NIST Call for Papers on Executive Order 14028 – Position Paper on Area 5, Section 4(e)(vi) - Guidelines for software integrity chains and provenance.

Stuart Phillips - sphillips@interos.ai
Product Marketing Director at Interos (willing to speak)
Kate Stewart - kstewart@linuxfoundation.org
VP, Dependable Embedded Systems at the Linux Foundation

NIST Request - Focus Area - *Guidelines for software integrity chains and provenance*. See EO Sections 4(e)(vi).

Position – Use Software bill of materials (SBOM) information to proactively map, monitor, and model the software supply chain (software code or components, and controls on internal and third-party software components, tools, and services present in software development processes). This effort will reduce the cybersecurity, governance, and resilience risks of the organization and will provide a method maintaining accurate and up-to-date data, provenance (i.e., origin) of the software supply chain, and performing audits and enforcement of these controls repeatedly;

Mapping the Software Supply Chain with SBOM

The SBOM contains the Supplier name of the object, as well as other information. It is an excellent resource to leverage when mapping the software supply chain, and organizations should use this information to create a multi-dimensional map.

- The organization should export this information into a trackable database or electronic list using automated methods like creating an .XLS, .JSON or .XML file using SPDX format. At least one of the recognized SBOM formats (SWID, SPDX, CycloneDX) from NTIA's SBOM multistakeholder framing guidance should be used
- This database or list should be updated as the software supply chain changes
- The organization should implement controls to confirm the provenance of the internal and third-party software components, tools, and services through other means, such as online research or direct contact with the supplier
- The organization will then create unique identifiers for each supplier with details, geographic location, contact information, and geographic location added to the database
- This database would include embedded suppliers on multiple levels and relationships.
    - Various suppliers will have numerous interconnections within the software supply chain
    - For example, Company A uses software from Company B who then sells it back to Company A as a new product. Visually map the multi-dimensional aspect if possible.

Monitoring the Software Supply Chain with SBOM

Organizations should use tools to track events affecting the software supply chain. Open projects like Community Health Analytics Open Source Software (CHAOSS) focuses on creating analytics and

metrics to help define open-source software community health and identify risk factors. Many commercial projects that track supplier risk or the organization could create their tools as long as at least one of these tools can track events within their software supply chain and affect this party risk.

Organizations benefit from tracking events in areas other than just cybersecurity. For example, Synopsys software estimates that ninety-one percent of codebases contained components that either was more than four years out of date or had no development activity in the past two years.

Example of possible Risk factors;

- Cybersecurity
  - Cybersecurity risk includes both uncovered vulnerabilities within a software component and also attacks that affect the supplier itself.
- Regulatory
  - Regulatory risk refers to factors that can affect the relationship with a supplier, such as sanctions, prohibited supplier country lists, commerce, and national security.
- Operations
  - Operations risk is related to natural disasters, weather-related disruption propensity, transportation, and infrastructure capacity issues.
- Geographic
  - Geographic risk relates to socio-economic development levels, the rule of law, political stability, war/unrest, and concentration.
- Financial
  - Financial risk factors are related to solvency, valuation, and profitability. This concern the ability of a supplier to continue its operations and provide updates if needed.
- Environmental, Social, and Governance (ESG)
  - ESG risk refers to uncovering and removing suppliers because of sustainability, environmental impact, diversity, unethical labor practices, and other social concerns.

Tracking risk factor events to internal and third-party software components, tools, and services allow the organization to rate them by risk and be aware of possible exposure to the software supply chain resilience.

Modeling the Software Supply Chain with SBOM

Organizations should leverage the SBOM maps to model their entire software supply chain regularly. The model is a valid supply chain representation either in whole or a section, such as “show us all our suppliers in Africa.” Making proactive changes to reduce future risks is the goal of modeling.

This exercise will allow an organization to understand correlating risk factors such as a high concentration of geographic location by suppliers. Awareness of the software supply chain model enables an organization to make proactive changes such as selecting new vendors in a different area because of this uncovered existing geographic concentration risk.

Modeling also allows what-if-type exercises. This exercise enables an organization to discuss changes to the software supply chain ecosystem, either a single action such as removing a high-risk supplier or more strategic such as transitioning from offshore to onshore. What-if excesses uncover the scope of effort, potential roadblock, and other factors when making these strategic changes.