Automated Indicator Sharing (AIS) Status Service

V1.0

Publication: December 2021
Cybersecurity and Infrastructure Security Agency

Contents

1 What is the AIS Status Service?

The AIS Status Service enables users to check the processing status of their STIX submission as well as if there were any issues with their submission. In particular, the AIS Status Service reports on whether the objects in the submission passed validation against the AIS Profile and STIX 2.1 Specification and if the submission is undergoing human review for personally identifiable information (PII) such as an individual's name, email, or social security number. [1][2]

2 Why Does AIS Include this Function?

For AIS to function properly, CISA uses automated functions to validate that all STIX submissions are valid with respect to the AIS Profile and STIX 2.1 Specification. This means that some submissions may not be shared with AIS participants if they are determined not to be valid.

Further, in accordance with Cybersecurity Information Sharing Act of 2015 and associated privacy and civil liberties guidelines,[3] CISA is required to validate, prior to sharing submissions with other AIS participants, that submissions do not contain PII unless directly related to the cybersecurity threat. This means that some submissions may need to undergo human review, which may result in a delay in those submissions being shared with AIS participants. If PII not directly related to the cybersecurity threat is ultimately identified in a submission, the submission might be modified prior to being shared (by CISA creating new objects removing the PII) or not shared at all if the PII cannot be removed in a way that leaves further information to be shared.

Such delay, submission rejection, or change to submissions could leave users wondering what happened to their submission. The AIS Status Service therefore provides users with a mechanism by which they can see where the submission is within the review process and if any changes need to be made for it to be successfully processed and shared out with AIS participants.

3 How Does the AIS Status Service Work?

The AIS Status Service leverages the status capability native to TAXII, which allows users, via a TAXII client, to check the status of a previous request to submit STIX objects to a TAXII server.[4] A TAXII client is any software that connects to a TAXII server and supports the exchange of cyber threat intelligence. A TAXII server is any software that supports the exchange of cyber threat intelligence via the TAXII standard.

In TAXII, when a TAXII client requests the status of a submission, the TAXII server may respond with either Status: Pending or Status: Complete. AIS uses the status values as follows.

Status	Description
Pending	Indicates that submission processing is not complete and further updates to the status of a submission may be made.

[1] https://www.cisa.gov/publication/automated-indicator-sharing-ais-documentation
[2] https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html
[3] https://www.cisa.gov/publication/cybersecurity-information-sharing-act-2015-procedures-and-guidance
[4] https://docs.oasis-open.org/cti/taxii/v2.1/os/taxii-v2.1-os.html#_Toc31107530

Status	Description
Complete	Indicates that submission processing is complete and no additional updates to the status of the submission will be made.

Table 1: AIS Submission Status Values

In addition to returning a status value, the TAXII server response may include a message with additional information. In AIS, the TAXII server response will include a message, which indicates where the submission (and the individual objects contained therein, by identifier) is in the processing workflow.

Status	Message	Description
Pending	_	Indicates that at least one STIX object has been received by the TAXII Server.
	Pending Validation	Indicates that the STIX object associated with the noted identifier is undergoing validation against the AIS Profile and STIX 2.1 Specification.
	Pending Human Review	Indicates that the STIX object associated with the noted identifier is undergoing human review for PII.
Complete	Failure	Indicates that the STIX object associated with the noted identifier failed validation against the AIS Profile or STIX 2.1 Specification or contained PII not directly related to a cyber threat that could not be redacted in a way that leaves further information to be shared.
	Success	Indicates that the STIX object associated with the noted identifier passed validation against the AIS Profile and STIX 2.1 Specification and either did not contain PII not directly related to a cyber threat or a duplicate object was made with such PII removed and was shared over AIS.

Table 2: Descriptions of AIS Submission Status Values and Messages

The steps for using the AIS Status Service are as follows:

1. The submitter organization submits STIX objects to the AIS TAXII Server via its TAXII client.
2. The STIX objects are received by the AIS TAXII Server and the AIS TAXII Server responds with a Status: Pending status, along with a message that provides the submitter organization with a status identifier that can be used by the submitter organization to look up the status of the submission with the AIS TAXII Server, as well as the list of STIX objects (by identifier and version of the STIX object (i.e. modified property)) that were received. Then, the STIX objects undergo validation against the AIS Profile and STIX 2.1 Specification and, if necessary, human review (i.e. if automated processing identifies the potential presence of two or more different categories of PII in an individual property of a STIX object).

