

원저

인증형 방위산업 사이버보안 법령체계 도입 연구: 미 사이버보안 성숙도모델 인증제도(CMMC) 관련 법령과 비교를 중심으로

송광석

법무법인(유) 율촌 변호사

교신저자: 송광석 (sks9567@gmail.com)

요약

본 연구는 현행 방위사업 사이버보안 제도를 글로벌 표준에 부합하는 인증형 사이버보안 제도로 법령체계를 개선하기 위한 방안을 2025년 11월 10일부터 정식 발효된 미 국방부 사이버보안 성숙도모델 인증(CMMC) 제도와 법·제도 측면에서 비교·분석하여 제시하는 것을 목적으로 한다. 이를 위해 미국의 법령체계에 대한 이해를 바탕으로 CMMC 제도를 구성하는 연방법령과 국방조달규정을 국내 방위사업법령 및 방위산업보안 관련 법령체계와 비교법적 방법을 적용하여 분석하였다. 분석 결과, 미국은 연방 법령과 규정을 근거로 CMMC 제도를 통해 입찰절차에 사이버보안 인증을 연계하고 정보 유형별 단계적 제3자 인증 평가체계를 계약체결 자격 요건으로 명시하여 시행 중이나, 한국은 다수의 개별 법령으로 각종 정보보호의무를 부여하지만 업체가 취급하는 정보별 사이버보안 역량 인증을 계약의 조건으로 삼지 않는다. 본 연구는 국내 방산 사이버보안 법령체계를 국제적 기준에 부합하도록 정비하고, 향후 CMMC와의 상호인정을 포함한 기존 제도와 연계한 데이터 중심 인증제도 도입, 평가·인증기관 역할 정립 등의 구체적 개선 방향을 제시하고자 한다.

핵심어

사이버보안, 사이버보안 성숙도모델인증(CMMC), 보안측정, 통합실태조사, 상호인정협정

차례

1. 서론
2. 미국의 연방 법령체계와 사이버보안 법령
3. 사이버보안 성숙도모델(CMMC) 인증제도 관련 법령 체계 분석
4. 국내와 미국 사이버보안 법령 체계 비교와 개선 방안
5. 결론

Open Access

접수일: 2026년 6월 08일
수정일: 2026년 7월 25일
게재승인일: 2026년 8월 07일
출판일: 2026년 9월 30일

Copyright © 2026 Author(s).

This is an Open Access article distributed under the terms of the Creative Commons CC BY 4.0 license (<https://creativecommons.org/licenses/by/4.0/>) which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Original Article

A Study on the Legal Framework for Introducing a Certification-Based Cybersecurity Regime in the Defense Industry: Focusing on a Comparative Analysis of Laws and Regulations Related to the U.S. Cybersecurity Maturity Model Certification (CMMC)

Kwangseok Song

Attorney at Law, Yulchon LLC, Republic of Korea

Corresponding Author: Kwangseok Song (sks9567@gmail.com)

ABSTRACT

This study aims to propose improvements to the legal framework necessary for transforming the current cybersecurity regime in the Korean defense industry into a certification-based system aligned with global standards. To this end, it conducts a comparative legal analysis centered on the U.S. DoD Cybersecurity Maturity Model Certification (CMMC) program and applies a comparative law methodology to examine the federal statutes, regulations, and DFARS constituting the CMMC program and compares them with Korea's regulatory framework.

The analysis reveals that the US integrates the CMMC requirements into the defense contracting process and establishes a tiered third-party assessment and certification framework based on the sensitivity of information and explicitly requires certification as a condition of contract eligibility. In contrast, while Korea imposes various security obligations through multiple statutes and regulations, it does not require certified cybersecurity capabilities as a prerequisite for contract award.

Based on these findings, this study suggests policy and legislative directions and proposes the introduction of a data-centric certification regime linked to existing defense security systems, the development of mechanisms for future mutual recognition with the CMMC framework, and the establishment of clear roles and responsibilities for assessment and certification bodies.

KEYWORDS

Cybersecurity, CMMC, Security Assessment, Integrated Security Inspection, Mutual Recognition Agreement (MRA)

1. 서론

최근 방위산업을 둘러싼 안보환경은 무기체계의 디지털화와 방산 공급망의 글로벌화로 인해 방산 기업과 정부 획득기관이 취급하는 각종 방산계약 관련 정보에 대한 사이버공간에서 침해는 단순한 정보보호 문제를 넘어 국가안보 차원의 위협으로 인식되고 있다. 특히 방산 공급망을 구성하는 중소·중견 기업은 사이버보안 체제의 취약성으로 인해 기술탈취의 주요대상이 되고 있음에도 실질적인 사이버안보의 통제대상에서는 벗어나 있다. 이러한 취약점을 통한 군사 기술 유출은 직접적인 군의 작전 수행 능력 저하로 직결될 수 있다는 점에서 방위산업 사이버보안 역량은 방산기술을 포함한 각종 국가핵심기술과 전략기술을 보호와 관련된 경제안보 및 국가안보 역량을 평가하는 주요 지표로 여겨지고 있다.

이러한 배경에서 미국은 방산 공급망 전반의 사이버보안 역량 강화를 위해 오랜 기간에 걸쳐 관련 연방법규를 개정하여 CMMC 제도를 시행하고 있다. 미국은 국방조달에 참여하는 모든 계약자들이 계약과정에서 취급하는 정보의 중요도에 따라 요구되는 단계적 사이버보안 수준에 대한 제3자 인증을 도입하였다. 또한 이를 공급망 참여의 전제조건으로 연방조달규정에 명시하여 CMMC 자격인증은 국방조달계약의 낙찰자가 되기 위한 필수 요건으로 적용하도록 단계적으로 추진하고 있다. 따라서 미국 방산 시장에 진출하고자 하는 우리나라를 포함한 해외 방산 기업에도 CMMC 인증요건은 시장참여를 위한 입장권과 같은 것으로 작용할 것이다.

한편 한국의 방산 사이버보안 제도는 방위사업법령과 방위산업기술보호법령을 중심으로 방산업체 및 협력업체에 보안 관리 의무를 규정하고 있으나, 취급 정보에 대한 체계적인 분류와 이를 기준으로 한 사이버보안 역량 인증 제도는 시행되지 않고 있다. 더욱이 방산계약 이행과정에서 다양한 보호가 필요한 계약정보를 취급하지만 사이버보안 역량을 갖추지 못하여 기술탈취의 주요 대상이 되는 수많은 협력업체들은 통제 대상에서 벗어나 있다. 이로 인해 방산 사이버보안 제도에 공백이 발생할 수 있으며 향후 미국시장 진출을 위해서 국내 사이버보안 제도와 별도로 미 CMMC 제도를 준수해야 하는 추가적인 부담이 발생할 수 있다.

이에 본 논문은 미국 CMMC 제도의 법적 근거와 운영 구조를 관련 법령을 세부적으로 분석하고, 이를 한국의 방산 사이버보안 법령체계를 구성하는 근거 법령, 적용대상, 인증 제도를 포함한 운영방식, 운영기관 측면에서 비교하여 현행 제도의 한계와 이를 극복하기 위한 법령 체계의 개정 필요성을 규명하고자 한다. 이를 통해 향후 CMMC 제도와 상호인정이나 미 CMMC 체제 하에서 국내 공식 인증기관 기능을 인가받는 방안을 포함한 한국형 방산 사이버보안 인증체계(K-CMMC) 도입을 위한 법제적 개선 방향을 도출하여 한국 방위산업의 국제 경쟁력을 강화하기 위한 기술보호와 국가안보 역량을 제고하는 한편 미국 시장 진출을 계획하는 국내 업체들의 부담을 경감하기 위한 정책적 시사점을 도출하고자 한다.

2. 미국의 연방 법령체계와 사이버보안 법령

2.1. 미국의 연방주의에 따른 법령 체계

미국은 전통적으로 초기 영국 이민자들의 법률 문화로 인하여 영국과 함께 불문법과 판례법이 일차 재판규범인 보통법 국가(Common Law State)로 분류되었다.[1] 그러나 유럽 대륙에서 후기 이민자들이 들어오면서 성문법 체계(Civil Law System)가 법령체계에 편입되었고, 현재는 연방의회뿐 아니라 주 의회 및 지방자치단체 의회 등 수많은 입법기관에서 법률과 규정들이 제정되고 있으며, 특히 공법 분야는 성문법이 지배적 법령체계를 구성하고 있다.[2]

미국 법률체계의 위계질서는 미 연방헌법을 “국가의 최고 법(the Supreme Law of the Land)”으로 연방법률과 연방규정 그리고 주 법률의 순으로 구성되어 있다(미국헌법 제6조). 따라서 미국 대법원은 모든 법률과 국제 조약도 헌법에 반할 수 없도록 해석한다.[1,2] 대통령과 연방기관에 의한 행정명령이나 행정입법이 법률의 위임을 받거나 혹은 법률의 위임이 없이 제정되기도 하는데 대통령의 행정명령이나 법률에 위임을 받은 연방규정은 법률로서 효력을 가진다.[2-5]

2.2. 미국 연방 법령의 위계 관계

2.2.1. 연방의회의 입법절차와 연방법률

미국 연방법률은 하원(House of Representatives)과 상원(Senate)으로 구성된 양원제 의회에서 제정된다. 상원과 하원은 서로를 견제하는 역할을 하며 법안이 통과되려면 양원 모두에서 과반수의 동의를 얻어야 한다.[2] 위원회를 통과한 법안은 발의된 상·하원의 본회의에서 과반수 찬성으로 승인되며, 다른 의회로 넘어가 양원에서 승인된 법안은 대통령에게 전달되어 10일의 기간 동안 서명 혹은 아무런 조치가 없는 경우 법안으로 성립되지만 대통령이 거부권(veto)을 행사하면 양원에서 각 3분의 2 이상의 찬성 투표가 있어야 법안으로 성립된다.[2]

연방법률이 제정된 경우 개별 법률은 단행법(Slip law)의 형태로 국립문서기록관리청(National Archives and Records Administration, NARA)의 산하기관인 연방기록청(Office of the Federal Register, OFR)에서 초안을 준비하고, 정부출판청(Government Publishing Office, GPO)에서 공식 발행되어 대중에게 공개된다. 법안(Bill)이 법률로 확정되면 공법의 경우 “Public Law(PL) 회기번호- 일련번호”로 명명되며, GPO에서 연방법률총서(United States Statutes at Large: Statutes at Large)로 출판되는데 “125 Stat. 753”은 Statutes at Large 제 125권 753페이지를 의미한다.[6] 한편, 미국 연방법전(U.S. Code: USC)은 연방법률을 54개의 주제별로 정리한 공식 문서로 1926년부터 매 6년마다 GPO에서 각 법률 주제별로 누적하는 방식으로 보충판을 발간하여 업데이트되고 있다.[6] 현행 USC는 GPO의 웹사이트[7]와 미 하원 웹사이트[8]에서 각각 찾아볼 수 있다.

2.2.2. 대통령 행정명령

미국 헌법 제2조 제1항은 행정권을 대통령에게 부여하고 있는데 대통령은 이에 근거하여 행정기관이나 관료에게 일정한 행위나 정책 집행을 직접적으로 부과하는 문서를 행정명령이라고 한다.[3] 대통령 행정명령은 그 제정과 개정 절차에 연방행정 절차법(APA: Administrative Procedure Act)이 적용되지 않고 제정 또는 개정될 수 있어서 제정절차가 매우 간단하지만 법률과 동일한 효과가 있어 대통령이 행정명령을 발령할 유인은 매우 강력하다.[9] 따라서 미국 대통령들은 자신의 선거 공약을 구현하기 위해서 매우 적극적으로 행정명령을 발령하였는데 예를 들어 2017년 오바마 대통령의 재임기간까지 행정명령이 13,764건이나 발령되었다.[5] 2025년 1월 20일 취임한 트럼프 대통령도 다소 급진적인 자신의 선거 공약과 정책을 실현하기 위해서 2025년 말까지 143건의 행정명령을 발령하였다.[10]

2.2.3. 연방규정

연방규정은 연방법률 실행을 위해 법률에서 위임된 사항과 구체적 법률의 집행을 위해서 필요한 사항을 규정한 연방기관들이 제정하는 행정입법을 말한다. 미국 연방법원은 의회의 위임을 받은 범위에서 적법한 제정절차를 거쳐 제정된 연방규정은 법률과 동일한 효력이 있다고 판결하였

다.[11] 미국 행정절차법(APA, 5 USC§553)에서는 연방 규정을 제정 또는 수정하기 위해서는 초안 작성 후 연방 관보(Federal Register)에 게시하고 30일 이상 일반 대중 및 이해 관계자에게 서면 의견을 제출할 기회를 부여하도록 하였다. 의견수렴 이후 연방기관은 초안을 수정한 최종 규정(Final Rule)을 만들어 다시 연방 관보에 게시하며 규정의 시행일을 최종 규정 게시일 30일 이후로 지정한다.[12]

최종 규정은 이후 연방규정집(Code of Federal Regulations: CFR)에 통합되어 시행되며, CFR은 50개의 주제(Titles)로 구분되어 연방법률에 대한 구체적인 지침과 실행 세부사항을 규정하고 있다. 현행 CFR은 미국 연방기록관리청 사이트(<https://www.ecfr.gov>)를 통해서 확인이 가능하다.

