Information Exchange Policy v2 JSON Implementation Standard

Copyright Notice

Abstract

The FIRST Information Exchange Policy (IEP) framework enables threat intelligence providers to inform users 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.

Co-chairs

The FIRST IEP-SIG Co-chairs at the time of release were:

- Terry MacDonald
- Paul McKitrick
- Merike Kaeo
- Steve Mancini

Editors

The FIRST IEP v2 JSON Implementation Standard was created and edited by the following people:

- Terry MacDonald
- Paul McKitrick

Contributors

The following people contributed to the FIRST IEP v2 JSON Implementation Standard:

- Terry MacDonald
- Paul McKitrick

Contents

1. Introduction

1.1 Purpose

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[1] (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.

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.

The FIRST IEP Special Interest Group (IEP-SIG) was formed to develop, oversee and grow the IEP Framework and to ensure it met the needs of the community.

1.2 Requirements

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

An implementation is not compliant if it fails to satisfy one or more of the MUST or REQUIRED level requirements for the protocols it implements. An implementation that satisfies all the MUST or REQUIRED level and all the SHOULD level requirements for its protocols is said to be "unconditionally compliant"; one that satisfies all the MUST level requirements but not all the SHOULD level requirements for its protocols is said to be "conditionally compliant."

[1] https://en.wikipedia.org/wiki/Traffic_Light_Protocol

1.3 Terminology

Creator: The organization or individual who defines the IEP Policy, and creates the Policy Statements that define the IEP Policy. The Creator typically creates an Embedded Policy and stores it in an Internet accessible Policy File to allow Providers to reference it.

Recipient: An organization or individual that receives Threat Intelligence from another organization or individual.

IEP: Information Exchange Policy framework. Enables threat intelligence providers to inform users of how they may use the threat intelligence they receive.

IEPv2: Version 2 of the Information Exchange Policy framework described in this document.

Implementation: Software or hardware that implements the Information Exchange Policy framework.

Policy: A collection of Policy Statements that together form an IEP Policy.

Policy File: A File containing one or more IEP Policies.

Policy Statement: A JSON name/value pair that is used to construct an IEP Policy.

Policy Reference: An object that references an IEP Policy.

Policy Reference Statement: A JSON name/value pair that is used to construct an IEP Policy Reference.

Provider: An organization or individual that produces Threat Intelligence that another organization or individual will consume.

2. Architecture

IEP is designed to be succinct, flexible and descriptive. It tries to help producers describe to consumers exactly what they can and can't do with the threat intelligence that they receive.

The IEP framework is built from a series of structures that work together to convey the Providers intent.

The Providers intent is documented by an IEP Policy. The IEP Policy is constructed from a series of Policy Statements that together form an IEP Policy.

An IEPv2 Policy can be created as a standalone Policy File (and that file referenced from elsewhere), or can be embedded within another protocol structure such as STIX. This difference is shown below in Figure 1 - Embedded vs Referenced.

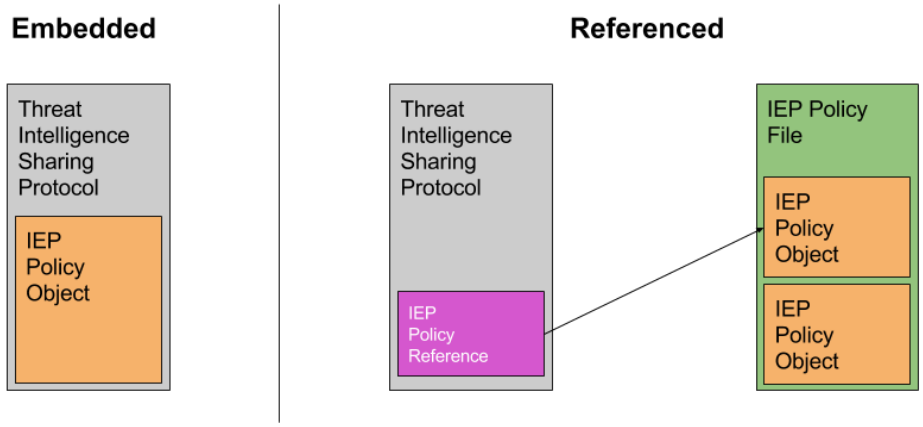

Figure 1 - Embedded vs Referenced

An IEP Policy File MUST contain at least one IEP Policy, but MAY contain more than one IEP Policy. Each IEP Policy MUST have a unique Policy ID.