3. At any time after receiving the status identifier, the submitter organization may look up the status of their submission by making a status request to the AIS TAXII Server via their TAXII client. How this is done will vary from TAXII client to TAXII client. Some TAXII clients may manage the status identifiers associated with submissions and get the status of a submission automatically whereas other TAXII clients may require that the organization use the TAXII client to explicitly make a status request using the status identifier.
4. Upon receiving a status request, the AIS TAXII Server responds with either Status:Pending or Status:Complete along with where the submission is in the submission processing workflow (e.g., pending validation, pending human review, failed validation, or passed validation).

This interaction between the TAXII client and AIS TAXII Server is shown below in Figure 1.

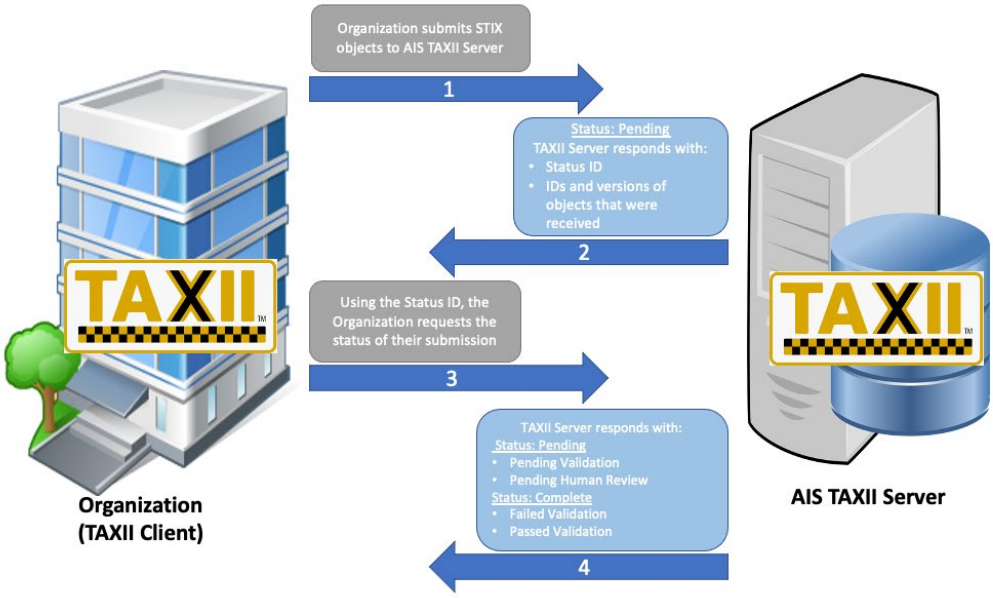

Figure 1: How the AIS Status Service Works

4 Examples of Status Service

The following examples show the status that is returned when submitting STIX objects as well as the different responses that may be returned from status requests indicating if a submission is pending validation, pending human review, failed validation, or passed validation. The examples are categorized based on the status value when they occur.

4.1 Status: Pending

The following subsections describe the interactions between a TAXII client and the AIS TAXII Server when the response status value is Pending.

4.1.1 Submission Received

When a submission is made to the AIS TAXII Server, the server returns a Status: Pending response with a status identifier that can be used to make status requests for the latest status information about the submission as well as the list of STIX objects (by identifier and version (i.e. modified property)) that were received. Figure 2 shows this interaction between a TAXII client and the AIS TAXII Server.

