



Billing Code: 3510-13

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No. : 170331340-7340-01]

National Cybersecurity Center of Excellence (NCCoE) Trusted Geolocation in the Cloud 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 Trusted Geolocation in the Cloud 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 Trusted Geolocation in the Cloud 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. 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 building block has been completed, NIST will post a notice on the NCCoE Trusted Geolocation in the Cloud website at

https://nccoe.nist.gov/projects/building_blocks/trusted_geolocation_in_the_cloud

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 9700 Great Seneca Highway, Rockville, MD 20850. Letters of interest must be submitted to trusted-cloud-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:

<https://nccoe.nist.gov/library/nccoe-consortium-crada-example>.

FOR FURTHER INFORMATION CONTACT: Mike Bartock and Murugiah Souppaya via email to trusted-cloud-nccoe@nist.gov; by telephone 301-975-5358; or by mail to National Institute of Standards and Technology, NCCoE; 100 Bureau Drive Mail Stop 2002 Gaithersburg, MD 20899. Additional details about the Trusted Geolocation in the Cloud Building Block are available at:

https://nccoe.nist.gov/projects/building_blocks/trusted_geolocation_in_the_cloud.

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 Trusted Geolocation in the Cloud Building Block. The full building block can be viewed at:

https://nccoe.nist.gov/projects/building_blocks/trusted_geolocation_in_the_cloud.

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 building block 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 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: The building block provides details about the implementation of trusted resource pools to aggregate trusted systems and segregate them from untrusted resources, which results in the separation of higher-value, more sensitive workloads from commodity application and data workloads. A detailed description of the Trusted Geolocation in the Cloud Building Block is available at:

https://nccoe.nist.gov/projects/building_blocks/trusted_geolocation_in_the_cloud.

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 5 of the Trusted Geolocation in the Cloud Building Block (for reference, please see the link in the PROCESS section above) and include, but are not limited to:

1. Commodity servers with hardware cryptographic module
2. Commodity network switches
3. Hypervisors
4. Operating systems
5. Application containers
6. Attestation server
7. Orchestration and management servers

8. Database servers
9. Directory servers
10. Software defined network
11. Data encryption and key management server
12. Cloud service

Each responding organization's letter of interest should identify how its products address one or more of the following desired solution characteristics in section 3 of the Trusted Geolocation in the Cloud Building Block (for reference, please see the link in the PROCESS section above):

1. Platform Attestation and Safer Hypervisor or Operating System Launch
2. Trust-Based Homogeneous Secure Migration within a Single Cloud Platform
3. Trust-Based and Geolocation-Based Homogeneous Secure Migration within a Single Cloud Platform
4. Data Protection and Encryption Key Management Enforcement Based on Trust-Based and Geolocation-Based Homogeneous Secure Migration within a Single Cloud Platform
5. Persistent Data Flow Segmentation Before and After the Trust-Based and Geolocation-Based Homogeneous Secure Migration within a Single Cloud
6. Industry Sector Compliance Enforcement for Regulated Workloads Before and After the Trust-Based and Geolocation-Based Homogeneous Secure Migration
7. Trust-Based and Geolocation-Based Homogeneous and Policy Enforcement in a Secure Cloud Bursting across Two Cloud Platforms

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 Trusted Geolocation in the Cloud 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)

Additional details about the Trusted Geolocation in the Cloud Building Block are available at

https://nccoe.nist.gov/projects/building_blocks/trusted_geolocation_in_the_cloud.

NIST cannot guarantee that all 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 Trusted Geolocation in the Cloud 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 Trusted Geolocation in the Cloud Building Block. 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 Trusted Geolocation in the Cloud 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 the trusted geolocation in the cloud 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/>.

Kevin Kimball,
Chief of Staff.

[FR Doc. 2017-09502 Filed: 5/10/2017 8:45 am; Publication Date: 5/11/2017]