SBOM for AI Use Cases

Use cases and recommendations to operationalize Software Bills of Materials (SBOMs) for Artificial Intelligence (AI).

CISA SBOM for AI Tiger Team

Version: 0.3 Draft
Date: June 23, 2025

Disclaimer

This document was drafted in an open process by a community of Software Bill of Materials (SBOM) experts, facilitated by the Cybersecurity and Infrastructure Security Agency (CISA). CISA did not draft and is not the author of this document, nor does this document represent an official CISA and/or U.S. Government policy. CISA and the U.S. Government do not specifically adopt or endorse the views expressed in this document.

Nothing in this document should be considered binding on any organization and instead should be viewed as forming a basis for future requirements covering SBOM consumption and usage.

Contents

Executive Summary

Organizations worldwide are rapidly adopting the latest innovations in Artificial Intelligence (AI), such as Generative AI and Large Language Models (LLMs). This new technology introduces a range of business, legal, and security risks—many of which require new strategies, but some of which mirror known software supply chain challenges.

Software Bills of Materials (SBOMs) have become a globally adopted standard for managing software supply chain risk. Similarly, SBOM for AIs offer a practical and standardized way to improve transparency, security, and trust across AI systems, supporting stakeholders across security, compliance, governance, and legal teams.

This document provides an overview of SBOM for AIs, focusing on key use cases that help organizations manage risks and responsibilities across industries.

At a high level, SBOM for AIs enable organizations to:

- **Compliance**: Meet emerging regulatory and customer expectations for AI transparency and accountability through structured, auditable inventories of AI components.
- **Vulnerability and Incident Management**: Improve visibility into models and datasets, enabling faster impact analysis, dependency mapping, and integration with automated incident response workflows.
- **Legal and Intellectual Property Protections**: Ensure the permissible use of models and datasets by tracking provenance, licensing, and modifications to avoid regulatory or legal exposure.
- **Third-Party AI Risk Management**: Gain visibility into vendor-supplied AI systems by identifying underlying models, datasets, and their associated risks for purchasing and operations.
- **Open Source Model Risk Assessment**: Evaluate the trustworthiness and compliance of publicly sourced models and datasets before integration into internal systems.
- **Model Lifecycle and Asset Management**: rack model lineage, configurations, datasets, and energy usage to improve reproducibility, lifecycle oversight, inventory accuracy, and sustainability metrics..

Implementation Priorities

To support AI transparency, security, and compliance, organizations should focus on these key priorities:

- **Generate SBOM for AIs for internally developed models** using standard formats (e.g., CycloneDX, SPDX) to build a reliable inventory of AI components across the enterprise.
- **Generate SBOM for AIs for open-source AI** models and datasets to assess risks related to provenance, licensing, and potential compliance or security concerns.

- **Require SBOM for AIs from third-party vendors** to ensure visibility into externally sourced AI models and datasets as part of procurement and risk management.
- **Use SBOM for AIs as a foundation for model cards** to standardize documentation and support governance, transparency, and cross-team understanding.
- **Maintain a unified inventory of all models and datasets** including provenance, lineage, dependencies, and training context for improved oversight and risk mitigation.
- **Integrate SBOM for AIs into security and compliance workflows** such as incident response, vulnerability management, and regulatory audits.
- **Automate generation and monitoring of SBOM for AIs** to enable scalable, real-time oversight while reducing manual effort.
- **Adopt a crawl/walk/run approach**—start small with available metadata rather than delaying until standards or processes are perfect.

Common Audience and Roles

This document is intended for diverse stakeholders within organizations who are involved in managing, deploying, securing, and overseeing AI systems. The following roles represent typical personas who could leverage AI Software Bills of Materials (SBOM for AIs) for operationalizing transparency, compliance, security, and governance in AI ecosystems. These examples are illustrative and not exhaustive:

