What is Material to the AI Bill of Materials?

Global Cyber Security Capacity Centre
Department of Computer Science and Oxford Martin School
University of Oxford

15 January, 2026

Introduction

Supply-chain risks comprise economic, environmental, political and ethical threats that have the potential to either disrupt the flow of services and goods within a supply-chain network or ecosystem (CWSI, 2025).

- They are one of the top risks concerning cybersecurity professionals and business leaders (WEF, 2025, 2026), with a significant percentage of organisations experiencing third-party cyber incidents (Security Scorecard, 2025; Verizon, 2025; BlueVoyant,2024).

AI supply-chain risks are emerging as a priority concern as organisations rush to adopt AI technology (OWASP, 2025; WEF, 2026), as a security control and expertise gap emerges despite the efforts within the AI cybersecurity community towards understanding vulnerabilities and misuse (MIT, 2025; GitHub, 2025; AVID, 2025).

- Emerging policies seek to help address trust in the AI supply-chain by using Software Bills of Materials (SBOMs) as a transparency tool to improve the trustworthiness of component parts.

“SBOM is an often-cited tool which lists the component parts and software dependencies of a software package, and is designed to help vendors and developers better understand the open source and third party components it may contain. This should be an exhaustive list which includes open-source libraries, proprietary software, and licensed dependencies. Some may also include the tools used to produce the software, along with other provenance information.” NCSC (2026).

Research Question

SBOM movements have a place to help AI procurement and, in the face of an incident, to triage and quickly understand inherited vulnerabilities in the supply chain, informing recovery choices, future resilience planning, and also potentially attack attribution and intent.

Given the threat posed on AI supply chains, what could be achievable using Software and AI Security Bills of Materials (SBOMs and AI SBOMs)?

- Thematic analysis of semi-structured interviews to 9 experts in communities and platforms with initiatives related to AI BOMs.

Some Preliminary Findings

- **Urgent topic**: SBOMs are regulatory requirements in some countries, entailing commercial restrictions for exporting organisations.

- **Uncoordinated efforts with similar routes**: Existing initiatives aim to define governance stances under major international technical standards bodies to promote transparency and interoperability.

- **Not reinventing the wheel**: AI is a subset of software, and existing effective cybersecurity frameworks could be revised to address the new nature of risks posed by AI technologies.

- **Main challenges**: The significant gap in global repository of AI vulnerabilities, and how to attest the integrity of all elements forming an AI system.

- **Necessary but not sufficient**: Complementary policies are required to enhance security postures across the AI supply chain.

Thank You!

patricia.esteve-gonzalez@cs.ox.ac.uk

Global Cyber Security Capacity Centre

OXFORD MARTIN SCHOOL

UNIVERSITY OF OXFORD

DEPARTMENT OF COMPUTER SCIENCE

UK Government