STATEMENT:

The National Society of Professional Engineers believes that policymakers and regulatory bodies should work in tandem with the engineering community to establish comprehensive regulations and policies that promote software supply chain security. These regulations should encourage transparency, accountability, and continuous improvement.

Discussion

NSPE recognizes the paramount importance of securing the software supply chain in our increasingly interconnected world. Engineers play a pivotal role in enhancing the resilience and security of software systems critical to our society. By upholding ethical standards, promoting best practices, and collaborating with stakeholders, we can collectively work towards a more secure and robust software supply chain, ultimately ensuring the safety and well-being of the public.

1. Essential Infrastructure:

Software is a critical component of our nation's infrastructure, impacting everything from healthcare and transportation to energy and communication systems. The security and integrity of the software supply chain are paramount to protect public safety and national security.

2. Ethical Responsibility:

Engineers have an ethical responsibility to prioritize the security of the software supply chain. This includes designing, developing, and maintaining software systems with a strong emphasis on security, and promoting the use of best practices to safeguard against vulnerabilities and threats.

3. Collaboration and Best Practices:

NSPE encourages collaboration among software engineers, developers, security experts, and policymakers to establish and promote best practices for secure software development and supply chain management. Industry standards and guidelines should be developed and updated to reflect evolving cybersecurity threats.
4. **Risk Assessment and Mitigation:**

Engineers should conduct thorough risk assessments throughout the software supply chain to identify vulnerabilities and potential threats. Mitigation strategies, including regular security updates and patches, should be implemented to address these risks.

5. **Supply Chain Transparency:**

Transparency within the software supply chain is essential. Organizations should strive for transparency in their sourcing of software components and dependencies. This includes understanding the origins of software components, monitoring for vulnerabilities, and ensuring timely updates.

6. **Secure Development Lifecycle:**

NSPE advocates for the adoption of secure development lifecycles in the software industry. Engineers and software developers should integrate security considerations into every phase of the software development process, from design and coding to testing and deployment.

7. **Continuous Education and Training:**

To address the evolving nature of cybersecurity threats, NSPE supports ongoing education and training for engineers and software professionals. These programs should emphasize cybersecurity best practices and emerging threats to ensure that professionals remain current in their knowledge and skills.

8. **Software Professional Certification**

NSPE maintains that individuals engaged in securing the software supply chain should be held to a professional standard. At a minimum, these individuals should hold a certification that addresses the items discussed in this position statement. Certification ensures that those working on software systems possess the necessary qualifications, experience, and commitment to uphold the public's well-being.