Traffic Light Protocol 2.0 User Guide

Publication: September 2022
Cybersecurity and Infrastructure Security Agency

Table of Contents

Background **3**

Purpose **3**

TLP 2.0 Changes **3**

TLP Usage Guidance **3**

Appendix A: TLP 2.0 Definitions **5**

Appendix B: TLP 2.0 Terminology Definitions and Colors **6**

TLP 2.0 Terminology Definitions **6**

TLP 2.0 Color Coding **6**

Appendix C: TLP Use Cases **7**

TLP Recipient-Based Chart of Use Cases **7**

Appendix D: TLP 2.0 Frequently Asked Questions **11**

Background

Traffic Light Protocol (TLP) is a system of markings that designates the extent to which recipients may share potentially sensitive information. Though the protocol has been in use for nearly two decades by the incident coordination and response community, the Forum of Incident Response and Security Teams (FIRST) formally published TLP 1.0 in August 2016. FIRST published TLP 2.0 in August 2022.

Note: TLP is not legally binding and does not override legal restrictions or obligations. TLP is not a formal classification scheme and was not designed to handle licensing terms, nor information handling or encryption rules. TLP labels and their definitions are not intended to have any effect on freedom of information or "sunshine" laws or other laws in any jurisdiction, including the Cybersecurity Information Sharing Act of 2015, which provides certain protections for cyber threat indicators shared with federal agencies and also requires those agencies to share with one another.

Purpose

According to FIRST, the purpose of TLP is "to facilitate greater sharing of potentially sensitive information and more effective collaboration." Version 2.0 improves TLP by further clarifying sharing restrictions.

TLP 2.0 Changes

FIRST released TLP 2.0 in early August 2022 so that it may be fully implemented by January 2023. With TLP 2.0, TLP markings and their definitions are more comprehensive and accessible. TLP 2.0 brings two major changes:

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

See Appendix A for revised definitions of TLP markings and Appendix B for TLP 2.0 definitions for the following terms: community, organization, and clients.

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

TLP Usage Guidance

TLP provides a schema for communicating information sharing permissions. With TLP, the information sender takes the following steps to instruct recipients on how far they may reshare the information.

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 TLP marking. (See appendices.)
2. Label your information with the selected TLP designation. (See Appendix B for color coding.)
    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 TLP level as the default level if the speaker does not provide a designation.

Appendix A: TLP 2.0 Definitions

In TLP 2.0, FIRST further clarified the meanings of the four TLP designations. (Gray text is 1.0; black text is 2.0.)

1.0 TLP:RED = Not for disclosure, restricted to participants only. 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. Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.

2.0 TLP:RED = For the eyes and ears of individual recipients only, no further disclosure. Sources may use TLP:RED when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved. Recipients may therefore not share TLP:RED information with anyone else. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting.

1.0 TLP:AMBER = Limited disclosure, restricted to participants' organizations. Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.

2.0 TLP:AMBER = Limited disclosure, recipients can only spread this on a need-to-know basis within their organization and its clients. Note that TLP:AMBER+STRICT restricts sharing to the organization only. Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. **Note:** If the source wants to restrict sharing to the organization only, they must specify **TLP:AMBER+STRICT**.

1.0 TLP:GREEN = Limited disclosure, restricted to the community. 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. Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.

2.0 TLP:GREEN = Limited disclosure, recipients can spread this within their community. Sources may use TLP:GREEN when information is useful to increase awareness within their wider community. Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. TLP:GREEN information may not be shared outside of the community. **Note:** When "community" is not defined, assume the cybersecurity/cyber defense community.

1.0 TLP:WHITE = Disclosure is not limited. 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. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

2.0 TLP:CLEAR = Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

Appendix B: TLP 2.0 Terminology Definitions and Colors

TLP 2.0 Terminology Definitions

In TLP 2.0, FIRST has provided the following definitions for commonly used terms:

Community: Under TLP, a *community* is a group who share common goals, practices, and informal trust relationships. A community can be as broad as all cybersecurity practitioners in a country (or in a sector or region).

Organization: Under TLP, an *organization* is a group who share a common affiliation by formal membership and are bound by common policies set by the organization. An organization can be as broad as all members of an information sharing organization, but rarely broader.

Clients: Under TLP, *clients* are those people or entities that receive cybersecurity services from an organization. Clients are by default included in **TLP:AMBER** so that the recipients may share information further downstream in order for clients to take action to protect themselves. For teams with national responsibility, this definition includes **stakeholders** and **constituents**.[1]

TLP 2.0 Color Coding

In TLP 2.0, FIRST has provided color coding in RGB, CMYK, and Hex.