2.3. 미국 사이버보안 관련 연방 법령 체계

2.3.1. 개관

미국은 1980년대 개인 컴퓨터(Personal Computer: PC)가 등장하고 컴퓨터를 이용한 범죄를 예방하기 위한 법률을 중심으로 사이버보안 관련 법률이 발전하기 시작하였다. 이후 컴퓨터라는 신종 정보관리시스템을 통해서 관리되는 연방의 중요 정보를 보호하기 위한 컴퓨터 보안법 (PL 100-235, Computer Security Act of 1987)이 제정되고 국가안보국(National Security Agency, NSA)의 지원을 통해서 국립표준국(National Bureau of Standards, NBS)을 연방 사이버보안 표준을 개발하는 주관기관으로 지정하였다. 이 법은 2002년에 연방정보보안관리법(Federal Information Security Management Act of 2002, FISMA 2002)으로 대체되면서 NBS의 후신인 미국표준기술국(National Institute of Standards and Technology, NIST)을 연방기관의 시스템 보안을 위해 사용되는 보안가이드 라인과 지침을 개발하는 기관으로 지정했다.[13]

2010년대에 들어서면서 스마트폰이 급속도로 보급되고 전세계의 인터넷 의존도가 심화되면서 사이버보안의 중요성도 증대되었고, 2013년도에 발생한 스노든 사건을 계기로 기존의 FISMA 2002가 연방정보보안현대화법(PL 113-283 Federal Information Security Modernization Act of 2014, FISMA 2014)으로 개정되었다. 이 법을 통해 연방정부의 정보보호 및 사이버안보에 관한 사무를 국토안보부(Department of Homeland Security, DHS)으로 대폭 이관하고, 대통령실 행정관리에산국(Office of Management and Budget, OMB)이 연방기관의 사이버보안 표준과 가이드라인에 대한 운용지침을 수립하고 이행여부를 감독하도록 하였으며, 사이버보안강화법(PL 113-274 Cybersecurity Enhancement Act of 2014)을 통해서 사이버위협 감소를 위한 표준과 대응절차를 수립을 위해 NIST에 부여한 임무를 법제화하고 공공·민간 파트너십을 강화하도록 하였다.[13]

2.3.2. NIST의 사이버 보안 기준

NIST의 사이버보안 기준은 개별 법률과 대통령 행정명령에 근거를 가지고 연방기관의 정보시스템에서 유통되는 정보의 기밀성이나 보호의 필요성을 고려하여 다양한 기술적 요구사항을 반영하여 발간되는 연방규정이다. NIST는 FISMA 2014와 트럼프 대통령이 발표한 E.O. 13800에 근거하여 특별 간행물(Special Publication: SP) 800-37를 발간하여 연방정보시스템 및 조직에 RMF(Risk Management Framework) 개념을 적용하기 위한 지침을 제공하였다.[14] 또한 NIST는 FISMA 2014와 OMB Circular A-130에 근거하여 2022년 1월 25일에 SP 800-53 r5. 연방 정보시스템 및 기관의 보안과 개인정보 통제(Security and Privacy Controls for Federal

Information Systems and Organizations)에 대한 최종 규칙을 발행하여 다양한 위험 수준에 따라 단계별 최소 보안 통제(Minimum requirements)를 통한 다층적 보안통제를 도입하였다.[15] NIST의 일련의 정보시스템 보호 지침은 32 CFR Part 117 국가산업보안프로그램운영규정(National Industrial Security Program Operating Manual, NISPOM)을 통해서 국방부의 기밀정보를 취급하게 되는 연방 계약자의 정보시스템에도 적용하도록 하고 있다.

한편 E.O. 13526에서는 비밀이 아니지만 일정한 보호가 필요한 통제필요정보(Controlled Unclassified Information, CUI)에 대해서 규정하고 있는데, 해당 정보를 유통하는 비 연방정부 정보시스템에서는 E.O. 13556에 따른 NIST SP 800-171에 명시된 기준을 적용하고 있다.[16] E.O. 13556에서는 CUI 프로그램을 이행하는 책임기관으로 NARA를 지정하고 모든 연방기관이 CUI의 지정과 보호를 위한 통일된 기준을 수립하여 이를 이행하는 것을 감독하도록 하였다. NARA의 권한은 32 CFR Part 2002를 통해 ISOO로 위임되어 각 연방기관이 제출한 CUI 목록을 CUI Registry를 통해서 공공에 공개하는 역할을 담당하고 있다. 현재 각 연방정부기관별 CUI 목록은 NARA의 CUI Registry 웹사이트에서 확인할 수 있다.[17] NIST SP 800-171은 개정을 거듭하여 현재 2024년 5월 14일에 발간된 NIST SP 800-171 r3가 최신 버전으로 적용되고 있으며 기존의 NIST SP 800-171 r2와의 차이는 단순한 개정이 아니라 NIST SP 800-53 r5와의 정합성을 확보하고, CMMC 2.0 및 Zero Trust 환경을 반영하기 위한 전면적인 개편이라는 점이다.[18] 다만 현재까지는 미 국방부는 r3를 적용하기 위한 규정 개정작업을 진행 중이므로 여전히 CMMC 프로그램은 NIST SP 800-171 r2에 의해서 운영되고 있다.[19]

한편, CUI가 중요한 사업이나 고가치 자산과 연관되어 활용되는 경우, 고도화된 지속적인 위협(Advanced Persistent Threat: APT)의 대상이 될 가능성이 있다. 이러한 APT의 표적이 될 수 있는 CUI를 보호하기 위해서 NIST SP 800-171 기준에 보다 강화된 보안 요구사항을 추가하여 (1) 침투 저항 아키텍처, (2) 피해 제한 작용, (3) 사이버 회복력과 생존성을 달성하기 위한 설계를 적용한 NIST SP 800-172가 제시되었다.[20] NIST SP 800-172는 NIST SP 800-171에 추가하여 종심깊은 보호 방어전략(Defense-in-Depth Protection Strategy)을 적용하여 24개의 영역에 대해서 강화된 보안 요구사항을 포함하고 있다.

2.3.3. 미국의 방위산업 사이버보안 관련 연방 법령체계

미국의 방위산업 보안 법령 체계는 방산업체(Defense Industrial Base: DIB)들이 취급하는 정보를 기밀정보와 통제필요정보(CUI) 또는 연방계약정보(FCI)로 구분하고 정보의 중요성에 따라 각각의 보안 요구조건과 보안정책에 차이를 두고 있다. 먼저 비밀 계약을 체결하는 업체는 연방규정인 32 CFR Part 117 NISPOM에 규정된 사이버보안을 포함한 일련의 보안요건을 준수하여야 한다. NISPOM은 기밀정보를 취급하는 계약자의 정보시스템에 대해서 NIST SP 800-37 r2, NIST SP 800-53 r5 기준을 준수하여 RMF 기반의 정보시스템 보안 프로그램을 적용하도록 하고 있다(32 CFR §117.18).

한편, NISPOM 정보시스템 보안 관련 규정에는 기밀이 아닌 CUI를 취급하는 정보시스템에 대해서는 CUI의 취급에 따른 계약상 요구를 이행해야 한다는 부분을 포함하고 있다(32 CFR §117.18(f)). CUI의 보호를 위한 구체적인 국방부의 정책은 E.O. 13556, 48 CFR part 204, 32 CFR part 170, NIST SP 800-171, NIST SP 800-172 등의 행정명령과 연방규정 등에 규정화되어 있는 CMMC제도를 통해서 이행되고 있다.

3. 사이버보안 성숙도모델(CMMC) 인증제도 관련 법령 체계 분석

3.1. CMMC 프로그램 연혁

미 의회는 2019년 국방수권법(PL 116-92 NDAA Section 1648 FRAMEWORK TO ENHANCE CYBERSECURITY OF THE UNITED STATES DEFENSE INDUSTRIAL BASE)을 통해서 국방부장관에게 진화하는 DIB에 대한 사이버보안 위협에 대응하기 위하여 제3자 인증방식을 도입한 CMMC 제도를 시행하기 위한 프레임워크를 개발하도록 하였다. 이에 따라 국방부는 2020년 3월에 5개 성숙도 등급과 17개 도메인, 171개 프랙티스로 구성된 CMMC 1.0을 발표하고, 같은 해 9월 CMMC 임시규칙을 발표하여 5년의 단계적 적용 기간을 두고 임시 적용을 시작하였다. 이후 위 임시규칙에 대해서 제도 적용에 따른 각종 부담으로 인해 미국 내 방산업체들의 심한 반대에 직면하였으며 2021년 12월에 3개 성숙도 등급과 14개 도메인, 110개 프랙티스로 구성된 현행 CMMC 모델 2.0을 발표하였다.[21]

3.2. CMMC 프로그램 규정의 구체적 내용 분석

3.2.1. CMMC 프로그램 법령체계

현행 CMMC는 2024년 12월 16일부터 32 CFR Part 170 CMMC 프로그램 규칙이 공식 시행되면서 방산업체들 스스로 CMMC 요구조건을 충족시킬 수 있는 민간 생태계를 통한 자율이행 단계(Market roll-out)에 들어섰다. 이후 2025. 11. 10. 48 CFR Part 204을 통해 CMMC는 국방 조달 계약을 체결의 전제 조건에 정식으로 편입되어 완전 적용까지 업체의 적응기간을 고려한 2028. 11. 10.까지 4단계에 걸친 단계적 이행절차(Phased roll-out)가 진행되고 있다.

CMMC 프로그램의 특징은 먼저 계약자의 정보시스템에 유통되는 정보를 연방계약정보(FCI)와 통제필요정보(CUI)로 구분하여 이에 따라 3단계 등급에 따른 단계적 사이버보안 수준을 결정한다는 것이다. CMMC 인증을 받는 기업이나 단체는 일정한 정보시스템에 대해서 CMMC 등급을 갖추거나 유지하기 위해서 자체심사와 제3자 인증심사를 추진하는 ‘평가추진기관’(Organization Seeking Assessment, OSA)과 제2단계, 3단계 인증심사를 얻거나 유지하기 위하여 제3자 인증심사를 받으려는 ‘인증추진기관’(Organization Seeking Certification, OSC)으로 구분하며 OSA는 OSC를 포함한 개념이다(32 CFR §170.4(b)).

3.2.2. CMMC 등급 구분 및 등급별 보안 기준

3.2.2.1. CMMC 1등급(Level 1)

먼저 CMMC 1등급은 FCI를 처리하는 연방계약자에게 요구되는 것으로 48 CFR §52.204-21에 규정된 15개의 보안요건을 충족해야 한다(32 CFR §170.14(c)(2)). CMMC 1등급은 연방계약자가 자신의 시스템을 스스로 평가하는 방식으로 CMMC Level 1(self)로 표기한다. 연방계약자는 자체 평가에 앞서서 인원, 시설, 시스템의 규모 등을 고려하여야 하며, 32 CFR §170.15에 상세하게 제시된 바와 같이 2018년 6월에 발간된 NIST SP 800-171A에 따른 보안요건 달성여부를 자체평가한 후 그 결과를 국방부의 공급자 이행 위험시스템(Supplier Performance Risk System, SPRS)에 등록해야 한다. CMMC Level 1(Self)를 달성한 연방계약자는 규정상 요구조건을 지속적으로 준수하고 있다는 사실을 매년 SPRS에 보고하여 확인해야 하며 이러한 절차를 거치지 않는 경우 자격요건이 취소된다.

