This position paper is being sent in response to the National Institute of Standards and Technology (NIST) Workshop and Call for Position Papers on Standards and Guidelines to Enhance Software Supply Chain Security[1] to help NIST fulfill Executive Order (EO) on Improving the Cybersecurity of the Federal Government (14028) [2]. I applaud both the workshop and the EO and have great confidence in NIST's ability to fulfill its mission in the area of supply chain security. I unfortunately will be unable to attend the workshop, but I would like NIST to consider my views as an individual citizen with expertise in this field. The views expressed are my own and do not represent any organizations I participate in nor any of my clients or previous employers.

This paper addresses my positions on area 2: "*Initial list of secure software development lifecycle(SDLC) standards, best practices, and other guidelines*". I have participated in national and international standards efforts for over 40 years and I would request NIST to move quickly in the area of supply chain security and take a more agile and iterative approach than is typically taken in standards. I believe stressing evolving best practices and encouraging innovation is needed as opposed to 'picking a winner'. Let's make data driven decisions, which requires that get we started with something so that we'll be dealing with data from actual use. Having said that, there are many existing best practices and standards with which to get started. I recommend NIST develop best practices for making use of:

1. All the work being done in the NTIA Open and Transparent Process on Software Component Transparency [3,4]. I.e. to meet EO paragraph 4.e.i.F.vii , use all of NTIA's work, not just the minimum element work called out in EO paragraph 4.f.
    a. In particular, encourage/allow the use of CycloneDX[5] and SPDX[6] in addition to the existing NIST SWID format. Significant innovation has occurred in the last 3 years on all SBOM formats, at least partially spurred by competition between these formats. As they are easily converted between, IMHO all 3 formats should be allowed and encouraged.
2. OASIS Structured Threat Information Expression (STIX™)[7]
3. OASIS Collaborative Automated Course of Action Operations (CACAO) Playbooks[8]
4. OASIS Open Command and Control (OpenC2) [9]
5. Industry best practices in the area of quantitative risk analysis such as the work by Hubbard/Seiersen[10] and/or the FAIR Institute[11]
6. The DIE Triad[12]
7. Integrated Adaptive Cyber Defense (IACD)[13]

Best practices around STIX, CACAO, and OpenC2 may appear at first glance to not be "*within the scope of the assignments specified by the EO*". However, to meet the EO objectives will require vendor-agnostic, machine-speed cyber-defense automation as proposed by IACD, and it will require that automation through the entire supply chain. I.e. the best practices for SDLC will need to extend beyond what is typically considered SDLC to include the cybersecurity controls of the supplier.

To meet the goals of the EO will require adoption of these best practices beyond the borders of the US. I recommend NIST take a more active role in international standards bodies to gain awareness and adoption of NIST efforts in supply chain security. In particular, NIST should regularly participate and provide their expertise to ITU-T SG17 (Cybersecurity) as well as aid ITU-D with cybersecurity capacity development for developing countries (in coordination with the US State Department and USAID).

Thank you for the opportunity to input into the process.

Respectfully,
Duncan Sparrell
CISSP, CSSLP, CCSK
https://www.linkedin.com/in/duncan-sparrell-cissp-csslp-ccsk-038137/

Footnote References:

[1] Workshop and Call for Position Papers on Standards and Guidelines to Enhance Software Supply Chain Security, May 18, 2021, https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/workshop-and-call-position-papers
[2] Executive Order 14028, Improving the Nation's Cybersecurity, May 12, 2021, https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity
[3] NTIA Open and Transparent Process on Software Component Transparency, May 23, 2021 https://www.ntia.gov/SoftwareTransparency
[4] Software Bill of Materials, May 23, 2021 https://www.ntia.gov/sbom
[5] CycloneDX, May 23, 2021 https://cyclonedx.org/tool-center/
[6] SPDX, May 23, 2021 https://github.com/spdx/tools
[7] Structured Threat Information Expression (STIX™) https://www.oasis-open.org/2021/02/01/stix-version-2-1-from-cti-tc-approved-as-a-committee-specification-2/
[8] OASIS Collaborative Automated Course of Action Operations (CACAO) Playbooks https://docs.oasis-open.org/cacao/security-playbooks/v1.0/security-playbooks-v1.0.html
[9] Open Command and Control (OpenC2), https://openc2.org/
[10] How to Measure Anything in Cybersecurity Risk by Hubbard, Seiersen, https://books.google.com/books?id=AwD0BgAAQBAJ
[11] The FAIR Institute https://www.fairinstitute.org/
[12] The DIE Triad (Distributed, Immutable, Ephemeral) https://www.rsaconference.com/Library/presentation/USA/2021/death-to-cia-long-live-die-how-the-die-triad-helps-us-achieve-resiliency
[13] Integrated Adaptive Cyber Defense https://www.iacdautomate.org/