- **AI Platform Engineers** – Implement and manage SBOM for AI tools within ML pipelines, maintaining inventories of models, datasets, and components.
- **AI Engineers and Data Scientists** – Select and document compliant AI components, ensuring completeness and accuracy of SBOM for AI metadata.
- **Data Engineers** – Manage data pipelines and dataset versioning used in AI training and deployment.
- **Product Security Teams** – Track AI-related vulnerabilities and dependencies to assess and mitigate risks in AI-powered products.
- **Compliance Officers** – Oversee regulatory adherence and respond to transparency and audit requests using SBOM for AI documentation.
- **Legal and Audit Teams** – Verify dataset legality, model licensing, and responsible AI usage aligned with IP and regulatory requirements.
- **Incident Response and Vulnerability Management Teams** – Use SBOM for AIs to identify impacted components and accelerate incident resolution.
- **Security Analysts** – Evaluate AI model and dataset integrity, third-party risks, and secure component integration.
- **Third-Party Risk Management Teams** – Assess vendor AI products using SBOM for AIs to ensure compliance during purchasing and operations and reduce supply chain risk.
- **Vendors and Suppliers** – Provide SBOM for AIs to demonstrate transparency and support customer compliance assessments.
- **Regulators and Standards Bodies** – Leverage SBOM for AIs to enforce transparency, inform policy development, and support industry audits.

Introduction

What is an SBOM for AI?

An **SBOM for AI** (Software Bill of Materials for (Artificial Intelligence) is an extension of a traditional SBOM—defined in resources such as CISA's "Framing Software Component Transparency: Establishing a Common Software Bill of Materials (SBOM)" (2024)—designed to provide transparency, security, and compliance for AI systems. It is machine-readable (e.g., JSON, XML formats) and aligns with existing SBOM frameworks, incorporating AI-specific fields such as model metadata, training data, and inference behaviors.

An SBOM for AI includes detailed information such as the type and provenance of training data, model architecture and versioning, base or parent models, hyperparameters, dependencies on external libraries or APIs, model inference characteristics, and deployment configurations. Crucially, an SBOM for AI is not a new standalone standard; rather, it integrates seamlessly with established, open, and globally recognized standards such as SPDX (Software Product Data eXchange, including AI and Dataset Profiles) and CycloneDX (including ML-BOM extensions).

The need for AI component traceability and transparency, which SBOM for AIs aim to address, is increasingly reflected in leading AI security and governance frameworks, including NIST's AI Risk Management Framework[1], OWASP Top 10 for LLM security[2], CISA's Secure AI guidance for critical infrastructure[3], and National Cyber Security Centre (NCSC) secure AI development code of practice implementation guidance[4]. While 'SBOM for AI' as a term is still emerging, the underlying principles are gaining traction and are actively being explored by initiatives like CISA's SBOM for AI Tiger Team.

Out of scope of SBOMs for AI

SBOMs for AI are not intended to capture every detail about an AI system. Just like traditional SBOMs, they do not include vulnerabilities, risk assessments, or mitigations. Their purpose is to provide a structured view of model or dataset metadata, while security analysis and risk scanning should be handled by separate tools.

This document focuses on the use cases for SBOMs for AI and does not cover implementation details, nor does it explore whether or how to incorporate additional data or capabilities beyond the core SBOM concept.

[1] https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf

[2] https://genai.owasp.org/resource/owasp-top-10-for-llm-applications-2025/

[3] https://www.dhs.gov/sites/default/files/2024-04/24_0426_dhs_ai-ci-safety-security-guidelines-508c.pdf

[4] https://assets.publishing.service.gov.uk/media/679cae441d14e76535afb630/Implementation_Guide_for_the_AI_Cyber_Security_Code_of_Practice.pdf

Detailed SBOM for AI Use Cases

Use Case 1: Compliance

Problem Statement

AI systems are complex, dynamic, and often opaque. Regulators, auditors, and other stakeholders are increasingly demanding greater transparency into how AI models are built, trained, and maintained. Compliance with SBOM and AI-specific regulations—such as the Federal Acquisition Regulation[5] (FAR), the EU AI Act[6], U.S. Food and Drug Administration (FDA) Guidance[7], and industry-specific guidelines (e.g., HHS ONC HTI-1[8] in healthcare—requires a clear, traceable record of every component used throughout AI development and deployment.

Without a comprehensive SBOM for AI, organizations face several challenges:

- **Limited Transparency** – Difficulty tracking the origin, purpose, and dependencies of AI components used in production systems.
- **Compliance Gaps** – Inability to demonstrate adherence to regulatory requirements related to accountability, explainability, and fairness.
- **Audit Complexity** – Responding to audits becomes a manual and time-consuming task due to the lack of structured AI documentation.
- **Regulatory Risk** – Non-compliance can lead to legal penalties, reputational damage, and operational disruptions.
- **Manual Overhead** – Tracing AI system components without automation consumes significant resources and expertise.

Benefits

SBOM for AI provides a structured, machine-readable inventory of AI components—enabling compliance, auditability, and operational control.