A Policy Reference contains a URL and a Policy ID that refers to a particular IEP Policy housed within an Internet accessible IEP Policy File. Policy References are designed to be used within other threat intelligence sharing standards and protocols to enable easy reuse of common Information Exchange Policies.

3. JSON IEP Format

The JSON IEP format uses the JSON text format for the serializations of structured data as defined in RFC7159 [1].

4. Versioning IEP Policies

IEP policy objects are immutable once they have been published. If any value within an IEP Policy is changed the IEP Policy MUST be republished with a new id.

5. IEP Policy

5.1 IEP Policy Structure

A JSON IEP Policy MUST be defined as a single JSON Object.

Each JSON IEP Policy JSON Object MUST contain one of each of the IEP Policy Statements as defined in the list below. The mandatory policy statements in IEP Framework v2 are:

- `id`
- `name`
- `version`
- `start-date`
- `end-date`
- `encrypt-in-transit`

- `encrypt-at-rest`
- `permitted-actions`
- `affected-party-notifications`
- `tlp`
- `attribution`
- `obfuscate-affected-parties`
- `unmodified-resale`
- `external-reference`

5.2 Using an IEP Policy

As mentioned earlier an IEP Policy is defined using an IEP Policy JSON Object. This IEP Policy JSON Object can be used in one of two ways:

- Directly embedded in another intelligence sharing protocol or standard such as STIX, OR
- Written into an Internet-accessible IEP Policy File, and referenced using an IEP Policy Reference.

More information about the difference between embedded and referenced IEP Policies can be found in section 9.3.

5.3 Caching IEP Policies

A Recipient SHOULD keep a cached copy of all IEP Policies that mark threat intelligence stored within its threat intelligence repository, so that all threat intelligence marked with IEP Policies will have a corresponding IEP Policy locally available.

6. IEP Policy Statements

Each IEP Policy Statement is a JSON name / value pair (also known as a member), where the name is a string, and it is separated from the value by a colon. An example IEP Policy Statement for the encrypt-in-transit Policy Statement is shown below:

```
"encrypt-in-transit": "MAY"
```

6.1 id

The id statement is used to identify the IEP Policy Object, and to allow the IEP Policy Object to be identified and referenced from other protocols and standards. The id statement MUST be a JSON name/value pair. The id statement MUST be included in a IEP Policy object. The id statement name MUST be the JSON string “id”, and it must be in lowercase. The id statement value MUST be a UUIDv4 identifier as defined in RFC4122 [2].

6.2 name

The name statement is a human readable name for the IEP Policy Object. The name statement MUST be a JSON name/value pair. The name statement MUST be included in a IEP Policy object. The name statement name MUST be the JSON string “name”, and it must be in lowercase. The name statement value MAY be written in any language.

6.3 version

The version statement describes which version of the Information Exchange Policy framework that the IEP Policy Object adheres to. The version statement MUST be a JSON name/value pair. The version statement MUST be included in a IEP Policy object. The version statement name MUST be the JSON string “version”, and it must be in lowercase. The version statement value MUST be the JSON number 2.

6.4 start-date

The start-date statement describes when the IEP Policy Object begins to apply to threat intelligence that references the IEP Policy Object.

The start-date statement MUST be a JSON name/value pair. The start-date statement MUST be included in a IEP Policy object. The start-date statement name MUST be the JSON string “start-date”, and it must be in lowercase. The start-date statement value MUST either be a date string in Co-ordinated Universal Time (UTC) as per RFC3339 [3], or the JSON literal null value **`null`**. **`null`** MUST be used as the start-date statement value when the producer wishes the IEP Policy object to take effect as soon as the recipient receives it.

6.5 end-date

The end-date statement describes when the IEP Policy Object ceases to apply to threat intelligence that references the IEP Policy Object.

The end-date statement MUST be a JSON name/value pair. The end-date statement MUST be included in a IEP Policy object. The end date statement name MUST be the JSON string “end-date”, and it must be in lowercase. The end-date statement value MUST either be a date string in Co-ordinated Universal Time (UTC) as per RFC3339 [3], or the JSON literal null value **`null`**. **`null`** MUST be used as the end-date statement value when the producer wishes the IEP Policy object to apply to the threat intelligence forever.

