Billing Code: 3510-13

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No.: 200501-0125]

National Cybersecurity Center of Excellence (NCCoE) 5G Cybersecurity: Preparing a Secure Evolution to 5G

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 5G Cybersecurity: Preparing a Secure Evolution to 5G project. 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 5G Cybersecurity: Preparing a Secure Evolution to 5G project. Participation in the building block is open to all interested organizations.

DATES: 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].

ADDRESSES: The NCCoE is located at 9700 Great Seneca Highway, Rockville, MD 20850. Letters of interest must be submitted to 5g-security@nist.gov or via hardcopy to National Institute of Standards and Technology, NCCoE; 9700 Great Seneca Highway, 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 consortium Cooperative Research and Development Agreement (CRADA) with NIST. An NCCoE consortium CRADA template can be found at: https://nccoe.nist.gov/node/138.

FOR FURTHER INFORMATION CONTACT: Jeff Cichonski via email to 5g-security@nist.gov; by telephone 301-975-0200 or by mail to National Institute of Standards and Technology, NCCoE; 9700 Great Seneca Highway, Rockville, MD 20850. Additional details about the 5G Cybersecurity: Preparing a Secure Evolution to 5G project are available at https://www.nccoe.nist.gov/projects/building-blocks/5g-secure-evolution.

SUPPLEMENTARY INFORMATION: 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. When the building block has been completed, NIST will post a notice on the NCCoE 5G Cybersecurity: Preparing a Secure Evolution to 5G project website at https://www.nccoe.nist.gov/projects/building-blocks/5g-secure-evolution announcing the completion of the building block and informing the public that it will no longer accept letters of interest for this building block.

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 5G Cybersecurity: Preparing a Secure Evolution to 5G project. The full building block can be viewed at: https://www.nccoe.nist.gov/projects/building-blocks/5g-secure-evolution.

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: This project will demonstrate how the components of the 5G architecture can provide security capabilities to mitigate identified risks and meet industry sectors' compliance requirements. The proposed proof-of-concept solution will integrate commercial and open source products that leverage cybersecurity standards and recommended practices to demonstrate the use case scenarios and showcase 5G's robust security features. This project will result in a publicly available NIST Cybersecurity Practice Guide as a Special Publication 1800 series, a detailed implementation guide

describing the practical steps needed to implement a cybersecurity reference implementation. The publication can assist organizations that are considering adopting and deploying 5G technology with the design, acquisition process (including Request for Information [RFI] and Request for Proposal [RFP] development and response), integration, and operation of 5G-based networks. The findings from this work can be used by NIST and the industry collaborators to prioritize their contributions in standards developing organizations. A detailed description of the 5G Cybersecurity: Preparing a Secure Evolution to 5G is available at: https://www.nccoe.nist.gov/projects/building-blocks/5g-secure-evolution.

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 5G Cybersecurity: Preparing a Secure Evolution to 5G project description (for reference, please see the link in the Process section above) and include, but are not limited to:

- Commodity hardware with trust measurement capability
- Local and network storage
- Switches and routers
- Security gateways (SEGs), firewalls (e.g., roaming General Packet Radio Service [GPRS] Tunneling Protocol [GTP] control [GTP-C]/GTP user data tunneling [GTP-U] FW, SGi/N6 interface FW)
- Virtualization software

- Security and policy enforcement software, governance, risk, & compliance (GRC) / security information and event management (SIEM) / dashboard
- Virtualized LTE EPC components
- Home Subscriber Server (HSS)
- LTE eNodeB
- 5G NR gNodeB
- 5G NR UE / consumer IoT (CIoT) device
- Universal Integrated Circuit Card (UICC) components
- False base station detection capability
- Simulation equipment
- Network and telecommunication test tools

Each responding organization's letter of interest should identify how their products help address one or more of the following desired security characteristics and properties in section 3 of the 5G Cybersecurity: Preparing a Secure Evolution to 5G project (for reference, please see the link in the PROCESS section above):

1. Trusted Hardware – The computing hardware will provide the capability to measure platform components and store the measurements in a hardware root of trust for later attestation. Custom values can be provisioned to the computing hardware root of trust, known as asset tags, which can also be used for future attestation.
2. Isolation and Policy Enforcement – Once trust is established in the infrastructure, workloads can be restricted to run only on trusted hardware that

meets specific asset policies. The platform trust measurement and asset tagging can also be used as part of the data protection policy of the workloads.

3. Visibility and Compliance – Technical mechanisms will be continuously enforced and assessed to secure the environment over the lifecycle of the platform and workloads. These mechanisms enable the organization to manage risks and meet the compliance requirements by documenting and monitoring configuration changes.
4. EPC-Based Security Feature Enablement – The EPC in the NSA deployment can be configured in accordance with recommended practices, including enabling standards-based security features and configuring parameters in accordance with relevant guidelines.
5. False Base Station Protections - Utilizing commercial solutions to provide protections from false base stations that are not provided by the 3GPP standards.
6. Prevent Downgrade to Legacy Technology by Disabling UE's 2G Radio by use of standards based configurable parameters or commercial solutions.

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 5G Cybersecurity: Preparing a Secure Evolution to 5G project phase 1 for multiple sectors in NCCoE facilities which will be conducted in a manner consistent with the following standards and

guidance: FIPS 200, FIPS 201, SP 800-53, SP 800-147B, SP 800-155 and SP 800-161. Additional details about the 5G Cybersecurity: Preparing a Secure Evolution to 5G project are available at https://www.nccoe.nist.gov/projects/building-blocks/5g-secure-evolution.

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 5G Cybersecurity: Preparing a Secure Evolution to 5G project. 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 5G Cybersecurity: Preparing a Secure Evolution to 5G project. 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 5G Cybersecurity: Preparing a Secure Evolution to 5G project capability will be announced on the NCCoE Web site at least two weeks in advance at https://nccoe.nist.gov/. The expected outcome will demonstrate how the components of the 5G architecture can provide security capabilities to mitigate identified risks and meet industry sectors' compliance requirements. 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 https://nccoe.nist.gov/.

Kevin A. Kimball,
Chief of Staff.
[FR Doc. 2020-10866 Filed: 5/19/2020 8:45 am; Publication Date: 5/20/2020]