

변화하는 SBOM 규제와 트렌드

LG전자 차세대컴퓨팅(연) SW Security Governance팀
오혜진 책임

목차

규제 동향

1. SBOM 개요와 필요성
2. 글로벌 규제와 가이드
3. 미국 동향
4. EU 동향
5. 기타 국가 동향

기술 트렌드와 대응

6. SBOM과 VEX
7. 한계점
8. SBOM의 확장
9. 제조사의 대응 과제

1. SBOM의 개요와 필요성

■ SBOM의 정의

- SBOM (Software Bill of Materials)은 소프트웨어의 '재료 목록'
- 소프트웨어를 이루는 구성요소를 기록



식품유형 과 재음료	
소비기한	용기상단 또는 뚜껑 표기일까지
제조원	우일음료(주)F8:경상북도 예천군 예천읍 농공단지길 9, 톨립인터내셔널(주) F12:경상북도 예천군 보문면 산단길 13-3
유통전문판매원	롯데칠성음료(주) 서울특별시 서초구 서초대로 70길 15
품목보고번호	F8:19960571018664, F12:20190575042105
원재료명	정제수, 오렌지농축액(오렌지와즙 80%, 스페인산), 구연산, 천연향료(오렌지향 2종), 비타민C, 글루콘산아연, 스테비올배당체
<p>*우유, 메밀, 견과, 대두, 콩, 곡물, 아, 도마도, 아황산류, 호두, 잣을 사용한 제품과 같은 시설에서 제조하고 있습니다. *직사광선을 피해 서늘한 곳에 얼지 않게 보관하시고, 개봉 후 냉장 보관하여 빨리 드십시오. *용기의 변형, 팽창, 손상 및 내용을 변질 시 음용하지 마십시오. *소비자 분쟁해결기준(공정위고시)에 의거 교환 또는 보상을 받을 수 있습니다. *교환: 롯데칠성음료(주) 소비자상담팀 (☎수신자부담080-730-1472) 및 구입처·부정·불량식품 신고: 국번없이 1399</p> <p>리활·재도 포장·PP</p>	
<p>DEL MONTE 및 는 델몬트 푸즈의 등록 상표입니다. (Under License from Del Monte Foods, Inc.)</p>	

제품 = 소프트웨어

성분표(원재료명) = SBOM

1. SBOM의 개요와 필요성

■ SBOM의 필요성

- 사상 최악의 오픈소스 보안 취약점 Log4j (CVE-2021-44228)
 - 수만개 이상의 소프트웨어 및 IT 서비스에서 활용되어 심각한 이슈로 부각됨
 - 원인 : JNDI Lookup method를 호출할 때 로그에 기록되는 특정 문자열을 검증 없이 신뢰함 → 원격 코드 실행 취약점(RCE) 유발
 - SBOM을 보유한 기업은 기업 내 DB를 통해 해당 컴포넌트 포함 여부 및 취약 버전 식별하여 긴급 패치 적용/대응 가능하였음



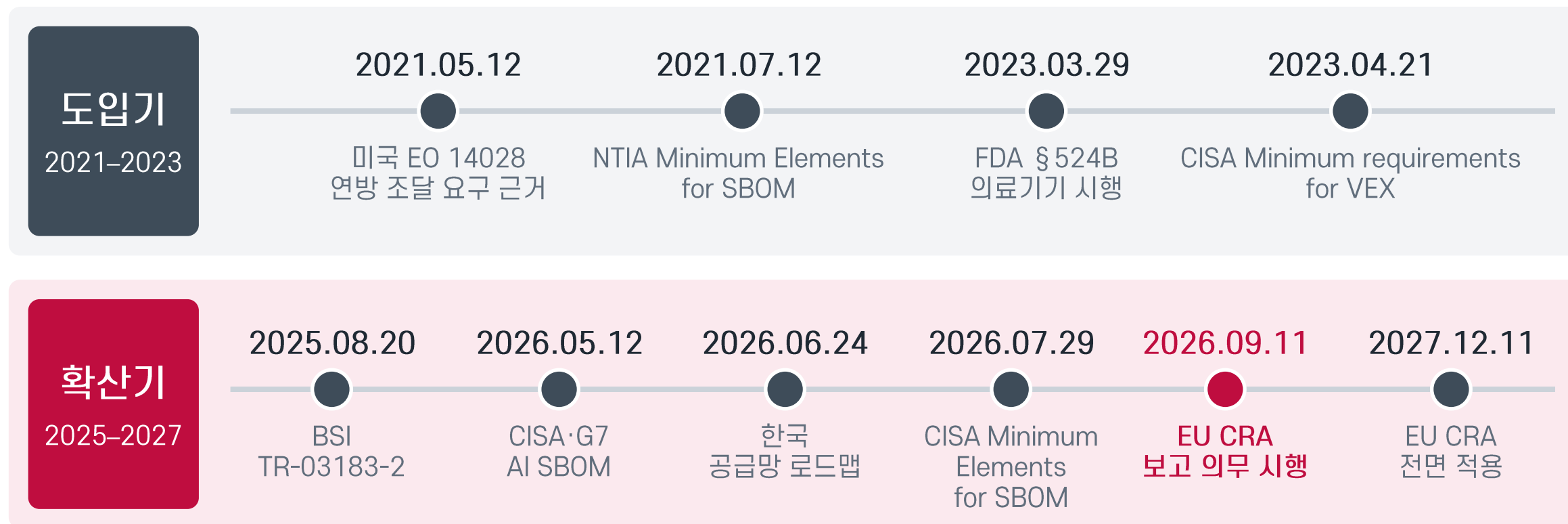
1. SBOM의 개요와 필요성

■ SBOM의 중요성



2. 글로벌 규제와 SBOM 가이드

- 2021년 미국 EO 14028에서 출발 → 2026년 미국·EU 가이드와 규제가 일제히 강화
- EU CRA 보고 의무는 이미 시작 — 남은 것은 2027년 전면 적용