6.6 encrypt-in-transit

The encrypt-in-transit statement is used to inform the recipient if the received information must be encrypted when it is retransmitted by the recipient.

The encrypt-in-transit statement MUST be a JSON name/value pair. The encrypt-in-transit statement MUST be included in a IEP Policy object. The encrypt-in-transit statement name MUST be the JSON string “encrypt-in-transit”, and it must be in lowercase.

The encrypt-in-transit statement value MUST be set to one of the following two Policy Enumeration strings:

- “MUST”
- “MAY”

As the encrypt-in-transit statement value is a policy enumeration string, it MUST be in uppercase.

6.7 encrypt-at-rest

The encrypt-at-rest statement is used to inform the recipient if the received information must be encrypted when it is stored by the recipient.

The encrypt-at-rest statement MUST be a JSON name/value pair. The encrypt-at-rest statement MUST be included in a IEP Policy object. The encrypt-at-rest statement name MUST be the JSON string "encrypt-at-rest", and it must be in lowercase.

The encrypt-at-rest statement value MUST be set to one of the following two Policy Enumeration strings:

- "MUST"
- "MAY"

As the encrypt-at-rest statement value is a policy enumeration string, it MUST be in uppercase.

6.8 permitted-actions

The permitted-actions statement is used to inform of what actions they may take with the threat intelligence they receive.

The permitted-actions statement MUST be a JSON name/value pair. The permitted-actions statement MUST be included in a IEP Policy object. The permitted-actions statement name MUST be the JSON string "permitted-actions", and it must be in lowercase.

The permitted-actions statement value MUST be set to one of the following five Policy Enumeration strings:

- "NONE"
- "CONTACT FOR INSTRUCTION"
- "INTERNALLY VISIBLE ACTIONS"
- "EXTERNALLY VISIBLE INDIRECT ACTIONS"
- "EXTERNALLY VISIBLE DIRECT ACTIONS"

As the permitted-actions statement value is a policy enumeration string, it MUST be in uppercase.

6.9 affected-party-notifications

The affected-party-notifications statement is used to tell the recipient if they may contact parties who are affected by the threat intelligence received by the recipient.

PLEASE NOTE: This does not allow the recipient to forward copies of the threat intelligence directly to the affected party, but it instead allows the recipient to contact the affected party via any means and inform them of the parts of the threat intelligence that directly affects them.

PLEASE NOTE: The sharing restrictions set by the tlp statement can be overridden by the setting of the affected-party-notifications statement. As an example the tlp statement could be set to "RED" and the affected-party-notifications statement could be set to "MAY". This example would not allow any sharing except with any affected parties.

The affected-party-notifications statement MUST be a JSON name/value pair. The affected-party-notifications statement MUST be included in a IEP Policy object. The affected-party-notifications statement name MUST be the JSON string "affected-party-notifications", and it must be in lowercase.

The affected-party-notifications statement value MUST be set to one of the following two Policy Enumeration strings:

- “MAY”
- “MUST NOT”

As the affected-party-notifications statement value is a policy enumeration string, it MUST be in uppercase.

If the affected-party-notifications statement value is set to “MAY”, then the recipient MAY contact parties who are affected by the threat intelligence received by the recipient. Note - this does not allow the recipient to forward the threat intelligence directly to the affected party, but it instead allows the recipient to contact the affected party and tell them the part of the threat intelligence that affects them.

If the affected-party-notifications statement value is set to “MUST NOT”, then the recipient MUST NOT contact any affected parties in regards to the threat intelligence they received. Please note that in some cases the recipient is required to report the threat intelligence to law enforcement or other officials due to laws in their local jurisdiction.

6.10 tlp

The tlp statement is used to inform the recipient who they may re-share copies of the threat intelligence with. IEP uses the FIRST TLP-SIG definition of TLP [4].

PLEASE NOTE: The sharing restrictions set by the tlp statement can be overridden by the setting of the affected-party-notifications statement. As an example the tlp statement could be set to “RED” and the affected-party-notifications statement could be set to “MAY”. This example would not allow any sharing except with any affected parties.

The tlp statement MUST be a JSON name/value pair. The tlp statement MUST be included in a IEP Policy object. The tlp statement name MUST be the JSON string “tlp”, and it must be in lowercase.

