Billing Code: 3510-13

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

Docket No.: 150318278-5278-01

National Cybersecurity Center of Excellence Access Rights Management Use Case for the Financial Services 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 access rights management for the financial services 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 financial services 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. 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 [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 financial services sector program website at http://nccoe.nist.gov/financial-services 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 9600 Gudelsky Drive, Rockville, MD 20850. Letters of interest must be submitted to financial_NCCoE@nist.gov or via hardcopy to National Institute of Standards and Technology, NCCoE; 9600 Gudelsky Drive; 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: http://nccoe.nist.gov/node/138.

FOR FURTHER INFORMATION CONTACT: Michael Stone via email at financial_NCCoE@nist.gov; or telephone 240-314-6813; National Institute of Standards and Technology, NCCoE; 9600 Gudelsky Drive; Rockville, MD 20850. Additional details about the Financial Services Sector program are available at http://nccoe.nist.gov/financial-services.

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 Access Rights Management use case for the Financial Services Sector. The full use case can be viewed at:

http://nccoe.nist.gov/sites/default/files/NCCoE_FS_Use_Case_IDAM_FinalDraft_20140501.pdf

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. 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: The goal of this project is to demonstrate ways to link together the management of existing disparate identity and access mechanisms and systems into a comprehensive identity and access management (IDAM) system. This will enable financial sector entities to centrally issue, validate, and modify or revoke access rights for their entire enterprise based on easy-to-understand business rules. This IDAM system

will abstract, unify, and simplify the complex task of dealing with multiple types of access systems, such as Windows Active Directory, Unix/Linux, Resource Access Control Facility (RACF), automatic class selection (ACS2) and myriad legacy and internally developed application-specific mechanisms. This IDAM system will also produce consolidated reports and statistics so that administrators and managers can make accurate risk management decisions. This IDAM system will, at a minimum, automate the monitoring and analysis of identity related activities in a manner that enables administrators and managers to make timely and informed risk management decisions.

Requirements: Each responding organization's letter of interest should identify which security platform components or capabilities it is offering. Components are listed in section six (for reference, please see link in PROCESS section above) of the Access Rights Management for the Financial Services Sector use case and include, but are not limited to:

- Mainframe (may be simulated or remotely accessed) such as RACF
- Representative "homemade" financial sector application(s) with internal user access database and logging system

Each responding organization's letter of interest should identify how their products address one or more of the following desired solution characteristics in section two (for reference, please see link in PROCESS section above) of the Access Rights Management for the Financial Services Sector use case:

1. Is a single system that is capable of interacting with multiple existing accesses

2. Has management systems to provide a complete picture of access rights within the organization
3. Complements, and does not replace, existing security infrastructure
4. Utilizes secure communications among all components
5. Automates logging, reporting and alerting of identity and access management events across the enterprise
6. Can be queried for information (ad-hoc reporting) in order to answer management, performance and security questions (i.e. show all activity for a given user in a certain time period)
7. Does not introduce new attack vectors into existing systems
8. Supports multiple access levels for the IDAM system (e.g. administrator, operator, viewer)
9. Provides fine-grain privilege controls (e.g. groups, users, directory, file, and record)
10. Provides the ability to attach expiration dates/time limits on access controls
11. Provides the ability to map user's access requests via "service" account access

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 Access Rights Management use case for the Financial Services Sector 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 Access Rights Management for the Financial Services sector use case are available at:

http://nccoe.nist.gov/sites/default/files/NCCoE_FS_Use_Case_IDAM_FinalDraft_20140501.pdf

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 agreement in the development of the Access Rights Management for the Financial Services 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 prospective participant will train NIST personnel as necessary, to operate its product in capability demonstrations to the financial services 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 Access Rights Management for the Financial Services sector use case. These descriptions will be public information. Under the terms of the consortium agreement, 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 Access Rights Management for the Financial Services 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 access rights management across an entire financial services 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/.

Richard Cavanagh
Acting Associate Director for Laboratory Programs

[FR Doc. 2015-07590 Filed: 4/2/2015 08:45 am; Publication Date: 4/3/2015]