2. 글로벌 규제와 SBOM 가이드

- 규제는 '**무엇을**', 가이드/표준은 '**어떻게**', 데이터 표준은 '**어떤 형식으로**'를 정함

규제 (법적 의무)

EU CRA

보고 의무: '26.9.11 시행
전면 적용: '27.12.11 예정

미국 FD&C Act § 524B

'23.3.29 시행

BIS 커넥티드 차량 기술 및 서비스 공급망 보안

소프트웨어 : 27년형 이후 모델부터
하드웨어 : 30년 모델부터
(모델 연도가 없는 경우는 29.1.1부터)

FCC 무선 장비 필수 인증

제안 단계, 시행일 미정

가이드라인·표준

CISA 2026 SBOM 최소요소

'26.7.29 발표

CISA VEX 최소요구사항

'23.4.21 발표

독일 BSI TR-03183-2 v2.1.0

'25.8.20 발표

EU 조화표준 prEN 40000-1-3

'25.10.31 발표 (Draft)

미국 FDA 사이버보안 가이드

'26.2.3 개정

CISA·G7 AI SBOM 최소요소

'26.5.12 발표

데이터 표준

SPDX 3.0.1

CycloneDX 1.7

CSAF 2.0

OpenVEX 0.2.0

3.1 FDA 의료기기 SBOM 의무화 조항

- 대상: 소프트웨어를 포함하고 인터넷 연결이 가능한 'cyber device'의 인허가 제출
- 의료기기 한정 — SBOM이 시장 진입 요건이 된 대표 사례, 일반 가전과 범위 구분
- 시행: 2023.3.29 / 2023.10.1부터 요건 미충족 시 접수 거부

원문

FD&C Act § 524B

SEC. 524B. ENSURING CYBERSECURITY OF DEVICES.

(b) CYBERSECURITY REQUIREMENTS.—The sponsor of an application or submission described in subsection (a) shall—

...

(3) provide to the Secretary a software bill of materials, including commercial, open-source, and off-the-shelf software components; and

3.2 Minimum Elements of SBOM 변천

2021: 정보의 "출처" 요구 → 2026: SBOM 문서 자체의 "신뢰"까지 요구

NTIA 2021

21.7 NTIA (EO 14028 대응)

- 데이터 필드 7개
- 최상위 의존성 + 하위 추적 가능
- 오류 수용
- 서명 등은 고려되지 않음

CISA 2025 (Draft)

25.8.22 CISA 공개 의견수렴

- 데이터 필드 11개
- 전이 의존성 포함, 최소 깊이 없음
- 정정, 갱신 수용
- 서명 필드가 추가됨 (권고)

CISA 2026 (최종안)

26.7.29 CISA 및 해외 15개 기관

- 데이터 필드 17개
(Meta Data + Component Data)
- 전이 의존성 포함, 최소 깊이 없음
- 정정, 갱신 수용 + 모름/비공개 구분
- 작성자 서명, SBOM 버전, 포맷, 도구 버전이 정식 필드로 반영

3.2 Minimum Elements of SBOM (2026)

누가

SBOM 작성자 서명

작성자로부터 변조 없이 왔음을 보증

무엇으로

도구명 · 도구 버전

도구에 따른 결과 차이를 해석

어떻게

생성 맥락

빌드 전(소스) / 빌드 중 / 빌드 후(바이너리)
빌드 시점 SBOM이 일반적으로 가장 정확

실물 일치

컴포넌트 해시

실제 배포된 바이너리와 대조

[참고] Minimum Elements of SBOM (2026)

구분	Data Field	Definition (원문)	변경
SBOM Metadata	SBOM Author	The name of the entity that creates the SBOM data for the target component.	Major
	SBOM Author Signature	A digital signature attributable to the SBOM author.	New
	SBOM Data Format Name	The name of the data format used to represent the SBOM data.	New
	SBOM Data Format Version	Identifier designated by the SBOM data format to specify the version of the data format.	New
	SBOM Generation Context	The relative software lifecycle phase and data available at the time the SBOM author generated the SBOM.	New
	SBOM Timestamp	Record of the date and time of the most recent update to the SBOM data.	Minor
	SBOM Tool Name	The name of the tool used by the SBOM author to generate or amend the SBOM.	New
	SBOM Tool Version	Identifier for the version of the tool identified in the SBOM Tool Name element.	New
	SBOM Version	Identifier designated by the SBOM author to specify a change in the SBOM document from a previously identified version or to indicate that it is the first version.	New
Component Data	Component Producer	The name of an entity that creates, defines, and identifies components.	Major
	Component Name	The name assigned by the component producer to a software component.	Minor
	Component Version	Identifier used by the component producer to specify a change in a software component from a previously identified version or to indicate that it is the first version.	Major
	Component Identifiers	Identifiers used to identify a component or serve as a look-up key for relevant databases.	Major
	Component Hash Value	The output generated from applying a cryptographic hash algorithm to an executable component artifact.	New
	Component Hash Algorithm	The cryptographic algorithm used to compute the Component Hash Value of the software component.	New
	Component License	The identifiers for the licenses under which the software component is available.	New
	Component Dependency Relationship	The relationship between two components, where one component is necessary for the operation of the other.	Minor

