Timeline of Executive Order 14028: Improving the Nation's Cybersecurity V2

Removing Barriers to Sharing Threat Information
Enhancing Software Supply Chain Security

Sec. 2. Removing Barriers to Sharing Threat Information

Secretary of Homeland Security
2(g)(i) Recommend to the FAR Council the contract language defining cyber incidents requiring reporting, the information that must be reported, National Security Systems reporting requirements, time periods, and the types of service providers covered

Director of OMB
2(b), 2(c) Recommend updates to contract language to ensure that IT and OT service providers collect, preserve, and share with agencies information and reporting relevant to cybersecurity event prevention, detection, response, and investigation

Director of CISA
2(i) Review current agency-specific cybersecurity requirements and recommend to the FAR Council standardized contract language

Director of the NSA, Attorney General, Secretary of Homeland Security, Director of National Intelligence
2(g)(iii) Jointly develop procedures for ensuring that cyber incident reports are promptly and appropriately shared among agencies

FAR Council
2(d) Preview contract language proposed by Director of OMB and publish proposed updates to the FAR for public comment

Secretary of Homeland Security and Director of OMB
2(e) Ensure that service providers share data with agencies, CISA, and the FBI as necessary to respond to cyber threats, incidents, and risks

FAR Council
2(j) Review recommended contract language from the Director of CISA and publish proposed updates to the FAR for public comment

FAR Council
2(g)(ii) Review recommendations on types of incidents and information required from Secretary of Homeland Security and publish proposed updates to the FAR for public comment

Sec. 4. Enhancing Software Supply Chain Security

Director of NIST
4(b) Solicit stakeholder input to identify existing or develop new standards, tools, and best practices for complying with the order

Director of NIST
4(g) Publish a definition of the term "critical software"

Director of NIST
4(i) Publish guidance outlining security measures for "critical software"

4(r) Publish guidelines for minimum standards for vendors' testing of their software source code

Secretary of Commerce
4(f) Publish the minimum elements for an SBOM

Director of CISA
4(h) List of software categories meeting the definition of "critical software"

Administrator of the Office of Electronic Government
4(j) Require that agencies comply with NIST guidance on security measures for "critical software"

Director of NIST
4(c) Publish preliminary guidelines based on consultations and on existing documents for enhancing software supply chain security

Director of NIST
4(e) Publish guidance on practices that enhance software supply chain security:
- secure software development environments
- tools to maintain trusted source code
- tools to check for and remediate vulnerabilities
- publicly available summary information demonstrating conformance
- accurate, up-to-date provenance of software and components
- SBOMs
- vulnerability disclosure program
- attesting to secure software development practices and the integrity and provenance of open source software

4(t) Identify IoT cybersecurity criteria for a consumer labeling program

4(u) Identify secure software development practices for a consumer software labeling program

Administrator of the Office of Electronic Government
4(k) Require that agencies comply with the NIST guidelines with respect to software procured after the date of this order

Director of NIST
4(d) Publish additional guidelines for enhancing software supply chain security as well as procedures for periodic updating

Secretary of Homeland Security
4(n) Recommend contract language to the FAR Council requiring software suppliers to comply with and attest to complying with the order

4(p) Following any final amendments to FAR, agencies shall remove software products that do not meet the requirements

Administrator of the Office of Electronic Government
4(q) Require agencies employing legacy software to either comply with the order or provide a plan outlining actions to remediate or meet the requirements of the order, unless an extension or waiver is granted

Director of NIST
4(w) Review the pilot programs focused on security capabilities of IoT devices and software development practices

Secretary of Commerce
4(x) Report to President the progress made under this section and outline additional steps needed to secure the software supply chain

MAY 12 2021

JUNE 11 *30 days*
If you want to give input on supply chain standards and best practices, now's the time.

JUNE 26 *45 days*
☐ Can I publish an SBOM that meets these requirements?

JULY 11 *60 days*
☐ Does my source code testing meet these standards?

JULY 26 *75 days*
☐ Is my product "critical software"?

AUGUST 10 *90 days*
NIST security measures for critical software now take effect!!

SEPTEMBER 9 *120 days*
If you want to give input on contract language, mark these dates!

SEPTEMBER 24 *135 days*

NOVEMBER 8 *180 days*

FEBRUARY 6, 2022 *270 days*
☐ Software supply chain security practices finalized. Are we compliant with that long list?

MARCH 8, 2022 *300 days*
☐ Can I sell my product to federal agencies (or to companies that sell to federal agencies)?

MAY 7, 2022 *360 days*

MAY 12, 2022 *1 year*
☐ Can I comply with the contract language... and prove it?
☐ Can federal agencies still use my legacy products?
☐ Do I have a remediation plan for my legacy products?

Note: The EO text has been adjusted for brevity and clarity.

NIST = National Institute of Standards and Technology
CISA = Cybersecurity & Infrastructure Security Agency
FAR = Federal Acquisition Regulation
SBOM = Software Bill of Materials
OMB = Office of Management and Budget
IoT = Internet of Things

www.adolus.com
+1-866-423-6587
@aDolus_Inc
https://www.linkedin.com/company/adolus