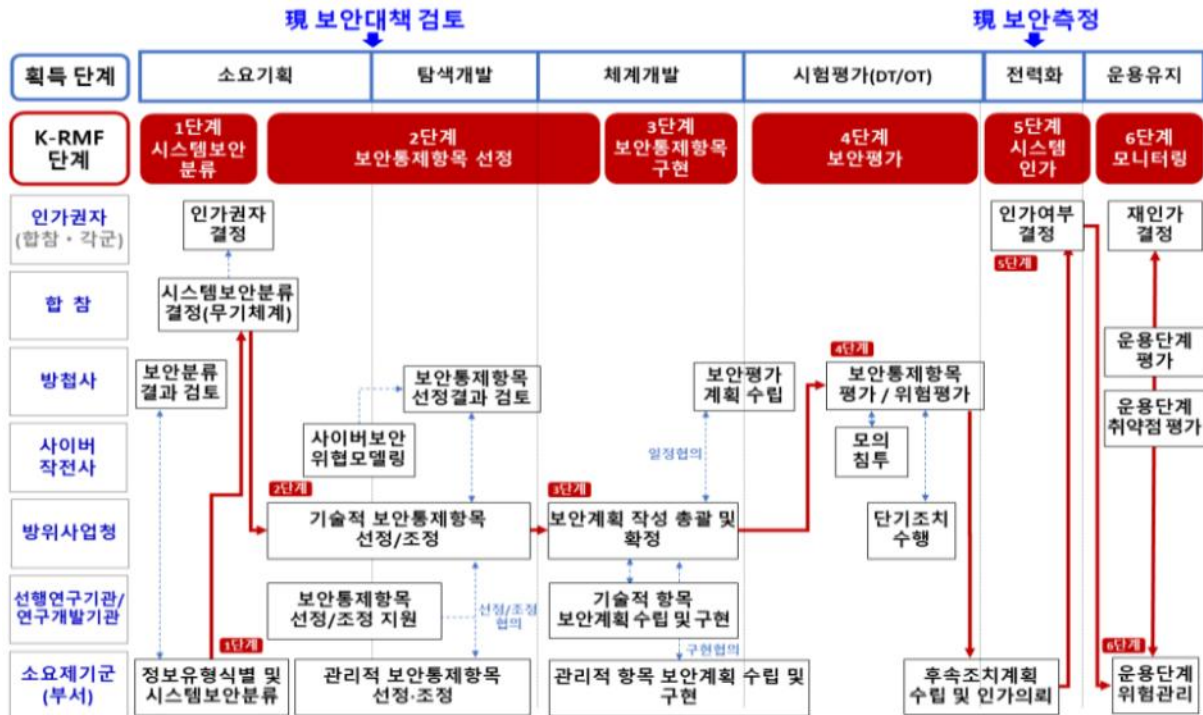
□ 이에 따라, 국방부는 국방 사이버보안 위험관리(영문 약칭 K-RMF¹⁾)에 관한 행정규칙(「국방 사이버보안 위험관리 지시」)을 2024년 4월에 마련하여 사이버보안 위험관리 업무를 수행중²⁾임.

동 행정규칙은 사이버보안 업무를 효율화하기 위해 유사·중복되는 절차 등을 점진적으로 K-RMF로 통합한다는 기본 원칙을 제시하고, 체계적인 업무 수행을 위한 제도적 근거로써 각 기관별 임무 분장 및 권한과 책임 등을 무기·전력지원체계 획득 절차에 따라 명시하고 있음.

1) 국방 사이버보안 위험관리의 영문약칭: K-RMF(Korea-Risk Management Framework)

2) 「국방 사이버보안 위험관리 지시」: 2024.4.12. 시행한 국방부장관 지시(행정규칙)

[K-RMF를 통한 통합적인 사이버보안 위협관리 수행절차]



□ 그런데 해당 행정규칙은 무기·전력지원체계의 전 수명주기 관점에서 사이버보안 위협을 관리하기 위한 절차 및 방법을 규율하고 있는 반면, 근거조항인 법 제21조제3항제5호는 ‘국방정보침해에 대한 대응 및 복구’를 주요 내용으로 하고 있어,

현행법 제21조제3항제5호가 해당 행정규칙의 근거조항으로 기능하기에는 다소 미흡한 측면이 있음.

「국방정보화 기반조성 및 국방정보자원관리에 관한 법률」 제21조(국방정보침해에 대한 대응 및 복구)

- ③ 국방부장관은 국방정보에 대한 침해에 대비하고 침해된 국방정보를 신속하게 복구하기 위하여 다음 각 호의 시책을 강구하여야 한다.
1. 침해·위협 정보기술의 동향조사 및 분석
 2. 침해된 정보의 유통 또는 유통시도에 대한 감시체계의 구축
 3. 침해·위협에 대한 역추적 등 대응기술의 개발
 4. 침해된 국방정보 및 정보시스템의 신속한 복구를 위한 정책개발, 평가, 기술개발
 5. 그 밖에 국방정보보호를 위하여 국방부장관이 필요하다고 인정하는 사항

□ 따라서 개정안은 국방부장관이 국방 사이버보안 위협관리를 시행하기 위한 체계적 방안을 마련하도록 하고, 관계기관 및 부대는 국방부장관이 마련한 체계적 방안에 따라 군의 사이버보안 업무를 국방 사이버보안 위협관리(K-RMF)로 통합 수행하도록 하기 위한 법적 근거를 명확히 하고자 하는바, 그 취지와 내용은 타당한 것으로 보임.

또한 국방 사이버보안 위협관리(K-RMF)제도는 미국 국방부의 RMF 제도를 기반으로 하여 우리나라 환경에 맞게 적용된 것으로, 이 제도를 명확히 함으로써 한·미간 무기체계 및 전력지원체계의 협력에도 긍정적인 영향을 미칠 것으로 기대됨.

□ 국방부는 국방 사이버보안 위협관리제도의 법적 근거를 명확히 하고, 국방부 장관이 사이버보안 위협을 관리하기 위한 체계적인 방안을 마련하고 기관 및 부대가 관련 업무를 수행하도록 하는 개정안에 동의한다는 입장임.

국가정보원은 국방부의 사이버보안 업무가 「국가정보원법」상 국가정보원의 사이버보안 업무소관³⁾과 중복되지 않아야 한다는 입장으로, 국방정보시스템 및 무기·전력지원체계로 한정되는 개

3) 국가정보원은 「국가정보원법」 제4조제1항제4호에 해당하는 국가정보원의 업무소관과 중복되지 않아야 한다는 입장임.

「국가정보원법」 제4조(직무) ① 국정원은 다음 각 호의 직무를 수행한다.

4. 다음 각 목의 기관 대상 사이버공격 및 위협에 대한 예방 및 대응

가. 중앙행정기관(대통령 소속기관과 국무총리 소속기관을 포함한다) 및 그 소속기관과 국가인권위원회, 고위공직자범죄수사처 및 「행정기관 소속 위원회의 설치·운영에 관한 법률」에 따른 위원회

나. 지방자치단체와 그 소속기관

다. 그 밖에 대통령령으로 정하는 공공기관

정안의 적용 범위에 대해 동의한다는 입장임.

문 의 처
02)6788-5310