TLP Colors	RGB: font			RGB: background			CMYK: font				CMYK: background				Hex: font	Hex: background
	R	G	B	R	G	B	C	M	Y	K	C	M	Y	K		
TLP:RED	255	43	43	0	0	0	0	83	83	0	0	0	0	100	#FF2B2B	#000000
TLP:AMBER	255	192	0	0	0	0	0	25	100	0	0	0	0	100	#FFC000	#000000
TLP:GREEN	51	255	0	0	0	0	79	0	100	0	0	0	0	100	#33FF00	#000000
TLP:CLEAR	255	255	255	0	0	0	0	0	0	0	0	0	0	100	#FFFFFF	#000000

Note: TLP is designed to accommodate individuals with low vision, who struggle to read text or cannot see it at all when there is too little color contrast between text and background. Originators should adhere to the TLP color coding to ensure enough color contrast for such readers.

[1] CISA considers "clients" to be stakeholders and constituents that have a legal agreement with CISA.

Appendix C: TLP Use Cases

TLP Recipient-Based Chart of Use Cases

The following chart may be helpful in determining how you may share information that you receive with TLP markings. In all cases, if you and others are co-recipients of the same TLP-marked information, you may discuss and share that information with one another regardless of the TLP marking.

I am a …	Can I share this information with …	Answer
A staff member that serves a cybersecurity function within a government agency.	• Constituents,* • National security partner agencies, and • Regional governments? *See **Appendix B** above for definition of *client*, which includes *constituents.*	You may share **TLP:CLEAR** information.
		You may share **TLP:GREEN** information with recipients who are part of the community as defined by the caveat. • When "community" is not defined, recipients should assume they may share **TLP:GREEN** information with the cybersecurity/cyber defense community. • Originators concerned that recipients may share their **TLP:GREEN** information further than intended should add a caveat that defines the community for the information.
		You may share **TLP:AMBER** information with clients, which in this context includes constituents, national security partner agencies, and regional governments that have a need to know the information (e.g., they provide cybersecurity services). When you do so, you should mark it **TLP:AMBER+STRICT** to ensure that recipients do not further disseminate it to their constituents, as only your organization has been authorized to do that by the originator. **Note:** TLP assumes the originator and recipient have agreed to protect the information. • As with **TLP:GREEN**, originators concerned that recipients may share their **TLP:AMBER** information further than intended should add a caveat to explicitly communicate sharing restrictions for the information.
		You may not share **TLP:AMBER+STRICT** information with organizations outside your immediate agency without permission. If further sharing is desired, contact the originator to request permission to share with other organizations. **Note:** You may use this information to protect outside organizations without sharing the document with them.
		You may not share **TLP:RED** information.

I am a …	Can I share this information with …	Answer
Multinational conglomerate staff member.	• Subsidiaries, • My parent company, and • Our branch organizations domestically and in other countries?	You may share **TLP:CLEAR** information.
		You may share **TLP:GREEN** information with recipients who are part of the community as defined by the caveat. • When "community" is not defined, recipients should assume they may share **TLP:GREEN** information with the cybersecurity/cyber defense community. • Originators concerned that recipients may share their **TLP:GREEN** information further than intended should add a caveat that defines the community for the information.
		You may share **TLP:AMBER** information with subsidiaries, your parent company, and/or branch organizations if your organization provides cyber services for them; however, you must mark the information **TLP:AMBER+STRICT** to ensure these recipients do not further share the information (e.g., to other subsidiaries) without explicit permission from the originator. **Note:** TLP assumes the originator and recipient have agreed to protect the information.
		You may not share **TLP:AMBER+STRICT** information with subsidiaries, your parent company, and/or branch organizations without obtaining permission from the originator. You may share **TLP:AMBER+STRICT** information with staff members within your immediate organization who help your team provide cybersecurity services. **Note:** You/your team/your organization may use this information to protect subsidiaries, your parent company, and/or branch organizations without sharing the information to them.
		You may not share **TLP:RED** information.
A member of a critical infrastructure sector.	• Peers in my sector?	You may share **TLP:CLEAR** and **TLP:GREEN** information.
		You may not share **TLP:AMBER** information with peers unless they are your clients and have a need to know the information.
		You may not share **TLP:AMBER+STRICT** outside your organization unless the peer you wish to share with is a co-recipient of this information, as described above.
		You may not share **TLP:RED** information.