The tlp statement value MUST be set to one of the following four Policy Enumeration strings:

- “RED”
- “AMBER”
- “GREEN”
- “WHITE”

As the tlp statement value is a policy enumeration string, it MUST be in uppercase.

6.11 attribution

The attribution statement allows the provider to communicate if it wants to be known as the producer of the threat intelligence if the threat intelligence is re-shared, or if it wants to remain anonymous.

The attribution statement MUST be a JSON name/value pair. The attribution statement MUST be included in a IEP Policy object. The attribution statement name MUST be the JSON string “attribution”, and it must be in lowercase.

The attribution statement value MUST be set to one of the following three Policy Enumeration strings:

- “MAY”
- “MUST”
- “MUST NOT”

As the attribution statement value is a policy enumeration string, it MUST be in uppercase.

If the attribution statement value is set to “MUST”, then the recipient MUST ensure that any threat intelligence that refers to the IEP Policy MUST maintain attribution of the threat intelligence to the producer when the threat intelligence is re-shared.

If the attribution statement value is set to “MUST NOT”, then the recipient MUST ensure that any threat intelligence that refers to the IEP Policy MUST NOT attribute the threat intelligence to the producer in any way when the threat intelligence is re-shared.

If the attribution statement value is set to “MAY”, then it is up to the recipient if they wish to attribute the threat intelligence to the producer when the threat intelligence is re-shared.

6.12 obfuscate-affected-parties

The obfuscate-affected-parties statement allows the provider to communicate if the consumer needs to obfuscate the identities of the affected parties contained within the threat intelligence if the threat intelligence is re-shared.

The obfuscate-affected-parties statement MUST be a JSON name/value pair. The obfuscate-affected-parties statement MUST be included in a IEP Policy object. The obfuscate-affected-parties statement name MUST be the JSON string “obfuscate-affected-parties”, and it must be in lowercase.

The obfuscate-affected-parties statement value MUST be set to one of the following three Policy Enumeration strings:

- “MAY”
- “MUST”
- “MUST NOT”

As the obfuscate-affected-parties statement value is a policy enumeration string, it MUST be in uppercase.

If the obfuscate-affected-parties statement value is set to “MUST”, then the recipient MUST ensure that any threat intelligence that refers to the IEP Policy MUST obfuscate the identities of affected parties mentioned within the threat intelligence when the threat intelligence is re-shared.

If the obfuscate-affected-parties statement value is set to “MUST NOT”, then the recipient MUST ensure that any threat intelligence that refers to the IEP Policy MUST NOT obfuscate the identities of affected parties mentioned within the threat intelligence when the threat intelligence is re-shared.

If the obfuscate-affected-parties statement value is set to “MAY”, then it is up to the recipient if they wish to obfuscate the identities of affected parties mentioned within the threat intelligence when the threat intelligence is re-shared.

6.13 unmodified-resale

The unmodified-resale statement allows the provider to communicate if the consumer is permitted to resell the threat intelligence information they receive from the producer within their own product offerings in an unmodified state or one that is semantically equivalent. Semantically equivalent in this context means transposing the data from one format to another i.e. transposing the information from a .csv file format to a .json file format would be considered semantically equivalent.

The unmodified-resale statement MUST be a JSON name/value pair. The unmodified-resale statement MUST be included in a IEP Policy object. The unmodified-resale statement name MUST be the JSON string “unmodified-resale”, and it must be in lowercase.

The unmodified-resale statement value MUST be set to one of the following two Policy Enumeration strings:

- “MAY”
- “MUST NOT”

As the unmodified-resale statement value is a policy enumeration string, it MUST be in uppercase.

If the unmodified-resale statement value is set to “MAY”, then it the consumer MAY sell the threat intelligence they receive in an unmodified or semantically equivalent format without restriction.

If the unmodified-resale statement value is set to “MUST NOT”, then the recipient MUST NOT sell or resell any threat intelligence that refers to the IEP Policy in an unmodified or semantically equivalent format.

PLEASE NOTE: Setting the unmodified-resale statement value to MUST NOT does not restrict the consumer from deriving their own threat intelligence from the threat intelligence provided by the producer, and then selling their own derived threat intelligence.

6.14 external-reference

The external-reference statement allows the provider to provide a URI that provides further human readable information about the policy described in the IEP policy. This allows a provider to provide more context about the IEP policy and to document why the certain IEP statement values were selected, and what the IEP Policy was developed to control.

