NIST SPECIAL PUBLICATION 1800-37

Addressing Visibility Challenges with TLS 1.3 within the Enterprise
High-Level Document

Bill Newhouse
Murugiah Souppaya
David Cooper
Tim Polk*
National Institute of Standards

William Barker
Stratvia LLC

Karen Scarfone
Scarfone Cybersecurity

John Kent
Julian Sexton
Michael Dimond
Josh Klosterman
Ryan Williams
The Mitre Corporation

David Wells
Johann Tonsing
Mira Security

Sean Turner
sn3rd

Patrick Kelsey
Not for Radio

Russ Housley
Vigil Security LLC

Tim Cahill
JPMorgan Chase & Company

Muralidharan Palanisamy
AppViewX

Dung Lam
F5

Paul Barrett
Ray Jones
Sandeep Jha
Netscout

Steven Fenter
Jake Wills
US Bank Corporation

Jane Gilbert
D'Nan Godfrey
Thales TCT

Dean Cocklin
Avesta Hojjati
DigiCert

*Contributed while a NIST Employee

September 2025

FINAL

This publication is available free of charge from
https://www.nccoe.nist.gov/addressing-visibility-challenges-tls-13

NIST SPECIAL PUBLICATION 1800-37

Addressing Visibility Challenges with TLS 1.3 within the Enterprise High-Level Document

Bill Newhouse
Murugiah Souppaya
David Cooper
Tim Polk*
National Institute of Standards

William Barker
Stratvia LLC

Karen Scarfone
Scarfone Cybersecurity

John Kent
Julian Sexton
Michael Dimond
Josh Klosterman
Ryan Williams
The Mitre Corporation

David Wells

Johann Tonsing
Mira Security

Sean Turner
sn3rd

Patrick Kelsey
Not for Radio

Russ Housley
Vigil Security LLC

Tim Cahill
JPMorgan Chase & Company

Muralidharan Palanisamy
AppViewX

Dung Lam
F5

Paul Barrett
Ray Jones
Sandeep Jha
Netscout

Steven Fenter
Jake Wills
US Bank Corporation

Jane Gilbert
D'Nan Godfrey
Thales TCT

Dean Cocklin
Avesta Hojjati
DigiCert

*Contributed while a NIST Employee

Final
September 2025

U.S. Department of Commerce
Howard Lutnick, Secretary

National Institute of Standards and Technology
Craig Burkhardt, Acting Under Secretary of Commerce for Standards and Technology and Acting NIST Director

DISCLAIMER

Certain commercial entities, equipment, products, or materials may be identified by name or company logo or other insignia in order to acknowledge their participation in this collaboration or to describe an experimental procedure or concept adequately. Such identification is not intended to imply special status or relationship with NIST or recommendation or endorsement by NIST or NCCoE; neither is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

While NIST and the NCCoE address goals of improving management of cybersecurity and privacy risk through outreach and application of standards and best practices, it is the stakeholder's responsibility to fully perform a risk assessment to include the current threat, vulnerabilities, likelihood of a compromise, and the impact should the threat be realized before adopting cybersecurity measures such as this recommendation.

National Institute of Standards and Technology Special Publication 1800-37, Natl. Inst. Stand. Technol. Spec. Publ. 1800-37, 63 pages, (September 2025), CODEN: NSPUE2

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity issues. This public-private partnership enables the creation of practical cybersecurity solutions for specific industries, as well as for broad, cross-sector technology challenges. Through consortia under Cooperative Research and Development Agreements (CRADAs), including technology partners—from Fortune 50 market leaders to smaller companies specializing in information technology security—the NCCoE applies standards and best practices to develop modular, adaptable example cybersecurity solutions using commercially available technology. The NCCoE documents these example solutions in the NIST Special Publication 1800 series, which maps capabilities to the NIST Cybersecurity Framework and details the steps needed for another entity to re-create the example solution. The NCCoE was established in 2012 by NIST in partnership with the State of Maryland and Montgomery County, Maryland.

To learn more about the NCCoE, visit https://www.nccoe.nist.gov/. To learn more about NIST, visit
https://www.nist.gov.