3.2.2.2. CMMC 2등급(Level 2)

CUI를 처리하는 연방 계약자의 경우에는 DFARS §252.204-7012에 따라서 32 CFR §170.16 자체심사와 확인 요구조건(CMMC Level 2 self-assessment and affirmation requirements)에 따라 CMMC Level 2(self) 자체심사와 32 CFR §170.17 인증심사 및 확인 요구사항(CMMC Level 2 certification assessment and affirmation requirements)에 따른 CMMC Level 2(C3PAO)에 의한 제3자 인증을 받아야 한다. CMMC 2등급 보안요건은 현재 32 CFR §170.14(c)(3)와 연방조달규정(Defense Federal Acquisition Regulation Supplement, DFARS) §252.204-7012에 따라 NIST SP 800-171 r2.의 14개 범주와 110개의 보안요구사항 기준이 적용된다.

한편 최종 규정에는 방산업체들이 2등급 이상의 CMMC 자체심사(self assessment)나 제3자 인증심사(certification assessment)에서 180일의 기간 동안 흠결을 보완하는 것을 조건으로 임시로 계약 참여를 허용하는 이행계획과 일정(Plan of Action and Milestone, POA&M) 제도를 두고 있다. 이러한 조건부 자격은 Conditional Level 2(Self)와 Conditional Level 2 (C3PAO)로 구분된다. 이후 OSA는 POA&M 계획과 일정에 맞추어 미흡한 요건을 보완하여 마감평가(closeout assessment)를 거쳐 Final Level 2(Self) 또는 Final Level 2(C3PAO)의 자격을 보유한다.

CMMC Level 2(Self)의 자격요건을 갖춘 연방계약자는 매년 기준의 지속적인 준수여부를 미 국방부 SPRS에 입력하여 스스로 확인(affirmation)하는 절차를 거쳐야 한다. 한편 CMMC Level 2(C3PAO)의 경우에는 인증심사를 진행한 C3PAO가 인증결과를 CMMC 기업업무보장지원서비스(Enterprise Mission Assurance Support Service: eMASS)에 입력하면 그 결과가 SPRS에 게시된다. CMMC Level 2를 충족하는 OSA나 OSC의 인증요건은 3년간 유효하며(32 CFR §170.16(a)(1), §170.17(a)(1)), 인증결과에 따른 보안요건을 준수여부를 매년 자체평가하여 SPRS를 통해서 확인하는 절차를 거쳐야 하며 이를 해태할 경우 연방계약 자격이 취소될 수 있다(32 CFR §170.16(b), §170.17(b)).

3.2.2.3. CMMC 3등급(Level 3)

최고 레벨인 CMMC 3등급 보안요구사항은 APT 위협이 있는 중요사업이나 고가치 자산과 관련된 계약을 이행하는 계약자의 경우에는 CMMC 2등급 보안요구 사항을 모두 충족하면서 NIST SP 800-172에 명시된 24개의 요구사항을 추가로 충족시켜야 한다. 3등급 인증심사는 국방계약관리국(Defense Contract Management Agency, DCMA)의 방위산업망 사이버보안 평가센터(Defense Industrial Base Cybersecurity Assessment Center, DIBCAC)를 통해서 3년마다 이루어져야 하며, 결과는 DIBCAC에 의해서 CMMC eMASS에 입력되면 해당 정보는 SPRS에 게시된다. OSC의 Level 3(DIBCAC) 인증 범위는 32 CFR §170.19(d)에 따라 정해지며 사내 전체 네트워크 또는 특정한 구역이나 네트워크에 대한 인증도 가능하다.

한편 DIBCAC가 OSC를 평가한 결과 일부 중요 보안요건을 제외한 미흡사항이 있을 경우에는 POA&M을 수립하여 이를 보완할 기회를 부여하고 임시로 Conditional Level 3(DIBCAC) 자격을 인정할 수 있다. OSC가 180일의 기간 동안 미흡사항을 보완하고 DIBCAC가 마감평가를 실시하여 보안요건을 모두 충족한 것으로 평가된 경우 Final Level 3(DIBCAC) 자격을 부여한다.

DIBCAC이 OSC에 대한 평가결과를 CMMC eMASS에 입력해야 해당 정보는 SPRS에 게시된다. DIBCAC의 Level 3 인증결과는 3년간 유효하며, OSC는 32 CFR §170.18(a)(22)와 §170.22에 따라 자체 평가를 통해서 Level 3(DIBCAC) 요구조건을 준수하고 있다는 확인을 SPRS에 매년

입력해야 하는데 이를 해태했을 경우에는 연방계약을 위한 자격요건이 취소된다(32 CFR §170.18(b)).

3.2.3. CMMC 생태계 구성 기관

3.2.3.1. 계약담당자(Program Manager and requiring activities)

32 CFR §170.5에서는 각종 국방조달사업 계약담당자가 § 170.5(b)(1-5)에 열거된 요소를 고려하여 적용 가능한 CMMC Level을 결정하고 해당 기준은 하청업체에도 적용되도록 요구할 수 있는 권한을 부여하고 있다(§170.23). 한편 국방부 각군이나 기관의 국방조달계약을 담당하는 책임자는 CMMC 요구조건에 대한 면제를 적용할 수도 있다.

3.2.3.2. CMMC 프로그램 관리사무소(CMMC Program Management Office: PMO)

CMMC 프로그램 관리사무소(CMMC Program Management Office, CMMC PMO)는 미 DoD CIO 소속으로 그 기능은 §170.6에 명시되어 있다. DoD CIO 산하의 사이버보안 담당 부책임관실(DoD CIO(CS))은 CMMC 프로그램의 감독권을 가지며, CMMC 평가·인증·교육 요건의 수립, CMMC 프로그램 정책의 개발 및 갱신, 이행 지침의 마련에 대한 책임을 진다(§170.6(a)). CMMC PMO는 CMMC 인증기관(Accreditation Body)의 성과를 모니터링하고, 효과적인 수행과 관련된 문제를 해결하기 위해 필요한 조치를 취할 책임이 있다(§170.6(b)).

3.2.3.3. 국방계약관리국 방위산업사이버보안평가센터(DCMA DIBCAC)

DCMA DIBCAC는 CMMC 프로그램을 지원하기 위하여 인증기관(Accreditation Body) 및 C3PAO에 대해 CMMC 2등급 평가를 수행하며, CMMC 3등급 인증을 추진하는 OSC에 대한 평가결과 기록, 인증서 발급, 이의제기 추적, 기록 보존 등의 업무를 수행한다(§170.7). CMMC 프로그램 감독 기능 중 평가는 관련 평가정보 검토 및 48 CFR 252.204-7020에 따라 DCMA DIBCAC가 OSA를 재평가할 수 있는 권리를 포함한다(§170.6(e)). DCMA DIBCAC 평가 결과 요구되는 CMMC 지위가 달성이 되지 않았거나 유지되지 않은 것으로 확인될 경우, 그 평가 결과는 SPRS 또는 그 후속 시스템에 기록된 기존 CMMC 지위보다 우선한다.

3.2.3.4. CMMC 인증기관(CMMC Accreditation Body, Cyber AB)

CMMC 인증기관(CMMC Accreditation Body, Cyber AB)의 임무와 역할 등은 §170.8에 규정되어 있다. Cyber AB는 미주지역 인증협력체(Inter-American Accreditation Cooperation: IAAC)의 회원이자, 국제 시험기관인정 협력체(International Laboratory Accreditation Cooperation: ILAC)의 상호인정협정(MRA)의 서명 당사자로서, ISO/IEC 17020:2012(E), 17024:2012(E), ISO/IEC 17011:2017(E) 규격을 충족하여야 한다. 현재까지 CMMC 프로그램은 단 하나의 인증기관만 존재하며 그 주요 임무는 C3PAO의 인가 및 인증이다. 또한 인증기관은 CAICO(CMMC 평가자 및 강사 인증기관)를 감독하여 ISO/IEC 17020:2012(E) 준수 여부와 교육·시험 자료의 품질을 보장해야 한다. 인증기관은 국가안보 신원조사, 외국인 소유 제한, 보고의무, 정보보호, 이의절차 등에 관한 세부요건을 준수해야 한다. 또한 ISO/IEC 17011:2017 및 DoD 요건을 충족하는 이해상충(CoI), 전문행동강령(CoPC), 윤리(Ethics) 정책을 수립해야 한다. 이러한 정책은 인증기관 및 CMMC 생태계의 모든 구성원에게 적용된다. 인증기관이 사용하는 정보시스템은 CMMC 2등급 보안요건을 충족해야 하며, DCMA DIBCAC의 평가를 받아야 한다.

3.2.3.5. CMMC 제3자인증기관(CMMC C3PAO)

CMMC C3PAO는 CMMC 2등급 인증평가를 수행하는 기관으로 그 역할, 책임 및 자격요건은 §170.9에 명시되어 있다. C3PAO는 평가 결과를 eMASS에 제출하고 §170.17의 요건에 따라 모든 보안요건이 충족된 경우 평가 인증서를 발급할 수 있다. C3PAO는 국가안보 신원조사, 외국소유 제한, 보고, 기록관리, 정보보호, 품질보증, 이의절차 등에 대한 세부요건을 준수해야 하며 정보시스템은 CMMC 2등급 요건 충족여부를 DCMA DIBCAC로부터 평가받아야 한다. 또한 ISO/IEC 17020:2012(E) 및 인증기관에 요구되는 각종 윤리 정책을 준수해야 한다.

3.2.3.6. CMMC 평가자 및 강사 인증기관 (CMMC Assessor and Instructor Certification Organization: CAICO)

CMMC 생태계에서 CMMC 평가자, 강사, 그리고 관련 전문가들에 대한 교육·시험·인가·인증을 담당하는 CMMC 평가자 및 강사 인증기관 (CMMC Assessor and Instructor Certification Organization: CAICO)의 역할, 책임 및 요건은 §170.10에 규정되어 있다. 현재 CMMC 프로그램에서는 CAICO는 하나의 기관만 인정되고 있으며 Cyber AB의 완전 자회사인 비영리기관으로 운영되면서 ISO/IEC 17024:2012 및 인증기관으로서 윤리정책과 시험, 품질보증, 이의절차, 기록관리, 보고, 직무분리, 정보보호 등의 요건을 준수해야 한다.

3.2.3.7. 공인 CMMC 평가자(CMMC Certified Assessor, CCA) 및 전문가(CMMC Certified Professional, CCP)

CMMC 2등급 인증 평가를 담당하는 CMMC 평가자(CMMC Certified Assessor, CCA)의 임무와 역할은 §170.11에 명시되어 있다. CCA 후보자는 먼저 CCP(CMMC Certified Professional) 자격을 취득해야 하며, §170.10 및 §170.8(b)(17)의 요건을 준수하고, Tier 3 동등한 수준의 신원 조사를 완료해야 한다.

CMMC 전문가(CMMC Certified Professional, CCP)의 역할과 책임은 §170.13에 규정되어 있으며 고객에 대한 자문, 컨설팅, 권고를 수행한다. CAICO는 §170.13(b)에 따라 CCP 후보를 교육 및 시험하며, 합격 시 CCP 인증을 부여한다. CCP는 CCA의 감독 하에 2등급 인증평가에 참여할 수 있으나, 최종 평가판단은 CCA가 책임진다.

3.2.3.8. 공인 CMMC 강사(CMMC Certified Instructor, CCI)

공인 CMMC 강사(CMMC Certified Instructor, CCI)의 역할과 책임은 §170.13에 규정되어 있으며 기본적으로 CCA 후보를 교육하는 역할을 수행한다. CCI 후보는 CAICO에서 교육 및 시험을 치르며(§170.12(b)), CCI 자격 유지 및 취득 요건에는 인증기관 정책 준수, 업무제한, 비밀유지, 비공개 정보 보호, 금지된 컨설팅 행위, 보고의무 등이 포함되어 있다.

3.2.3.9. CMMC 등록 실무자(Registered Practitioner, RP)와 등록실무자기관(Registered Practitioner Organization, RPO)

CMMC는 평가가 이루어지기 전에 먼저 실행(implementation)되어야 하므로 평가나 인증 이전에 방산업체(Defense Contractors)가 CMMC를 이해하고 여기에 적절한 규모의 투자를 통해 구현하고 평가를 준비할 수 있도록 돕는 개인 및 기관에 대한 수요가 존재한다. 이러한 수요에 대응하는 CMMC 등록실무자(CMMC Registered Practitioner, RP)는 CMMC 실행 컨설팅 서비스를 통해서 OSC의 보안체계상 격차(gap)를 식별하고 보완 전략(mitigation strategy)을 제시하여

인증평가에 대응하도록 도와주는 역할을 수행한다. RP들은 RP 기관(Registered Practitioner Organization, RPO)의 일원으로 임무를 수행하거나 개인 자격으로 계약을 맺어 활동할 수도 있다.[22] 컨설팅 서비스와 관련된 자격 및 조직은 RP, RPA, RPO로 나눌 수 있으며 특기할 만한 것은 국적요건에 한국이 명시되어 있다.