The external-reference statement MUST be a JSON name/value pair. The external-reference statement MUST be included in a IEP Policy object. The external-reference statement name MUST be the JSON string “external-reference”, and it must be in lowercase.

The external-reference statement value MUST be a valid URI as described by

If the external-reference statement value is set to “MAY”, then it the consumer MAY sell the threat intelligence they receive in an unmodified or semantically equivalent format without restriction.

If the external-reference statement value is set to “MUST NOT”, then the recipient MUST NOT sell or resell any threat intelligence that refers to the IEP Policy in an unmodified or semantically equivalent format.

7. IEP Policy Object Example

The following is an example of a complete IEP Policy JSON Object:

```
{
      "id": "01bc4353-4829-4d55-8d52-0ab7e0790df9",
      "name": "FIRST IEP-SIG TLP-AMBER",
      "version": 2
      "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"
}
```

8. IEP Policy File

8.1 IEP Policy File Structure

A JSON IEP Policy file MUST contain at least one IEP policy object within it. A JSON IEP file MAY contain multiple IEP policy objects within it if desired. A JSON IEP Policy file MUST NOT contain any other JSON structure other than one or more IEP Policy Objects.

If the JSON IEP Policy File contains a single IEP Policy, then the file MUST only contain the single IEP Policy JSON object, e.g.

```
{
      "id": "01bc4353-4829-4d55-8d52-0ab7e0790df9",
      "name": "FIRST IEP-SIG TLP-AMBER",
      "version": 2
      "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"
}
```

If the JSON IEP Policy File contains multiple IEP Policies, then the IEP Policy File MUST only contain a single JSON array containing all the IEP Policy JSON objects as members of the JSON array, e.g.

```
[
  {
    "id": "01bc4353-4829-4d55-8d52-0ab7e0790df9",
    "name": "FIRST IEP-SIG TLP-AMBER",
    "version": 2,
    "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"
  },
  {
    "id": "9891b2be-aa5a-4cb2-8a87-b3af93744d85",
    "name": "FIRST IEP-SIG TLP-RED",
    "version": 2,
    "start-date": "2017-01-01T00:00:00Z",
```

```
      "end-date": null,
      "encrypt-in-transit": "MUST",
      "encrypt-at-rest": "MAY",
      "permitted-actions": "INTERNALLY VISIBLE DIRECT ACTIONS",
      "affected-party-notifications": "MUST NOT",
      "tlp": "RED",
      "attribution": "MUST NOT",
      "obfuscate-affected-parties": "MUST",
      "unmodified-resale": "MUST NOT",
      "external-reference": " https://www.first.org/about/policies/bylaws"
   }
]
```

8.2 IEP Policy File naming

JSON IEP files SHOULD end with a ".iepj" file extension where possible.

8.3 IEP Policy File network accessibility

Creators SHOULD ensure that IEP Policy Files are made available at the network accessible URLs. Providers SHOULD ensure that when IEP Policy References are used to mark threat intelligence that Recipients will be able to access the referenced IEP Policy Files. To clarify, IEP Policy Files MAY be publicly accessible on the Internet, or MAY be housed within a private or restricted network – the only requirement is that the Recipient of the threat intelligence marked with the IEP Policy has the ability to access them.

If an IEP Policy File needs to be moved to a different URL, then a URL redirection SHOULD be made to ensure that implementations that ingest old threat intelligence marked with an IEP Policy will still work as they will be redirected to the new IEP Policy location.

9. IEP Policy Reference

IEP Policy References are used to reference an IEP Policy located somewhere else. This functionality was designed to allow the development of commonly used IEP Policies to enable faster, automated sharing, and to reduce the communication overhead of embedding the same IEP Policies over and over again.

9.1 IEP Policy Reference Structure

A JSON IEP Policy Reference MUST be defined as a single JSON Object.

Each JSON IEP Policy Reference JSON Object MUST contain one of each of the IEP Policy Reference Statements as defined in the list below. The mandatory policy reference statements in IEP Framework v2 are:

- `id-ref`

- `url`
- `version`

9.2 IEP Policy Reference naming

As mentioned in section 8.2, JSON IEP files SHOULD end with a ".iepj" file extension where possible. This in turn means that JSON Policy Reference URL SHOULD also end with a ".iepj" file extension where possible.

