AMENDMENT TO RULES COMM. PRINT 119–33
OFFERED BY MS. BYNUM OF OREGON

At the end of subtitle B of title XV, insert the following new section:

SEC. 15___. ARTIFICIAL INTELLIGENCE FUNCTIONAL BILL OF MATERIALS.

(a) ARTIFICIAL INTELLIGENCE FUNCTIONAL BILL OF MATERIALS.—The Secretary of Defense, in coordination with the Under Secretary of Defense for Research and Engineering, the Under Secretary of Defense for Acquisition and Sustainment, the Chief Digital and Artificial Intelligence Officer, and the Chief Information Officer shall revise the Department of Defense Supplement to the Federal Acquisition Regulation to prohibit the Department of Defense from entering into, renewing, or extending a contract for the procurement of goods or services that utilize artificial intelligence, unless the contractor—

(1) submits to the Chief Digital and Artificial Intelligence Officer an artificial intelligence functional bill of materials prior to the award, renewal, or extension of the contract; and

(2) maintains the bill of materials such that the contractor can deliver an updated bill of materials to

the relevant component of the Department of Defense within 48 hours of a request for such bill of materials.

(b) FORMAT AND CONTENTS OF ARTIFICIAL INTELLIGENCE FUNCTIONAL BILL OF MATERIALS.—

(1) IN GENERAL.—A functional bill of materials described under subsection (a) shall—

(A) include details related to the software, data, and hardware underpinning systems utilizing artificial intelligence in accordance with paragraphs (2), (3) and (4) of this subsection;

(B) be machine-readable; and

(C) disclose sufficient detail to enable a timely assessment by the Department of Defense of the impact of—

(i) newly identified vulnerabilities;

(ii) security risks;

(iii) integrity concerns affecting software, models, or data; and

(iv) other newly available risk-relevant information affecting components incorporated into or relied upon by the artificial intelligence system.

(2) MINIMUM REQUIREMENTS FOR SOFTWARE SECTION OF ARTIFICIAL INTELLIGENCE FUNC-

TIONAL BILL OF MATERIALS.—The software section of the artificial intelligence functional bill of materials required under subsection (a) shall include the following minimum elements:

(A) A description of all models of the artificial intelligence, including—

(i) pre-trained foundation models;

(ii) fine-tuned models customized for specific Department of Defense use cases through transfer learning or additional training;

(iii) internally trained models, including custom architectures and algorithms for the Department of Defense;

(iv) other model versions and configurations deployed in production, along with their hyperparameters and deployment context; and

(v) for each model described in clauses (i) through (iv)—

(I) the model name;

(II) the model identifiers;

(III) the model version or release identifier;

(IV) the model supplier;

(V) the model origin;

(VI) the model lineage;

(VII) the model license;

(VIII) the integrity reference;

(IX) a description of any self-hosted or custom models across containers or virtual machines;

(X) any model source registries and versions; and

(XI) a description of artificial intelligence agents and their functional boundaries (abilities to read, write, and execute).

(B) A description of the dependencies of the artificial intelligence, including—

(i) the machine-learning frameworks used to build and run the artificial intelligence;

(ii) the developer-level artificial intelligence technologies and software development kits, including integrated development environment extensions;

(iii) any third-party packages, including supporting libraries and open-source

components that models of the artificial intelligence depend on;

(iv) the runtime dependencies necessary for training, serving, or orchestrating artificial intelligence models in production; and

(v) any direct and nested transitive relationships.

(C) The security and governance of the artificial intelligence, including—

(i) identity verification and access, including service accounts, roles, permissions, and credentials the artificial intelligence system uses;

(ii) access paths, including external application programming interfaces;

(iii) security controls, such as policies, classifiers, and validation mechanisms that apply to the artificial intelligence components;

(iv) guardrail safety configurations and filters; and

(v) model context protocol server tool configurations.

(D) Any access history and permissions granted by the artificial intelligence, including—

(i) a description of the ownership of and access to the artificial intelligence system by the Department of Defense;

(ii) the change history, including audit trails that show who modified components, when, and why; and

(iii) a description of the approval workflows, including processes that govern how artificial intelligence components move through development, testing, and production.

(E) The performance metrics and model updates, including—

(i) use cases, prioritizing high-impact use cases; and

(ii) performance metrics, such as accuracy and latency.