3.2.3.10. 기타 관련 자격요건 및 서비스 신청

위와 같은 CMMC 생태계를 구성하는 기관이나 인원들에 대해서는 32 CFR에서 그 자격 요건을 규정한 내용을 확인해 보면 미국 국적 보유 등을 요구하고 있지 않다. 하지만 DCMA의 Tier 3 신원조사 또는 동등 심사 완료하여야 하고, 관련 문서는 모두 영어로 제출하도록 하면서 기관의 경우에는 NISPOM에서 요구하는 FOCI 리스크 평가 및 필요한 완화조치 진행하도록 하여 외국의 영향으로 인한 위험을 완화할 수 있다는 것을 조건으로 외국인이나 기관의 생태계 참여를 형식적으로는 허용하고 있다.[23]

CMMC 서비스를 필요로 하는 업체(OSC)들은 CyberAB가 구축한 온라인 플랫폼인 CMMC 마켓플레이스(CMMC Marketplace)를 통해서 자신이 필요로 하는 CMMC 서비스를 제공할 C3PAO 및 CCA 또는 RPO와 연결을 할 수 있다. 이 플랫폼은 CMMC 평가 및 인증 절차의 조달을 용이하게 하며, OSC가 공인된 자격을 갖춘 평가자를 한곳에서 찾을 수 있는 중앙화된 자원(centralized resource) 역할을 수행한다.[24]

3.3. CMMC 프로그램의 단계적 시행

미 국방부(DoD)는 2025년 9월 10일에 최종 CMMC 조달규칙을 발표했으며 2025년 11월 10일부터 발효되었다.[25] 이러한 최종 연방규정 발효와 함께 DFARS 252.204-7025을 개정하여 계약 체결 전(pre-award) 단계의 CMMC 요건을 명시하는 조항이 추가되었다. 또한 DFARS 252.204-7021을 개정하여 계약 체결 후(post-award) 단계의 새로운 CMMC 요건을 반영하였으며 국방부는 CMMC를 1단계 (Phase 1)는 2025년 11월 10일에, 2단계 (Phase 2)는 2026년 11월 10일에, 3단계 (Phase 3)는 2027년 11월 10일에 그리고 마지막 4단계 (최종 단계, Phase 4)는 2028년 11월 10일 적용을 시작하도록 4단계를 거쳐서 CMMC 수준별 요구사항을 점진적으로 추가하는 방식을 취하고 있었다.

미 국방부(DoD)는 필요한 평가자 수를 교육할 시간과 기업이 CMMC 요구사항을 이해하고 이를 구현할 시간을 제공하기 위해 단계적인 CMMC 구현을 추진하면서 각 단계의 세부 사항은 32 CFR§170.3(e)에 규정하였다. 1단계에서는 제안요청서에서 업체에게 CMMC 1단계와 2단계의 자체 평가를 완료할 것을 요구한다. 2단계는 CMMC Level 2(C3PAO) 인증을 요구하게 되고, 그 후 다시 1년이 경과된 시점에서는 3단계로 CMMC Level 3(DIBCAC)를 충족할 것을 요구할 수 있다. 결과적으로 1단계 이행계획을 시작한 후 3년이 지나면 최종적으로 4단계(완전 구현)에 진입하면 국방부는 모든 적용 가능한 CMMC 요구사항을 계약체결의 조건으로 포함시키는 계획을 가지고 있었다.

실제로 미 국방조달공고 공식 사이트인 System for Award Management (SAM)을 확인해 보면 2025. 10. 28. 동부시간 10:56에 공고된 주일미군 공병부 특별공지사항(Special Notice W912HV-26-Z-0001)에서 2025. 11. 10. 이후 발행되는 모든 입찰과 계약은 CMMC Level 1 또는 그 이상의 인증요건을 요구할 것이며 만약 해당 등급 요건을 갖추지 못한 회사는 계약의 낙찰자가 될 수 없다고 명시하고 있다.[26] 한편 미 국방부는 2026. 7. 13.에 같은 해 11. 10.부터 적용 예정이던 2단계 적용을 전격 유예하고 프로그램 전반을 재검토하기 위한 “CMMC 검토·개혁 TF”

를 구성한다고 발표하였다.[27] 현재 활동 중인 C3PAO의 심사만으로는 계획대로 2단계 진입이 힘들 것이라는 판단에 따른 것이지만 현재 시행 중인 1등급 인증과 2등급 자체심사 그리고 사이버 보안 의무 자체는 계속 유지되며 오히려 2등급 자체심사 대상을 확대하는 계기가 될 수 있다. 따라서 미국 진출을 계획 중인 국내 업체들은 참여할 국방조달사업의 구체적 조건에 따라 2등급 요건 충족을 위한 대비 필요성이 여전히 있을 수 있다.[28]

4. 국내와 미국 사이버보안 법령 체계 비교와 개선 방안

4.1. 현행 방위산업보안 및 사이버보안 법령 체계 개관

4.1.1. 법령상 방위산업 보안 개념의 변천

방위산업 보안의 정의는 방위산업 발전과 관련 법령의 변화에 따라 함께 변화한다.[29] 방산보안 관련 법령은 1973년 군수조달에 관한 특별조치법, 1983년 방위산업에 관한 특별조치법, 2006년 방위산업법, 2015년 방위산업기술보호법, 2021년 국방과학기술혁신촉진법과 방위산업발전 및 지원에 관한 법률 등이 제정 또는 개정되면서 변천되어 왔다.[29] 방위산업보안업무훈령에서는 방산보안을 방위산업과 관련하여 국가안보 등을 위해 유무형 자산(인원, 문서, 자재, 시설, 정보통신, 군사기밀, 국방기술 등)을 제 요소의 누설, 파괴, 침해 등 대내외 각종 위해 행위로부터 보호하는 제반활동으로 정의하고 있다. 위 훈령은 주로 군사기밀 보호를 위한 지침으로 역할을 하고 있으며, 방위산업기술보호는 2015년 제정된 방위산업기술보호법령과 방위사업청 훈령인 방위산업기술보호지침에 따르고 있어 현행 법령상 방산보안은 군사기밀 보호와 방위산업기술보호로 이원화되어 있다.[29]

류연승은 방위산업보안 관련 법령 변천에 있어서 2016년부터 시행된 방위산업기술보호법을 기준으로 그 이전과 이후를 방산보안 1.0과 2.0으로 나누고 보고 있다. 방산보안 1.0은 군사기밀보호법에 따른 군사기밀보호 위주의 방산업체를 대상으로 한 물리보안 중심으로 군기관의 통제와 감독을 통한 폐쇄적 제도로 운영되었다. 하지만 방산보안 2.0은 방산기술 보호로 방산보안의 범위가 확대되면서 대상기관도 민간기관인 전문연구기관과 대학 등이 방산업체와 함께 방산보안의 대상기관으로 확대되었으며 사이버보안과 무기체계 자체의 보안 그리고 방산보안제도의 운영에서 대학, 학회 등 학계의 지원을 포함한 다양한 기관의 협력과 지원을 통한 개방적 제도 운영이 필요하다는 것이다.[29] 여기에 더 나아가서 방산보안 3.0은 4차 산업혁명 시대에 범정부차원에서 추진되는 정보보호 패러다임에 부응하여 군사기밀과 방위산업기술을 그 중요도에 따라 포괄적으로 하나의 데이터 분류 및 위험관리에 기반한 데이터 중심의 정보보호 제도로 발전되어야 하며 이를 위해 관련 법령과 제도의 대대적인 혁신과 변혁을 추진해 나아가야 한다.[29] 이와 같은 방산보안 3.0의 개념은 사이버 보안 측면에서 취급되는 정보의 중요도에 따라 단계적 사이버보안 수준을 요구하는 미국의 CMMC 제도에 부합하는 방식이라고 볼 수 있다.

4.1.2. 현행 방산보안법령상 사이버보안 제도

우리나라의 방산 사이버보안 제도는 먼저 특정업체가 방산업체로 지정을 받으려는 경우 또는 비밀 정보를 취급하는 사업을 수행하는 경우 등에 있어서 방위사업법령과 군사기밀보호법령, 보안업무규정, 방위산업보안업무훈령에 근거한 보안측정 절차 중 정보통신 분야 보안 요건 충족 여부를 검증하는 것이 가장 대표적이다. 한편 보안측정을 통과한 방산업체 등이 방위사업 추진 과정에서 방위산업기술을 취급하는 경우에는 방산기술보호법령과 방산기술보호지침에 따른 정보통신 보안 요건에 사이버보안 관련 기준을 포함시켜 해당 요건을 준수하도록 요구한다. 그리고 군사보안과

방산기술보호와 관련된 사이버보안 기준의 준수 여부는 매년 방사청, 국정원 그리고 방첩사령부에 의해서 실시하는 통합실태조사를 통해서 점검하고 있다. 이처럼 방산보안법령 상 보안측정, 방산 기술보호를 위한 통합실태조사 등의 근거가 되는 법령은 방위사업법령과 군사기밀보호법령, 보안 업무규정, 국방과학기술법령이며 실제 구체적인 기준은 방산보안업무훈령과 방산기술보호지침에 명시되어 있다. 이러한 현행 사이버보안 관련 제도를 관련 법령과 함께 구체적으로 살펴보면 아래와 같다.

4.1.2.1. 보안측정

방위사업법 제3조와 제35조에 따라 방산업체로 지정되기 위해서는 일정한 보안요건을 충족해야 한다. 방산업체의 지정에 필요한 보안요건 중 사이버보안과 관련된 내용은 방위사업법 시행령 제44조 제1항 제6호 통신시설 및 통신수단에 대한 보안대책, 제7호 각종 자료의 정보처리과정 및 정보처리 결과자료의 보호대책, 제8호 보안사고에 대비한 관계정보기관과의 유기적인 통신수단 등과 관련된 보안측정 기준과 연관되어 있다. 방위사업청장은 방산업체의 지정, 취소뿐 아니라 방위사업법 제3조 제10호의 방산물자의 연구개발·시험·측정, 방산물자의 시험 등을 위한 기계·기구의 제작·검정, 방산업체의 경영분석 또는 방산 관련 소프트웨어의 개발을 위하여 전문연구기관의 위촉과 위촉해지를 위한 요건을 평가하기 위해서도 보안요건의 측정을 요구한다(방위사업법시행령 제44조 제1항 제1호, 제2호). 이러한 경우에도 보안측정을 실시하게 되며 함께 사이버보안 관련 분야도 점검을 하게 된다.

보안측정 결과 75점 미만 점수를 받은 경우 미흡사항을 보완하여 다시 보안측정을 신청해야 하며 보안측정의 유효기간은 방산업체 및 방산관련 업체는 3년이며, 전장관리정보체계 개발업체 등은 1년으로 규정하고, 보안측정 대상업체 등은 유효기간 도래 3개월 전에 보안측정을 다시 받도록 하고 있다.[29] 이와 같이 보안측정은 방산업체뿐 아니라 방산물자 등의 연구·개발 등에 참여하는 일반 업체나 연구기관 등에 대해서도 일반적으로 요구되는 가장 광범위한 사이버보안 관련 제도로 할 수 있다.

4.1.2.2. 군사기밀보호법 및 방산기술보호법 관련 사이버보안 요건

국가정보원법, 보안업무규정과 군사기밀보호법령 등을 근거로 한 방산보안업무훈령에는 군사기밀과 관련된 정보보호시스템의 운영과 관련된 요건들이 세부적으로 규정되어 있다. 그러나 정작 그 세부적인 내용은 보안을 이유로 외부에 공개되고 있지 않다. 한편 방사청장이 지정·고시한 방산기술을 보호하기 위한 방산기술보호법령과 이에 따른 방산기술보호지침 제5장 정보보호에 규정된 제29조 내지 제32조의3에서 정보보호시스템의 설치 및 운용 등 사이버보안과 관련된 세부적인 내용은 모두 공개되어 있는데 실질적으로 방산보안업무훈령의 해당 요구조건과 매우 유사하다.