Key benefits include:

- **Compliance Assurance** – Demonstrates adherence to traceability, fairness, and transparency requirements across evolving regulatory frameworks.
- **Streamlined Audits** – Reduces time, effort, and cost in responding to regulatory and internal audits.

[5] https://www.federalregister.gov/documents/2023/10/03/2023-21328/federal-acquisition-regulation-cyber-threat-and-incident-reporting-and-information-sharing
[6] https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai
[7] https://www.fda.gov/medical-devices/software-medical-device-samd/transparency-machine-learning-enabled-medical-devices-guiding-principles
[8] https://www.healthit.gov/topic/laws-regulation-and-policy/health-data-technology-and-interoperability-certification-program

- **Improved Risk Management** – Helps identify non-compliant or unauthorized components before they enter production.
- **Efficiency Gains** – Supports automation of documentation, monitoring, and reporting workflows.
- **Trust and Accountability** – Builds confidence with regulators, partners, and customers through clear, verifiable records of AI system components.

Example Scenario

Scenario 1: Ensuring Compliance for AI-enabled Medical Wearable Devices

A medical technology company develops an AI-powered wearable device that monitors heart activity to detect early signs of arrhythmia. This device, classified as a medical device by the US Food and Drug Administration (FDA), must comply with the agency's stringent guidelines regarding software safety, efficacy, and security.

Software Validation and Verification

FDA regulations require rigorous validation and verification of software used in medical devices to ensure their safety and efficacy. By using an SBOM for AI, the company documents every software component, library, and model used in the device's AI system.

Regulatory Submissions and Documentation

For FDA approval, the company must submit comprehensive documentation, including details of the AI algorithms and software architecture of every component. While an SBOM for AI does not replace this documentation, it provides a machine-readable inventory of components, simplifying the regulatory submission process by supporting software traceability and ensuring visibility into dependencies and provenance.

The SBOM helps the company adhere to the FDA's Premarket Approval (PMA) or 510(k) pathways, providing information that allows the company to review the list of included components and ensure such components meet regulatory requirements..

Post-Market Surveillance and Updates

FDA regulations require ongoing monitoring and updates for medical devices after they are launched. If the AI-powered wearable device requires a software update (e.g.,to improve algorithm performance or address a vulnerability), the SBOM for AI ensures that the changes are clearly documented and that the updated components remain compliant with FDA regulations.

Third-Party Vendor Compliance

The wearable device uses third-party components and libraries for its AI functions. The SBOM for AI makes it possible to check third-party AI software used for compliance with FDA regulations, and the company can verify that its suppliers are following best practices for medical device software security and quality.

Outcome

By ensuring that the elements in the SBOM for AI meet the appropriate compliance requirements, a company can confidently demonstrate to the FDA that the AI-powered wearable device aligns with regulatory standards for software safety, security, and efficacy. This transparency can streamline the approval process, reduce associated costs, and support patient safety by enabling effective processes for identifying and managing risks related to AI components.

Use Case 2: Vulnerability and Incident Management

Problem Statement

The rapid integration of AI into organizational workflows has introduced new risks, particularly in managing security vulnerabilities tied to AI models and datasets. Risk teams, IT departments, and cybersecurity professionals must rapidly assess and respond to issues within AI systems. However, traditional workflows for vulnerability management often fail to address AI-specific challenges, leading to gaps in visibility and traceability.

Traditional vulnerability management relies on databases of known vulnerabilities and software identifiers to detect threats and associate them with affected components. In contrast, vulnerabilities in AI systems are often more complex and may arise from issues within AI models, the datasets used to train them, or the context in which they operate. Factors such as bias, ethical considerations, or safety concerns are not captured by the traditional frameworks used for software vulnerabilities, further complicating AI-specific risk management.

To address these challenges, organizations must first establish a **comprehensive inventory of AI models, datasets, and dependencies**, and **map them to applications, services, and business processes**. This foundational mapping supports risk prioritization and provides the operational context needed for effective response.

The **LAION-5B incident of December 2023** illustrates these challenges clearly. When a widely used dataset—used to train models like Stable Diffusion—was found to contain thousands of instances of CSAM (child sexual abuse material), organizations worldwide were left scrambling to answer critical questions:

- Have any of our models been trained on this dataset?
- Are we using Stable Diffusion or any derivatives in production?
- What business services or customer-facing products might be affected?