NIST CYBERSECURITY PRACTICE GUIDES

NIST Cybersecurity Practice Guides (Special Publication 1800 series) target specific cybersecurity challenges in the public and private sectors. They are practical, user-friendly guides that facilitate the adoption of standards-based approaches to cybersecurity. They show members of the information security community how to implement example solutions that help them align with relevant standards and best practices, and provide users with the materials lists, configuration files, and other information they need to implement a similar approach.

The documents in this series describe example implementations of cybersecurity practices that businesses and other organizations may voluntarily adopt. These documents do not describe regulations or mandatory practices, nor do they carry statutory authority.

ABSTRACT

The Transport Layer Security (TLS) protocol is widely deployed to secure network traffic. TLS 1.3 protects the contents of its previous TLS communications even if a TLS-enabled server is compromised. This is known as forward secrecy. The approach used to achieve forward secrecy in TLS 1.3 may interfere with passive decryption techniques that enterprises rely on to have visibility into their TLS 1.2 traffic. Enterprises' authorized network security staff rely on that visibility to protect its data and systems with critical cybersecurity controls to meet operational needs and legal requirements. Adoption of the TLS 1.3 protocol can disrupt current approaches to observing and monitoring internal network communications within an enterprise.

The NCCoE, in collaboration with technology providers and enterprise customers, initiated a project to demonstrate options for maintaining visibility within the TLS 1.3 protocol using several standards-compliant builds that enterprises can use for real-time and post-facto systems monitoring and analytics capabilities.

This publication contains demonstrated proofs of concept along with links to detailed technical information online on NIST pages. This publication also includes links to mappings of TLS 1.3 visibility principles to commonly used security standards and guidelines.

KEYWORDS

bounded lifetime; break and inspect; ephemeral; key management; middlebox; passive decryption; passive inspection; protocol; Transport Layer Security (TLS); visibility.

ACKNOWLEDGMENTS

We are grateful to the following individuals for their generous contributions of expertise and time.

Name	Organization
Ravishankar Chamarajnagar	AppViewX
Michael Ackermann	Blue Cross Blue Shield
Jonathan Chen	F5
Ryan Johnson	F5
Brad Otlin	F5
Kevin Stewart	F5
Nanjaiah Vijayalakshmi	NETSCOUT Corporation
Gina Scinta	Thales Trusted Cyber Technologies
Lauren Brown	JPMorgan Chase & Company

The Technology Partners/Collaborators who participated in this build submitted their capabilities in response to a notice in the Federal Register. Respondents with relevant capabilities or product components were invited to sign a Cooperative Research and Development Agreement (CRADA) with NIST, allowing them to participate in a consortium to build this example solution. We worked with:

Technology Partner/Collaborator	Build Involvement
AppViewX	NETSCOUT Corporation
DigiCert	Not for Radio LLC
F5	Thales Trusted Cyber Technologies
JPMorgan Chase & Company	U.S. Bank Corporation

Technology Partner/Collaborator	Build Involvement
Mira Security, Inc.	

DOCUMENT CONVENTIONS

The terms “shall” and “shall not” indicate requirements to be followed strictly to conform to the publication and from which no deviation is permitted. The terms “should” and “should not” indicate that among several possibilities, one is recommended as particularly suitable without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required, or that (in the negative form) a certain possibility or course of action is discouraged but not prohibited. The terms “may” and “need not” indicate a course of action permissible within the limits of the publication. The terms “can” and “cannot” indicate a possibility and capability, whether material, physical, or causal.

NOTICE: The Information Technology Laboratory (ITL) has requested that holders of patent claims whose use may be required for compliance with the guidance or requirements of this publication disclose such patent claims to ITL. However, holders of patents are not obligated to respond to ITL calls for patents and ITL has not undertaken a patent search in order to identify which, if any, patents may apply to this publication.

As of the date of publication and following call(s) for the identification of patent claims whose use may be required for compliance with the guidance or requirements of this publication, no such patent claims have been identified to ITL.

No representation is made or implied by ITL that licenses are not required to avoid patent infringement in the use of this publication.

Table of Contents

List of Figures

List of Tables