9.3 IEP Policy Reference or Embedded IEP Policy

It is up to the protocol or standard using IEPv2 to decide if will apply the IEP Policy to threat intelligence objects by embedding the IEP Policy JSON Objects directly within the protocol or standard, or if it will make use of the IEP Policy Reference feature, or if it will support both.

Any protocols or standards that leverage IEPv2 SHOULD support both embedded IEP Policy objects and IEP Policy References. This provides Providers with the greatest flexibility in how they apply the IEP Policy to their threat intelligence.

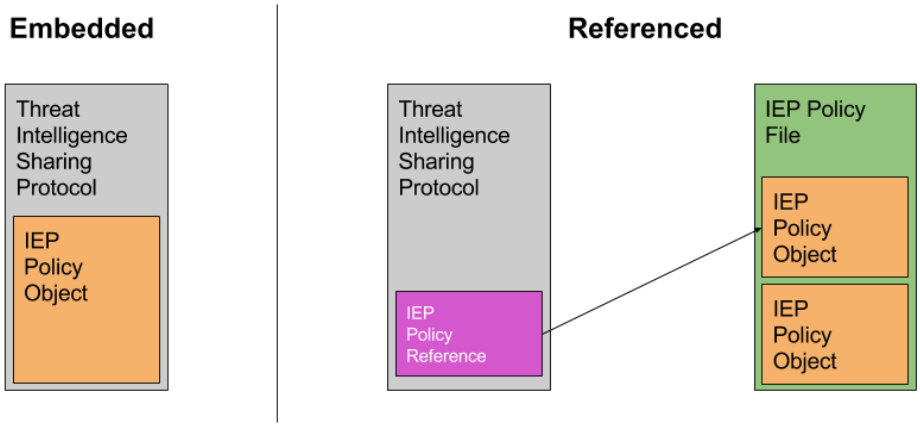

Figure 2 - Embedded vs Referenced

9.4 IEP Policy Reference lookups

IEP Policy Reference lookups use the following steps to resolve the references to retrieve the IEP Policy identified by the IEP Policy Reference:

1. The id-ref Policy Reference Statement is read and the id-ref extracted.
2. The Implementation checks if it has a cached version of the IEP Policy whose id matches the id-ref, and checks the cache timer hasn't expired.
3. If the cached copy of the IEP Policy has expired, then the url Policy Reference Statement is read and the URL extracted.
4. The Implementation accesses the URL and downloads the IEP Policy File at the URL.
5. The Implementation checks the IEP Policy File to ensure that it is valid.
6. If the IEP Policy File is invalid then the process in section 12 – "Handling IEP Policy Errors" is followed.
7. If the IEP Policy File is valid, then the IEP Policy File is checked for an IEP Policy whose id matches the id-ref extracted earlier.

8. If the IEP Policy has the correct id and is valid then the local cached copy is updated, and the Implementation lookup has ended.
9. If the IEP Policy File is valid but there is no IEP Policy with the correct id within the Policy File then the process in section 12 – "Handling IEP Policy Errors" is followed.

10. IEP Policy Reference Statements

Each IEP Policy Reference Statement is a JSON name / value pair (also known as a member), where the name is a string, and it is separated from the value by a colon. An example IEP Policy Reference Statement for the url Policy Reference Statement is shown below:

```
"url": "https://www.first.org/iep/v2/first-iep-sig-tlp-amber.iepj"
```

10.1 id-ref

The id-ref statement is used to identify the IEP Policy Object that resides within the IEP Policy File referenced and located at the URL also provided. The id-ref statement MUST be a JSON name/value pair. The id-ref statement MUST be included in a IEP Policy Reference object. The id-ref statement name MUST be the JSON string "id-ref", and it must be in lowercase. The id-ref statement value MUST be a UUIDv4 identifier as defined in RFC4122 [2], and MUST be an identifier that exists within the IEP Policy File referenced and located at the URL also included within the IEP Policy Reference object.

10.2 url

The url statement is used to specify the URL that will enable the recipient to access and read the IEP Policy File that contains the IEP Policy that the threat intelligence has been marked with.

The url statement MUST be a JSON name/value pair. The url statement MUST be included in a IEP Policy Reference object. The url statement name MUST be the JSON string "url", and it must be in lowercase. The url statement value MUST be a URL as defined in RFC3986 [5], and MUST point to an Internet accessible IEP Policy File.

