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 5–10–17; 8:45 am]

BILLING CODE 3510–13–P

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

Request for Participation on Developing Industrial Wireless Systems Best Practices Guidelines

AGENCY: National Institute of Standards and Technology, Commerce.

ACTION: Notice.

SUMMARY: The Intelligent Systems Division of NIST is forming a technical working group (TWG) to develop best practices guidelines in selecting and deploying industrial wireless solutions within industrial environments such as process control and manufacturing. Guidelines will consider the entire wireless ecosystem within factories with emphasis on wireless networks operating on the factory floor. This includes factory/plant instrumentation, control systems, and back-haul networks. The guidelines will be technology and vendor agnostic and will address the current needs of industry to have independent guidelines based on user requirements and measurement science research.

DATES: Intention to participate must be received by 180 days after date of publication in the **Federal Register**.

ADDRESSES: Intention to participate may be submitted in one of two ways.

- By sending an email to *iwstwg@nist.gov.*
- By written request: National Institute of Standards and Technology ATTN: Richard Candell 100 Bureau Drive, Stop 8230 Gaithersburg, MD 20899–8615.

Please direct media inquiries to NIST's Office of Public Affairs at 301–975–2762.

SUPPLEMENTARY INFORMATION: More information on industrial wireless systems research may be found on the NIST home page for Industrial Wireless Systems at *https://www.nist.gov/programs-projects/wireless-systems-industrial-environments.*

Kevin Kimball,

NIST Chief of Staff.

[FR Doc. 2017–09503 Filed 5–10–17; 8:45 am]

BILLING CODE 3510–13–P