U.S. Department of Homeland Security (DHS)

# TLP to IEP Evolution: What, Why & How

30th Annual FIRST Conference, Kuala Lumpur, Malaysia
June 28, 2018

Tom Millar


Homeland Security

TLP:WHITE

# Disclaimer & Notification

This presentation is intended for informational and discussion purposes only.

The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding this information. In no event shall the United States Government or its contractors or subcontractors be liable for any damages, including but not limited to, direct, indirect, special or consequential damages, arising out of, resulting from, or in any way connected with this information, whether or not based upon warranty, contract, tort, or otherwise, whether or not arising out of negligence, and whether or not injury was sustained from, or arose out of the results of, or reliance upon the information.

The display of the DHS official seal or other DHS visual identities shall not be interpreted to provide any person or organization the authorization to use the official seal, insignia or other visual identities of the Department of Homeland Security. The DHS seal, insignia, or other visual identities shall not be used in any manner to imply endorsement of any commercial product or activity by DHS or the United States Government. Use of the DHS seal without proper authorization violates federal law (e.g., 18 U.S.C. §§ 506, 701, 1017), and is against DHS policies governing usage of its seal.

This presentation is Traffic Light Protocol (TLP): WHITE. Recipients may share TLP: WHITE information without restriction, subject to copyright controls. For more information on the TLP, see http://www.us-cert.gov/tlp.

DHS does not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply their endorsement, recommendation, or favoring by DHS.

# Who am I?

Member of US-CERT since 2007

- Served as a Network Analyst, Senior Watch Officer, and Chief of Communications
- Led the implementation of Traffic Light Protocol (TLP) across US-CERT's entire product line beginning in 2011
- Supported initial conception and development of the Structured Threat Information eXchange (STIX) and Trusted Automated eXchange of Indicator Information (TAXII)

Currently assigned as a Technical Advisor to the Under Secretary of the National Protection and Programs Directorate in DHS

Co-chair of the FIRST Traffic Light Protocol SIG and FIRST Ethics SIG

TLP:WHITE

"TLP is a set of designations used to ensure that sensitive information is shared with the appropriate audience."*

It's a simple system for sharing across boundaries (organizational, public-private, geopolitical, etc.)

It's designed to help pre-empt the question "Can I share this with...?" when sending threat or vulnerability information

TLP is not a "control marking" or classification scheme.

*https://first.org/tlp/

# What is TLP?
## (A refresher)

# What is TLP? (A refresher, slide 2)

| | | |
|---|---|---|
| **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. |
| **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.** |
| **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 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. |

# Known limitations of TLP

TLP is for people. It is not optimized for networks of automated indicator sharing systems.


AMBER can be ambiguous at times (such as when recipients are expected to strictly adhere to “share, but only within your own organization” rules)

There is no standardized way of including additional caveats, such as “for passive detection only / do not block”

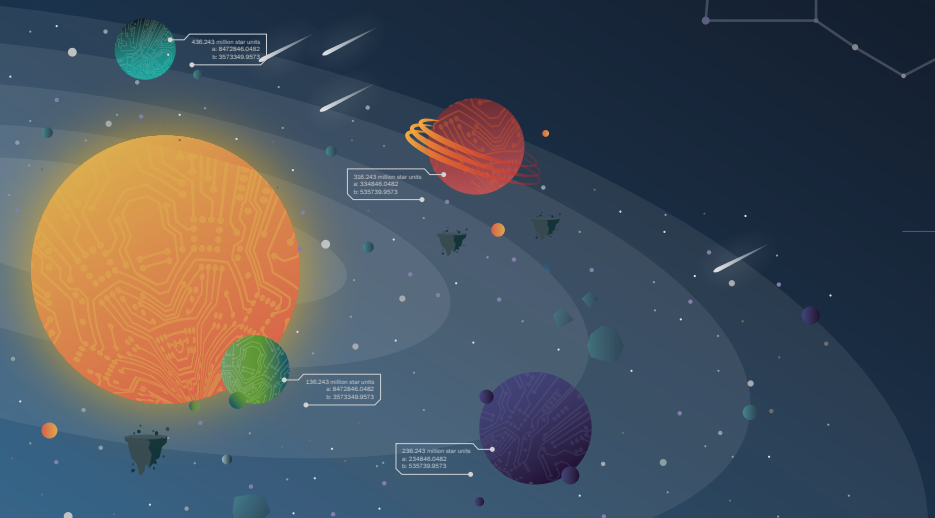
- This is on purpose, by the way…

“TLP only has four colors; any designations not listed in this standard are not considered valid by FIRST”

TLP is simple; for better and for worse.

TLP:WHITE

# Introducing: THE Information Exchange Protocol (IEP)



- The IEP is intended to support existing approaches to defining information exchange policies used by CSIRTs, as well as enabling newer information exchange policies that organizations need as their sharing activities mature and evolve.
- Developed by the FIRST IEP SIG
- Currently in 1.0*, version 2.0 coming very soon.

*https://first.org/iep/

TLP:WHITE

# Why IEP?

**The communities that CSIRTs and PSIRTs inhabit are growing**, just as FIRST is - small trust groups of perhaps one or two hundred individuals are now groups of one or two hundred teams, comprising thousands of individuals. (See: “Dunbar’s Number”)

**Threat (and Vulnerability) Intelligence as-a-Service** is now regularly offered by many different types of organizations, to many different groups and communities

**Increasing automation**, and increasing interoperability of automated systems

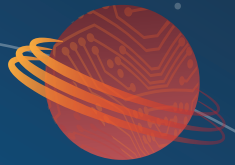
TLP:AMBER

Lastly: See previous slide on **TLP’s limitations**

TLP:WHITE

# IEP 1.0 101

- IEP is fully compatible with TLP
- However, it extends far beyond what TLP is designed to express
- It provides four Policy Types:
  - Handling, for any obligations or controls on the information, e.g. ENCRYPT IN TRANSIT
  - Action, for permitted actions or uses of the information, e.g. INTERNALLY VISIBLE ACTIONS
  - Sharing, for any permitted redistribution, e.g. TRAFFIC LIGHT PROTOCOL
  - Licensing, for any applicable agreements, licenses, or terms of use, e.g. UNMODIFIED RESALE
- It's a framework that allows (and encourages) machine-readable implementations for automation and information management (an example JSON implementation is included in Appendix A of 1.0)



# IEP 1.0 102

- IEP answers for a significant number of use cases that we have seen over the years, at US-CERT and at our partner organizations, especially large Information Sharing and Analysis Centers (ISACs):
  - **Embargo dates:** IEP policy statements can carry start and end date metadata, so it's possible to have TLP:RED end and TLP:GREEN begin at a particular point in time.
  - **"Chatham House Rule:"** IEP allows for Sharing policy statements beyond TLP, including "PROVIDER ATTRIBUTION": "MUST NOT"
  - **Standardized caveats:** IEP provides a framework for establishing a dictionary of caveats and reference URLs.

TLP:WHITE

# IEP: HOW?

- Read up on the framework at **first.org/iep**
- Join the IEP SIG mailing list
  - IEP has been added as a marking type in STIX 2.1, coming soon
  - DHS plans to begin IEP adoption in 2019, along with STIX 2.1
    - » Check out the Terms of Use and other documentation at **us-cert.gov/ais** to see if you can take advantage of our Automated Indicator Sharing program.

A couple of points to note:

IEP does not solve the issue of having to negotiate and agree upon terms and conditions with your community (in other words, it does not make lawyers obsolete) - but if your trust groups and automated sharing efforts are outgrowing TLP, then you should consider IEP as a potential next step.


Homeland Security