DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

RIN: 0693-XC127

National Cybersecurity Center of Excellence (NCCoE) *Software Supply Chain and DevOps Security Practices*

AGENCY: National Institute of Standards and Technology, Department of Commerce.

ACTION: Notice.

SUMMARY: The National Institute of Standards and Technology (NIST) invites organizations to provide letters of interest describing products and technical expertise to support and demonstrate an applied risk-based approach and recommendations for secure DevOps (software development and operations) and software supply chain practices for the *Software Supply Chain and DevOps Security Practices* project. This notice is the initial step for the National Cybersecurity Center of Excellence (NCCoE) in collaborating with technology companies to address DevOps and software supply chain security challenges identified under the *Software Supply Chain and DevOps Security Practices* project. Participation in the project is open to all interested organizations.

DATES: Collaborative activities will commence as soon as enough completed and signed letters of interest have been returned to address all the necessary components and capabilities, but no earlier than [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: The NCCoE is located at 9700 Great Seneca Highway, Rockville, MD 20850. Letters of interest must be submitted to devsecops-nist@nist.gov or via hardcopy to National Institute of Standards and Technology, NCCoE; 9700 Great Seneca Highway, Rockville, MD 20850. Interested parties can request the letter of interest template by visiting https://www.nccoe.nist.gov/projects/software-supply-chain-and-devops-security-

practices and completing the letter of interest webform. NIST will announce the completion of the selection of participants and inform the public that it is no longer accepting letters of interest for this project at https://www.nccoe.nist.gov/projects/software-supply-chain-and-devops-security-practices. Organizations whose letters of interest are accepted in accordance with the process set forth in the **SUPPLEMENTARY INFORMATION** section of this notice will be asked to sign a consortium NCCoE Cooperative Research and Development Agreement (CRADA) with NIST; a template NCCoE Consortium CRADA can be found at: https://nccoe.nist.gov/library/nccoe-consortium-crada-example.

FOR FURTHER INFORMATION CONTACT: Paul Watrobski via email devsecops-nist@nist.gov, by telephone at (240) 479-1830, or by mail to National Institute of Standards and Technology, NCCoE; 9700 Great Seneca Highway, Rockville, MD 20850. Additional details about the *Software Supply Chain and DevOps Security Practices* project are available at https://www.nccoe.nist.gov/projects/software-supply-chain-and-devops-security-practices.

SUPPLEMENTARY INFORMATION:

Background: The NCCoE, part of NIST, is a public-private collaboration for accelerating the widespread adoption of integrated cybersecurity tools and technologies. The NCCoE brings together experts from industry, government, and academia under one roof to develop and document an applied risk-based approach and recommendations for secure DevOps (DevSecOps) and software supply chain practices consistent with the Secure Software Development Framework (SSDF), Cybersecurity Supply Chain Risk Management (C-SCRM), and other NIST, government, and industry guidance. Industry, government, and other organizations could then apply the guidelines when choosing and implementing DevSecOps practices in order to improve the security of the software they

develop and operate. That, in turn, would improve the security of the organizations using that software, and so on throughout the software supply chain.

Process: NIST is soliciting responses from all sources of relevant security capabilities (see below) to enter into a Cooperative Research and Development Agreement (CRADA) to provide products and technical expertise to support and demonstrate an applied risk-based approach and recommendations for secure DevOps (software development and operations) and software supply chain practices for the *Software Supply Chain and DevOps Security Practices* project. The full project can be viewed at: https://www.nccoe.nist.gov/projects/software-supply-chain-and-devops-security-practices.

