

Executive Order 14306

And Its Impacts On Software Supply Chain Management

Adam A. Bartolanzo | SW Supply Chain Day | November 12, 2025



Meet Today's Presenter



Adam A. Bartolanzo, Principal
Miles & Stockbridge
Government Contracts
abartolanzo@milesstockbridge.com
(202) 465-8388

A Shifting Landscape?



Agenda

- Background
- Impacts to Secure Software Development Framework Compliance
- Impacts to Artificial Intelligence
- Impacts to Cyber Threat Defense
- Other Changes
- What Hasn't Changed?
- Takeaways

Background

- Executive Order No. 13694, Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities (Apr. 1, 2015)
- Executive Order No. 14144, Strengthening and Promoting Innovation in the Nation's Cybersecurity (Jan. 16, 2025)
- Executive Order No. 14306, Sustaining Select Efforts to Strengthen the Nation's Cybersecurity and Amending Executive Order 13694 and Executive Order 14144 (June 6, 2025)

Impacts to SSDF Compliance

▣ Removed:

- ▣ Attestations of compliance with the SSDF

▣ But NIST SP 800-218 remains the benchmark

- ▣ EO requires NIST to develop and publish a preliminary update to the SSDF by **December 1, 2025**
- ▣ EO retains directive for NIST to establish a consortium with industry at the National Cybersecurity Center of Excellence to develop guidance updates

Impacts to Artificial Intelligence

❑ Removed:

- ❑ Directives prioritizing use of AI for development of cyber defense

❑ Retains:

- ❑ Information sharing on existing cyber defense research
- ❑ Interagency coordination for management of AI software vulnerability



Impacts to Cyber Threat Defense

- Major cyber threat actors identified by name:

- **CHINA**
- Russia
- Iran
- North Korea



Other Changes

- ▢ Scales back requirements for OMB to issue guidance to address critical risks and adapt modern practices and architecture across federal information systems and networks
- ▢ Requires establishment of a pilot program of a rules-as-code approach for machine-readable versions of cyber-related policy and guidance
- ▢ Eliminates prior directives to accept digital identities for public benefits programs

Other Changes continued

- ❑ Removes preferences for and foreign collaboration on post-quantum cryptography
- ❑ Amends who may be sanctioned for malicious cyber-enabled activities originating from or directed outside the U.S.



What Hasn't Changed?

- ❑ “U.S. Cyber Trust Mark” for IoT Products
- ❑ Internet Traffic Security
- ❑ DNS Encryption
- ❑ Commercial Preferences
- ❑ EO 14028 or SBOMs
- ❑ NIST SP 800-171 or CMMC



❑ ***CMMC has begun and is here to stay!***

Takeaways

- Don't sideline the SSDF just yet!
 - Attestations may be out, but NIST SP 800-218 is not going away
- Expect industry to play a much greater role in establishing best practices for secure software development at the federal level
 - Shifting away from a Government top-down approach
- Track software requirements in solicitations closely
 - SBOMs as a condition for award and secure software development experience as an evaluation criterion are likely to pop up more frequently

Takeaways

- ▢ Monitor your software supply chain for potential cyber threats
 - ▢ Software components originating from any of the named cyber threat actors will be lightning rods to agency evaluators and procurement officials
- ▢ Keep up to date on all things cyber and emerging technologies
 - ▢ CMMC, AI, Quantum Computing – these are all happening **now!!!**



Thank You!



Adam A. Bartolanzo, Principal
Miles & Stockbridge
Government Contracts
abartolanzo@milesstockbridge.com
(202) 465-8388

Disclaimer

Miles & Stockbridge is an Am Law 200 law firm with more than 200 lawyers and offices in Maryland, Washington, D.C., Virginia and New York. The firm's lawyers help global, national, local and emerging business clients preserve and create value by helping them solve their most challenging problems.

The opinions expressed and any legal positions asserted in this presentation are those of the authors and do not necessarily reflect the opinions or positions of Miles & Stockbridge P.C. or its other lawyers. No part of this presentation may be reproduced or transmitted in any way without the written permission of the author. Images are subject to copyright. All rights reserved.



Miles & Stockbridge



Miles & Stockbridge



@mstockbridgelaw