Answering these questions requires more than ad hoc documentation. It demands a **standardized, machine-readable representation of AI system components**—one that can be used to **aggregate, track, and operationalize metadata** across the AI lifecycle. This is where the concept of an **AI Software Bill of Materials (SBOM for AI)** becomes essential.

Benefits

- **Faster Incident Response** – SBOM for AIs make it easier to identify which models or datasets are affected during an incident, enabling quicker containment and remediation.
- **Clear Asset Inventory** – By maintaining a machine-readable inventory of AI components and their relationships to business systems, organizations gain critical visibility needed for efficient risk triage.

- **Proactive Risk Management** – Up-to-date SBOMs support proactive scanning and monitoring of AI dependencies, helping to identify and mitigate potential risks in the AI lifecycle before they escalate.
- **Improved Transparency and Accountability** – SBOM for AIs enhance visibility across teams and stakeholders, supporting informed decision-making and compliance with internal governance practices.
- **Streamlined Collaboration** – The standardized, tool-agnostic format of SBOM for AIs allows seamless integration with existing cybersecurity tools and facilitates secure information sharing across teams or organizations.

Example Scenario

Scenario 1: A Different Approach to LAION-5B

Context

In December 2023, the LAION-5B dataset—one of the largest publicly available AI training datasets—was discovered to contain child sexual abuse material (CSAM). This dataset had been used to train popular AI models, including Stable Diffusion, which many organizations had incorporated into their products and services. The discovery led to widespread concern, as companies scrambled to determine whether their AI models were affected.

Organizations faced critical questions:

- *Have we trained any of our models on the compromised dataset?*
- *Do we use Stable Diffusion anywhere in our enterprise?*
- *Which business applications and services might be impacted?*

Without a structured SBOM for AI, answering these questions would require manual investigations, compilation of fragmented asset inventories, and reliance on documentation that may not be complete. This results in delayed response efforts and increased regulatory and reputational risks.

How an SBOM for AI and Automation Could Have Changed the Response:

1. Automated Impact Analysis: The SBOM for AI would have provided an automated, real-time inventory of all AI models and datasets used within the organization. Security teams could have instantly queried their SBOM for AI database to identify whether any AI assets had dependencies on LAION-5B or Stable Diffusion.

- **Immediate detection of affected models:** SBOM for AI metadata would have flagged models trained on LAION-5B, enabling instant risk assessment.
- **Dependency mapping:** SBOM for AI relationships would have traced the impact across derived models and applications, revealing where compromised AI outputs were being used.

2. Rapid Incident Containment: With SBOM for AI automation integrated into the organization's security stack, an incident response workflow could have been triggered as soon as the LAION-5B compromise was reported.

- **Automated alerts:** Security teams would have received instant notifications if affected AI models were deployed in production systems.
- **Access controls and quarantine:** AI models linked to LAION-5B could have been automatically flagged for removal or restricted from further deployment.
- **Audit trail for compliance:** SBOM for AI records would have provided a clear history of how and where the dataset was used, supporting legal and regulatory responses.

3. Coordinated Remediation and Recovery: Once affected AI assets were identified, response teams could have taken swift action to mitigate risks.

- **Retraining and validation:** Organizations could have systematically replaced compromised training data, retraining models using verified datasets.
- **Policy enforcement:** SBOM for AI policies could have been updated to prevent future usage of datasets flagged for security, ethical, or legal concerns.
- **Stakeholder communication:** Security, compliance, and business teams would have been automatically notified about remediation progress and risk mitigation strategies.

Outcome: A Faster, More Automated Response

By leveraging SBOM for AIs, organizations could have transformed their incident response to the LAION-5B crisis from a weeks-long manual effort into an automated, structured process. Instead of scrambling to map affected models and datasets, security teams would have had immediate visibility, enabling faster remediation and reducing operational and reputational risks.

Use Case 3: Assessing Risk in Open-Source Models & Datasets

Problem Statement

Organizations are increasingly incorporating open-source AI models and datasets to accelerate development and reduce costs. These assets, much like third-party software, become part of the organization’s supply chain and must be properly vetted and managed.

However, open-source models and datasets often lack transparency about their provenance, composition, licensing, and training data, introducing serious risks—including regulatory non-compliance, bias propagation, legal exposure, and supply chain vulnerabilities. **Current practices** such as manual documentation reviews, limited testing, and community-based reputation checks **are time-consuming, inconsistent, and fail to provide a complete picture**.