10.3 version

The version statement describes the IEP Framework version that this Policy Reference is.

The version statement MUST be a JSON name/value pair. The version statement MUST be included in a IEP Policy Reference object. The version statement name MUST be the JSON string "version", and it must be in lowercase. The version statement value MUST be the JSON number 2.

11. IEP Policy Reference Complete Example

An example IEP Policy Reference JSON object is shown below:

```
{
      "id-ref": "01bc4353-4829-4d55-8d52-0ab7e0790df9",
      "url": "https://www.first.org/iep/v2/first-iep-sig-tlp-amber.iepj",
      "version": 2
}
```

12. Handling IEP Policy Errors

This section provides guidance on how to handle IEP errors gracefully.

12.1 No IEP Policy

If some threat intelligence is received, and that threat intelligence is not marked with an IEP Policy, then the recipient MUST follow whatever guidelines they have agreed with the Provider. In this case no IEP Policy has been applied to the threat intelligence, and IEP is not being used to control how the recipient is allowed to use the received threat intelligence.

12.2 Invalid IEP Policy

If some threat intelligence is received, and that threat intelligence is marked with an IEP Policy, but that IEP Policy is invalid, then the recipient MUST contact the Provider to clarify what restrictions they should apply to the received threat intelligence. The Creator or Provider SHOULD correct the Invalid IEP Policy and the Provider SHOULD reissue the threat intelligence with a valid IEP Policy.

12.3 Missing IEP Policy

If some threat intelligence is received, and that threat intelligence is marked with an embedded IEP Policy, but that IEP Policy is missing, then the recipient MUST contact the Provider to clarify what restrictions they should apply to the received threat intelligence. The Provider SHOULD correct the missing IEP Policy and SHOULD reissue the threat intelligence with a valid embedded IEP Policy.

12.4 IEP Policy References pointing to non-existent IEP Policy Files

If some threat intelligence is received, and that threat intelligence is marked with an IEP Policy Reference, but that IEP Policy Reference points to a URL that is unreachable, then the following rules apply:

1. If the Recipient had previously successfully accessed the IEP Policy File at the URL defined in the IEP Policy Reference, and the Policy File was valid, and one of the IEP Policies contained within the IEP Policy File had the same id as the id-ref contained within the IEP Policy Reference, and the Recipient has a cached copy of the IEP Policy, then the Recipient MAY continue to use the previous cached copy of the IEP Policy as if the IEP Policy Lookup worked correctly.
2. If the Recipient had **never** successfully accessed the IEP Policy File at the URL defined in the IEP Policy Reference, then the Recipient MUST contact the Provider to clarify what restrictions they should apply to the received threat intelligence.
3. If the Recipient had previously successfully accessed the IEP Policy File at the URL defined in the IEP Policy Reference, and the Policy File was valid, and the Recipient has a cached copy of the IEP Policy, but the id-ref contained within the IEP Policy Reference does not match any of the id's within the IEP Policy File, then the Recipient MUST contact the Provider to clarify what restrictions they should apply to the received threat intelligence.
4. A Recipient SHOULD keep a cached copy of all IEP Policies that mark threat intelligence stored within its threat intelligence repository, so that all threat intelligence marked with IEP Policies will have a corresponding IEP Policy locally available.

5. If a recipient has attempted to contact the Provider for clarification on use of the threat intelligence but has been unable to get a response, or if the recipient is unable (or unwilling) to contact the Provider, then the Default Unknown IEP Policy applies. This is defined in section 12.6 - “Default Unknown IEP Policy” later in this document.

The Creator SHOULD ensure that the missing IEP Policy File is made available at the URL. If an IEP Policy File needs to move to a different URL, then a URL redirection SHOULD be made to ensure that old threat intelligence marked with an IEP will be redirected to the new location.

Implementations SHOULD periodically try to access missing IEP Policy Files to see if the IEP Policy File now exists.

