Guidance on Traffic Light Protocol

Published by authority of the Secretary General

September 2021

International Civil Aviation Organization

GUIDANCE ON TRAFFIC LIGHT PROTOCOL

1. Introduction and Scope

The human element is at the core of addressing cybersecurity and cyber resilience in aviation. As such, raising awareness of everyone is imperative to support a secure and resilient sector. It is equally important that policies are established to ensure the implementation of clear guidelines that minimize confusion over actions to be taken.

When information is received through a communication channel, understanding which information is shareable with others and with whom to share that information is one of the core actions that require raising awareness. Sharing information beyond its intended "sphere of distribution" can result in unintended dissemination of sensitive information that could be exploited and potentially result in damages to the information source.

Accordingly, and in order to ensure clear communication and information sharing guidelines between all aviation stakeholders, ICAO, in cooperation with experts from the Secretariat Study Group on Cybersecurity (SSGC), developed this guidance material on the use of Traffic Light Protocol (TLP).

This guidance is in line with the Cybersecurity Action Plan[1] which action item CyAP5.4 recommends to "Use TLP (Traffic Light Protocol) to state the level of distribution/restrictions when distributing and further sharing cyber-information." Moreover, the use of TLP may be expanded so that TLP could be used in any communication to highlight the sharing permission intended by the source.

States and stakeholders are encouraged to use this guidance material to develop and implement policies for the use of TLP.

2. Objective

This document sets forth guidance on requirements for the use of TLP when sharing information.

3. TLP Guidance

3.1 TLP intent

The Traffic Light Protocol (TLP) was created in order to facilitate greater sharing of information. TLP is a set of designations used to ensure that information is shared with the appropriate audience. It employs colours to indicate expected sharing boundaries to be applied by the recipient(s). TLP has four colours as defined in section 5 below.

TLP provides a simple and intuitive schema for indicating when and how sensitive information can be shared, facilitating more frequent and effective collaboration. TLP is not a "control marking" or classification scheme. TLP is not designed to handle licensing terms, handling & encryption rules, and restrictions on action or instrumentation of information. TLP labels and their definitions are not intended to have any effect on freedom of information or "sunshine laws"[2] in any jurisdiction.

TLP is optimized for ease of adoption, human readability and person-to-person(s) sharing; it may be used in automated sharing exchanges, although is not optimized for that use.

---

[1] ICAO State letter 2020/114

[2] Sunshine laws are regulations requiring transparency and disclosure in government or business. Sunshine laws make meetings, records, votes, deliberations, and other official actions available for public observation, participation, and/or inspection.

TLP is distinct from the Chatham House Rule (when a meeting, or part thereof, is held under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed), but may be used in conjunction if it is deemed appropriate by participants in an information exchange.

3.2 TLP requirements (R)

- R1: The source of information has the duty to allocate the relevant TLP marking to the shared information.
- R2: The recipient of TLP marked information shall comply with the TLP marking.
- R3: The TLP marking shall be allocated by the source considering the need to know basis of the recipient(s) and its(their) ability to conduct actions based on the information being shared and its TLP marking.
- R4: The source is responsible for ensuring that recipients of TLP information understand and can follow TLP sharing guidance.
- R5: If a recipient needs to share the information more widely than indicated by the original TLP designation, they shall obtain explicit permission from the original source.
- R6: It is recommended to have a single TLP marking per document, however if a document has different TLP markings, the marking of each line or section shall be clearly expressed.
- R7: If some specific restrictions for further distribution going beyond the definition of the allocated TLP marking (e.g. TLP:GREEN only for the aviation community), it shall be clearly expressed.
- R8: The recipient of TLP marked information shall not change the TLP marking when further distributing information received from a source.

4. How to use TLP

4.1 How to use TLP in email

TLP-designated email correspondence should indicate the TLP colour of the information in the Subject line and in the body of the email, prior to the designated information itself. The TLP colour must be in capital letters: TLP:RED, TLP:AMBER, TLP:GREEN, or TLP:WHITE. Below is a sample of the TLP colour indication:

4.2 How to use TLP in documents

TLP-designated documents should indicate the TLP colour of the information in the header and footer of each page. To avoid confusion with existing control marking schemes, it is advisable to right-justify TLP designations. The TLP colour should appear in capital letters and in 12 point type or greater. Below is a sample of the TLP colour indication:

5. TLP definitions[3] [4]

The Traffic Light Protocol (TLP) provides a means for the Information source to categorize Information, and specify the limitations on dissemination of each class of the Information that it provides.

The TLP designations and associated restrictions on use and limitations are as:

TLP DESIGNATION	RESTRICTION ON ACCESS AND USE	EXAMPLE
TLP:RED	Not for disclosure, restricted to Recipients 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.	Information shared with people in a meeting; direct email with TLP:RED Categorization.
TLP:AMBER	Limited disclosure, restricted to Recipients' 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.**	Sharing of Indicators of Compromise (IoCs) to an organisation's CSIRT. These could be forwarded to the SOC for further action.
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	Sharing of a malware analysis with the local aviation industry sector.

[3] See: https://www.cisa.gov/tlp
[4] See: https://www.first.org/tlp

	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.	
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.	Public security advisory.

6. Acronyms

CSIRT	Computer Security Incident Response Team
ICT	Information and Communication Technology
IoCs	Indicators of Compromise
SOC	Security Operation Centre
TLP	Traffic Light Protocol

— END —