# TLP | TRAFFIC LIGHT PROTOCOL

| When should it be used? | Color | How may it be shared? |
|---|---|---|
| Sources may use TLP: RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused. | RED | Recipients may not share TLP: RED information with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed. |
| Sources may use TLP: AMBER when information requires support to be effectively acted upon, but carries risks to privacy, reputation, or operations if shared outside of the organizations involved. | AMBER | Recipients may only share TLP: AMBER information with members of their own organization who need to know, and only as widely as necessary to act on that information. |
| Sources may use TLP: GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector. | GREEN | Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. |
| Sources may use TLP: WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. | WHITE | TLP: WHITE information may be distributed without restriction, subject to copyright controls. |

US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

# TLP | FAQ

## What is TLP?

The Traffic Light Protocol (TLP) is a set of designations used to ensure that sensitive information is shared with the correct audience. It employs four colors to indicate different degrees of sensitivity and the corresponding sharing considerations to be applied by the recipient(s).

The originator of information to be handled according to TLP should label the information with the correct TLP color in order to indicate how widely that information may be disseminated, usually by including "TLP: [Color]" in unambiguous text in the header and footer of the document and initialing the markings. If a recipient needs to share the information more widely than indicated by the original TLP designation, they must refer back to the original source.

Please refer to the TLP Matrix above for more detailed information on when to employ the TLP colors (Red, Amber, Green, and White) and how each type of TLP designated information can be shared.

## Why use TLP?

US-CERT works closely with domestic agencies, international governments, and private sector organizations to coordinate cyber incident identification and response. TLP provides a simple and intuitive schema for indicating when and how sensitive cybersecurity information can be shared within the global cybersecurity community of practice, encouraging more frequent and effective collaboration between US-CERT and its partners.

## How is TLP related to other classification and marking schemes?

TLP does not apply to classified information.

The Controlled Unclassified Information (CUI) program seeks to standardize the way U.S. Executive departments and agencies handle sensitive but unclassified (SBU) information, including information marked as "For Official Use Only (FOUO)," "Law Enforcement Sensitive (LES)," and others. It should be noted that the TLP designations are not a category or sub-category under the CUI program.

## Does TLP designation hold any implications regarding the Freedom of Information Act (FOIA)?

TLP designation does not have any bearing on FOIA or any other law governing public access to government-held information.

## Who else uses TLP?

In addition to US-CERT and other domestic communities of cybersecurity practitioners, TLP is also employed by public and private sector organizations within Australia, Canada, Finland, France, Germany, Hungary, Italy, Japan, Netherlands, New Zealand, Norway, Sweden, Switzerland, and the United Kingdom.

U.S. DEPARTMENT OF HOMELAND SECURITY

US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM