Billing Code: 3510-13

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

Docket No.: 160830797-6797-01

National Cybersecurity Center of Excellence (NCCoE) Mobile Application Single Sign On (SSO) for the Public Safety & First Responder 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 Mobile Application Single Sign On (SSO) for the Public Safety & First Responder 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 Public Safety & First Responder sector program. Participation in the use case 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 use case has been completed, NIST will post a notice on the NCCoE Public Safety & First Responder sector program website at https://nccoe.nist.gov/projects/building_blocks/mobile-sso announcing the completion of the use case and informing the public that it will no longer accept letters of interest for this use case.

ADDRESSES: The NCCoE is located at 9700 Great Seneca Highway, Rockville, MD 20850. Letters of interest must be submitted to PSFR-NCCoE@nist.gov or via hardcopy to National Institute of Standards and Technology, 100 Bureau Drive Mail Stop 2002 Gaithersburg, MD 20899. 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: http://nccoe.nist.gov/node/138.

FOR FURTHER INFORMATION CONTACT: Paul Grassi or William Fisher via email to PSFR-NCCoE@nist.gov; by telephone 301-975-0200; or by mail to National Institute of Standards and Technology, NCCoE; 100 Bureau Drive Mail Stop 2002 Gaithersburg,

MD 20899. Additional details about the Public Safety & First Responder sector program are available at https://nccoe.nist.gov/projects/building_blocks/mobile-sso.

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 Mobile Application Single Sign On (SSO) for the Public Safety & First Responder Sector. The full use case can be viewed at:

https://nccoe.nist.gov/projects/building_blocks/mobile-sso

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 use case 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 use case. 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.

Use Case Objective:

When responding to an emergency, public safety personnel require on-demand access to data. The ability to quickly and securely authenticate in order to access public safety data is critical to ensuring that first responders can deliver the proper care and support during an emergency. In order to adequately meet the need of diverse public safety personnel, missions, and operational environments, authentication mechanisms need to support deployments where devices may be shared amongst personnel and authentication factors have usability constraints.

The challenge that first responders face in authenticating quickly and securely to public safety systems is compounded when a first responder is forced to authenticate

individually to multiple mobile applications. In addition, when authorizing application access to shared resources, first responders may be subjected to an additional authentication step at the resource provider. To address the challenge identified by the public safety community, the National Cybersecurity Center of Excellence (NCCoE) plans to develop a Mobile Application Single Sign On (SSO) reference design and implementation that meets these unique authentication requirements and allows first responders to take advantage of the latest mobile authentication technology and best practices.

A detailed description of the Mobile Application Single Sign On (SSO) is available at: https://nccoe.nist.gov/projects/building_blocks/mobile-sso.

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 section 3 of the Mobile Application Single Sign On (SSO) for the Public Safety & First Responder use case (for reference, please see the link in the PROCESS section above) and include, but are not limited to:

- Mobile devices
- Mobile platforms for biometric authentication
- Hardware based authenticators that interoperate with mobile platforms
- Software Development Kit (SDK) or platform that enables mobile single sign on capabilities

Each responding organization's letter of interest should identify how their products address one or more of the following desired solution characteristics in section 3 of the Mobile Application Single Sign On (SSO) for the Public Safety & First Responder use case (for reference, please see the link in the PROCESS section above):

1. A standards-based approach and a solution architecture that selects the most effective and secure approach to implement mobile SSO leveraging native capabilities of the mobile OS.
2. Support mobile SSO both for authentication and delegated authorization (as in OAuth Client Applications).
3. Ensure that mobile applications do not have access to user credentials.
4. Support multiple authenticators taking into account unique environmental constraints faced by first responders in emergency medical services, law enforcement, and the fire service such as:
    a. Gloved, one-handed, or hands-free operation
    b. Use of smoke hoods, fire hoods or gas masks that may prevent facial or iris recognition
    c. Proximity based authenticators (new yubikeys)
    d. Biometric based continuous authentication mechanisms that meet the requirements of draft NIST Special Publication 800-63B
5. Allow multi-user operation of shared mobile devices
6. Support for multiple authentication protocols. If appropriate, public sector agencies must be able to leverage multifactor authentication. This may be accomplished by adopting Fast IDentity Online (FIDO 2.0) Universal

Authentication Framework (UAF), Universal 2nd Factor (U2F), PKI, or some other means.

7. Support a spectrum of BYOD (Bring Your Own Device) and COPE (Corporate Owned, Personally Enabled) scenarios.

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 Mobile Application Single Sign On (SSO) for the Public Safety & First Responder 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 Mobile Application Single Sign On (SSO) for the Public Safety & First Responder sector use case are available at: https://nccoe.nist.gov/projects/building_blocks/mobile-sso

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 Mobile Application Single Sign On (SSO) for the Public Safety & First Responder sector capability. 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 to the Public Safety & First Responder 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 Mobile Application Single Sign On (SSO) for the Public Safety & First Responder 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 Mobile Application Single Sign On (SSO) for the Public Safety & First Responder 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 to improve mobile application single sign-on across an entire Public Safety & First Responder 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/.

Kent Rochford
Associate Director for Laboratory Programs
[FR Doc. 2016-28627 Filed: 11/28/2016 8:45 am; Publication Date: 11/29/2016]