세부적으로 보호지침 제29조 제1항에서는 방산업체를 포함한 대상기관의 장은 방산기술을 포함한 관리대상기술과 관련된 전산자료를 정보통신망을 이용하여 처리·관리하는 경우 운영되어야 하는 정보보호시스템으로 방화벽, 침입방지시스템(IPS: Intrusion Prevention System) 또는 통합위협관리장비(UTM: Unified Threat Management)(제1호), 컴퓨터 바이러스 백신 프로그램(제2호), 디지털 저작권 관리(DRM: Digital Rights Management)(제3호), 데이터 유출 방지(DLP: Data Leakage Prevention) 체계(제4호), 네트워크 접근제어·인증 시스템(NAC: Network Access Control)(제5호)을 제시하고 있다.

같은 조 제2항에서는 대상기관의 장은 정보보호시스템 도입·운용 시 IT 보안인증 사무국으로부터 정보보호 제품 평가·인증을 획득한 제품 또는 국가정보원으로부터 보안적합성 검증을 획득한

제품을 선정하고(제1호), 정보보호시스템 관리자를 임명 후 정보보호시스템 설치 및 운용에 대한 내용을 내규에 반영·시행하며, 정보보호시스템 보안정책을 목록화하여야 하고(제2호), 정보보호시스템의 보안정책 변경 이력 유지·관리(제3호)하도록 요구하고 있다. 또한 비인가자 출입통제가 가능하고 보호관리가 용이한 곳에 정보보호시스템을 설치하고, 출입 및 운용·점검 현황을 유지하며(제4호), 정보통신망의 안전한 운용을 위한 목적으로만 정보보호시스템을 사용하고, 설치 목적 외의 사용 및 기능의 임의 변경을 금지(제5호)하고 있다.

위 지침에서는 정보보호시스템 운용시 준수사항으로 방화벽, IPS, UTM, 컴퓨터 바이러스 백신 프로그램, DRM 시스템, DLP, NAC 등의 운용시 세부적인 준수사항을 제시하고 있으며 (제29조 제3항), 정보보호시스템을 관리 운영하는데 있어 변경된 보안정책 이력 및 정보보호시스템 운용시 준수사항에 따라 존안한 로그기록을 2년간 보관하여야 하고(제4항), 정보보호시스템에 대한 취약점 분석·평가를 받기 1회 실시하고, 수시 자체 점검 후 결과를 존안하여야 한다(제5항). 한편, 방위사업청장은 대상기관의 정보보호시스템에 대한 취약점 분석·평가를 실시할 수 있으며, 그 결과에 따라 보완이 필요한 사항에 대하여 대상기관에 적절한 조치를 요구할 수 있는데 이 경우 필요시 국가정보원장과 협의할 수 있다(제6항). 이외에도 정보통신망 관리·운용 시 해킹 등 사이버 위협에 대응하기 위한 외부망 차단체계 구축 운용(제30조), 정보통신기기 및 저장매체의 관리(제31조), 전산자료 반출 관리(제32조), 대상기관장의 업무자료 송·수신 시 방산메일시스템(KDIMS) 운용 사항 등을 세부적으로 규정하고 있다(제32조의3).

4.1.2.3. 통합실태조사

방산 사이버보안을 위한 핵심적인 제도 중 하나로 통합실태조사가 있다(방산기술보호법 제12조). 2020년 이전에는 방위사업청에서 방산기술보호법을 근거로 방위산업기술 보호체계 구축·운영실태를 점검·평가하기 위해 방산업체 실태조사를 실시하였고, 국군방첩사령부(구 기무사령부)는 군사기밀보호법과 방산보안업무훈령을 근거로 방산업체의 비밀관리 실태 등에 대한 보안감사를 각각 별도로 실시하였다.[21] 하지만 이와 같은 실태조사와 보안감사의 중복 시행이 방산업체에 부담을 준다는 의견이 대두되어 2020년부터는 방위사업청이 주관하여 국정원, 방첩사 등 3개 기관이 통합하여 방산기술보호지침 별표 12의 5개 점검분야에 군사보안을 추가한 6개 점검분야에 대해서 통합실태조사를 실시하고 있다(방산기술보호지침 제42조의2 제5항).

실태조사의 대상은 방산기술보호법 제2조 제2호에 규정된 방위산업기술을 보유하거나 방위산업기술과 관련된 연구개발사업을 수행하고 있는 대상기관으로서 국방과학연구소법에 따른 국방과학연구소, 방위사업법에 따른 방위사업청·각군·국방기술품질원·방위산업체 및 전문연구기관, 그 밖에 기업·연구기관·전문기관 및 대학 등을 포함한다(방산기술보호지침 제42조 제1항). 실태조사는 방산기술보호법 제5조에 따른 방산기술보호 시행계획에 포함되어 실시되는 정기 실태조사와 방사청 기술보호국장이 필요하다고 인정할 경우 실시하는 수시 실태조사로 구분한다(제2항). 통합실태조사 항목 중 사이버보안과 관련된 정보보호 분야는 국정원과 방첩사가 합동으로 실시를 하며 아래 표 1과 같이 21개 지표에 대해서 점검을 한다(제5항, 제43조 제1항 별표12).

표 1. 방산기술보호지침 [별표 12] 실태조사 핵심 점검항목 중 4. 정보보호 내용

- UTM(방화벽, IPS 기능 포함) 또는 방화벽, IPS 설치·운영
- 바이러스 백신 프로그램 설치·운영(PC 및 서버 등 숲 전산 장비)
- DRM 설치·운영
- 기술 접속하는 시스템·컴퓨터 등과 외부망 차단(정보보호시스템 또는 물리적 차단)
- 네트워크 접근제어(NAC)를 설치하여 비인가 기기 접속 통제

- 보안관제 시스템 설치·운영
- 사이버 침해사고 등 긴급사태 발생에 대한 관리대상기술자료 백업 및 복구계획 수립
- 지정된 부서에서 정보통신기기 및 저장매체 도입 총괄·관리
- 자료유출방지시스템(DLP) 설치·운영
- 정보보호시스템 보안정책 변경 이력 등 관련 로그 존안
- 정보보호시스템 보안 취약점 분석 및 평가
- 정보통신망에 대한 분기별 취약점 분석·평가
- 관리대상기술 자료별 접근범위 및 권한에 대한 정책 수립
- 기술자료 보관 주 컴퓨터(서버) 접속 기록 생성·유지
- 서버 및 네트워크 운영 및 관리
- 외부 이메일 발송 시 해당 부서장 승인 전송
- PC 및 노트북 외부 반출 시 기술보호 전담부서 중앙통제
- e-mail을 통한 무단자료반출 확인 및 추후조치
- 이동식 저장매체 관리
- PC·노트북 등 자산관리
- 인터넷 PC에서 문서편집 프로그램 등을 활용한 업무자료의 작성 및 저장 금지

통합 실태조사는 현장 방문 또는 서면 조사의 방식으로 실시할 수 있다(제42조의2 제6항). 방위사업청장은 통합실태조사를 실시한 이후 실시결과를 국방부장관에게 보고 후 대상기관 장에게 서면으로 통지하며(제42조의2 제4항), 방위산업기술 보호체계 구축·운영 현황에 대한 부실 여부 등을 판단하고, 필요한 경우에는 방산기술보호법 제13조제2항에 따라 대상기관의 장에게 이행기간을 명시하여 개선을 권고할 수 있다(제43조 제1항, 제2항). 개선권고를 받은 대상기관의 장은 이행기간 만료 후 30일 이내에 개선권고 처리결과를 서면으로 제출해야 한다(제3항). 개선권고를 이행하지 않거나 불성실하게 이행한 경우 대상기관의 장에게 시정을 명할 수 있다(제44조). 이러한 시정명령을 이행하지 않거나 실태조사와 관련된 자료를 미제출하거나 허위로 제출한 경우에는 과태료 부과대상이 될 수 있다(방산기술보호법 제24조 제2호, 제13조 제3항, 제24조 제4호, 제18조 제4호). 한편, 정기 통합 실태조사 결과는 「방위력개선사업 협상에 의한 계약체결기준」의 연구개발사업 제안서의 기술유출방지대책 평가항목에 반영할 수 있도록 하여 실효성을 확보하고 있다(제42조의2 제7항).

4.1.3. 우리와 미국의 방산 사이버보안 법령과 제도 비교·분석

4.1.3.1. 사이버보안 기준과 적용대상에 대한 근거 법령 체계

미국의 방산 사이버보안 법령은 FISMA 2002, FISMA 2014, 사이버보안강화법(PL 113-274) 등 연방법률을 근거로 NIST를 연방기관의 보안가이드 라인과 지침을 개발하는 기관으로 지정하고 사이버위협 대응의 표준을 수립하는 임무를 법제화하였다. 한편, 방산업체 등이 취급하는 정보의 성격을 근거로 국방부의 기밀정보를 취급하게 되는 연방 계약자는 E.O. 13800에 근거하여 NIST SP 800-37 R2와 SP 800-53 R5를 적용한 RMF에 기반한 정보보호지침을 NISPOM 32 CFR §117.18에 따라 정보시스템에 적용하도록 하고 있다. 이러한 요건의 준수는 개별 비밀조달 계약에 참여하기 위한 시설보안허가(Facility Clearance:FCL)의 요건이 된다.

비밀이 아니지만 통제가 필요한 FCI와 CUI의 보호는 2020년 국방수권법(PL 116-92 NDAA Section 1648), E.O. 13556, 48 CFR part 204, 32 CFR part 170, NIST SP 800-171, NIST SP 800-172, DFARS §252.204-7012, 252.204-7021 252.204-7025 등의 규정과 지침을 적용한 CMMC제도를 통해서 이행하고 있다. 그리고 CMMC 제도는 개별적인 미 국방조달사업에 참여하려는 모든 업체에게 적용되는 구체적인 입찰참가의 전제조건이다. 이와 같이 미국의 사이버보

안 관련 법령체계는 연방법령과 대통령 행정명령 등 명시적인 법령상 근거를 가지고 NIST가 제시하는 공개되고 통일된 사이버보안 관련 기준을 통해서 유통되는 정보의 종류에 상응하는 보안요건 준수하도록 하는 데이터 중심의 계층적 사이버보안 제도를 갖추고 이를 해당 정보를 취급하는 국방조달에 참여하는 모든 업체들에게 필수적인 요건으로 요구하고 있다.

한편 우리의 경우에는 방위산업과 관련된 군사기밀과 방산기술보호를 위한 사이버보안기준 및 적용대상이 방위사업법령과 군사기밀보호법령과 이에 따른 하위 행정규정인 방산보안업무훈령과 방산기술보호지침에 규정되어 있다. 먼저 적용대상에 대해서는 방위사업법상 방산업체 등 대상의 성격과 방산기술의 취급여부 등 대상기관이 취급하는 정보를 기준으로 하는 방식을 병행하고 있으며, 각 기관이 취급하는 정보의 성격이 군사기밀과 방산기술에 동시에 해당할 경우에는 각 기준이 중복되어 적용될 여지도 있다. 그러나 적용대상이 준수해야 할 구체적이고 세부적인 국가기밀과 방산기술에 따른 사이버보안 규정은 공개된 법령체계에 의한 국가적으로 일률적인 기준에 의해서 규율되고 있다고 보기는 어렵다. 오히려 방위사업청, 국정원과 국군방첩사령부 등 관련 법령에 의해서 군사기밀 및 방산기술을 보호를 담당하는 국가기관들이 내부적으로 정한 행정규칙에 의해서 실질적인 규율이 이루어지고 있다. 더욱이 그중에 군사비밀을 다루는 방산업체와 관련 기관 등에 적용되는 방산보안업무훈령은 외부에 공개되지 않는 행정규칙에 의해서 대부분의 사이버보안 기준과 제도가 운영되고 있다는 문제가 있다.

