SECURE SOFTWARE REGULATIONS AND SELF-ATTESTATION REQUIRED FOR FEDERAL CONTRACTORS

Date: 19 May 2023

US Policy and Regulatory Alert

By: Guillermo S. Christensen, Sheila A. Armstrong, Brian J. Hopkins, Tara D. Hopkins

Government contractors providing software across the federal government's supply chain will be required later this year to comply with a new Secure Software Design Framework (SSDF). The SSDF requires software vendors to attest to new security controls in the design of code used by the federal government.

CYBERSECURITY COMPROMISES OF GOVERNMENT SOFTWARE ON THE RISE

In the aftermath of the cybersecurity compromises of significant enterprise software systems embedded in government supply chains, the federal government has increasingly prioritized reducing the vulnerability of software used within agency networks. Recognizing that most of the enterprise software that is used by the federal government is provided by a wide range of private sector contractors, the White House has been moving to impose a range of new software security regulations on both prime and subcontractors. One priority area is an effort to require government contractors to ensure that software used by federal agencies incorporates security by design. As a result, federal contractors supplying software to the government now face a new set of requirements to supply secure software code. That is, to provide software that is developed with security in mind so that flaws and vulnerabilities can be mitigated before the government buys and deploys the software.

THE SSDF AS A GOVERNMENT RESPONSE

In response, the White House issued Executive Order 14028, “Executive Order on Improving the Nation's Cybersecurity” (EO 14028), on 12 May 2021. EO 14028 requires the National Institute of Standards and Technology (NIST) to develop standards, tools, and best practices to enhance the security of the software supply chain. NIST subsequently promulgated the SSDF in special publication NIST SP 800-218. EO 14028 also mandates that the director of the Office of Management and Budget (OMB) take appropriate steps to ensure that federal agencies comply with NIST guidance and standards regarding the SSDF. This resulted in OMB Memorandum M-22-18, “Enhancing the Security of the Software Supply Chain through Secure Software Development Practices” (M-22-18). *The OMB memo provides that a federal agency may use software subject to M-22-18's requirements only if the producer of that software has first attested to compliance with federal government-specified secure software development practices drawn from the SSDF*. Meaning, if the producer of the software cannot attest to meeting the NIST requirements, it will not be able to supply software to the federal government. There are some exceptions and processes for software to gradually enter into compliance under various milestones for improvements, all of which are highly technical and subjective.

In accordance with these regulations, the Cybersecurity and Infrastructure Security Agency (CISA) of the Department of Homeland Security issued a draft form for collecting the relevant attestations and associated information. CISA released the draft form on 27 April 2023 and is accepting comments until 26 June 2023.[1]

SSDF IMPLEMENTATION DEADLINE AND REQUIREMENTS FOR GOVERNMENT SUPPLIERS

CISA initially set a deadline of 11 June 2023 for critical software and 13 September 2023 for non-critical software to comply with SSDF. Press reports indicate that these deadlines will be extended due to both the complexity of the SSDF requirements and the fact that the comment period remains open until 26 June 2023. However, CISA has not yet confirmed an extension of the deadline.

ATTESTATION AND COMPLIANCE WITH THE SSDF

Based on what we know now, the attestation form generally requires software producers to confirm that:

- The software was developed and built in secure environments.
- The software producer has made a good-faith effort to maintain trusted source code supply chains.
- The software producer maintains provenance data for internal and third-party code incorporated into the software.
- The software producer employed automated tools or comparable processes that check for security vulnerabilities.

Software producers that must comply with SSDF should move quickly and begin reviewing their approach to software security. The SSDF requirements are complex and likely will take time to review, implement, and document. In particular, many of the requirements call for subjective analysis rather than objective evaluation against a set of quantifiable criteria, as is usually the case with such regulations. The SSDF also includes numerous ambiguities. For example, the SSDF requires versioning changes in software to have certain impacts in the security assessment, although the term “versioning” does not have a standard definition in the software sector.

NEXT STEPS AND RISK OF NONCOMPLIANCE

Critically, the attestations on the new form carry risk under the civil False Claims Act for government contractors and subcontractors. Given the fact that many of the attestations require subjective analysis, contractors must take exceptional care in completing the attestation form. Contractors should carefully document their assessment that the software they produce is compliant. In particular, contractors and other interested parties should use this opportunity to share feedback and insights with CISA through the public comment process.

K&L Gates lawyers in our US National Security and Law Policy practice are closely tracking the implementation of these new requirements and can assist with understanding how they will impact specific organizations.

FOOTNOTES

[1] 88 Fed. Reg. 25,670.

KEY CONTACTS

GUILLERMO S. CHRISTENSEN
PARTNER

WASHINGTON DC
+1.202.778.9095
GUILLERMO.CHRISTENSEN@KLGATES.COM

SHEILA A. ARMSTRONG
PARTNER

DALLAS
+1.214.939.4960
SHEILA.ARMSTRONG@KLGATES.COM

BRIAN J. HOPKINS
ASSOCIATE

WASHINGTON DC
+1.202.778.9052
BRIAN.HOPKINS@KLGATES.COM

