DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No.: 210914-0185]

National Cybersecurity Center of Excellence (NCCoE) ***Addressing Visibility Challenges With TLS 1.3***

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 letters of interest describing products and technical expertise to support and demonstrate security platforms for the *Addressing Visibility Challenges With TLS 1.3* 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 *Addressing Visibility Challenges With TLS 1.3* project. Participation in the project 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 applied-crypto-visibility@nist.gov or via hardcopy to National Institute of Standards and Technology, NCCoE; 9700 Great Seneca Highway, Rockville, MD 20850. Interested parties can access the letter of interest template by visiting https://www.nccoe.nist.gov/projects/building-blocks/applied-cryptography/cmvp-automation and completing the letter of interest webform. NIST will announce the completion of the selection of participants and inform the public that it will

no longer accept letters of interest for this project at https://www.nccoe.nist.gov/projects/building-blocks/applied-cryptography/addressing-visibility-challenges-tls-13. Organizations whose letters of interest are accepted 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: Tim Polk via phone (301) 975-0225 or email applied-crypto-visibility@nist.gov; by mail to National Institute of Standards and Technology, NCCoE; 9700 Great Seneca Highway, Rockville, MD 20850. Additional details about the *Addressing Visibility Challenges With TLS 1.3* project are available at https://www.nccoe.nist.gov/projects/building-blocks/applied-cryptography/addressing-visibility-challenges-tls-13.

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 *Addressing Visibility Challenges With TLS 1.3* project. The full project can be viewed at: https://www.nccoe.nist.gov/projects/building-blocks/applied-cryptography/addressing-visibility-challenges-tls-13.

Interested parties can access the template for a letter of interest by visiting the project website at https://www.nccoe.nist.gov/projects/building-blocks/applied-cryptography/addressing-visibility-challenges-tls-13 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 as accurate, and submit to NIST by email or hardcopy. NIST will contact interested parties if there are questions regarding the responsiveness of the letters of interest to the project 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 project. When the project has been completed, NIST will post a notice on the *Addressing Visibility Challenges With TLS 1.3* project website at https://www.nccoe.nist.gov/projects/building-blocks/applied-cryptography/addressing-visibility-challenges-tls-13 announcing the completion of the project and informing the public that it will no longer accept letters of interest for this project. Completed letters of interest should be submitted to NIST and will be accepted on a first come, first served basis. There may be continuing opportunity to participate even after initial activity commences for participants who were not selected initially or have submitted the letter of interest after the selection process. Selected participants will be required to enter into a consortium CRADA with NIST (for reference, see ADDRESSES section above).

Project Objective: Deployment of new protocols for exchanging encrypted information, in particular the latest version of the Transport Layer Security (TLS) protocol, TLS 1.3, can impact the ability of some organizations to meet their regulatory, security, and operational requirements due to loss of visibility into the content of communications within their environments. The objective of this project is to demonstrate practical and implementable approaches to help those organizations adopt TLS 1.3 in their private data centers and in hybrid cloud environments while meeting their existing requirements. 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 *Addressing Visibility Challenges with TLS 1.3* project description at https://www.nccoe.nist.gov/projects/building-blocks/applied-cryptography/addressing-visibility-challenges-tls-13. 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 for Letters of Interest: 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 *Addressing Visibility Challenges with TLS 1.3* project description at https://www.nccoe.nist.gov/projects/building-blocks/applied-cryptography/addressing-visibility-challenges-tls-13 and include, but are not limited to:

- Network infrastructure, such as firewalls, routers and switches, and load balancers
- Physically hosted and cloud-based servers, network-attached storage, application servers, web servers, databases, and identity management systems

- Additional components required to achieve visibility (e.g., traffic collection or sensors), as identified in proposed solutions

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 *Addressing Visibility Challenges with TLS 1.3* project description at https://www.nccoe.nist.gov/projects/building-blocks/applied-cryptography/addressing-visibility-challenges-tls-13:

- Proposed contributions must support addressing security, operational, or compliance requirements where traffic is encrypted between one or more sets of components in the demonstration architecture. For example, a solution might focus on achieving visibility into information exchanges between cloud-hosted application servers to support troubleshooting. Alternatively, a solution might analyze information exchanges between physically hosted web servers with hardware security modules and cloud-based services relying on software-based cryptographic modules to monitor for fraudulent transactions. Solutions are not required to address all challenges or all components in the architecture, although comprehensive solutions are strongly encouraged.
- The use of visibility technologies within the enterprise data center environment is generally acceptable in ways that visibility technologies on the public Internet may not be. However, contributions that forgo forward secrecy within the enterprise must be deployable in a manner that preserves forward secrecy for information exchanges over the internet if they are to be accepted.
- While visibility challenges are not limited to a single protocol, the focus for this project is TLS 1.3. Proposed contributions must be compatible with TLS 1.3, excepting those solutions relying upon an alternative network security protocol as

a replacement for TLS. That is, proposed contributions that modify TLS 1.3 or restrict enterprises to earlier version of TLS will not be considered.

- Contributions must support scalable solutions.
- Contributions must support solutions that are relatively easy to implement/deploy.
- Contributions must support solutions that are protocol agnostic.
- Contributions must support solutions that are usable in real time and post-packet capture.
- Contributions must support solutions that are effective for both security and troubleshooting purposes.
- Contributions must support solutions that are widely available and supported in mainstream commercial products and services.
- The baseline criteria apply across the full range of scenarios described in the project description, but some characteristics are more relevant to different categories of solutions than others. Specific characteristics relevant to different classes of solutions include:
    - For solutions that achieve visibility through endpoint mechanisms (e.g., logging) or network architectures (middle boxes, overlays, or mesh service architectures), components need to support demonstration of scalability, ease of deployment, and reliable and timely access to information. For example, scalability and reliable access to historical information would be an area of interest for centralized logging solutions.
    - For solutions that achieve visibility through key management mechanisms that share keys to facilitate TLS decryption, components need to support demonstration that security of keys and data against misuse or compromise and assurance that recorded traffic is not indefinitely at risk of compromise. Specifically, components would need to support

demonstration that (1) the security of systems and procedures used to transmit, store, provide access to, and use the keys, and (2) mechanisms that ensure comprehensive deletion of decryption keys when established temporal or data protection limits are met.

    - For solutions that achieve visibility through analysis of encrypted data, components would need to support demonstrating the capabilities and limitations of these emerging tools with respect to each of the four scenarios.
    - For solutions that rely on alternative network security protocols, components would need to support demonstrating scalability, usability, and ease of deployment. If the solution also includes key management mechanisms to share keys for decryption, the properties identified above would need to be demonstrated.

- For all cases, support for demonstration of management, operational, and technical security controls that compensate and mitigate any potential new risks that may be introduced into the environment will be required.

In their letters of interest, responding organizations need to acknowledge the importance of and 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 *Addressing Visibility Challenges with TLS 1.3* project will be conducted in a manner consistent with the most recent version of the following standards and guidance: FIPS 200, SP 800-37, SP 800-52, SP 800-53, SP 800-63, and SP 1800-16. Additional details about the Addressing *Visibility Challenges with TLS 1.3* project are available at

https://www.nccoe.nist.gov/projects/building-blocks/applied-cryptography/addressing-visibility-challenges-tls-13.

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 *Addressing Visibility Challenges with TLS 1.3* 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 *Addressing Visibility Challenges with TLS 1.3* 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 *Addressing Visibility Challenges with TLS 1.3* 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 solutions that address *Visibility Challenges with TLS 1.3* 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/.

Alicia Chambers,

NIST Executive Secretariat.

[FR Doc. 2021-20907 Filed: 9/24/2021 8:45 am; Publication Date: 9/27/2021]