I am a …	Can I share this information with …	Answer
A member of an information sharing and analysis center (ISAC)/formal sharing group.	• Other members in the ISAC/formal sharing group?	You may share **TLP:CLEAR** information with ISAC/formal sharing group members.
		You may share **TLP:GREEN** information with recipients who are part of the community as defined by the caveat. • When "community" is not defined, recipients should assume they may share **TLP:GREEN** information with the cybersecurity/cyber defense community. Originators concerned that recipients may share their **TLP:GREEN** information further than intended should add a caveat that defines the community for the information.
		If you are a member of the of the ISAC/formal sharing group *management body*, you may share **TLP:AMBER** information with the group members if the information was sent to the ISAC/formal sharing group. You may not share the information with the members if you are not part of the ISAC/formal sharing group's management body. **Note:** TLP assumes that the ISAC/formal sharing group and its members have agreed to protect **TLP:AMBER** information.
		You may not share **TLP:AMBER+STRICT** information with members unless you obtain permission from the originator to do so. **Note:** Even when **TLP:AMBER+STRICT** information is sent to the ISAC/formal sharing group management body, the management body may not share it with members without first obtaining permission from the originator.
		Do not share **TLP:RED** information.
An organization that receives outsourced cybersecurity services.	• Organizations providing us cybersecurity services?	You may share **TLP:CLEAR** and **TLP:GREEN** information with organizations providing you cybersecurity services.
		Do not share **TLP:AMBER** or **TLP:AMBER+STRICT** information without obtaining permission from the originator. **Note:** TLP assumes the originator and recipient have agreed to protect the information.
		Do not share **TLP:RED** information.
An organization that receives outsourced		You may share **TLP:CLEAR** with organizations providing you services you wish to protect.

I am a …	Can I share this information with …	Answer
services (e.g., payment, HVAC, chip manufactures, website).	• Organizations providing us these services?	You may share **TLP:GREEN** information that your organization receives with organizations that provide services to you. **Note:** When "community" is not defined, assume the cybersecurity/cyber defense community.
		You may not share **TLP:AMBER** or **TLP:AMBER+STRICT** information without permission. **Note:** TLP assumes the originator and recipient have agreed to protect the information.
Anyone receiving TLP-marked information regularly from an organization.	• Organizations and/or individuals outside the limitation of the TLP marking?	You must obtain permission from the originator to share outside the TLP limitation. To seek this permission, you can: • Request the orginator add a caveat stating the information can be shared to the recipients. • Establish a formal agreement with the originator that describes the specific recipients with whom you will further share their information. • Ask the originator for permission—each time you receive information from them—to further share to specific recipients. Examples of caveats: • *You may share this information with any [domestic] organization providing you with cyber-related services. [Organizations providing you cyber services may not use the information for other clients.]* This generic wording allows for both ongoing services as well as incident response services. The word "domestic" is optional. The restriction on use for other clients is optional; it is implied for **TLP:AMBER+STRICT**. • *You may share this information with your parent organization. They may not share it with any sub-organizations without explicit permission.*

Appendix D: TLP 2.0 Frequently Asked Questions

1. ***What should I do if the information I have received has a TLP marking that restricts me from sharing it with a client/peer/trust group/service provider that needs to know this information?***

   You can take one of three actions to resolve this issue:

   a. Contact the originator and request permission to share it with your client/peer/trust group/service provider.

   b. Establish an agreement with the originator.

   c. Request that the originator add explicit permissions so that you may share the information with your need-to-know client/peer/trust group/service provider.

2. ***If I have received TLP:AMBER information and shared it with my clients, why can't I simply allow those clients to further share this information with their cyber services providers at TLP:AMBER?***

   Allowing recipients of **TLP:AMBER** information to share it at the **TLP:AMBER** level with their cyber services providers would not restrict those providers from further sharing the information to other clients, who may in turn share the information on to their respective clients and service providers, effectively making **TLP:AMBER** the same as **TLP:GREEN**.

3. ***What possibilities should I take into consideration when permitting recipient organizations to further share my TLP:AMBER information with their cyber services and incident response providers?***

   Consider that the provider may be from another country and/or government. When in doubt, reach out to the recipient to fully understand with whom they would like to share the information.

4. ***What should I keep in mind when sharing information at the TLP:GREEN level?***

   To avoid a recipient sharing **TLP:GREEN** further than you intended, ensure recipients understand they are receiving the information because they are members of a defined community.

5. ***What should I do if none of the TLP levels fit how I want to share my information?***

   You may add a caveat to the TLP level you choose for your information that provides explicit details on the extent to which the information may be shared. You may also choose to establish an agreement with the recipient organization that includes these details for all information being shared from your organization.