(3) DATA SECTION OF ARTIFICIAL INTELLIGENCE BILL OF MATERIALS.—The data section of the artificial intelligence functional bill of materials required under subsection (a) shall include the following minimum elements:

(A) The training data, including datasets used to train or fine-tune models of the artificial intelligence, including their origin, licensing, and any applied preprocessing.

(B) The inference-time data, such as data sources any model of the artificial intelligence accessed during production, including real-time APIs, feature stores, or data warehouses.

(C) Data storage, including the underlying storage systems, such as cloud storage, databases, or vector databases, that hold artificial intelligence-related data.

(D) Metadata on components' name, precise version, file paths, open-source licenses, package managers, and unique identifiers such as purl or cryptographic hashes.

(E) For each dataset described in subparagraphs (A) through (D)—

(i) the dataset name;

(ii) the dataset version or date of creation or last update, whichever is more recent;

(iii) the dataset location;

(iv) the integrity reference;

(v) the sensitivity of the data;

(vi) the license to use such data;

(vii) the data supplier;

(viii) the creator of the data contained in the dataset;

(ix) the data origin;

(x) the data lineage;

(xi) the country of origin; and

(xii) the data processing history.

(4) HARDWARE SECTION OF ARTIFICIAL INTELLIGENCE FUNCTIONAL BILL OF MATERIALS.—The hardware section of the artificial intelligence functional bill of materials required under subsection (a) shall include relevant information of the physical infrastructure that the artificial intelligence runs on, including the following minimum elements:

(A) Compute resources, including graphics processing units, tensor processing units, and other acceleration hardware artificial intelligence workloads use.

(B) Any storage and networking that supports the artificial intelligence, including the cloud infrastructure supporting artificial intelligence operations and other network paths between components.

(C) Cloud environments, including accounts, regions, and deployment boundaries on which artificial intelligence workloads run.

(c) APPLICABILITY OF SOFTWARE BILL OF MATERIALS REQUIREMENTS TO ARTIFICIAL INTELLIGENCE.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Defense, in coordination with the Under Secretary of Defense for Research and Engineering, the Under Secretary of Defense for Acquisition and Sustainment, the Chief Digital and Artificial Intelligence Officer, and the Chief Information Officer shall develop regulations, guidance, and policies to ensure that current policies, regulations, and guidance relating to the use, submission, or maintenance of a software bill of materials shall apply to the software that underpins artificial intelligence systems used, developed, or procured by the Department of Defense.

(2) REPORT.—Not later than one year after the date of the enactment of this Act, the Secretary of Defense shall submit to the Committee on Armed Services of the Senate and the Committee on Armed Services of the House of Representatives a report on—

(A) the status of the implementation of the regulations, guidance, and policies developed under paragraph (1), including any challenges, recommendations, and legislative or regulatory action needed to enhance the effectiveness of such implementation;

(B) the feasibility and necessity of updating Department of Defense Instruction 5000.87, Operation of the Software Acquisition Pathway (October 2, 2020) and the software acquisition pathway established under section 3603 of title 10, United States Code, with requirements for—

(i) an artificial intelligence software bill of materials; and

(ii) a more detailed software bill of materials in the procurement of software, hardware, artificial intelligence technologies, and cryptographic technologies; and

(C) the estimated costs of implementing the requirements described in subparagraph (B).

(d) CYBERSECURITY CONSIDERATIONS FOR BILL OF MATERIALS.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Director of the Defense Systems Agency and Chief Information Officer shall issue guidance on to procuring agencies on appropriate storage of any bill of material submitted under subsection (a) to align with the cybersecurity requirements of the Department of Defense.

(2) CONTENTS.—The guidance issued under paragraph (1) shall include—

(A) strict access controls;

(B) digital signing and hashing;

(C) secure sharing mechanisms; and

(D) centralized repositories to prevent tampering and unauthorized access.

(e) DEFINITIONS.—In this section:

(1) ARTIFICIAL INTELLIGENCE.—The term ''artificial intelligence'' has the meaning given such term in section 5001 of the National Artificial Intelligence Initiative Act of 2020 (15 U.S.C. 9401).

(2) SOFTWARE BILL OF MATERIALS.—The term ''software bill of materials'' means the records kept in the normal course of business that identify each

component, library, and dependency comprising a software application.

☒