4.1.3.2. 제도의 운영 방식

앞에서 살펴본 사이버보안 법령체계의 구조에 따른 차이에 따른 구체적인 제도의 운영상 차이점을 살펴보면 먼저 미 CMMC 제도의 경우에는 FCI나 CUI 등 업체가 연방계약의 체결과 이행과정에서 취급하는 정보의 중요성에 따라 3등급의 사이버보안 기준을 차등 적용하면서 2등급부터는 제3자의 인증을 받는 제도를 도입하였다. 이미 살펴본 바와 같이 2025. 11. 10.부로 미국 방산 시장에 진출하기 위한 CMMC 인증 요건을 갖추 것을 요구하는 조항이 DFARS에 반영되어 2028. 11. 10.까지 3년의 시간을 두고 단계적으로 적용(Phased roll-out)되었다가 현재는 적용 일정이 유예되어 유동적인 상황이다. 하지만 국적과 상관없이 모든 업체는 미국 국방조달 시장에 진출하기 위해서는 위 검토 기간 동안 미국의 CMMC 제도에서 요구하는 인증기준에 따른 인증심사를 받고 이를 SPRS에 등록 후 CMMC 고유번호(Unique Identifier: UID)를 발급받아야만 한다(DFARS §252.204-7021). 각 계약의 성격에 따라 요구되는 CMMC 인증 요건을 충족하지 못한 경우에는, 비록 POA&M 제도를 통해서 예외적으로 소정의 유예기간을 부여하기는 하지만, 연방조달규정 및 국방부조달규정을 통해서 국방조달 계약 참가자격 자체를 박탈하는 방식으로 제도적 실효성을 확보하고 있다.

한편, 우리의 방위사업법령과 방산보안업무훈령에 따른 보안측정의 경우 방산업체로 지정을 받으려는 경우이거나 기타 비밀관련 사업에 참여하려는 기관을 대상으로 하며, 방첩사가 해당 업무를 전담하고 있다. 그리고 그 준수여부는 통합실태조사 과정에서 점검을 받는다. 또한 방산기술을 보유한 업체 등을 대상으로 요구되는 방위산업기술보호법령에 따른 방위산업기술 보호와 관련된 요건 준수여부도 방위사업청과 국정원, 방첩사 등이 통합으로 실시하는 정기 또는 수시 실태조사를 통해서 정기적 또는 부정기적인 점검을 하고 있다. 따라서 보안측정과 실태조사 모두 CMMC와 같은 제3자 인증제도와는 차이가 있다.

방위사업 계약 참여와 관련하여 보안측정의 경우에는 75점의 기준을 통과하는 경우에는 보안요건을 충족한 것으로 보고 있어 일부 조건이 미흡한 경우라도 계약자로서 자격에는 문제가 없다. 또한 통합실태조사 등을 통한 점검 결과 방산기술보호 등과 관련된 요건에 미흡요소가 있을 경우 이를 시정하도록 하고 이를 시정하지 않는 경우 과태료를 부과하거나 혹은 방위력 개선사업 입찰절

차에서 제안서 평가시 가점이나 감점을 부여하는 방식을 취하고 있어 조달계약 참가의 필수 요건으로 규정하지 않고 있다. 특히 각 방산업체나 대상기관이 취급하는 정보의 중요도와 무관하게 동일한 보안측정이나 실태조사 기준을 적용하고 있어 계약이행 과정에서 상대적으로 중요도가 떨어지는 정보를 취급하는 일부 중소기업 등에게는 과도한 부담으로 작용할 수 있다. 한편 보안측정과 실태조사에 적용되는 점검항목과 CMMC 2단계 인증심사 기준인 NIST SP 800-171의 110개의 이행과제를 비교해 보면 28개의 CMMC 2단계 인증심사 이행과제가 포함되지 않은 것으로 확인되었다.[30]

4.1.3.3. 운영기관

미국의 CMMC 제도는 미 국방부 최고정보책임자(CIO)가 운영을 총괄하며 CMMC 프로그램 관리사무소(CMMC PMO)가 세부적인 정책적 운영을 책임지고 있다. 또한 국방부의 DCMA DIBCAC가 Cyber AB나 C3PAO에 대한 2등급 인증 심사 및 3등급 인증 심사를 담당하고 있으나, 계약자에 대한 2등급 인증심사는 Cyber AB나 C3PAO 중심의 민간 생태계를 이용한 인증체계를 운영하고 있다. 이러한 정보의 중요도에 따른 인증심사의 수준은 각 조달계약을 담당하는 계약담당자(CO)가 사업별 특성을 고려하여 결정하여 입찰공고에 명시하도록 하고 있다. 한편 CMMC 인증제도의 핵심 기능을 민간 생태계 기관이 담당하도록 하면서 Cyber AB는 IAAC, ILAC의 상호인정협정(MRA)의 서명 당사자로서, ISO/IEC 17020:2012(E)와 ISO/IEC 17011:2017(E) 등 국제적인 인증 기준을 충족하여야 하고, C3PAO도 ISO/IEC 17020:2012(E)의 인증요건을 충족할 것을 요구하여 국제적인 기준에 따른 인증심사 기관 자격을 요구하고 있다.

반면 우리의 경우에는 보안측정이나 실태조사를 모두 방사청, 국정원, 기품원, 방첩사 등 국가기관이 담당하고 있다. 보안측정의 경우에는 산업통상부의 방산업체 지정 등 방위산업에 참여하기 위한 자격요건의 일부를 구성하는 기능을 가지고 있으나 국제적인 인증 기준 등을 고려한 인증체제로서의 성격은 없다. 또한 방산기술보호법에 따른 사이버보안체계는 관련 법령상 제시된 기준을 준수하는지를 국가기관이 통합실태 조사를 통해 매년 또는 수시로 점검하는 방식으로 민간 생태계가 참여하는 인증체계와는 무관하게 운영되고 있다.

4.1.3.4. 각 제도의 비교·분석 개관

지금까지 비교·분석한 내용을 개관하면 아래 표 2와 같다.

표 2. 미 CMMC 제도와 국내 방산사이버 보안제도 비교

구분	미국	대한민국	비고
근거 법령	FISMA 2002 FISMA 2014 사이버보안강화법(PL 113-274) 2020 PL 116-92 NDAA Section 1648, E.O. 13556 48 CFR 204 32 CFR 170 NIST SP 800-171, NIST SP 800-172, DFARS §252.204-7012, 7021,7025	방위사업법, 방산기술보호법, 군사기밀보호법, 방산보안업무훈령, 방산기술보호지침	미국 비밀정보 취급 계약자는 E.O. 13800, NIST SP 800-37 R2, SP 800-53 R5 NISPOM 32 CFR §117.18에 따라 RMF 정보 보호 시스템에 적용

적용 대상	FCI, CUI를 취급하는 미 국방조달 계약에 참여하려는 모든 업체	방산업체, 비밀사업 참여업체, 방산기술 취급 업체 및 기관 등	- 미 CMMC는 구체적 계약 참여업체별로 해당 인증요건을 준수 확인하는 방식 - 우리는 개별계약과는 무관하고 대상기관의 성격에 따른 기준 준수 여부를 국가기관이 점검
운영 방식	정보의 중요도에 따른 차등 제3자 인증제도(3단계) 1등급 자율인증 2등급 C3PAO 인증 3등급 DIBCAC 인증	보안측정이나 방산기술보호가 요구되는 대상기관의 성격에 따른 일률적인 사이버보안 기준 적용 후 국가기관의 실태조사를 통한 정기 또는 수시 확인·점검	
운영 기관	국가 기관	산업통상부 방위사업청 기품원 국가정보원 국군방첩사령부	- 미 CMMC 제도는 인증, 교육, 컨설팅, 등에서 민간 생태계가 제도운영의 핵심역할을 수행 우리는 국가기관 중심의 제도 운영
	DOD CIO CMMC PMO DCMA DIBCAC NARA NIST		
	민간 영역		
	CYBER AB C3PAO (CCP, CCA): 인증 CCI : 교육 RPO (RP, RPA) : 컨설팅		

4.2. 개선 방안

4.2.1. 방산 사이버보안 법령체계 개선의 기본 방향

미국 방산 사이버보안 법령체계는 연방법률과 규정을 근거로 CMMC 제도를 도입하여 제도를 운영하는 민간생태계를 포함한 각 기관의 임무와 역할을 명시하고, 방산공급망에 참여하는 업체가 준수해야 할 사이버보안 기준 등이 연방기관에 적용되는 통일적이고 공개된 NIST 기준을 적용하도록 하고 있다. 이러한 미국의 법령체계는 사이버보안 법제도 정비의 방향에 있어서 법령상 명확한 근거를 가지고 관계부처와 기관 역할을 구분하고, 주도기관이 필요한 역량과 권한을 부여해야 하며, 다방면의 사이버 위협 정보탐지와 공유를 활성화하기 위한 정보공유 체계 정립 및 활성화, 그리고 사이버보안 관련 산업 육성과 인력양성이 보장되도록 해야 한다는 견해와 부합한다.[31]

이미 살펴본 바와 같이 CMMC 제도의 사이버보안 기준인 NIST SP 800-171, SP 800-172 등은 시스템에 유통되는 정보의 중요도를 기준으로 모든 연방 시스템에 일률적으로 적용되는 공개된 연방규정의 성격을 가진다. 미 국방부는 이와 같이 공개된 국가 공통기준을 국방공급망에 참여하는 업체에게 동일하게 준수하도록 하여 명확한 방산업체들의 추가적인 부담을 최소화하고 있다. 따라서 현행 방산 사이버보안 법령체계의 개선 방향도 명확한 법령 상 근거를 가지고 제도를 운영할 기관과 역할을 정립하고, 방산업체 등에 요구될 사이버보안 기준 등도 유통되는 정보의 중요도를 따라 단계적인 요건을 차등 적용하도록 법령상 명시하는 방안을 적극 고려할 필요가 있다.[29]

현행 법령상 군사기밀을 포함하여 방위사업 추진 과정에 유통되는 정보는 방위사업법령, 군사기밀보호법령 그리고 방산기술보호법령 체계에 따른 분류기준을 적용하여 개별적인 보호수준을 요구하고 있다. 새로운 방산 사이버보안 법령체계는 먼저 이러한 법령별로 상이한 분류 기준 및 보호 기준을 위협관리에 기반한 데이터의 중요도를 기준으로 하는 새로운 정보분류 체계를 도입하는 방안을 고려할 수 있다. 방위사업 추진 과정에서 방산업체가 다루게 되는 군사기밀과 방위산업기술 관련 정보 등을 중요도에 따라 하나의 포괄적인 데이터 분류 및 위협관리에 기반한 데이터 중심의 새로운 정보분류체계로 개선하는 것이다. 그리고 이러한 분류체계에 따른 단계별 보호수준과 보안 기준을 적용한 인증체계의 도입, 그리고 인증체계를 운영하는 책임기관과 필요한 경우 민간 생태계 조성 등을 규정하는 가칭 한국형 사이버보안 인증심사제도(K-CMMC)가 근거 법령에 따라 운영될 수 있도록 기본법률을 제정하고 이를 구체화하는 대통령령, 각부처 시행규칙 등의 체계로 법

제화하는 방안이 고려될 수 있을 것이다.

4.2.2. 개정 법령상 K-CMMC 제도의 구체적 내용

이하에서는 개정 사이버보안 법령체계를 통해 한국형 사이버보안인증심사제도(K-CMMC)를 구현하기 위해서 포함되어야 할 구체적인 내용을 미국 CMMC 제도와 현행 법령상 사이버보안 제도를 비교한 기준에 따라 적용대상, 운영방식, 운영기관의 측면에서 살펴보고자 한다. 먼저 K-CMMC 제도의 적용대상은 방산공급망을 구성하는 모든 업체들을 대상으로 하여야 한다. 방산 공급망은 방산업체로 지정된 체계업체로부터 단순 부품이나 구성품을 제공하는 방산업체가 아닌 중소협력 업체 등에 이르기까지 취급하는 정보에 대한 보호의 필요성이 상이한 다양한 업체들로 구성된다. 미 CMMC 제도가 사이버침해의 주된 공격 대상이 되는 협력업체들을 효과적으로 보호할 수 있도록 방산 공급망을 구성하는 업체들을 모두 적용대상으로 한다. 따라서 K-CMMC의 적용대상 역시 방산공급망에 포함되어 방산정보를 취급하는 업체라면 현행법상 보안측정의 대상이 되는 방산업체인지와 무관하게 취급하는 정보의 중요도를 고려하여 이에 상응하는 사이버보안 기준 충족하도록 관련 법령에 규정하여야 할 것이다.[32]

한편, K-CMMC 제도의 운영방식은 정보의 중요도를 고려하여 기준 충족여부를 스스로 평가하거나 혹은 중요한 방산정보를 취급 시에 사이버보안 성숙도를 제3자를 통해서 인증을 받도록 요구하는 방식, 아니면 현행 제도와 같이 국가기관이 일정한 주기로 정기 또는 수시 점검을 하는 방식을 고려해 볼 수 있다. 국내에서 사이버보안에 인증방식을 채용한 제도로는 개인정보에 대한 사이버보안을 위한 정보보호 관리체계(Information Security Management, ISMS) 인증 제도를 들 수 있다.[33] ISMS 인증은 제3자 인증을 통해 정보보호 관리체계를 실질적으로 구축할 수 있으며, 정부 중심의 안전진단과 달리 심사기관의 독립성을 기반으로 현장의 보안 운영 환경을 실질적으로 평가할 수 있고, 인증취득 대상자와 정보보호 산업군에 대한 투자를 촉진시키는 것으로 분석되었다.[34] 하지만 ISMS 제도에 대해서는 인증을 위한 최소한의 보안요구만 충족시키고 개선 필요성이나 지속적인 정보보호 수준 향상을 위한 동기를 부여하지 못하는 문제점이 있어 이를 성숙도 평가모델에 기반한 인증제도로 개선할 필요성이 제기되고 있다.[34]

따라서 K-CMMC의 운영방식은 요구되는 사이버보안 요건의 충족여부를 실질적으로 확인할 수 있도록 취급정보의 중요도에 따른 단계별 제3자 인증방식을 도입하는 것이 바람직할 것으로 판단된다. 이러한 결론은 이후에 살펴볼 미 CMMC 제도와 상호인정 내지 호환성을 고려할 때도 더욱 타당성을 가진다고 볼 수 있다. 한편 새로 정립될 사이버보안 인증기준은 기존에 시행하던 보안측정과 실태조사에서 활용되었던 평가요소 중 CMMC 이행지표와 호환가능한 내용들은 최대한 그대로 적용되도록 하여 인증대상 방산업체들의 부담을 최소화하도록 하는 방안을 적극 고려해야 한다.

