Comments of the SBOM Special Interest Group (SIG)

The SBOM SIG members, listed below, wish to thank the National Institute of Standards and Technology (NIST) for the opportunity to file these comments in response to the Workshop and Call for Position Papers on Standards and Guidelines to Enhance Software Supply Chain Security, related to the May 12 Software Supply Chain Executive Order[3]. Information provided by the NCSC succinctly summarizes the real risks emanating from the Software supply chain [4][5]: “adversaries exploit supply chain vulnerabilities to steal America’s intellectual property, corrupt our software, surveil our critical infrastructure, and carry out other malicious activities. They infiltrate trusted suppliers and vendors to target equipment, systems, and information used every day by the government, businesses, and individuals.“ These comments are being provided to aid NIST in achieving its stated goals for the workshop, through the comments provided below, describing the critical role SBOM serves in addressing software supply chain risks [1][2][3][4][5][8][10][11]:

SBOM SIG members request that NIST, in their Executive Order deliverables, consider including the following items:

1. Explicitly include support for CycloneDX and SPDX SBOM formats
2. Recommend software supplier integrity verification of both SBOM data and Software provided to consumers, based on Supplier information contained in a vendor supplied SBOM, in accordance with NIST SP 800-161 *SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY* guidelines
3. Recommend that operators of vulnerability repositories prepare for an SBOM enabled world by supporting vulnerability searches based on SBOM data, in addition to existing practices, e.g. CPE and keyword search
4. Recommend that software vendors to the federal government supply SBOM’s in either SPDX or CycloneDX SBOM formats and recommend that government agencies use this vendor supplied SBOM data to proactively identify cybersecurity risks and support mitigating action.

The SBOM SIG thanks NIST for considering these comments and looks forward to collaborating with NIST, under NIST’s direction and guidance, to achieve the defined goals for this workshop and the development of supporting supply chain best practices to meet the goals and objectives contained in the Software Supply Chain Executive Order.

Respectfully submitted by SBOM SIG Members,

SBOM Special Interest Group (SIG) Members

SBOM SIG members do not represent NTIA nor any NTIA working group. All members are independent parties with one common objective, support for SBOM as a best practice for software supply chain risk management.

Name	Company Name
Cole Kennedy	BoxBoat Technologies LLC
Dick Brooks	Reliable Energy Analytics LLC
Frederick Kautz	Sharecare, SPIFFE Steering Committee
JC Herz	Ion Channel
Gareth Rushgrove	Snyk
Rich Steenwyk	Johnson Controls, Plc
Kate Stewart	Linux Foundation
Tony Turner	Fortress Information Security
Lila Kee	GMO GlobalSign Inc.
Steve Springett	Open Web Application Security Project (OWASP)

Proposed Speakers

Name	Title	Contact Information
Frederick Kautz	Director of Software Engineering, Sharecare	frederick.kautziv@sharecare.com frederick@kautz.dev
Cole Kennedy	Director Defense Initiatives	cole@boxboat.com