Billing Code: 3510-13

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

Docket No.: 161116999-6999-01

National Cybersecurity Center of Excellence (NCCoE) Multifactor Authentication for e-Commerce Project for the retail sector

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 products and technical expertise to support and demonstrate security platforms for the Multifactor Authentication for e-Commerce Project for the retail sector. This notice is the initial step for the National Cybersecurity Center of Excellence (NCCoE) in collaborating with technology companies to address cybersecurity challenges identified under the retail sector program. Participation in the Multifactor Authentication for e-Commerce Project is open to all interested organizations.

DATES: Interested parties must contact NIST to request a letter of interest template to be completed and submitted to NIST. Letters of interest will be accepted on a first come, first served basis. 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 [PLEASE INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]. When the Multifactor Authentication for e-Commerce Project search for collaborators has been completed, NIST will post a notice on the NCCoE retail sector program website at https://nccoe.nist.gov/projects/use_cases/multifactor-authentication-ecommerce announcing the completion of the search for collaborators and informing the public that it will no longer accept letters of interest for this Multifactor Authentication for e-Commerce Project.

ADDRESSES: The NCCoE is located at 9700 Great Seneca Highway, Rockville, MD 20850. Letters of interest must be submitted to consumer-nccoe@nist.gov or via hardcopy to National Institute of Standards and Technology, NCCoE; 9700 Great Seneca Highway, Rockville, MD 20850. 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 Cooperative Research and Development Agreement (CRADA) with NIST. A CRADA template can be found at: https://nccoe.nist.gov/library/nccoe-consortium-crada-example.

FOR FURTHER INFORMATION CONTACT: William Newhouse via email to william.newhouse@nist.gov; by telephone 301-975-0232; or by mail to National Institute of Standards and Technology, NCCoE; 9700 Great Seneca Highway, Rockville, MD 20850. Additional details about the Multifactor Authentication for e-Commerce Project are available at https://nccoe.nist.gov/projects/use_cases/multifactor-authentication-ecommerce.

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 practical, interoperable cybersecurity approaches that address the real-world needs of complex Information Technology (IT) systems. By accelerating dissemination and use of these integrated tools and technologies for protecting IT assets, the NCCoE will enhance trust in U.S. IT communications, data, and storage systems; reduce risk for companies and individuals using IT systems; and encourage development of innovative, job-creating cybersecurity products and services.

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 security platforms for the Multifactor Authentication for e-Commerce Project for the retail sector. The full

Multifactor Authentication for e-Commerce Project Description can be viewed at: https://nccoe.nist.gov/projects/use_cases/multifactor-authentication-ecommerce.

Interested parties should contact NIST using the information provided in the FOR FURTHER INFORMATION CONTACT section of this notice. NIST will then provide each interested party with a letter of interest template, which the party must complete, certify that it is accurate, and submit to NIST. NIST will contact interested parties if there are questions regarding the responsiveness of the letters of interest to the Multifactor Authentication for e-Commerce 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 below up to the number of participants in each category necessary to carry out this Multifactor Authentication for e-Commerce Project. However, there may be continuing opportunity to participate even after initial activity commences. Selected participants will be required to enter into a consortium CRADA with NIST (for reference, see ADDRESSES section above). NIST published a notice in the Federal Register on October 19, 2012 (77 FR 64314) inviting U.S. companies to enter into National Cybersecurity Excellence Partnerships (NCEPs) in furtherance of the NCCoE. For this demonstration project, NCEP partners will not be given priority for participation.

Multifactor Authentication for e-Commerce Project Objective: The goal of this project is to increase the confidence of user identity and reduce the risk of fraud in the online, Card-Not-Present (CNP) space by implementing multifactor authentication for e-commerce transactions along with other security controls. The solution will provide guidance for implementing multifactor authentication mechanisms, risk calculation, web analytics, and potentially identity federation, in retail IT architecture segments that support or interface with e-commerce transactions such as online shopping or loyalty points programs. It will produce an architecture that includes components that will integrate multifactor authentication mechanisms (certificate-based, biometric, or others), risk calculation engines (risk score calculation and decisions), web analytics (pertaining to known user behavior and/or web threat detection), potentially identity federation (which can include authentication and risk information sent from a third-party business partner and Identity Provider), and automated logging within and between each component.

A detailed description of the Multifactor Authentication for e-Commerce Project is available at: https://nccoe.nist.gov/projects/use_cases/multifactor-authentication-ecommerce.

Requirements: 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 the High-Level Architecture section of the Multifactor Authentication for e-Commerce Project Description (for reference, please see the link in the **Process** section above) and include, but are not limited to:

- Online/e-commerce shopping cart and payment system (in-house or outsourced)

- Multifactor authentication mechanisms (types of which to be determined)
- Risk calculation platform/engine
- Web analytics engine
- Logging of risk calculation and web analytics data
- Data storage for risk calculation and web analytics data
- Identity federation mechanism (optional)

Each responding organization's letter of interest should identify how their products address one or more of the following desired solution characteristics in the High-Level Architecture section of the Multifactor Authentication for e-Commerce Project Description for the retail use case (for reference, please see the link in the **Process** section above):

- Authentication mechanisms that meet business security and regulatory requirements
- Automated web analytics including monitoring of user behavior and contextual details
- Automated logging of web analytics and risk calculation data
- Automated data storage of web analytics and risk calculation data
- Ability to establish and enforce risk decisions including performing risk calculations
- Automated alerting of suspected fraudulent activity
- Ease of use for the consumer, no substantial increase in friction during the e-commerce transaction
- Identity federation (optional)

Responding organizations need to understand and, in their letters of interest, commit to provide:

1. Access for all participants’ project teams to component interfaces and the organization's experts necessary to make functional connections among security platform components
2. Support for development and demonstration of the Multifactor Authentication for e-Commerce Project for the retail use case in NCCoE facilities which will be conducted in a manner consistent with Federal requirements (e.g., FIPS 200, FIPS 201, SP 800-53, and SP 800-63)

Additional details about the Multifactor Authentication for e-Commerce Project for the retail sector use case are available at: https://nccoe.nist.gov/projects/use_cases/multifactor-authentication-ecommerce. 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 consortium CRADA in the development of the Multifactor Authentication for e-Commerce Project for the retail sector capability. Prospective participant’s 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 to the retail community. Following successful demonstrations, NIST will publish a description of the security platform and its performance characteristics sufficient to permit other organizations to develop and deploy security platforms that meet the security objectives of the Multifactor Authentication for e-Commerce Project for the retail sector use case. These descriptions will be public information.

Under the terms of the 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, security platform documentation, and demonstration activities.

The dates of the demonstration of the Multifactor Authentication for e-Commerce Project for the retail sector capability will be announced on the NCCoE Web site at least two weeks in advance at http://nccoe.nist.gov/. The expected outcome of the demonstration is added security and reduced fraud stemming from an increased use of multifactor authentication for e-commerce transactions across an entire retail sector enterprise. 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 Web site http://nccoe.nist.gov/.

Kevin Kimball
NIST Chief of Staff

[FR Doc. 2016-30435 Filed: 12/16/2016 8:45 am; Publication Date: 12/19/2016]