Strengthening License Compliance and Software Security with SBOM Adoption

The Linux Foundation launched the Software Package Data Exchange (**SPDX**) project in 2009, a **major milestone toward SBOM standardization**.

The US Executive Order 14028 **mandates federal agency use of SBOMs** for software procurement to **enhance supply chain security** amid rising cyber threats.

One of the key components of the European Union's **Cyber Resilience Act** is the introduction of a **recommended SBOM**, ensuring products are secure by design.

SBOMs safeguard software supply chains and **bolster national cybersecurity posture**, regardless of industry type or technology domain.

A **SBOM** is a **comprehensive, machine-readable inventory** detailing the constituent software components within an application, system, or software stack.

SBOMs typically comprise **5 key elements**: component inventory, origin information, dependency relationships, vulnerability intelligence, and metadata & annotations.

SBOMs are crucial for license compliance & cybersecurity, offering organizations essential insights into software components to **ensure license adherence & enhance cyber defenses**.

SBOMs empower license compliance teams to **mitigate legal, reputational, technical, & financial risks** associated with license violations.

SBOMs serve as early warning systems, enabling preemptive mitigation of security risks before they escalate & facilitating streamlined incident response & patch management efforts.

SBOM functionality is typically embedded as part of **software composition analysis (SCA) tools** to ensure open source license compliance & improve code security.

For effective implementation, organizations must **establish clear policies & roles** that help integrate SBOMs into compliance & security practices.

Organizations must **perform regular & timely updates** of SBOMs & **monitor the effectiveness of their implementation**.