Billing Code: 3510-13

**DEPARTMENT OF COMMERCE**

**National Institute of Standards and Technology**

**[Docket No.: 200921-0251]**

# National Cybersecurity Center of Excellence (NCCoE) Zero Trust Cybersecurity: Implementing a Zero Trust Architecture

**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 Zero Trust Cybersecurity: Implementing a Zero Trust Architecture 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 Zero Trust Cybersecurity: Implementing a Zero Trust Architecture 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 nccoe-zta-project@list.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/library/nccoe-consortium-crada-example.

**FOR FURTHER INFORMATION CONTACT:** Alper Kerman via email to nccoe-zta-project@list.nist.gov; or by telephone at 301-975-0200. Additional details about the Zero Trust Cybersecurity: Implementing a Zero Trust Architecture project are available at https://www.nccoe.nist.gov/zerotrust.

**SUPPLEMENTARY INFORMATION:** Interested parties can access the letter of interest template by visiting the project website at https://www.nccoe.nist.gov/zerotrust and completing the letter of interest webform. Completed letters of interest should be submitted to NIST and 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 Zero Trust Cybersecurity: Implementing a Zero Trust Architecture project website at https://www.nccoe.nist.gov/zerotrust 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 Zero Trust Cybersecurity: Implementing a Zero Trust Architecture project. The full building block can be viewed at: https://www.nccoe.nist.gov/zerotrust.

Interested parties can access the letter of interest template by visiting the project website at https://www.nccoe.nist.gov/zerotrust and completing the letter of interest webform. On completion of the webform, interested parties will receive access to the 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 objective of this building block project is to produce an example implementation(s) of a zero trust architecture that is designed and deployed according to the concepts and tenets documented in the NIST Special Publication (SP) 800-207, *Zero Trust Architecture*. The proposed proof-of-concept solution(s) will integrate commercial and open source products that leverage cybersecurity standards and recommended practices to demonstrate the use case scenarios detailed in the *Implementing a Zero Trust Architecture* project description at https://www.nccoe.nist.gov/zerotrust. 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.

**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 *Zero Trust Cybersecurity: Implementing a Zero Trust Architecture* project description (for reference, please see the link in the Process section above) and include, but are not limited to:

**Core Components of Zero Trust Architecture**:

- Policy Engine: The policy engine handles the ultimate decision to grant, deny, or revoke access to a resource for a given subject. The policy engine calculates the trust scores/confidence levels and ultimate access decisions.

- Policy Administrator: The policy administrator is responsible for establishing and/or terminating the transaction between a subject and a resource. It generates any session-specific authentication and authentication token or credential used by a client to access an enterprise resource. It is closely tied to the Policy Engine and relies on its decision to ultimately allow or deny a session.
- Policy Enforcement Point: The policy enforcement point handles enabling, monitoring, and eventually terminating connections between a subject and an enterprise resource.

**Functional Components of Zero Trust Architecture**:

- The data security component includes all the data access policies and rules that an enterprise develops to secure its information, and the means to protect data at rest and in transit.
- The endpoint security component encompasses the strategy, technology, and governance to protect endpoints (e.g., servers, desktops, mobile phones, IoT devices) from threats and attacks, as well as protect the enterprise from threats from managed and unmanaged devices.
- The identity and access management component includes the strategy, technology, and governance for creating, storing, and managing enterprise user (i.e., subject) accounts and identity records and their access to enterprise resources.
- The security analytics component encompasses all the threat intelligence feeds and traffic/activity monitoring for an IT enterprise. It gathers security and behavior analytics about the current state of enterprise assets and continuously

monitors those assets to actively respond to threats or malicious activity. This information could feed the policy engine to help make dynamic access decisions.

**Devices and Network Infrastructure Components of a Zero Trust Architecture**:

- Assets include the devices/endpoints, such as laptops, tablets, and other mobile or IoT devices, that connect to the enterprise.
- Enterprise resources include data and computer resources as well as applications/services that are hosted and managed on-premise, in the cloud, at the edge, or some combination of these.

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 *Zero Trust Cybersecurity: Implementing a Zero Trust Architecture* project description (for reference, please see the link in the PROCESS section above):

- All interactions throughout the proposed architecture are achieved in the most secure manner available, with emphasis on protecting confidentiality and integrity through a consistent identification, authentication, and authorization scheme.
- All interactions throughout the proposed architecture are continually reassessed with possible reauthentication and reauthorization as necessary to mitigate unauthorized access to enterprise resources.
- Access to an enterprise resource is assessed on a per-session basis and authorized specifically for that enterprise resource.
- Access requests are evaluated dynamically based on organizational policies and rules for accessing enterprise resources, including the observable state of:

   a. subject identity (e.g., user account or service identity with associated attributes)
   b. requesting asset (e.g., laptop, mobile device, server) device characteristics (e.g., software version installed, security posture, network location, time/date of request, previously observed behavior, and installed credentials)
   c. requested resource (e.g., server, application, service) characteristics

- Enterprise assets and resources are continuously monitored and reassessed in order to maintain them in the most secure states possible.
- Log and event data generated about the current state of enterprise assets, resources, and interactions throughout the proposed architecture are collected and leveraged for better policy alignment and enforcement to increase the enterprise's overall security posture.
- Secure access to corporate resources, hosted either on-premise or within a cloud environment, as well as to non-corporate resources on the internet are provided without the use of conventional network and network perimeter access and security solutions.
- Integration with various directory protocols and identity management services (e.g., Lightweight Directory Access Protocol [LDAP], OAuth 2.0, Active Directory, OpenLDAP, Security Assertion Markup Language) is demonstrated.
- Integration with security information and event management tools through common application programming interfaces is demonstrated.
- Desired enterprise device security characteristics are demonstrated, including:

a. maintaining data protection at rest and in transit

b. remediating device vulnerabilities that could result in unauthorized access to data stored on or accessed by the device, and misuse of the device

c. mitigating malware execution on the device that could result in unauthorized access to data stored on or accessed by the device, and misuse of the device

d. mitigating the risk of data loss through accidental, deliberate, or malicious deletion or obfuscation of data stored on the device

e. maintaining awareness of and responding to suspicious or malicious activities within and against the device to prevent or detect a compromise of the device

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 Zero Trust Cybersecurity: Implementing a Zero Trust Architecture building block will be conducted in a manner consistent with the following standards and guidance: FIPS 200, SP 800-37, SP 800-53, SP 800-63, and SP 800-207. Additional details about the Zero Trust Cybersecurity: Implementing a Zero Trust Architecture project are available at https://www.nccoe.nist.gov/zerotrust.

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 Zero Trust Cybersecurity: Implementing a Zero Trust Architecture 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 Zero Trust Cybersecurity: Implementing a Zero Trust Architecture 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 Zero Trust Cybersecurity: Implementing a Zero Trust Architecture project capability will be announced on the NCCoE website at least two weeks in advance at https://nccoe.nist.gov/. The expected outcome will demonstrate how the components of the Zero Trust 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 website https://nccoe.nist.gov/.

**Kevin A. Kimball,**

*Chief of Staff.*

[FR Doc. 2020-23292 Filed: 10/20/2020 8:45 am; Publication Date: 10/21/2020]