[참고] Minimum Elements of SBOM 비교

요소	NTIA 2021	CISA 2025 초안	CISA 2026
SBOM 작성자	Author of SBOM Data	SBOM Author	SBOM Author
작성자 서명	–	– (Discussion에서 서명 활용만 권고)	SBOM Author Signature (신규)
생산자	Supplier Name	Software Producer	Component Producer
컴포넌트 이름	Component Name	Component Name	Component Name (복수 이름 허용)
버전	Version of the Component	Component Version (없으면 파일 생성일)	Component Version (없으면 unknown)
식별자	Other Unique Identifiers	Software Identifiers (1개 이상)	Component Identifiers (기계처리 가능)
의존 관계	Dependency Relationship	백포트·포크 계보(pedigree) 명시	Component Dependency Relationship
타임스탬프	Timestamp	ISO 8601	RFC 9557
해시	–	Component Hash (신규)	Hash Value + Hash Algorithm
라이선스	–	License (신규)	Component License
생성 도구	–	Tool Name (신규)	Tool Name + Tool Version
생성 맥락	–	Generation Context (신규)	SBOM Generation Context
SBOM 문서 정보	–	–	SBOM Version, Format Name·Version (신규)

3.2 Minimum Elements of SBOM (2026)

■ Practices and Processes: 운영 절차에서 지켜야 할 핵심

Coverage

- 전이 의존성 포함 전체 컴포넌트 정보를 포함해야 함
- 최소 깊이 제한 없음

Frequency

- 모든 버전·업데이트마다 SBOM 생성해야 함
- 새 정보·오류 발견 시 수정본 발행해야 함

Accommodation of Updates

- 정정을 포함한 SBOM 갱신을 수용
- 작성자는 오류를 신속히 정정

Explicitly Identifying Unknown Information

- '모름(Unknown)'과 '의도적 비공개(Withheld)'를 구분 표기
- 비공개 항목 문의 절차 마련해야 함

Machine-Processable Data

- SPDX·CycloneDX 등 상호호환 가능한 포맷 수용
- 신규 SW에 폐기(deprecated) 버전 사용 금지

Distribution and Delivery

- SBOM은 필요한 상대가 바로 받을 수 있게 제공해야 함
- SBOM에 대한 접근 권한 제한은 가능하나, 정당한 목적으로 SBOM을 공유하는 것을 막으면 안됨

3.3 U.S. Cyber Trust Mark

- FCC의 자발적 IoT 보안 라벨 (NIST IR 8425)
- SBOM/HBOM 내용은 제출 의무는 없으나, 보유 여부는 공개 필요
- 미국 정부기관에 납품하는 제품은 마크 부착 의무화 예정
※ FAR 위원회는 27.1.4까지 IoT 장비에 대한 FAR(연방조달규정) 개정 예정임

Security & Privacy Facts

Sustios Smart Voice-activated Thermostat 4MOG




U.S. CYBER TRUST MARK

More info

Sensor Data	
Collected	Audio, Humidity, Motion, Temperature
Shared	Audio, Humidity, Motion, Temperature
Security Updates	Consent-based
Access Control	Password - User Generated, Multi-factor Authentication

Security & Privacy Details

Sustios

Smart Voice-activated Thermostat 4MOG
Firmware version: 1.3 - updated on: 07/31/2023
The device was manufactured in: China



U.S. CYBER TRUST MARK

Security Mechanisms	Security updates	Consent-based - Available until at least 08/30/2026	
	Access control	Password - User Generated, Multi-Factor Authentication	
	Security oversight	www.thermostat.sustios.com/security_audits	
	Ports and protocols	www.thermostat.sustios.com/ports	
	Hardware safety	www.thermostat.sustios.com/hw_safety	
	Software safety	www.thermostat.sustios.com/sw_safety	
	Personal safety	www.thermostat.sustios.com/personal_safety	
	Vulnerability disclosure and management	www.thermostat.sustios.com/vul_report	
	Software and hardware composition list	www.thermostat.sustios.com/BOM	
	Encryption and key management	www.thermostat.sustios.com/encryption	

Data Practices	Sensor data collection	Audio	Motion
	Sensor type	Microphone	Motion sensor
	Collection frequency	When an event happens	When an event happens
	Purpose	Providing and improving device functions	Providing and improving device functions
	Data stored on the device	Aggregated or anonymized	Aggregated or anonymized
	Local data retention time	No retention	No retention
	Data stored in the cloud	Aggregated or anonymized	Aggregated or anonymized
	Cloud data retention time	No retention	No retention
	Data shared with	Manufacturer	Manufacturer
	Data sharing frequency	Continuous	Continuous
	Data sold to	None	None
	Other collected data	Account info, Contact info, Device setup info, Device usage info, Temperature, Humidity	
Data linkage	Data will not be linked with other data sources		
What will be inferred from user's data	No data inference		
Special data handling practices for children	Yes		
In compliance with	GDPR		
Privacy policy	iortregistry.us/sustios/4MOG/privacy		

More Information	Call Sustios with your questions at	1 000-000-0000
	Email Sustios with your questions at	info@sustios.com
	Functionality when offline	Limited functionality
	Functionality with no data processing	Limited functionality
	Physical actuations and triggers	Device blinks when motion is detected
	Compatible platforms	Mobile App, Amazon Alexa, Siri, Google Assistant

CMU IoT Security and Privacy Label CISPL 1.0 iotsecurityprivacy.org 

3.4 BIS 커넥티드 차량 기술 및 서비스 공급망 보안

- 대상 : 커넥티드 차량(VCS, ADS 시스템) 제조업체
 - ※ Vehicle Connectivity System, Automated Driving System
- 중국 및 러시아의 지시를 받거나 통제되는 주체가 설계, 개발, 제조, 공급한 특정 소프트웨어 및 하드웨어의 거래를 금지함
- 미국에서 차량을 수입, 판매 전에 BIS에 적합성 선언서를 의무적으로 제출해야하며, SBOM/HBOM 제출을 요구할 수 있음
 - ※ 실사(Due Diligence)를 하며, 증빙 문서를 보관하며, BIS 요청시 제공 필요
- 시행일
 - 소프트웨어가 포함된 차량의 수입·판매가 금지 : 2027년형 이후 모델부터
 - 하드웨어가 포함된 차량의 수입, 판매 금지 : 2030년 모델부터 (모델연도가 없는 경우는 2029.1.1 부터)
- 벌금/벌칙
 - 민사처벌: 건당 \$377,700 또는 위반 거래 금액의 두 배 중 더 높은 금액
 - 형사 처벌: 최대 \$1,000,000 벌금 또는 징역 20년(개인), 고의적 위반·위반 시도·공모·방조 시 대상



