Traffic Light Protocol

Moving to Version 2.0

September 2022

OVERVIEW

Managed by the Forum of Incident Response and Security Teams (FIRST), Traffic Light Protocol, or TLP, is a system of markings that communicates information sharing permissions. According to FIRST, the purpose of TLP is "to facilitate greater sharing of potentially sensitive information and more effective collaboration." **Note:** Unlike formal classification systems, TLP is not legally binding.

MOVING TO TLP 2.0

In August 2022, FIRST released a version 2.0 of TLP, which brings two major changes:

- TLP:CLEAR replaces TLP:WHITE.
- The new TLP:AMBER+STRICT supplements TLP:AMBER, designating that the information may be shared with the recipient's organization only.

The Cybersecurity and Infrastructure Security Agency will officially move from TLP 1.0 to TLP 2.0 on November 1, 2022.

HOW TO USE TLP 2.0

Senders of information use TLP to designate the extent to which recipients may share potentially sensitive information. The information sender takes the following steps to instruct recipients on how far they may reshare:

1. Determine the recipients with whom you would like to share your information and consult the TLP definitions and use cases to determine the appropriate marking. (See CISA's TLP 2.0 User Guide for definitions and use cases.)
2. Label your information with the selected TLP designation.
    a. **Documents:** Insert the TLP label and any caveats in the header and footer of each page. Right-justify the label, use at least a **12-point** font size, and use the correct color coding. Where needed, designate both the beginning and the end of the text to which each TLP label applies.
    b. **Automated Information Exchanges:** Exchange designers who have incorporated TLP 1.0 should ensure they upgrade their exchanges to TLP 2.0. Exchange designers should determine how best to incorporate TLP in their exchanges.
    c. **Emails and Chats:** TLP-labeled messaging must indicate the TLP label of the information, as well as any caveats, directly prior to the information itself. For emails, begin the subject line with the TLP label (include any caveat in the subject line or at the start of the message). Where needed, designate both the beginning and the end of the text to which

each TLP label applies. For standing chat channels, a pinned message or rules of behavior document may establish a default TLP level for the channel that applies in the absence of a specific marking.

d. **Verbal Discussions:** In verbal discussions, speakers may designate the information they are communicating at a TLP level and, if needed, caveat. Participants should assume information is TLP:CLEAR if the speaker does not provide a designation. Conference programs may designate TLP levels for speeches/discussions with the understanding that the lack of a designation signifies TLP:CLEAR. Conference programs may also designate a different TLP level as the default level if the speaker does not provide a designation.

RESOURCES

When in doubt as to whether or how you can share TLP-marked information, always circle back to the sender to clarify and seek permission. For additional resources, see:

- CISA's TLP 2.0 User Guide
- FIRST Standards Definitions and Usage Guidance — TLP Version 2.0