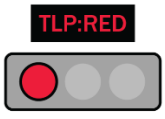
Federal Government Use of the Traffic Light Protocol

The U.S. Government (USG) supports the use of the Traffic Light Protocol (TLP) to foster trust and collaboration in the cybersecurity community and to guide the proper handling of threat intelligence and other cybersecurity data shared between the private sector, individual researchers, and Federal Departments and Agencies. The TLP standards are a marking system that designates information handling permissions for data, documents, or other communications. Organizations and individuals around the world rely on TLP to ensure potentially sensitive or proprietary cybersecurity information is received and not further disseminated except in the manner indicated by the sender.

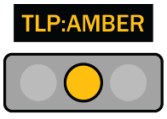
The USG follows TLP markings on cybersecurity information voluntarily shared by an individual, company, or other any organization, when not in conflict with existing law or policy. We adhere to these markings because trust in data handling is a key component of collaboration with our partners.

The Forum of Incident Response and Security Teams (FIRST) is the authoritative global lead of TLP standards and guidance, and the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) co-chairs the FIRST Special Interest Group where TLP is governed. While not legally binding, TLP is a globally accepted and practiced method of communicating expectations for dissemination of data. Through CISA, the USG will continue to lead in the use of TLP.

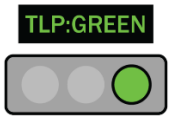
The definitions below are simplified versions of the internationally recognized authoritative language, which can be found at CISA.gov (https://www.cisa.gov/tlp) or FIRST.org (https://www.first.org/tlp).



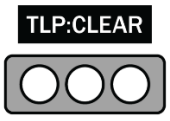
Information marked **TLP:RED** is not for disclosure, and should not be shared with any party outside of the specific exchange in which it was initially shared without explicit permission. This is the strictest TLP handling marking.



Information marked **TLP:AMBER** is for limited disclosure and may be shared on a need to know basis within a recipient's organization and those depending on the recipient to receive cybersecurity information. A more restrictive version of the Amber marking, TLP:AMBER+STRICT, is used to designate that information may be shared within the recipients organization only, and not to any outside parties.



Information marked **TLP:GREEN** is also for limited disclosure but may be shared within a recipient's community. Generally, information marked TLP:GREEN can be shared with peers and partner organizations, but not via publicly accessible channels.



Information marked TLP:CLEAR can be disclosed and shared freely; there are no associated information handling restrictions.

For further information on the TLP standards and detailed instructions on how to use it, please refer to guidance shared by the FIRST organization and CISA using the following resources:

- https://www.first.org/tlp
- https://www.cisa.gov/tlp
- https://www.cisa.gov/resources-tools/resources/tlp-20-user-guide
- https://www.cisa.gov/resources-tools/resources/tlp-20-fact-sheet