To effectively assess and manage these risks, organizations need a standardized, machine-readable way to capture and evaluate critical metadata. An SBOM for AI enables this by offering structured transparency into the origins, modifications, and risks associated with AI assets—empowering security, legal, and compliance teams to make informed decisions and strengthen trust in the AI ecosystem.

Benefits

- **Holistic Transparency** – Delivers structured insights into where AI models and datasets come from, how they were built, and what risks may be involved.
- **Better Risk Control** – Enables early detection of vulnerabilities, unauthorized components, or problematic licenses before models are used in production.
- **Streamlined Workflows** – Reduces manual review and improves consistency in assessments by integrating SBOM data into automated risk, security, and governance processes.
- **Simplified Compliance** – Supports alignment with regulatory frameworks and internal data governance policies by providing clear audit trails.
- **Stronger Stakeholder Confidence** – Demonstrates diligence in how open-source AI assets are evaluated, boosting trust across internal and external stakeholders.

Example Scenarios

Scenario 1: Preventing License Violations

A development team plans to integrate an open-source language model into its product. By consulting the SBOM for AI, the team discovers the model is trained on datasets with conflicting licenses that are incompatible with its product’s commercial use. The team opts to use a different model, avoiding potential legal disputes and product launch delays.

Scenario 2: Mitigating Supply Chain Risk

An AI developer intends to incorporate an open-source model into the developer's application. The SBOM for AI identifies the model's owner or author, which can then be used for trust analyses and model integrity checks to detect any tampering. Armed with this information, the developer decides to choose a different/more secure model, thereby preventing potential supply chain risk.

Scenario 3: Model Lineage and Model Provenance

A financial institution considers using an open-source model as a base for a credit scoring system. The SBOM for AI reveals the model's lineage—it is a fine-tuned version of another base model—and also its provenance, including the origin and development path of both models. This information highlights that the base model violates the institution's internal risk policies, preventing its adoption.

Use Case 4: Third-Party AI Risk Management

Problem Statement

Organizations increasingly embed third-party AI products and services into internal infrastructure and customer-facing applications. However, a lack of transparency into the underlying models, training datasets, and licensing terms exposes organizations to data privacy violations, regulatory non-compliance, security vulnerabilities, and ethical risks. Without comprehensive insight into these components, risk management becomes reactive and fragmented—leaving organizations exposed to liability and reputational harm.

Benefits

- **Comprehensive Visibility into AI Components** - SBOM for AIs reveal which models, datasets, and dependencies are embedded in third-party products—whether proprietary or open-source—including licensing and training context. This transparency is critical for aligning with internal policy and regulatory requirements.
- **Targeted Risk and Compliance Management** - Understanding what vendors use—and how—enables organizations to assess specific risks like bias, misuse of training data, or security flaws. SBOM for AIs help tailor mitigation strategies and support compliance with regulations like the EU AI Act and industry-specific standards.
- **Faster Incident Response** - When AI-related issues arise, SBOM for AIs help identify affected components quickly, enabling faster isolation, triage, and response to security, legal, or reputational risks.
- **Increased Vendor Accountability** - Requiring SBOM for AIs encourages vendors to maintain higher transparency and security standards. Detailed disclosures strengthen trust, reduce uncertainty, and support long-term, responsible partnerships.

Example Scenarios

Scenario 1: Healthcare Data Handling
A healthcare provider considers deploying an AI-driven diagnostic tool from a third-party vendor. Using the SBOM for AI, the provider identifies that the tool utilizes models trained on patient data from external sources with insufficient privacy controls. This insight prompts the provider to mandate stricter data governance and privacy assurances before deployment, avoiding potential HIPAA compliance issues.

Scenario 2: Financial Services and Bias Risk
A bank is evaluating a third-party AI solution for credit scoring and loan approvals. Reviewing the SBOM for AI, the bank discovers that the model training datasets lack diverse

demographic representation, potentially introducing bias. This finding leads the bank to require model retraining or select a different AI solution aligned with regulatory requirements and ethical standards.

Scenario 3: Vendor Dependency Management
An organization utilizes multiple AI-enabled services from various third-party providers. A security vulnerability is disclosed in a widely-used open-source language model. Leveraging the SBOM for AI, the organization quickly identifies all impacted third-party products, contacts relevant vendors, and applies mitigation strategies promptly, thereby significantly reducing potential exposure and business disruption.

Use Case 5: Intellectual Property & Legal Usage

Problem Statement

AI models often arrive at organizations with limited transparency about how they were trained, what data was used, and under which legal or ethical constraints they can be deployed. Without this visibility, organizations risk violating licensing agreements, regulatory mandates, or internal data governance policies—particularly when models are trained on proprietary data, personal information, or regulated datasets.

SBOM for AIs help mitigate these risks by offering a structured, machine-readable inventory of model lineage, provenance, licensing, and usage guidelines. This allows organizations to validate whether a model aligns with legal, contractual, and ethical standards—such as those defined by dataset licenses, model terms of use, and frameworks like the EU AI Act, GDPR, or sector-specific regulations.

Benefits

- **Legal Risk Mitigation** – Enables verification of dataset licenses, model usage rights, and training practices to reduce exposure to legal disputes and regulatory violations.
- **Policy Enforcement** – Supports admission control and governance workflows to prevent deployment of non-compliant or restricted models.
- **Informed Model Selection** – Provides transparency into data sources, licensing terms, and ethical restrictions to guide safer, compliant adoption decisions.
- **Oversight of Proprietary Content** – Enhances monitoring of models containing sensitive or proprietary data to protect intellectual property and ensure responsible use.
- **Regulatory Alignment** – Facilitates compliance with frameworks like the EU AI Act, GDPR, and industry-specific regulations by documenting relevant usage constraints and provenance.

Example Scenarios

Scenario 1: Unauthorized Training Data Usage

A financial institution plans to deploy an AI chatbot and needs to confirm whether the underlying LLM was trained using proprietary financial datasets. An SBOM for AI reveals that some training data sources are subject to restrictive licensing, prompting legal review before deployment.

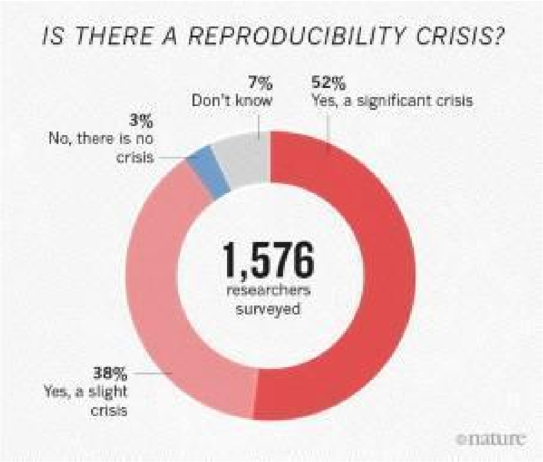
Scenario 2: Restricted Model Usage in High-Risk Domains

A government contractor is evaluating an AI model for cybersecurity threat detection. The SBOM for AI identifies that the model is governed by a responsible AI license prohibiting military applications. The contractor must seek an alternative model or negotiate licensing terms.

Use Case 6: Model Tracking, Reproducibility, and Lifecycle Management

Problem Statement

AI model development is inherently iterative, involving multiple rounds of experimentation with varying datasets, hyperparameters, and training methods. Without standardized documentation, organizations struggle to reproduce results, validate model performance, or track how models evolve over time. Traditional software tracking tools are not designed to capture the dynamic nature of AI experimentation.



An SBOM for AI provides a structured, machine-readable artifact that captures comprehensive metadata about data sources, model architecture, training procedures, tuning decisions, and computational environments. This enables accurate model tracking, supports reproducibility, and simplifies lifecycle oversight for audits and internal governance.

Benefits

- **Improved Reproducibility** – Captures detailed metadata that enables consistent replication of model experiments and faster validation cycles.
- **Transparent Model Development** – Provides a clear record of datasets, configurations, and training steps, supporting internal reviews and stakeholder confidence.
- **Lineage and Provenance Tracking** – Establishes traceable links across model versions, supporting audit readiness and regulatory compliance.
- **Streamlined Collaboration** – Centralizes model documentation in a standardized format, making it easier for teams to collaborate and transfer knowledge.
- **Lifecycle Oversight** – Enables continuous tracking of models from experimentation through deployment, supporting asset inventory and lifecycle management.

Example Scenarios

Scenario 1: Inconsistent Dataset Usage
A data science team discovers inconsistent outcomes due to slight variations in dataset versions used by different researchers. Without clear documentation, identifying the correct dataset version is challenging and may lead to confusion. By adopting an SBOM for AI, the team systematically records dataset versions and usage contexts. This ensures consistent use of datasets, clarity in data provenance, and accurate, reproducible results across experiments.