3.5 FCC 무선 장비 필수 인증

FCC 26-50의 Third FNPRM

(26년 7월 22일 채택/ 단, SBOM/HBOM 제출 의무에 대해서는 의무 대상 및 시행 일정 검토 중)

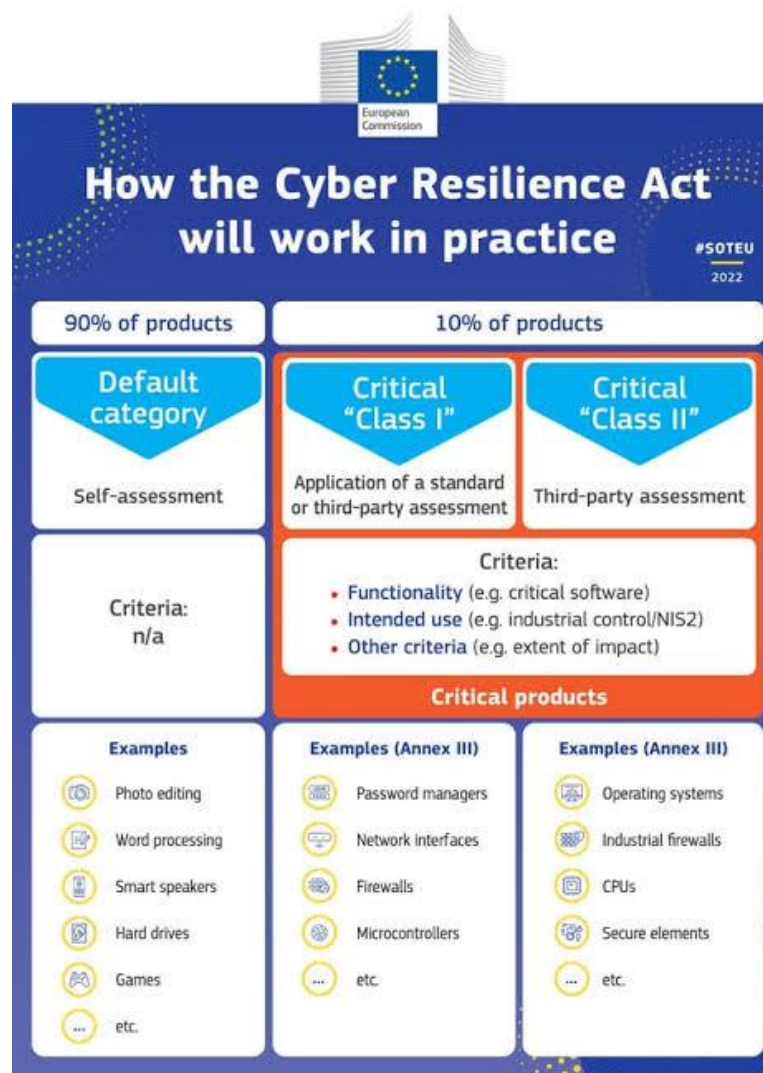
- 대상 : 무선 신호를 내보내는 모든 장비
 - ※ Wifi, 블루투스, 셀룰러 모듈이 들어간 장비
 - ※ 고위험 제품 or 특정 부품으로 한정할지 부분은 검토 중
- 인증 신청 시, **HBOM 및 SBOM을 제출해야 함**
- 해당 정보의 정확성, 완전성에 대해 서면 서명을 통해 보증해야 함
 - ※ 신청 회사의 대표자의 서명 필요
- 미국 출시 무선장비 제조사라면 SBOM, HBOM 외에
컴포넌트별 생산자·생산지·가치 비중 데이터를 별도로 관리해야 해야함
 - ※ CISA 최소요소에 없음

Federal Communications Commission		FCC-26-50
Before the Federal Communications Commission Washington, D.C. 20554		
In the Matter of	)	
Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program	)	ET Docket No. 21-232
THIRD REPORT AND ORDER AND THIRD FURTHER NOTICE OF PROPOSED RULEMAKING		
Adopted: July 22, 2026		Released: July 23, 2026
Comment Date: [30 days after date of publication in the Federal Register] Reply Comment Date: [45 days after date of publication in the Federal Register]		
By the Commission: Chairman Carr and Commissioner Trusty issuing separate statements.		
TABLE OF CONTENTS		
Heading		Paragraph #
I. INTRODUCTION		1
II. BACKGROUND		4
A. The First Report and Order and Further Notice		4
B. The Second Report and Order and Second Further Notice		7
C. Covered List additions of equipment "produced in a foreign country"		9
III. THIRD REPORT AND ORDER		13
A. Logic-Bearing Hardware Components		14
B. Components Prohibitions Limited to Producer/Provider-Based Determinations		37
C. Marketing		40
D. Clarifications regarding Modifications Such that Previously-Authorized Equipment Would Become Covered		78
E. Re-Certifications Required of Covered List Entities for Any Change to Equipment		84
F. Definition of "Critical Infrastructure" as used in the Covered List		89
G. Rule Correction and Clarification		96
H. Regulatory Impact Analysis		98
IV. THIRD FURTHER NOTICE OF PROPOSED RULEMAKING		128
A. Bifurcating Covered List rules		129
B. White Labeling		130
C. Hardware and Software Bill of Materials		139
D. Software and other Components produced by Covered List entities		147
E. Requiring certification for devices in Covered List sectors		153
F. Importation under 47 CFR § 2.1204		159
G. Marketing under 47 CFR § 2.803		168
H. Use of FCC Logo, 47 CFR § 2.1074		177
I. Streamlined revocation, 47 CFR § 2.939		182
J. Permitting permissive changes for basic software and hardware updates, even for "covered" equipment		187

