Billing Code: 3510-13

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket Number: 150508436-5436-01]

National Cybersecurity Center of Excellence, Attribute Based Access Control Building Block

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 Attribute Based Access Control Building Block. 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 Attribute Based Access Control Building Block. Participation in the building block 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 that identifies the organization requesting participation in the Attribute Based Access Control Building Block and the capabilities and components that are being offered to the collaborative effort. 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 building block has been completed, NIST will post a notice on the NCCoE Attribute Based Access Control Building Block website at http://nccoe.nist.gov/content/attribute-based-access-control announcing the completion of the building block and informing the public that it will no longer accept letters of interest for this building block

ADDRESSES: The NCCoE is located at 9600 Gudelsky Drive, Rockville, MD 20850. Letters of interest must be submitted to abac-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: Bill Fisher via email at to abac-nccoe@nist.gov, by telephone 240-314-6838; or by mail to National Institute of Standards and Technology, NCCoE; 9600 Gudelsky Drive; Rockville, MD 20850. Additional details about the Attribute Based Access Control Building Block are available at http://nccoe.nist.gov/content/attribute-based-access-control.

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 Attribute Based Access Control Building Block. The full building block can be viewed at: http://nccoe.nist.gov/content/attribute-based-access-control

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 and which identifies the organization requesting participation in the Attribute Based Access Control Building Block and the capabilities and components that are being offered to the collaborative effort. NIST will

contact interested parties if there are questions regarding the responsiveness of the letters of interest to the building block objective or requirements identified below and to obtain additional information. 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 the Attribute Based Access Control Building Block. 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.

Building Block Objective:

Enterprises face the continual challenge of providing access control mechanisms for subjects requesting access to corporate resources (e.g. applications, networks, systems and data). Authentication is required for a diverse set of subjects, who may be known or unknown to the enterprise, and may present the organization with differing credentials. Once authenticated, enterprises require a strong authorization system that enables fine-grain access decisions based on a range of users, resources, and environmental conditions. These challenges, combined with the growth and distributed nature of enterprise resources, as well as the need to share information among stakeholders that are

not managed directly by the enterprise, has spawned the demand for highly flexible access control mechanisms.

This building block will use commercially available technologies to demonstrate an enterprise Attribute Based Access Control implementation that makes run-time authorization decisions and enforces a rich set of access control policies consistently across an enterprise (or enterprises). Information about a subject, the resource being accessed, and the environmental context at the time of attempted access shall form the basis for access control decisions, rather than pre-provisioned privileges within individual systems.

Through the use of an attribute exchange platform, this project will exhibit a federated access control environment, allowing for the secure sharing of IT resources across multiple enterprises. In this manner, enterprises enable unanticipated, yet valid, federated identities to gain access, without the traditional challenge of waiting for identity provisioning or authorization approvals.

A detailed description of the Attribute Based Access Control Building Block are available at: http://nccoe.nist.gov/content/attribute-based-access-control.

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 ten of the Attribute Based Access Control Building Block (for reference, please see the link in the PROCESS section above) and include, but are not limited to:

- Identity management software that includes functions like: account provisioning, de-provisioning and directory services
- Platform for exchanging attributes
- Federation server
- Databases for policy database, identity store, subject attribute repository, object and attribute repository
- Policy server, to serve as the policy administration point
- Access management system, which may include the policy decision point, policy enforcement point and context handler
- Authentication server and components supporting two factor authentication
- Cryptographic means to protect subject privacy during interactions between RPs, IDPs, APs and the attribute exchange platform

Each responding organization's letter of interest should identify how their product(s) address one or more of the desired solution characteristics in section five of the Attribute Based Access Control Building Block description (for reference, please see link in PROCESS section above).

Additional details about the Attribute Based Access Control Building Block are available at: http://nccoe.nist.gov/content/attribute-based-access-control

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 Attribute Based Access Control Building Block. 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 security platform and its performance characteristics sufficient to permit other organizations to develop and deploy security platforms that meet the security objectives of the Attribute Based Access Control Building Block. These descriptions will be public information.

Under the terms of the consortium CRADA, participants will commit to providing:

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 Attribute Based Access Control Building Block 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)

In addition, 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 Attribute Based Access Control Building Block 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 Attribute Based Access Control within the 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. 2015-20041 Filed: 8/13/2015 08:45 am; Publication Date: 8/14/2015]