STIX Information Exchange Policy Marking

"What am I allowed to do with this intel?"

Please note: This proposal is for the upcoming IEP 2.0 standard which will be released within the next three months. IEP 2.0 is currently in draft status and will be undergoing public review over the next few months.

Also note: The URLs and IDs contained in this proposal are NOT final and may be changed in the final version.

What is it?

The FIRST Information Exchange Policy (IEP) Framework enables threat intelligence providers to inform recipients of how they may use the threat intelligence they receive. IEP ensures that both parties are aware of any restrictions on the use of the shared threat intelligence, and reduces the likelihood of misunderstandings.

FIRST, interested in enabling the global development and maturation of CSIRTs, recognized that the general lack of adequate policy supporting information exchange is increasingly becoming an impediment to information sharing amongst CSIRT teams.

Why do we need it?

Automating the exchange of security and threat information in a timely manner is crucial to the future and effectiveness of the security response community.

The timely distribution of sensitive information will only thrive in an environment where both producers and consumers have a clear understanding of how shared information can and cannot be used, with very few variations of interpretation.

The general lack of adequate policy that supports information exchange is increasingly becoming an impediment to timely sharing. This will only be exacerbated as more organizations start actively participating in information exchange communities and the volume of security and threat information being shared continues to grow.

The Traffic Light Protocol (TLP) is the most commonly used method to mark and protect information that is shared. The original intent behind TLP was to speed up the time-to-action on shared information by pre-declaring the permitted redistribution of that information, reducing the need for everyone to ask the producer if it could be “shared with XYZ in my organization” and for that purpose TLP still works.

The challenge for producers of information is that they need to be able to convey more than just the permitted redistribution of the information. There can be a lack of clarity when defining and interpreting the permitted actions and uses of information shared between organizations. This is compounded by the sensitive nature and commercially competitive aspects of security and threat information.

How would it work?

I propose that we add two new Information Exchange Policy Marking Objects to STIX 2.1.

1. An IEP Data Marking object
2. An IEP Reference Data Marking object

This would allow Threat Intelligence Producers to use IEP 2.0 to mark their threat intelligence with restrictions on Handling, Action, Sharing and Licensing. See the FIRST IEP-SIG Homepage for more information.

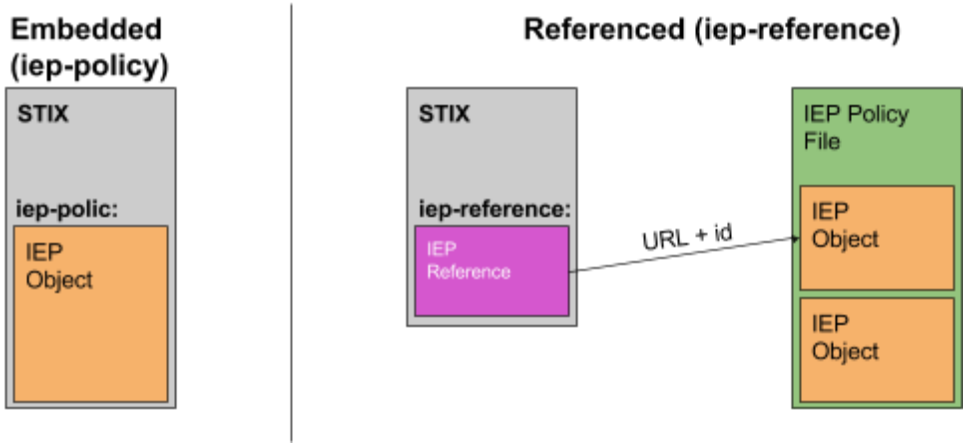
What benefits would it provide?

The Information Exchange Policy (IEP) Framework provides much more detail about what a Producer will let a Consumer do with the threat intelligence they receive. It is a LOT more detail than the commonly used TLP definitions provide, and this detail will go a long way towards making threat intelligence sharing operate effectively at scale.

