

From: [Moody, Dustin \(Fed\)](#)
To: [Regenscheid, Andrew R. \(Fed\)](#); [Chen, Lily \(Fed\)](#)
Subject: Re: Join Our Newest Applied Cryptography Project!
Date: Tuesday, September 28, 2021 1:14:37 PM

Ok.

No need to do it then.

From: Regenscheid, Andrew R. (Fed) <andrew.regenscheid@nist.gov>
Sent: Tuesday, September 28, 2021 1:05 PM
To: Chen, Lily (Fed) <lily.chen@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: Join Our Newest Applied Cryptography Project!

My thought would be to hold off until the similar announcement for the NCCoE PQC Migration project. (<https://www.nccoe.nist.gov/projects/building-blocks/post-quantum-cryptography>)

I don't think the TLS visibility project is particularly relevant to the PQC effort. But the PQC migration project would be.

I know Murugiah has been working on getting the FRNs out for a few different projects. The PQC project FRN probably isn't too far behind.

-Andy

From: Chen, Lily (Fed) <lily.chen@nist.gov>
Date: Tuesday, September 28, 2021 at 12:32 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Cc: Regenscheid, Andrew R. (Fed) <andrew.regenscheid@nist.gov>
Subject: Re: Join Our Newest Applied Cryptography Project!

Hi, Dustin,

We certainly can share. But it is more on TLS 1.3. Not too sure how many in the forum are TLS1.3 implementers. Especially, I am not sure how many care TLS visibility issue. Of course, we can forward the questions if we receive to Murugiah and others. Andy may understand the scope better.

Andy, What do you think?

Lily

From: Dustin Moody <dustin.moody@nist.gov>
Date: Tuesday, September 28, 2021 at 12:22 PM
To: Lily Chen <lily.chen@nist.gov>

Subject: Fw: Join Our Newest Applied Cryptography Project!

Lily,

Do you think this would be something that should be shared on the pqc-forum?

Dustin

From: National Cybersecurity Center of Excellence <nccoe@service.govdelivery.com>

Sent: Tuesday, September 28, 2021 11:07 AM

To: Moody, Dustin (Fed) <dustin.moody@nist.gov>

Subject: Join Our Newest Applied Cryptography Project!



[View As Web Page](#)

NCCoE UPDATES

Collaborate With NIST On Our Latest Applied Cryptography Project

Image removed by sender. TLS 1.3



The National Institute of Standards and Technology's (NIST's) [National Cybersecurity Center of Excellence](#) (NCCoE) has issued a [Federal Register Notice](#) (FRN) inviting industry participants and other interested parties to participate in the NCCoE's [Addressing Visibility Challenges With TLS 1.3](#) project.

This project aims to demonstrate practical and implementable approaches to help organizations adopt Transport Layer Security (TLS) protocol version 1.3 in their data centers and hybrid cloud environments while maintaining the visibility into communications needed for regulatory compliance, security, and operations purposes. The project focuses on the security implications of TLS 1.3 protocol implementations that provide system and application administrators and users the necessary visibility into the content of information being exchanged. Approaches that restore visibility into encrypted data in transit, such as alternative key establishment and management approaches or approaches involving tunneling visibility-supporting protocol versions through TLS 1.3, are of initial interest. Other approaches, such as analysis of encrypted data, enhanced auditing, and novel network architectures, will also be considered.

Join Us

There are two ways to engage with the TLS Visibility team on this project:

- **NCCoE Collaborator**—Collaborators are members of the project team and work alongside NCCoE staff to build the demonstration by contributing products, services, and technical expertise. Collaborators are expected to participate in regularly scheduled conference calls, and to help build and document the demonstration.
- **Get Started Today**—If you are interested in becoming an NCCoE collaborator for the TLS Visibility project, first review the requirements identified in the [Federal Register Notice](#) which is based on the [final project description](#). Once you have a good understanding about this project, please [complete this form](#) and you will receive instructions and a Letter of Interest (LOI) where you can present your capabilities. Completed LOIs are considered on a **first-come, first-served basis** within each category of components or characteristics listed in the Federal Register Notice, up to the number of participants in each category necessary to carry out the project build.
- **Collaborator Selection**—The TLS Visibility project team will review all LOIs and may follow up with respondents with questions or to discuss your capabilities. If selected, the TLS Visibility project team will notify you via email. Next, you will receive a [Cooperative Research and Development Agreement \(CRADA\)](#) for review and signature. Once the CRADA has been signed, participants can begin working with the NCCoE to develop an example solution for eventual publication in an NCCoE practice guide. This process can take anywhere from several weeks to a few months. If you submit an LOI and are not selected, the project team will notify you via email.
- **Community of Interest (COI) Membership**—COI members receive periodic updates and the opportunity to share your expertise and help shape this project. [Go here to join the TLS Visibility COI](#).

Questions?

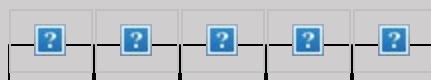
You can contact the project team at applied-crypto-visibility@nist.gov. Keep up with the latest happenings at NIST by following [@NISTcyber on Twitter](#).

Together in cybersecurity,

-TLS Visibility Project Team

[Download the FRN](#)

Connect with us



Received this email from a friend? [Subscribe here.](#)
[Privacy Policy](#)





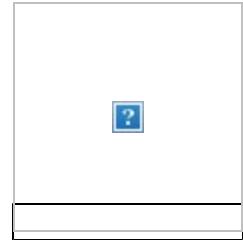
Subscriber services:

[Manage Preferences](#) | [Unsubscribe](#) | [Help](#)

If you have questions or problems with the subscription service, please contact subscriberhelp.govdelivery.com.

Technical questions? Contact inquiries@nist.gov. (301) 975-NIST (6478).

This service is provided to you at no charge by National Institute of Standards and Technology (NIST). 100 Bureau Drive, Stop 1070 · Gaithersburg, MD 20899 · 301-975-6478



|