4.1 EU CRA 규제



4.1 EU CRA 규제



4.1 EU CRA 규제

■ EU CRA 제조업체 보고 의무 (제14조, 2026.9.11~)

- EU 집행위 CRA 적용 가이드 (2026.7.27)

- 제품에서 악용 불가·미악용이면 의무 보고 대상 아님
- 단, 취약점 처리 의무와 상위 유지관리자 통보 의무는 유지

- 시사점

- "제품이 영향을 받는가"의 판단이 법적 효과를 가짐
- 판단과 근거를 기록·전달하는 수단 = VEX



4.1 EU CRA 규제

■ EU CRA 제조업체 주요 요구사항 (기타 조항, 2027.12.11~)

- 디지털 요소가 있는 제품과 관련된 **사이버 보안 위험을 평가**해야 함
 - 제품 라이프사이클 전 단계에 걸쳐 제품의 컴포넌트와 취약점을 식별·문서화 필요
- 널리 쓰이는 기계 판독 형식으로 최소한 최상위 의존성 포함하는 SBOM을 문서화해야 함
- 수정된 취약점 정보를 공유하고 공개해야 함
- 제조업체는 **지원 기간(최소 5년)동안** 제품의 취약점을 효과적으로 처리해야 함
- 각 보안 업데이트가 발행된 후, **최소 10년 (또는 지원 기간 중 더 긴 기간동안)** 유지해야 함
- 기술 문서 및 EU 적합성 선언서를 **최소 10년이상(또는 지원 기간 중 더 긴 기간동안)** 보관해야 함

4.1 EU CRA 규제

■ EU CRA의 SBOM 관련 법적 요구사항

조항	원문 (Regulation (EU) 2024/2847)	의미
Art. 3(39) 정의	'software bill of materials' means a formal record containing details and supply chain relationships of components included in the software elements of a product with digital elements;	SBOM = 구성요소의 상세와 공급망 관계를 담은 공식 기록
Annex I Part II (1)	[Manufacturers of products with digital elements shall:] identify and document vulnerabilities and components contained in products with digital elements, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the products;	작성 의무: 기계판독 형식, 최소 최상위 의존성
Annex VII 2(b)	necessary information and specifications of the vulnerability handling processes put in place by the manufacturer, including the software bill of materials, ...	기술문서(취약점 처리 절차)에 SBOM 포함
Annex VII (8)	where applicable, the software bill of materials, further to a reasoned request from a market surveillance authority provided that it is necessary in order for that authority to be able to check compliance with the essential cybersecurity requirements set out in Annex I.	시장감시기관의 이유 있는 요청 시 제출
Art. 13(24)	The Commission may, by means of implementing acts, ... specify the format and elements of the software bill of materials ...	포맷·요소는 이행법으로 구체화 가능 (아직 미채택)

4.1 EU CRA 규제

■ EU CRA 수평 조화 표준 (3종)



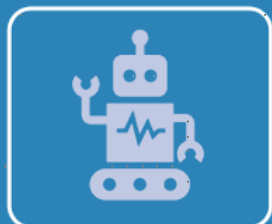
EN 40000-1-2: Principles for cyber resilience

- Covers CRA Annex I, Part 1, Requirement 1
- **Process** standard to ensure products are developed and maintained with a risk-based approach to cover **any** security risks (as a catch-all, as 2a-m do not cover all possible cybersecurity risks)
- Implementation demonstrated via documented process outputs



EN 40000-1-3: Vulnerability handling

- Covers CRA Annex I, Part 2
- **Process** standard to ensure products are maintained in a secure state using a risk-based approach
- Implementation demonstrated via documented process outputs and actions in the market (updates, notifications, recalls, etc.)



EN 40000-1-4: Generic security requirements

- Covers CRA Annex I, Part 1, Requirement 2 (a-m)
- **Product** standard addressing a specific set of security requirements by mapping security objectives to a catalog of possible security controls
- Implementation demonstrated via the product itself and/or supported by technical documentation

4.1 EU CRA 규제

■ prEN 40000-1-3 [PRE-7] SBOM 요구사항

ID	표준 원문	의미
PRE-7-RQ-01	All software components contained in the product shall be identified and documented.	전 컴포넌트 식별
PRE-7-RQ-02	For each component identified in [PRE-7-RQ-01], the following information shall be included: Software producer / For open-source software, which is supported by an open-source steward, this is the name of the stewarding organization : Component name, Component version	소프트웨어 제조자, 컴포넌트명, 컴포넌트 버전
PRE-7-RQ-03	An SBOM shall be drawn up, including at least the top-level dependencies that are contained in the product ...	최소 최상위 의존성
PRE-7-RQ-03-RE	All the software components identified in [PRE-7-RQ-01] shall be drawn up in the SBOM to detect transitive dependencies when technically feasible.	강화: 전이 의존성
PRE-7-RQ-04	The SBOM shall be assembled in a structured, machine-readable format.	기계판독 형식
PRE-7-RQ-05	If the software component is updated with a new build or release, a new SBOM shall be created ...	빌드마다 새 SBOM
PRE-7-RQ-06	Metadata for the SBOM shall include: SBOM Author, Version, Timestamp	작성자·버전·시각
PRE-7-RQ-07	... the following information shall be included: Information as required from [PRE-7-RQ-02] , Dependency Relationship, and Unique component identifiers	의존 관계·식별자
PRE-7-RQ-07-RE	If the supplier provides the hash and the corresponding algorithm for the component, it shall be included in the SBOM.	강화: 공급자 해시