12.5 IEP Policy References pointing to non-existent id

If some threat intelligence is received, and that threat intelligence is marked with an IEP Policy Reference, and that IEP Policy Reference points to a valid IEP Policy File, but the id-ref contained within the IEP Policy Reference does not match any of the id’s within the IEP Policy File, then the following rules apply:

1. If the Recipient had previously successfully accessed the IEP Policy File at the URL defined in the IEP Policy Reference, and the Policy File was valid, and one of the IEP Policies contained within the IEP Policy File had the same id as the id-ref contained within the IEP Policy Reference, and the Recipient has a cached copy of the IEP Policy, then the Recipient MAY continue to use the previous cached copy of the IEP Policy as if the IEP Policy Lookup worked correctly.
2. If the Recipient had previously successfully accessed the IEP Policy File at the URL defined in the IEP Policy Reference, and the Policy File was valid, and the Recipient has a cached copy of the IEP Policy, but the id-ref contained within the IEP Policy Reference does not match any of the id’s within the IEP Policy File, then the Recipient MUST contact the Provider to clarify what restrictions they should apply to the received threat intelligence.

Implementations SHOULD periodically try to access IEP Policy Files that IEP Policy References with missing ids were referring to in order to check if an IEP Policy with the correct id now exists within the IEP Policy File at the URL.

12.6 Default Unknown IEP Policy

This IEP Policy is designed to be the most restrictive as possible, as it is only used when Implementations know that an IEP policy was applied, but are unable to find out what it was, and no longer have a cached copy of the IEP Policy, and are unable to contact the Provider of the threat intelligence to provide guidance as to what the IEP Policy should be applied.

In this case the IEP framework applies a default restrictive policy to the threat intelligence to ensure that it cannot be shared to any other entity other than the Recipient.

The Default Unknown IEP Policy is below:

```
{
      "id": "e4eb1db1-e0fb-4200-9f4c-4c713bb197aa",
```

```
        "name": "FIRST IEP-SIG Unknown IEP",
        "version": 2
        "start-date": "2017-01-01T00:00:00Z",
        "end-date": null,
        "encrypt-in-transit": "MUST",
        "encrypt-at-rest": "MAY",
        "permitted-actions": "INTERNALLY VISIBLE ACTIONS",
        "affected-party-notifications": "MUST NOT",
        "tlp": "RED",
        "attribution": "MUST NOT",
        "obfuscate-affected-parties": "MUST",
        "unmodified-resale": "MUST NOT",
        "external-reference": " https://www.first.org/iep"
}
```

13. Pre-defined FIRST IEPv2 JSON Policy Files

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.

These policies are based on the FIRST TLP-SIG "TLP FIRST Standards Definitions and Usage Guidance — Version 1.0" available at https://www.first.org/tlp.

13.1 FIRST IEP-SIG IEPv2 TLP Red Policy

Policy Name	FIRST IEP-SIG IEPv2 TLP Red
Policy ID	5e607e88-ab70-4977-8c1b-ee3a16b0f68c
Policy URL	https://www.first.org/iep/v2/first-iep-sig-tlp-red.iepj

13.2 FIRST IEP-SIG IEPv2 TLP Amber Policy

Policy Name	FIRST IEP-SIG IEPv2 TLP Amber
Policy ID	01bc4353-4829-4d55-8d52-0ab7e0790df9
Policy URL	https://www.first.org/iep/v2/first-iep-sig-tlp-amber.iepj

13.3 FIRST IEP-SIG IEPv2 TLP Green Policy

Policy Name	FIRST IEP-SIG IEPv2 TLP Green
Policy ID	3903ce63-674c-4b70-9457-8c5527dd9115
Policy URL	https://www.first.org/iep/v2/first-iep-sig-tlp-green.iepj

13.4 FIRST IEP-SIG IEPv2 TLP White Policy

Policy Name	FIRST IEP-SIG IEPv2 TLP White
Policy ID	0d783790-b221-40c1-840a-5787330612c1
Policy URL	https://www.first.org/iep/v2/first-iep-sig-tlp-white.iepj

14. Bibliography

[1] “RFC7159,” March 2014. [Online]. Available: https://tools.ietf.org/html/rfc7159.

[2] “RFC4122,” July 2005. [Online]. Available: https://www.ietf.org/rfc/rfc4122.txt.

[3] “RFC3339,” July 2002. [Online]. Available: https://tools.ietf.org/html/rfc3339.

[4] F. TLP-SIG, “ Traffic Light Protocol,” August 2016. [Online]. Available: https://www.first.org/tlp.

[5] “RFC3986,” January 2005. [Online]. Available: https://tools.ietf.org/html/rfc3986.