다음으로 K-CMMC를 운영하는 기관 즉 제도가 운영되는 생태계를 어떻게 설계할 것인가의 문제가 있다. 현행 방산 사이버보안 요건 준수 여부는 방위사업청, 국정원 그리고 방첩사령부 등 국가기관이 보안측정과 실태조사를 통해서 점검하는 방식을 취하고 있다. 이러한 방식은 Cyber AB나 C3PAO 등 민간 생태계를 통해서 제도의 핵심인 CMMC 2등급 인증심사를 받도록 하는 CMMC 제도와는 큰 차이점이 있다. 그런데 미국이 사이버보안 제도의 핵심 영역을 민간생태계에 의존하는 것은 미 방산공급망에 참여하는 업체의 수가 20만 개 이상으로 국가기관이 모든 업체에 대해서 인증제도를 운영하는 것은 비효율적이라는 판단과 방대한 방산공급망의 규모를 고려시 민간생태계 운영 비용 부담 능력이 있다는 판단과 연관이 있다.[35] 반면 우리나라의 방산업체는 주요 방산업체가 67개, 일반방산업체가 17개로 총 84개가 지정되어 있다.[36] 그리고 이러한 방산

업체와 함께 방산공급망을 구성하는 협력업체의 수를 모두 합치더라도 미국의 방산공급망 참여업체 보다는 규모가 크지 않을 것이다. 또한 매년 실시되는 정기 통합실태조사의 대상을 살펴보면 2022년 기준으로 방산업체, 국과연, 기품원 등 정부출연기관의 국내외 사무소를 포함하여 160여 개의 사업장이 그 대상이 된 것으로 파악된다.[21]

결국 국내 사이버보안 법령체계의 운영방식으로 제3자 인증방식을 채용한다고 하더라도 미 CMMC 제도와 같이 거대한 민간 생태계가 필요할 것인가에 대해서는 신중한 접근이 요구된다고 볼 여지가 크다. 오히려 K-CMMC 제도의 적용 대상기관의 숫자나 중소기업 등의 민간생태계 운용에 따른 비용 부담 능력이 있는가 등을 고려할 때 인증 과정에서 업체에 개별적인 컨설팅이나 인증심사 비용 부담을 요구하는 민간 생태계의 역할을 확대하기보다는 국가기관인 방사청이나 기품원의 역할 확대가 바람직하고 효율적인 방안이 될 수 있다. 즉 취급하는 정보의 중요도를 고려하여 현행 실태조사의 대상 기관들에 대해서는 기품원의 방산기술보호센터를 국제적 인증기관 기준에 부합하는 인증기구로 개편하여 CMMC 2등급 또는 3등급 인증 제도와 호환 가능한 수준의 사이버보안 인증 제도와 컨설팅 서비스를 제공하고, 중소기업들의 경우에는 CMMC 1등급 혹은 2등급 자율심사에 상응하는 완화된 사이버보안 기준을 단계적으로 제정하여 이를 적용하거나 또는 국가예산지원을 통해서 민간 생태계를 통한 저비용의 컨설팅이나 자율심사 확인을 받도록 하는 2트랙 접근 방안도 고려해 볼 수 있다.

4.2.3. 미 CMMC 제도와 상호인증 등 추진을 위한 고려 사항

국가 사이버보안 거버넌스의 차원에서 주요기능은 국가 사이버보안 거버넌스의 정책을 수립·조정하는 기관의 확립과 공공영역과 민간영역 그리고 산업부분의 사이버 보안 역량을 동시에 강화하기 위해 국경선의 의미가 제한적인 사이버 공간에서 국제협력을 강화가 요구된다.[37] 따라서 미국과의 사이버보안 인증제도의 상호인증을 추진하여 국제협력을 강화하는 것은 국내 방산 사이버보안 제도를 고도화하는 한편, 국내 업체들의 미 방산시장 진출 부담을 최소화하기 위해 필요하다고 볼 수 있다.

또한 이미 살펴본 바와 같이 2025. 11. 10.부로 미국 방산 시장에 진출하기 위한 CMMC 인증요건을 갖추 것을 요구하는 조항이 DFARS에 반영되어 2028. 11. 10.까지 3년의 시간을 두고 단계적으로 적용(Phased roll-out)을 시작했으나 현재 잠정 유예 중이다. 따라서 미국 국방조달 시장에 국내 방산업체가 원활하게 진출하기 위해서는 현재 2단계 시행이 일부 유예되기는 하였으나 여전히 위 3년에 추가 유예된 검토 기간 동안 미국의 CMMC 제도에서 요구하는 인증기준에 따른 인증심사를 받아야 하는 상황에는 변화가 없다. 그런데 이와 같이 미 CMMC 제도의 인증절차를 추진하는 과정에서 미국의 인증 인력이 3년의 유효기간마다 주기적으로 우리 방산업체의 사이버보안 상태를 점검하고 심사하면서 우리의 방산 시스템을 모두 들여다 볼 수밖에 없어 방위산업 사이버안보의 주권 문제가 대두될 수 있다.[29] 이러한 문제점을 미연에 방지하기 위해서는 우리가 미 CMMC제도와 어느 정도 호환성을 겸비한 K-CMMC를 법제도적으로 정립하고 미국과 상호인정협정(Mutual Recognition Arrangement, MRA)을 체결하려는 노력이 요구된다. 미 CMMC 제도와 상호인증을 위한 요건과 관련해서는 미국의 외국인 투자심사위원회(Committee on Foreign Investment in the United States, CFIUS)의 외국인투자심사 과정에 적용되는 면제국가(Excepted foreign States) 제도를 참고할 필요가 있다.

31 CFR §800.219에 따른 면제국가 제도는 외국인투자심사를 면제받기 위한 전제조건으로 해당 국가에 외국인투자심사의 근거규정이 있는지 여부, 방위산업기술, 핵심시설 등 분야에 대한 투자심사여부, 국가안보를 위협하는 외국인 투자라고 판단된 경우 조건을 부과하거나 투자철회 등

권한 보유 여부, 외국인 투자의 최종수익자, 국가안보 위협 등에 대한 정보를 취득한 법령상 권한 여부, 민감정보의 보호 및 모니터링 정도, 미신고 투자의 모니터링 정도, 미국과의 관련 정보 공유에 관한 법령상 권한 여부 등 미국의 외국인투자심사제도를 구성하는 핵심요소를 포함하고 있을 것을 요구한다.[38] 결국 미국의 외국인 투자심사와 유사한 제도를 운영하면서 미국과의 공조가 가능한 법령체계를 갖춘 경우 면제국가 자격을 인정하는 것이다. 따라서 미 CMMC 제도와 상호인증을 원활하게 추진하기 위해서는 미 제도의 핵심 요소를 포함하고 미국제도와 공조 및 호환성을 갖춘 K-CMMC 제도의 운영이 가능하도록 관련 법제를 개선할 필요성이 있다고 볼 수 있다.

구체적인 개선 소요를 살펴보면 먼저 인증심사의 기준과 관련하여 법령상 취급 정보의 중요도를 기준으로 한 데이터 중심의 단계적 인증기준을 설정할 필요가 있다. 그리고 인증제도를 운영할 인증기관으로 현재 방사청과 기품원을 중심으로 방산기술보호센터를 확대 개편하여 방위산업 사이버보안 인증기구를 신설하는 방안을 추진 중에 있는데 이러한 기구는 기본적으로 미 CMMC가 요구하는 국제적인 인증기관으로서의 기준도 충족시킬 수 있도록 해야 할 것이다. 또한 미국과의 사이버보안과 관련 정보 공유 및 공조가 가능한 법령상 근거도 마련해야 할 것이다. 그런데 이러한 국내 사이버보안 법령체계의 제도적인 변화와 미 CMMC 제도와 상호인정협정 체결 등의 절차는 미국의 CMMC 제도가 현재 진행 중인 재검토 결과로 일부 연장될 여지는 있으나 결과적으로 확정된 완전 이행 시점 이전에 이루어져야 하는 시간적 제약이 현재까지는 여전히 유효하다. 그렇다면 상호인정협정 체결이 주어진 시간 내에 불가할 것에 대비하여 기품원 기술보호센터가 미국의 CMMC 제도하에서 적어도 Cyber AB의 역할 또는 C3PAO의 역할을 수행하여 미국의 Level2(C3PAO) 인증 심사가 가능한 민간 인증기구로서 자격을 인정받을 수 있도록 DCMA DIBCAC와 협력을 추진하는 실효적인 접근도 적극적으로 검토할 수 있을 것이다.

그리고 K-CMMC 민간생태계는 기품원 중심으로 미 CAICO의 역할을 수행하여 인증평가를 담당하는 CCA, CCP, 교육을 담당하는 CCI, 컨설팅을 담당하는 RP를 교육하고 자격증을 부여할 수 있는 권한을 부여하되 이러한 자격증이 미국의 CMMC제도와 상호 호환될 수 있도록 DCMA DIBCAC와 Cyber AB와 긴밀하게 협조를 하는 방안도 고려해 볼 수 있다. 한편 대학 등 교육 및 연구기관에 대해서 일정한 자격을 보유한 인원들에 대해서는 K-CMMC 컨설팅 및 교육을 진행할 수 있도록 하고 방산분야 중소기업에 대해서는 국가가 관련 비용을 보조하여 대학 등을 통한 컨설팅 서비스를 받을 수 있도록 지원하여 새로운 제도운영에 따른 부담을 최소화하도록 동시에 연구가 진행되는 것도 바람직할 것이다.

4.2.4. 과도기적 조치

지금까지 언급한 K-CMMC 제도를 운영하기 위한 법령체계와 실제적인 운영 기구 등이 완비되기까지는 일정한 시간이 필요하다. 미 CMMC제도도 2020년 국방수권법에서 최초로 제도의 시행을 요구한 이후 완전한 제도 시행까지는 5년의 기간동안 다양한 의견수렴과 관련 규정의 변화를 거쳐야 했다. 또한 기존에 2026. 11. 10.부터 미국 국방조달 시장 진출을 위해서는 Level 2(C3PAO) 인증을 요구하던 기존의 시행계획이 현재는 순연되기는 하였지만 CMMC 2등급 자체 인증은 여전히 국방 조달계약 참여조건으로 제시되고 있으며 오히려 확대될 가능성도 대두된다.[28] 따라서 미 CMMC의 완전시행 이전에 상호인정이나 국내에 C3PAO 인증을 수행할 수 있는 자격을 갖춘 기관이 설립되지 못할 가능성은 존재한다는 법제도적 한계가 있을 수 있다. 따라서 국내 제도의 개선이 이루어지기 이전이라도 미 CMMC 인증을 원하는 업체들에 대해서는 특히 실질적인 거래를 통한 수익에 비해서 CMMC 인증 추진을 위한 비용이 과도할 수 있는 중소 협력업체들에 대해서는 2단계 자체인증 심사단계까지 국가기관의 적극적인 지원이 제공될 필요가 있다. 다행히 방위산업진흥회에서는 지난 2025. 11. 14. 48 CFR Part 204 최종안 발표와 함께 CMMC

동향 설명회를 개최하였다. 또한 방위사업청 기술보호과와 함께 2026년 CMMC Level 1 컨설팅과 Level 2 컨설팅 희망업체 수료를 파악한 이후 CMMC Level 1 컨설팅은 통합실태조사와 연계하여 수행하며, Level 2에 대해서는 별도 컨설팅을 실시할 예정에 있다. 방사청과 방진회의 이러한 적극적인 움직임은 매우 바람직한 것이라고 할 수 있다.