4.1 EU CRA 규제

■ prEN 40000-1-3 [PRE-8] HBOM 요구사항

ID	표준 원문	의미
PRE-8-RQ-01	Hardware components that are integrated in the product shall be identified and documented.	하드웨어 컴포넌트 식별
PRE-8-RQ-02	<p>For each identified hardware component as per [PRE-8-RQ-01], the following information shall be recorded:</p> <ul style="list-style-type: none">— Hardware producer— Component name— Component identifier— If applicable, firmware version <p>... (중략)...</p> <p>NOTE 3 Further available information can be recorded, such as:</p> <ul style="list-style-type: none">— Part number— Serial number— Batch number— Component version— Production date— Hardware revision	하드웨어 컴포넌트 정보 기록

4.2 독일 BSI TR-03183 SBOM 가이드라인

- EU CRA 제조사 의무를 준수하기 위한 BSI 가이드라인 (총 4부 구성)
 - Part 1 : CRA 일반 요구사항
 - Part 2 : SBOM
 - Part 3 : 취약점 신고 및 통지
 - Module H : CRA 적합성 평가 (Full Quality Assurance)
 - ※ ISO/IEC 27001, 27002 요구사항 중심
- 법적 구속력은 없음
- 단, BSI가 독일 CRA 시장감시기관이 될 예정 → 사실상 심사 기준



4.2 독일 BSI TR-03183 SBOM 가이드라인

- **범위** : 제품과 함께 전달되는 모든 소프트웨어 (primary + 3rd party components)
- 하나의 소프트웨어 버전마다 별도의 SBOM 생성 필요
- **SBOM 문서(static data)에는 취약점 정보 포함하면 안됨** → 취약점 문서 (권고) : CSAF (VEX 포함)
- **포맷** : 기계처리 가능한 (machine-processable) CycloneDX 1.6+ or SPDX 3.0.1+ (JSON or XML)
- **작성 수준** : 재귀적 의존성을 끝까지 기재하고, 범위 밖은 각 경로마다 첫 컴포넌트까지 식별
- **SBOM 필수 필드** : 생성자, 타임스탬프
- **컴포넌트 필수 필드** : 생성자, 컴포넌트 명, 컴포넌트 버전, 컴포넌트의 파일명, 다른 컴포넌트 의존성, 배포 라이선스, 배포 가능한 해시값(SHA 512), Executable, Archive, Structured 속성
- PURL, CPE, SWID와 같은 식별자 정보가 있을 경우, 기재 필요

[참고] TR-03183-2 필드 ↔ CISA 2025 · 2026 비교

수준	BSI TR-03183-2 v2.1.0	분류	CISA 2025 초안	CISA 2026
SBOM	Creator of the SBOM (이메일·URL)	Required	SBOM Author	SBOM Author
SBOM	Timestamp	Required	Timestamp	SBOM Timestamp
SBOM	SBOM-URI	Additional	–	–
컴포넌트	Component Creator	Required	Software Producer	Component Producer
컴포넌트	Component Name / Version	Required	Component Name / Version	Component Name / Version
컴포넌트	Filename of the Component	Required	–	–
컴포넌트	Dependencies on Other Components	Required	Dependency Relationship	Component Dependency Relationship
컴포넌트	Distribution Licences	Required	License	Component License
컴포넌트	Hash of the Deployable Component (SHA-512)	Required	Component Hash	Component Hash Value
컴포넌트	Executable / Archive / Structured Property	Required	–	–
컴포넌트	Source Code URI / URI of the Deployable Component	Additional	–	–
컴포넌트	Other Unique Identifiers (PURL, CPE, SWHID)	Additional	Software Identifiers	Component Identifiers
컴포넌트	Original Licences	Additional	–	–
컴포넌트	Effective Licence / Source Code Hash / security.txt URL	Optional	–	–
CISA 전용	–	–	Tool Name, Generation Context	+ Tool Version, Hash Algorithm, Author Signature, Data Format Name·Version, SBOM Version

5. 한국: SW 공급망 보안 강화

- SW 공급망 보안 강화 로드맵 (과기정통부·국정원, 2026.6)
 - SW 공급망 보안 가이드라인 1.0 → 2.0 개편
 - 공공 정보화사업에 SBOM 제출·취약점 대응 절차 도입
 - 보안적합성 검증에 SBOM 제출 등 공급망 기준 추가
 - SBOM 생성·검증·취약점 분석 자동화 기술 개발
- KISA SBOM 기반 공급망 보안 모델 지원사업
 - 2025년 8개 기업 첫 시행 → 2026.4 사례집 발간
 - 2026년 8개 과제: 운영기업까지 참여, SBOM·VEX 운영 모델 실증
- 국정원·KISA, CISA 2026 최소요소 공동 작성기관으로 참여