An example IEP 2.0 JSON object is shown below as an illustration of the detail IEP provides:

```
{
	"id": "01bc4353-4829-4d55-8d52-0ab7e0790df9",
	"name": "FIRST IEP-SIG TLP-AMBER",
	"version": 2.0
	"start_date": "2017-01-01T00:00:00Z",
	"end_date": null,
	"encrypt_in_transit": "may",
	"encrypt_at_rest": "may",
	"permitted_actions": "externally-visible-direct-actions",
	"affected_party_notifications": "may",
	"tlp": "amber",
	"attribution": "must-not",
	"obfuscate_affected_parties": "may",
	"unmodified_resale": "must-not",
	"external_reference": " https://www.first.org/about/policies/bylaws"
}
```

An IEP can either be embedded in the Information Exchange Policy Data Marking Object, or can be placed into a network-accessible IEP Policy File, and can be referenced from the Information Exchange Policy Reference Data Marking Object. The difference between the two uses of IEP 2.0 is summarized in the diagram below:



STIX object proposal

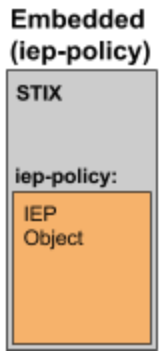
Information Exchange Policy (IEP) Data Marking Object Type

The IEP marking type defines how you would represent an Information Exchange Policy (IEP) marking in a definition field. The value of the **`definition_type`** property **MUST** be `iep-policy` when using this marking type.

Property Name	Type	Description
`definition_type` (required)	`string`	Value MUST be set to `iep-policy`.
`definition` (required)	`iep-policy`	Contains an embedded JSON IEP object as specified in the FIRST IEP JSON Specification available on the FIRST IEP-SIG website.

The **`definition`** field **MUST** only house an embedded JSON IEP object as defined in the FIRST IEP JSON Specification available on the FIRST IEP-SIG website. The embedded IEP JSON object contains a list of IEP Policy Statements that explicitly define what the Object Policy Authority will allow the Consumer to do with the threat intelligence information marked with this data marking.

The diagram below shows the relationship between STIX and the embedded IEP policy:



IEP Data Marking Object Example

An embedded IEP Policy example:

```
{
```

```
  "type": "marking-definition",
  "id": "marking-definition--34098fce-860f-48ae-8e50-ebd3cc5e41da",
  "created": "2016-08-01T00:00:00Z",
  "modified": "2016-08-01T00:00:00Z",
  "definition_type": "iep-policy",
  "definition":
    "id": "01bc4353-4829-4d55-8d52-0ab7e0790df9",
    "name": "FIRST IEP-SIG TLP-AMBER",
    "version": 2.0
    "start_date": "2017-01-01T00:00:00Z",
    "end_date": null,
    "encrypt_in_transit": "may",
    "encrypt_at_rest": "may",
    "permitted_actions": "externally-visible-direct-actions",
    "affected_party_notifications": "may",
    "tlp": "amber",
    "attribution": "must-not",
    "obfuscate_affected_parties": "may",
    "unmodified_resale": "must-not",
    "external_reference": " https://www.first.org/about/policies/bylaws"
  }
}
```

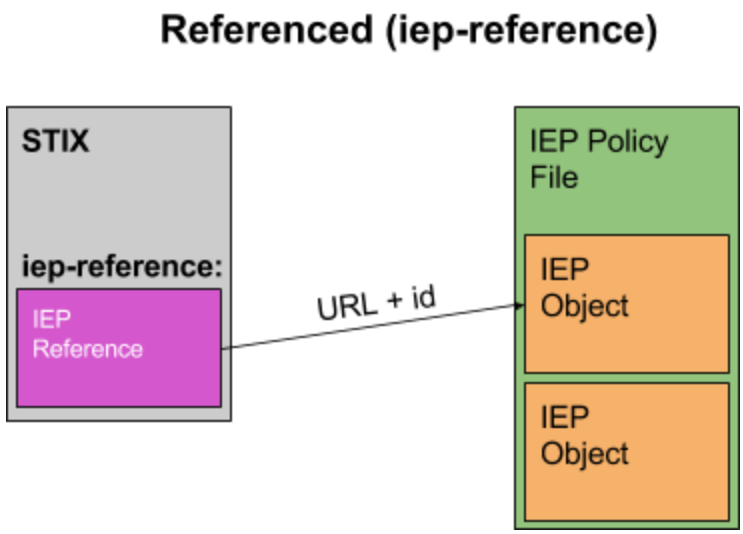
Information Exchange Policy (IEP) Reference Marking Object Type