Scenario 2: Model Reproducibility Issues
An external validation team is unable to replicate published model results due to missing or incomplete details about training conditions and hyperparameters. Without comprehensive metadata, discrepancies remain unresolved, diminishing trust in the original findings. Implementing an SBOM for AI captures detailed records of hyperparameters, input data, training methodologies, and computational environments, enabling precise replication and strengthening confidence in the validity of the results.

Scenario 3: Environment Drift
A researcher faces difficulty reproducing results from previous experiments due to updates in software libraries and system dependencies, resulting in environment incompatibility. Without detailed environment documentation, reproducing exact conditions may be cumbersome and prone to error. SBOM for AI addresses this by automatically capturing detailed computational environment specifications, including library versions and hardware details, enabling consistent replication and eliminating drift-related discrepancies.

Key Recommendations

SBOM for AI plays a critical role in strengthening transparency, security, and compliance within AI ecosystems. As AI adoption expands, organizations must take a proactive approach to managing risks, ensuring governance, and meeting regulatory expectations. Successfully operationalizing SBOM for AI requires more than documentation—it demands integration into security, risk, and compliance processes and tools, as well as automation for scalability and efficiency.

To effectively implement SBOM for AI and maximize its impact, organizations should focus on the following key areas:

1. SBOM for AI Interoperability

Ensuring SBOM for AI aligns with industry standards and can be seamlessly adopted across different sectors is key to its success. Organizations should:

- Adopt widely accepted formats for SBOM for AI such as SPDX and CycloneDX to ensure interoperability and regulatory compliance.
- Collaborate across industries to refine SBOM for AI specifications and avoid fragmentation.
- Engage with regulatory and standards bodies to shape SBOM for AI expectations in emerging laws and compliance frameworks.

2. Transparency and Reporting

SBOM for AI provides a clear, machine-readable inventory of AI components, models, datasets, and dependencies to enhance risk assessment, compliance, and accountability. Organizations should:

- Maintain an enterprise-wide inventory of models, datasets, and dependencies, including lineage, provenance, licensing, and training context.
- Leverage SBOM for AIs as a foundation for standardized model cards to support governance, documentation, and internal transparency.
- Include SBOM for AIs for open-source components to surface legal and security risks early in the adoption lifecycle.
- Use SBOM for AIs to support regulatory audits and internal risk assessments with verifiable, machine-readable artifacts.

3. Integration into Security Processes

AI should not be integrated into an organization's business processes without also including SBOM for AI as an integral part of security workflows, ensuring incident response, risk management, and continuous monitoring for AI systems. Organizations should:

- Embed SBOM for AI into incident response workflows to accelerate impact assessments during AI-related security events.

- Integrate SBOM for AIs into vulnerability and risk management pipelines to proactively detect issues across model dependencies.
- Automate SBOM for AI generation and monitoring to ensure real-time visibility and reduce manual effort.
- Adopt a crawl/walk/run approach—begin implementation with available metadata and expand coverage over time, building organizational maturity without delay.

Looking Ahead

Operationalizing SBOM for AI is not just a compliance exercise—it is an opportunity to strengthen AI resilience, enable responsible innovation, and build trust across AI ecosystems. By extending and integrating SBOM for AI into core security and governance strategies, organizations can future-proof their AI deployments while staying ahead of regulatory and industry shifts.

As AI systems evolve, scaling SBOM for AI adoption across industries will be crucial. Organizations that lead in transparency, security, and automation will be better positioned to navigate AI risks, meet compliance mandates, and drive responsible AI innovation.

Appendix A – SBOM for AI Glossary and Terminology

The SBOM for AI Use Cases White Paper is intended for readers from diverse backgrounds and disciplines. To ensure clarity and consistency, this glossary defines key terms that may have varying interpretations across different fields, providing a common reference point for understanding SBOM for AI concepts.

For general cybersecurity terms, readers should consult established references such as NIST SP 800-53 Rev. 5; this glossary does not attempt to redefine well-established cybersecurity terminology.

Term	**Definition**
AI System	**From 15 USC 9401(3)(e):** Any data system, software, hardware, application, tool, or utility that operates in whole or in part using AI. **From EU AI Act (2024/1689) Article 3:** A machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.
Artificial Intelligence (AI)	**From 15 USC 9401(3)(b):** A machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. AI systems use machine and human-based inputs to: (A) perceive real and virtual environments; (B) abstract such perceptions into models through analysis in an automated manner; (C) use model inference to formulate options for information or action. **Commentary:** The SBOM for AI project focuses specifically on statistical machine learning systems. These generate and use statistical models based on large quantities of training data (e.g., deep neural networks). SBOM for AI may also apply to other AI techniques such as planning, logic, and optimization. **Alternative Definitions:** ISO/IEC 22989:2022 - A technical and scientific field devoted to the engineered system that generates outputs such as content, forecasts, recommendations, or decisions.