2024. 05

SW 공급망 보안 가이드라인 v1.0

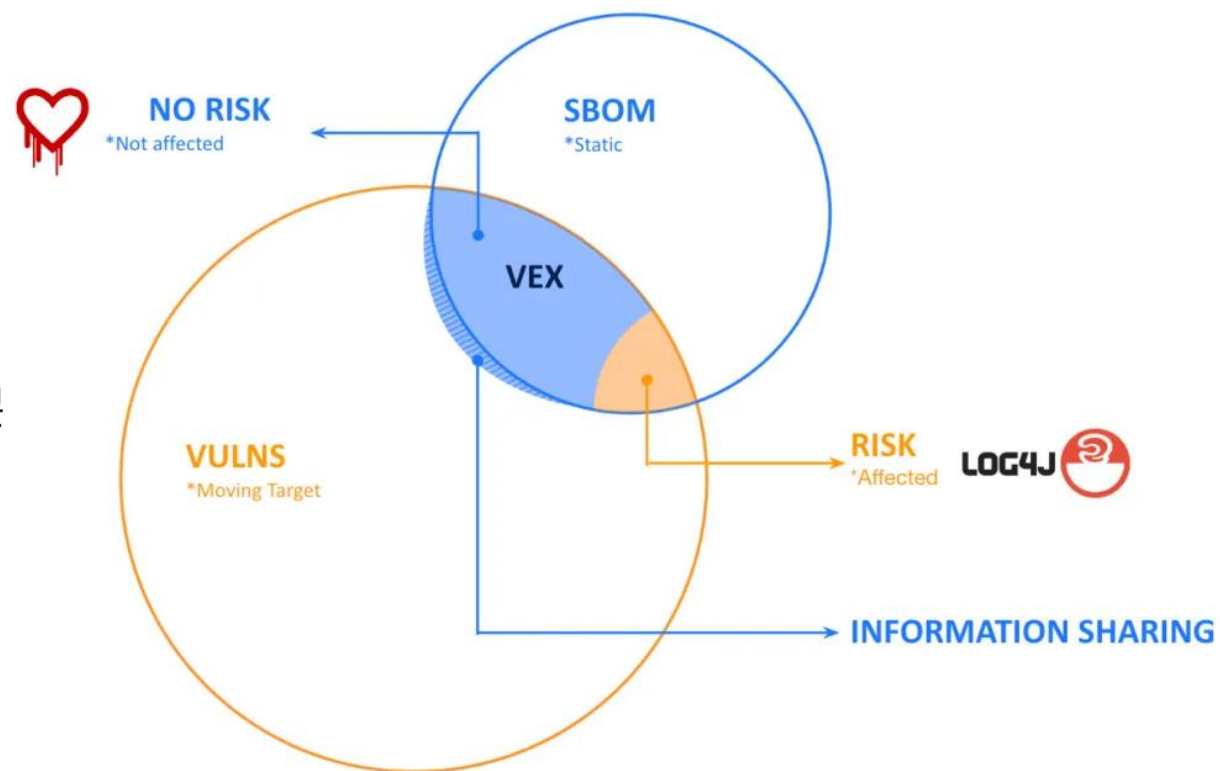
SW 공급망 보안 국제동향 및
SBOM 활용사례



6. SBOM과 VEX

VEX (Vulnerability Exploitability eXchange)은 보안 취약점이 실제 환경에서 악용 가능한지 여부를 알려줌

- SBOM: 정적 정보 (제품에 무엇이 들어 있는가)
- 취약점(VULNs): 계속 움직이는 정보
- 교집합 = VEX
 - 영향 있음(Affected), 없음(Not affected)을 구분
 - 그 판단과 근거를 공유 (Information sharing)



6. SBOM과 VEX

■ CISA VEX 최소요구사항 (2023.4)

- VEX 문서: 취약점 악용 가능 선언(VEX Statement) 1개 이상 + 문서 메타데이터

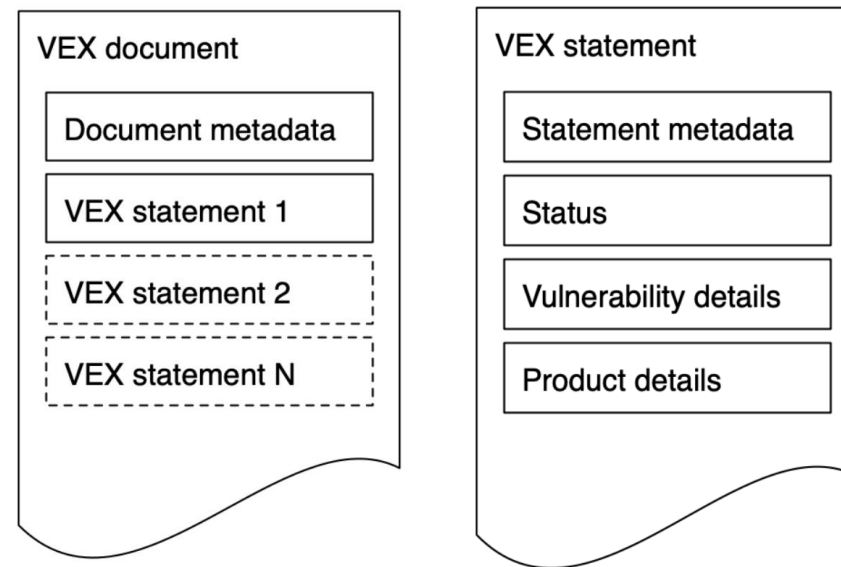
- doc_id · doc_version · author · 최초 발행·최종 수정 시각

- VEX Statement: 취약점 1개 × 상태 1개 × 제품 1개 이상

- statement_version · 최초 발행·최종 수정 시각 필수

- 상태별 필수 정보

- not_affected → 근거 또는 영향 설명 / affected → 조치 설명



- 서명은 권장이나 VEX 도구 및 구현체(implementation)에서의 서명 기능 지원은 필수

- 예: 형식(CSAF·CycloneDX·OpenVEX), 도구(vexctl·스캐너·관리 시스템)

- 서명할 경우 문서 메타데이터와 모든 VEX Statement를 포함

6. SBOM과 VEX

■ VEX status 및 Justification

status	원문 정의	추가 요구
not_affected	No remediation or mitigation is required. The vulnerability does not affect the listed [product_id]s.	justification 권장(SHOULD), 없으면 impact_statement 필수(MUST)
affected	Actions are recommended by [author] to remediate, mitigate, or otherwise address [vul_id]. The vulnerability affects the listed [product_id]s.	action_statement 필수(MUST)
fixed	The listed [product_id]s contain fixes for [vul_id].	—
under_investigation	The [author] of the VEX statement or other relevant parties are investigating and have not yet declared a final [status].	결론 후 상태 변경 예상

justification (not_affected 근거 5종)	의미
Component_not_present	취약 컴포넌트가 제품에 없음
Vulnerable_code_not_present	컴포넌트는 있으나 취약 코드는 빌드에서 제외
Vulnerable_code_not_in_execute_path	취약 코드가 있으나 호출·사용하지 않음
Vulnerable_code_cannot_be_controlled_by_adversary	사용되지만 공격자가 제어할 수 없음
Inline_mitigations_already_exist	우회·해제 불가능한 내장 보호 기능이 존재