Interested parties can access the template for a letter of interest by visiting the project website at https://www.nccoe.nist.gov/projects/software-supply-chain-and-devops-security-practices and completing the letter of interest webform. On completion of the webform, interested parties will receive access to the letter of interest template, which the party must complete, certify as accurate, and submit to NIST by email or hardcopy. NIST will contact interested parties if there are questions regarding the responsiveness of the letters of interest to the project objective or requirements identified below. NIST will select participants who have submitted complete letters of interest on a first come, first served basis within each category of product components or capabilities listed in the Requirements for Letters of Interest section below, up to the number of participants in each category necessary to carry out this project. There may be continuing opportunity to participate even after initial activity commences for participants who were not selected initially or have submitted the letter of interest after the selection process. Selected participants will be required to enter into an NCCoE consortium CRADA with NIST (for reference, see **ADDRESSES** section above).

When the project has been completed, NIST will post a notice on the *Software Supply Chain and DevOps Security Practices* project website at https://www.nccoe.nist.gov/projects/software-supply-chain-and-devops-security-practices announcing the completion of the project.

Project Objective:

This project's goal is to develop and document an applied risk-based approach and recommendations for DevSecOps practices. This project is intended to help enable organizations to maintain the velocity and volume of software delivery in a cloud-native way and take advantage of automated tools. The project's objective is to produce practical and actionable guidelines that meaningfully integrate security practices into development methodologies. The project intends to demonstrate how an organization can generate artifacts as a byproduct of its DevSecOps practices to support and inform the organization's self-attestation and declaration of conformance to applicable NIST and industry-recommended practices for secure software development and cybersecurity supply chain risk management. The project will also strive to demonstrate the use of current and emerging secure development frameworks, practices, and tools to address cybersecurity challenges.

Project Background:

DevOps brings together software development and operations to shorten development cycles, allow organizations to be agile, and maintain the pace of innovation while taking advantage of cloud-native technology and practices. Industry and government have fully embraced and are rapidly implementing these practices to develop and deploy software in operational environments, often without a full understanding and consideration of security. The NCCoE is undertaking a practical demonstration of technology and tools that meaningfully integrate security practices into development methodologies. DevSecOps helps ensure that security is addressed as part of all DevOps practices by

integrating security practices and automatically generating security and compliance artifacts throughout the processes and environments, including software development, builds, packaging, distribution, and deployment. Furthermore, there is increasing recognition of how security concerns inherent in modern day supply chains directly affect the DevOps process. DevSecOps practices can help identify, assess, and mitigate cybersecurity risk for the software supply chain.

Project Activities:

To meet the need to accelerate widespread adoption of improved DevOps and software supply chain security practices across various industry sectors, the NCCoE *Software Supply Chain and DevOps Security Practices* project will produce and demonstrate practical and actionable guidelines that meaningfully integrate security practices into development methodologies. Additionally, the project will demonstrate how an organization can generate artifacts as a byproduct of its DevSecOps practices to support and inform the organization's self-attestation and declaration of conformance to applicable NIST and industry-recommended practices for secure software development and cybersecurity supply chain risk management. The project will also strive to demonstrate the use of current and emerging secure development frameworks, practices, and tools to address cybersecurity challenges. Lessons learned during the project will be shared with the security and software development communities to inform improvements to secure development frameworks, practices, and tools. Lessons learned will also be shared with standards developing organizations to inform their DevSecOps-related work. The intention is to demonstrate DevSecOps practices, especially using automation, that would apply to organizations of all sizes and from all sectors, and to development for information technology (IT), operational technology (OT), Internet of Things (IoT), and other technology types.

Project Outcomes:

The proposed proof-of-concept solution(s) will integrate free and open source software (FOSS) and closed source software to demonstrate the use case scenarios detailed in Section 2 of the *Software Supply Chain and DevOps Security Practices* project description at https://www.nccoe.nist.gov/projects/software-supply-chain-and-devops-security-practices. This project will result in a publicly available NIST Cybersecurity Practice Guide as a Special Publication 1800 series, a detailed implementation guide describing the practical steps needed to implement a cybersecurity reference design that addresses this challenge. Supporting outputs may include public tools, code, and white papers.