5. 결론

미 CMMC 제도는 방산 공급망 전체의 사이버보안 역량을 체계적으로 관리하기 위해 취급하는 정보의 중요도에 따라 단계적인 인증 요건을 갖출 것을 미국의 모든 국방조달사업 참여의 전제조건으로 만든 전략적 제도라는 점을 고려할 때 우리의 방산 사이버 보안체계에서는 방산업체 및 일정한 보안 요건이 요구되는 사업에 참여하기 위한 보안측정과 통합실태조사 등의 비교적 충실한 법령상 제도와 인프라를 보유하고 있으나 방산 분야에 특화된 취급되는 정보중심의 정보보호 체계에는 미흡한 부분이 있다. 또한 정보의 중요도를 중심으로 한 사이버보안 인증체계와 국제적 기준에 부합하는 인증기관 등을 규정하는 법령체계가 부재한 것은 미국의 CMMC를 중심으로 한 사이버보안 법령체계와 상이하여 미 방산시장 참여를 위한 상호인정협정(MRA)을 체결하는 것을 비롯해서 국제적인 협력에 한계를 가지고 있다.

따라서 보다 혁신적인 방산 사이버보안 체계 구축을 위한 현행 법령체계에 대한 근본적인 변화를 위해서 보호가 필요한 취급정보에 대한 분류체계를 정립하고 이러한 정보의 중요도에 따른 통일된 국가 사이버보안 기준을 방산기술보호법령 등 개정을 통해 제시하여야 한다. 이러한 기준은 기본적으로 국제적인 인증기준과 미국의 CMMC 제도와 상호 운영이 가능한 방식으로 설정되어야 할 것이다. 방산 사이버 보안 체계를 개선하는 법령에는 이를 담당하는 기관은 방사청과 기품원의 방산기술보호센터를 적극 활용하여 그 조직을 확대·개편하는 방향으로 접근하는 것이 효율적이고 민간 생태계를 구성하는 방식에 반드시 수반되는 방산업체들의 별도의 비용을 발생시키지 않도록 하여 현재 방산업체들 특히 중소 협력업체들의 부담을 최소화하는 것이다.

이를 위해 현행 방산 사이버보안 관련 법령체계를 개정하여 K-CMMC 제도 구축을 추진하면서 기존의 보안측정 제도와 통합실태조사를 통해서 축적된 사이버 보안과 관련된 각종 요구사항들을 최대한 활용하여 새로운 인증제도의 도입에 따른 방산업체 등의 부담을 최소화하면서 결과적으로는 국제적인 표준(ISO/IEC 17011, 17020 등)과 미국의 NIST SP 800-171등의 기준도 고려하여 향후 미국과의 상호인정협정이 가능하도록 제도를 구상할 필요가 있다. 그리고 이러한 제도의 운영을 위해서는 미국과 비교시 인증이 필요한 기관의 수가 한정된 우리의 상황을 고려할 때 기존의 보안측정이나 통합실태조사의 대상이었던 업체와 기관에 대해서는 국가기관인 방위사업청과 기품원의 방위산업기술보호센터 등의 기능을 확대하여 인증기관을 운영하면서 기존의 보안측정과 통합실태조사를 모두 면제하거나 상당 부분 해소해 주는 것이 바람직할 것으로 보인다.

그동안 방위사업청, 국정원, 방첩사령부 등 국가가 주도하여 사이버 보안과 관련된 보안측정과 통합실태조사를 운영해 왔던 경험과 역량을 최대한 발휘하여 궁극적으로는 미국의 CMMC 제도와 상호 호환이 가능한 한국형 CMMC 제도를 확립하는 것을 목표로 법령의 개정과 각종 정보시스템의 구축 등을 위한 지속적인 노력이 필요하다는 것은 자명하다. 그런데 이러한 노력은 미국의 국방조달 시장에 진입하기 위한 CMMC 인증 요건이 완전하게 적용되기 시작하는 2028. 11. 10. 이전에 그 결과를 볼 수 있도록 타임라인을 설계하여 추진되어야 실효적인 혜택을 국내 방산업체 및 협력업체들이 누릴 수 있을 것이라는 점을 주목해야 한다.

이러한 측면에서 보면 위와 같은 시간적 제약 속에서 미 CMMC 제도와와의 상호인정까지 달성할 수 있는 법령체계의 개선이 이루어지기는 매우 어려울 수 있다. 따라서 장기적으로는 K-CMMC

제도를 통해 미국과의 상호인정을 추진하되 단기적으로는 미 CMMC 제도상 2단계 인증에 주도적 역할을 수행하는 민간기구인 Cyber AB나 C3PAO의 기능을 수행할 수 있는 자격을 기품원 방산기술보호센터가 부여받는 방안에 대해서도 실효적인 접근이 이루어져야 한다. 그리고 방산기술보호센터를 중심으로 대학 및 연구기관 등을 통해 K-CMMC의 민간생태계를 구축하여 간이한 수준의 인증 및 교육·컨설팅 제도를 확립하여 중소 협력업체들에 대한 사이버보안 인증 지원 등이 이루어질 수 있도록 하는 2트랙 접근방식도 고려해 볼 수 있을 것이다.

참고문헌

- [1] Abernathy C. Law in the United States (American Casebook Series). West Academic Publishing. 2006.
- [2] Farnsworth E, Sheppard S. An Introduction to the Legal System of the United States (4th ed.). Oxford University Press. 2010.
- [3] 윤강욱. 미국 대통령 행정명령의 구조와 효력에 관한 연구. 행정법연구, 제54호, pp. 45-66. 2018. <https://doi.org/10.35979/ALJ.2018.08.54.45>
- [4] 조재현. 미국 대통령의 행정명령에 관한 연구: 행정명령이 대통령의 입법권한 행사에 미치는 시사점을 중심으로. 동아법학, 제94호, pp. 33-60. 2022. <https://doi.org/10.31839/DALR.2022.02.94.33>
- [5] 양정운. 미국 대통령의 행정명령에 대한 소고. 고려법학, 제84호, pp. 111-145. 2017. <https://doi.org/10.36532/kulri.2017.84.111>
- [6] Congressional Research Service. From Slip Law to United States Code: A Guide to Federal Statutes for Congressional Staff (CRS Report No. R45190). 2018.
- [7] GovInfo. United States Code. <https://www.govinfo.gov/app/collection/uscode> (검색일 2026. 7. 22).
- [8] Office of the Law Revision Counsel. United States Code. <http://uscode.house.gov> (검색일 2026. 7. 22).
- [9] Congressional Research Service. Executive Orders: An Introduction (CRS Report No. R46738). 2021.
- [10] Office of the Federal Register. Donald J. Trump Executive Orders. <https://www.federalregister.gov/presidential-documents/executive-orders/donald-j-trump-2025> (검색일 2026. 7. 22).
- [11] National Latino Media Coalition v. FCC, 816 F.2d 785 (D.C. Cir. 1987).
- [12] Congressional Research Service. An Overview of Federal Regulations and the Rulemaking Process (CRS Report No. IF10003). 2021.
- [13] 홍순좌. 미국의 사이버보안 역량 강화를 위한 연방법률 발전 현황 분석. 정보보호학회지, 제29권 제3호, pp. 51-65. 2019.
- [14] National Institute of Standards and Technology. Risk Management Framework for Information Systems and Organizations (NIST SP 800-37 Rev. 2). 2018. <https://doi.org/10.6028/NIST.SP.800-37r2>
- [15] National Institute of Standards and Technology. Security and Privacy Controls for Information Systems and Organizations (NIST SP 800-53 Rev. 5). 2020. <https://doi.org/10.6028/NIST.SP.800-53r5>
- [16] Executive Office of the President. Executive Order 13556: Controlled Unclassified Information. 2010.
- [17] National Archives. CUI Registry: Category List. <https://www.archives.gov/cui/registry/category-list> (검색일 2025. 11. 3).
- [18] National Institute of Standards and Technology. Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations (NIST SP 800-171 Rev. 3). 2024. <https://doi.org/10.6028/NIST.SP.800-171r3>

- [19] Office of Information and Regulatory Affairs. RIN 0790-AM01. <https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202510&RIN=0790-AM01> (검색일 2026. 7. 22).
- [20] National Institute of Standards and Technology. Enhanced Security Requirements for Protecting Controlled Unclassified Information (NIST SP 800-172). 2021. <https://doi.org/10.6028/NIST.SP.800-172>
- [21] 김동선, 류연승. 미국 CMMC 제도 대응을 위한 통합실태조사 제도 개선 연구. 한국방위산업학회지, 제29권 제3호, pp. 51-61. 2022. <https://doi.org/10.52798/KADIS.2022.29.3.4>
- [22] Cyber AB. Assessing and Certification. <https://cyberab.org/CMMC-Ecosystem/Ecosystem-Roles/Assessing-and-Certification> (검색일 2025. 11. 16).
- [23] Cyber AB. Consulting and Implementation. <https://cyberab.org/CMMC-Ecosystem/Ecosystem-Roles/Consulting-and-Implementation> (검색일 2025. 11. 16).
- [24] Cyber AB. Explore Our Marketplace. <https://cyberab.org/Catalog> (검색일 2025. 11. 16).
- [25] Department of Defense. Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041). 90 Fed. Reg. 43560-43577. 2025.
- [26] SAM.gov. Special Notice W912HV-26-Z-0001. <https://sam.gov/workspace/contract/opp/3fcd1106512442f99cc3d90d3a9c0be/view> (검색일 2025. 11. 16).
- [27] DoD CIO. Removing Barriers to Defense Industrial Base Expansion (Memorandum). 2026. <https://dodcio.defense.gov/Portals/0/Documents/Library/ImplementingSuspensionCMMC-PhaseII.pdf> (검색일 2026. 7. 24).
- [28] 뉴스투데이. [방산기술보호] 미 국방부, CMMC 2단계 적용 전격 유예...미 방산시장 진출 준비 기업 숨통 트였다. <https://www.news2day.co.kr/article/20260714500275> (검색일 2026. 7. 14).
- [29] 류연승 등. 방산안보학 개론. 박영사. 2024.
- [30] 방위사업청. 방산기술보호 성숙도 모델 인증제도 추진방안 연구. 2022.
- [31] 박상돈, 김소정. 사이버안보법 제정을 위한 국내 사이버안보 법률안 연구. 융합보안논문지, 제13권 제6호, pp. 91-98. 2013.
- [32] 한주희. 방위산업 협력업체 보안 통제모델 연구. 명지대학교 대학원, 박사학위논문. 2025.
- [33] 개인정보보호위원회. 정보보호 및 개인정보보호 관리체계(ISMS-P) 인증기준 안내서. 2023.
- [34] 이진용 등. 성숙도 평가모델에 기반한 정보보호 관리체계 인증에 관한 연구. 한국정보처리학회 ACK 2023 학술발표대회 논문집, pp. 165-167. 2023.
- [35] Government Accountability Office. Defense Industrial Base: Actions Needed to Address Risks Posed by Dependence on Foreign Suppliers (GAO-25-107283). 2025.
- [36] 한국방위산업진흥회. 방산업체 현황. https://www.kdia.or.kr/kdia/module/information_defense_defenseContractor.do (검색일 2025. 11. 18).
- [37] 주문호 등. 주요국 사이버보안 거버넌스 분석과 정책적 시사점. 정보보호학회논문지, 제28권 제5호, pp. 1259-1277. 2018. <https://doi.org/10.13089/JKIISC.2018.28.5.1259>
- [38] 정세정. 외국인투자심사에 관한 국제법적 고찰: 국가안보 예외 법리의 적용과 대안을 중심으로. 국제법학회논총, 제68권 제3호, pp. 255-298. 2023.