6. SBOM과 VEX

■ SBOM과 VEX: 분리할까, 통합할까

통합

장점

- 파일 하나로 배포·관리
- 컴포넌트 참조가 문서 안에서 해결

단점

- 취약점 상태가 바뀔 때마다 SBOM 재발행·재서명
- 구성정보와 보안 판단의 공개 범위가 묶임

분리

장점

- 정적 구성정보와 동적 판단의 수명주기 분리
- VEX만 수시 갱신, 배포 대상 별도 통제
- BSI Part 2 방식과 일치

단점

- 두 문서의 연결·동기화 관리 필요

6. SBOM과 VEX

■ SBOM과 VEX 분리·연결 예제 (CycloneDX)

- 판단이 바뀌면 VEX의 version만 올려 재게시 — SBOM은 재발행·재서명 불필요

SBOM — 릴리스마다 고정

```
{
  "serialNumber": "urn:uuid:3e671687-...",
  "version": 2,
  "components": [{
    "name": "log4j-core", "version": "2.14.1",
    "purl": "pkg:maven/org.apache.logging.log4j/log4j-core@2.14.1",
    "bom-ref": "comp-log4j-core"
  }]
}
```



VEX — 판단이 바뀔 때마다 갱신

```
{
  "serialNumber": "urn:uuid:9a1c...", "version": 1,
  "vulnerabilities": [{
    "id": "CVE-2021-44228",
    "analysis": { "state": "not_affected",
    "justification": "code_not_reachable" },
    "affects": [{ "ref":
      "urn:cdx:3e671687-.../2#comp-log4j-core" }]
  }]
}
```

PURL

컴포넌트 (무엇)

어느 형식·도구에서나 통하는 공통 이름

serialNumber + version

SBOM 발행본

어느 릴리스의 SBOM인지 지정

bom-ref

문서 안 컴포넌트

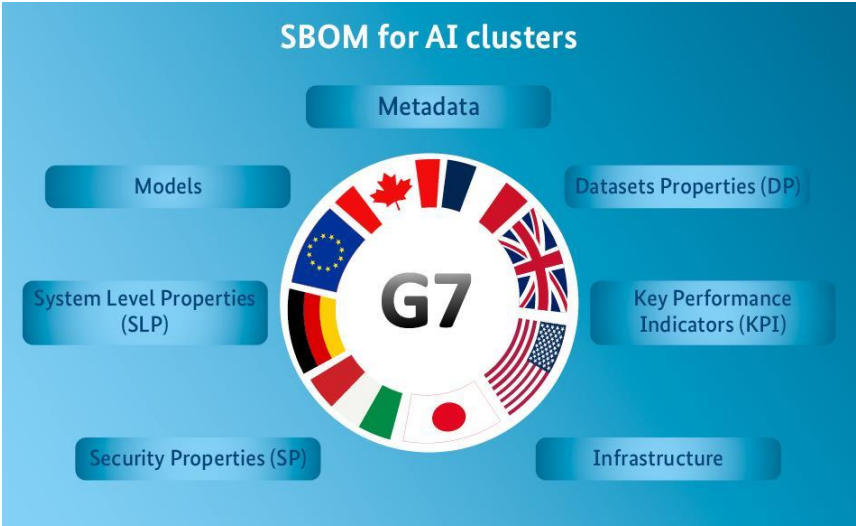
urn:cdx:...#bom-ref 로 정확히 지칭

7. 한계점

- 기준이 제각각
 - CRA·CISA·BSI·FDA·산업별로 요구 필드와 깊이가 다름
 - 같은 정보도 포맷·도구마다 위치·표현이 다름
- 도구 간 결과 불일치
 - 같은 제품도 도구·생성 시점에 따라 목록이 다름
 - 식별자(PURL·CPE) 누락 → 취약점 매칭 실패
- 임베디드·펌웨어의 사각지대
 - C/C++ 정적 링크, 패키지 관리자 밖 코드, 바이너리로만 받은 SW

8. SBOM의 확장

- AI 시스템의 특성을 반영한 구성요소·의존성을 투명하게 추적해 AI 공급망 보안을 강화하고자 함
- CISA·G7 공동 (2026.5) : G7 7개 기관 + EU 참여
- 의무 아닌 권고 : 일반 SBOM 최소요소에 추가
- AI 자율성 수준은 요소 미채택



클러스터	요소
Metadata	SBOM author · version · data format name/version · author signature · tool name/version · generation context · timestamp · dependency relationship
System Level Properties	System name · components · producer · version · timestamp · data flow · data usage · input/output properties · intended application area
Models	Model name · identifier · version · timestamp · producer · description · hash value · hash algorithm · properties · input-output properties · training properties · license · external references
Datasets Properties	Dataset name · description · content · identifier · hash · provenance · statistical properties · sensitivity · dependency relationship · license
Infrastructure	Infrastructure software · Infrastructure hardware (HBOM 링크)
Security Properties	Security controls · Security compliance · Cybersecurity policy information (security.txt) · Vulnerability referencing
KPI	Security metrics · Operational performance KPIs

9. 제조사의 대응 과제

공급업체 SBOM 관리

계약에 제출·갱신 기준 명시
(포맷, 최소요소, 갱신 주기)

품질 자동 검증

수신·생성 SBOM을 기준 프로파일로 점검

버전 추적 및 보관

출시 버전과 SBOM 1:1 연결
10년 보관

취약점 대응 자동화

SBOM 분석 → VEX 판단 → 24시간 보고 → 고객 공지

Q & A



hyejin.oh@lge.com