Requirements for Letters of Interest: Each responding organization's letter of interest should identify which security platform component(s) or capability(ies) it is offering. Letters of interest should not include company proprietary information, and all components and capabilities must be commercially available. Components are listed in Section 3 of the *Software Supply Chain and DevOps Security Practices* project description at https://www.nccoe.nist.gov/projects/software-supply-chain-and-devops-security-practices and include, but are not limited to:

- Developer endpoints, including PCs (desktops or laptops) and virtual environments, both PC-based and cloud-based
- Network/infrastructure devices
- Services and applications, both on-premises and cloud-based, including:
    - Toolchains and their tools (build tools, packaging tools, repositories, etc.)
    - Vulnerability management (patch and configuration)
    - Version control software and services
    - Software security review, analysis, and testing tools (e.g., static and dynamic code analyzers, fuzzers, just-in-time secure coding training for developers)

    - Secure software design tools (e.g., threat modeling tools)
    - Memory safe programming languages
- Build systems (test, integration, production)
- Distribution/delivery systems
- Production systems that host apps

Each responding organization's letter of interest should identify how their products help address one or more of the following demonstration scenarios in Section 2 of the *Software Supply Chain and DevOps Security Practices* project description at https://www.nccoe.nist.gov/projects/software-supply-chain-and-devops-security-practices:

- Free and open source software development
- Closed source software development

In their letters of interest, responding organizations need to acknowledge the importance of and commit to provide:

1. Access for all participants' project teams to DevOps component interfaces and the organization's experts necessary to make functional connections among DevOps components.
2. Support for development and demonstration of the *Software Supply Chain and DevOps Security Practices* project at the NCCoE, which will be conducted in a manner consistent with the most recent version of the following standards and guidance: Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (NIST SP 800-161) (https://doi.org/10.6028/NIST.SP.800-161r1), Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework) (https://www.nist.gov/cyberframework/framework), and Secure Software Development Framework (SSDF) (NIST SP 800-218)

(https://doi.org/10.6028/NIST.SP.800-218). Additional details about the *Software Supply Chain and DevOps Security Practices* project are available at https://www.nccoe.nist.gov/projects/software-supply-chain-and-devops-security-practices.

NIST cannot guarantee that all of the products proposed by respondents will be used in the demonstration. Each prospective participant will be expected to work collaboratively with NIST staff and other project participants under the terms of the NCCoE consortium CRADA in the development of the *Software Supply Chain and DevOps Security Practices* project. Prospective participants' contribution to the collaborative effort will include assistance in establishing the necessary interface functionality, connection and set-up capabilities and procedures, demonstration harnesses, environmental and safety conditions for use, integrated platform user instructions, and demonstration plans and scripts necessary to demonstrate the desired capabilities. Each participant will train NIST personnel, as necessary, to operate its product in capability demonstrations. Following successful demonstrations, NIST will publish a description of the DevSecOps proof-of-concept builds and their characteristics sufficient to permit other organizations to develop and deploy DevSecOps practices that meet the objectives of the *Software Supply Chain and DevOps Security Practices* project. These descriptions will be public information.

Under the terms of the NCCoE consortium CRADA, NIST will support development of interfaces among participants' products by providing IT infrastructure, laboratory facilities, office facilities, collaboration facilities, and staff support to component composition, platform documentation, and demonstration activities.

The dates of the demonstration of the *Software Supply Chain and DevOps Security Practices* project capability will be announced on the NCCoE website at least two weeks in advance at https://nccoe.nist.gov/. The expected outcome will demonstrate how the components of the solutions that address *Software Supply Chain and DevOps Security*

Practices can enhance capabilities that provide assurance of management of identified risks while continuing to meet industry sectors' compliance requirements. Participating organizations will gain from the knowledge that their products are interoperable with other participants' offerings.

For additional information on the NCCoE governance, business processes, and NCCoE operational structure, visit the NCCoE website https://nccoe.nist.gov/.

Alicia Chambers,
NIST Executive Secretariat.
[FR Doc. 2023-10221 Filed: 5/12/2023 8:45 am; Publication Date: 5/15/2023]