The IEP Reference marking type defines how you would represent a reference to a network accessible Information Exchange Policy (IEP) policy stored elsewhere from a definition field. The value of the **`definition_type`** property **MUST** be `iep-reference` when using this marking type.

Property Name	Type	Description
`definition_type` (required)	`string`	Value MUST be set to `iep-reference`.
`definition` (required)	`iep-reference`	Contains an IEP Policy Reference JSON object that points to a network accessible IEP Policy File as specified in the FIRST IEP JSON Specification available on the FIRST IEP-SIG website.

The **`definition`** field **MUST** only house an IEP Policy Reference JSON object as defined in the FIRST IEP JSON Specification available on the FIRST IEP-SIG website. The IEP Policy Reference JSON object contains a URL and an id_ref that points to a network accessible IEP Policy File that contains the IEP JSON object. The use of an IEP Reference provides a level of indirection that allows many different implementations to 'share' the same Information Exchange Policy, reducing the overhead of transmitting the IEP Policy multiple times, and allowing different implementations to reuse a common set of definitions.

The diagram below shows the relationship between STIX and the referenced IEP policy (handled via the iep-reference):



IEP Reference Data Marking Object Example

A referenced FIRST IEP TLP-Amber Policy example:

```
{
  "type": "marking-definition",
  "id": "marking-definition--34098fce-860f-48ae-8e50-ebd3cc5e41da",
  "created": "2016-08-01T00:00:00Z",
  "modified": "2016-08-01T00:00:00Z",
  "definition_type": "iep-reference",
  "definition": {
    "id_ref": "9891b2be-aa5a-4cb2-8a87-b3af93744d85",
    "url": "https://www.first.org/iep/2.0/first-iep-sig-tlp-amber.iepj",
    "version": 2.0
  }
}
```

9.1.7. Pre-defined FIRST IEP-SIG Policies

The FIRST IEP-SIG have developed some standard IEP Policy files and have made them Internet accessible to help Implementers standardize on a common set of IEP Policies. This will aid adoption and ensure all parties within a threat intelligence sharing community know what behaviour is expected of them.

FIRST IEP-SIG IEP 2.0 TLP Red Policy

Policy Name	FIRST IEP-SIG IEP 2.0 TLP Red
Policy ID	`5e607e88-ab70-4977-8c1b-ee3a16b0f68c`
Policy URL	https://www.first.org/iep/2.0/first-iep-sig-tlp-red.iepj

FIRST IEP-SIG IEP 2.0 TLP Amber Policy

Policy Name	FIRST IEP-SIG IEP 2.0 TLP Amber
Policy ID	`01bc4353-4829-4d55-8d52-0ab7e0790df9`

Policy URL	https://www.first.org/iep/2.0/first-iep-sig-tlp-amber.iepj

FIRST IEP-SIG IEP 2.0 TLP Green Policy

Policy Name	FIRST IEP-SIG IEP 2.0 TLP Green
Policy ID	3903ce63-674c-4b70-9457-8c5527dd9115
Policy URL	https://www.first.org/iep/2.0/first-iep-sig-tlp-green.iepj

FIRST IEP-SIG IEP 2.0 TLP White Policy

Policy Name	FIRST IEP-SIG IEP 2.0 TLP White
Policy ID	0d783790-b221-40c1-840a-5787330612c1
Policy URL	https://www.first.org/iep/2.0/first-iep-sig-tlp-white.iepj