Term	Definition
Bias	**From OECD:** An effect which deprives a statistical result of representativeness by systematically distorting it, as distinct from a random error which may distort on any one occasion but balances out on average. **Commentary:** Bias can refer to datasets, models, or AI system outputs that unfairly advantage or disadvantage a group. It may be difficult to define unbiased data in different contexts. **Alternative Definitions:** Inductive Bias - The set of assumptions that a learning system uses to interpolate and extrapolate from training data.
Bill of Materials (BOM)	**Adapted from DHS-CISA SBOM FAQ:** A formal record containing details and supply chain relationships of various components used in building a system, including libraries, modules, models, training data, and knowledge sources.
HDO	Healthcare Delivery Organization (such as Hospital or Clinic).
Machine Learning	**From 15 USC 9401(11):** An application of artificial intelligence that provides systems with the ability to automatically learn and improve on the basis of data or experience, without being explicitly programmed.
Model lineage	Tracks the full chain of derivation — how the model has been modified, fine-tuned, retrained, or otherwise transformed over time, including its dependencies on other models. Consider this as a model's "family tree" or evolution over time.
Model provenance	Refers to the origin and history of the model itself — who created it, when, under what conditions, with what datasets and licenses. Consider this as a model's "birth certificate."
Policy	In SBOM for AI, policy refers to the rules, guidelines, and best practices governing the behavior of an organization and its AI-related activities. The policy may or may not be codified. **Alternative Definitions:** Management Policy - Rules that govern an organization's behavior. IT Policy - Rules for accessing and using IT resources. ML/AI

Term	Definition
	System Policy - Strategies defining an agent’s decision-making process.
Vulnerability	**From NIST SP 800-53 Rev. 5:** A weakness in an information system, security procedures, internal controls, or implementation that could be exploited by a threat source.

Appendix B – Acknowledgments

This document was a community-driven effort, developed with the contributions of experts from both the public and private sectors who volunteered their time and expertise outside of their normal responsibilities to plan, draft, and refine this guidance.

The SBOM for AI Tiger Team was led by Helen Oakley, Daniel Bardenstein, and Dmitry Raidman, whose leadership, vision, and coordination were instrumental in shaping the content and direction of this work. We also acknowledge the valuable participation of working group members who brought deep experience in application security, software supply chain, AI governance, and tooling implementation.

Special thanks to our colleagues at CISA, and in particular to Allan Friedman, for his continuous support and guidance in bringing the community together and advancing the broader mission of software and AI transparency.

Participation in this initiative and inclusion in these acknowledgments do not imply endorsement of the document's content or conclusions.

Contributors & Reviewers

First Name	Last Name	Association / Organization
Helen	Oakley	SAP
Daniel	Bardenstein	Manifest
Dmitry	Raidman	Cybeats
Ed	Heierman	Abbott
John	Cavanaugh	ProCap360
Anant	Shrivastava	Cyfinoid Research
Gaurav	Srivastava	Siemens
Girish	Jorapurkar	Splunk
Allan	Friedman	CISA
Divjot	Bawa	CISA
Bob	Martin	MITRE
Anthony	Harrison	APH10
Jeremiah	Stoddard	INL
Claude	Baudoin	Object Management Group
Syed 'Z'	Hosain	Aeris Communications, Inc.
John D.	Nuckles	ODNI

Yotam	Perkal	Zscaler
Tom	Jacobson	DHS
Raymond	Sheh	Johns Hopkins and NIST
Marek	Grac	Red Hat
Brindusa	Curcaneanu	NeuroPace
Bertrum	Carroll	EMPLOYERS Insurance
James	Tramel	Finwilma
Elyas	Rashno	Queen's University
Cassie	Crossley	Schneider Electric
Arthit	Suriyawongkul	ADAPT Centre, Trinity College Dublin
Victor	Lu	Independent

Appendix C – History of Changes

March 31st, 2025: Initial Draft version 0.1

May 21st, 2025: Updated Draft version 0.2

June 23rd, 2025: Final Draft version 0.3