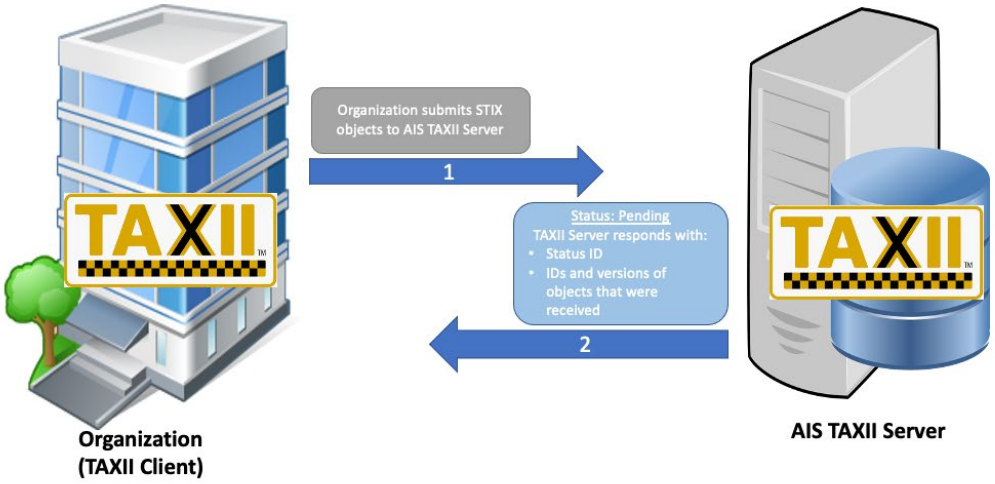

Figure 2: Status: Pending – Submission Received

4.1.2 Pending Validation

Pending Validation occurs when a status request is made to the AIS TAXII Server when STIX objects in the submission are undergoing validation against the AIS Profile and STIX 2.1 Specification. As described above, when a submission is made to the AIS TAXII server, the server returns a Status: Pending response with a status identifier that can be used to make subsequent requests for the latest status information about the submission as well as the list of STIX objects (by identifier and version (i.e. modified property)) that were received.

If a status request is made during validation, the AIS TAXII Server returns a Status: Pending response with a message indicating which STIX objects in the submission (by identifier and version (i.e. modified property)) are pending validation and the timestamp when the validation started. Figure 3 shows this interaction between a TAXII client and the AIS TAXII Server.

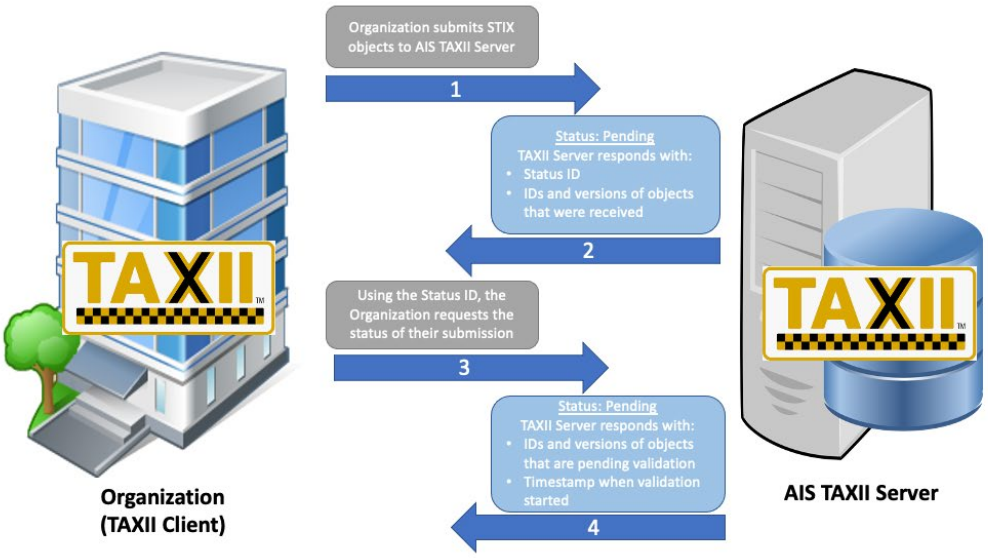

Figure 3: Status: Pending - Pending Validation

For a more detailed understanding of the requests and responses between a TAXII client and the AIS TAXII Server, please see Pending Validation in the Appendix – Low-level Details.

4.1.3 Pending Human Review

After a submission is made, it may need to undergo human review if possible PII is detected through automated processes, to ensure that all identified PII not determined to be directly related to the cybersecurity threat is removed prior to CISA sharing it further over AIS. As described above, when a submission is made to the AIS TAXII server, the server returns a Status: Pending response with a status identifier that can be used to make subsequent requests for the latest status information about the submission as well as the list of STIX objects (by identifier and version (i.e. modified property)) that were received.

If the status of a submission is checked after the need for human review has been identified and human review has begun but prior to human review being completed, a Status: Pending response is returned with a message indicating which STIX objects in the submission (by STIX object identifier and version (i.e. modified property)) are pending human review and the timestamp when human review started. Figure 4 shows this interaction between a TAXII client and the AIS TAXII Server.

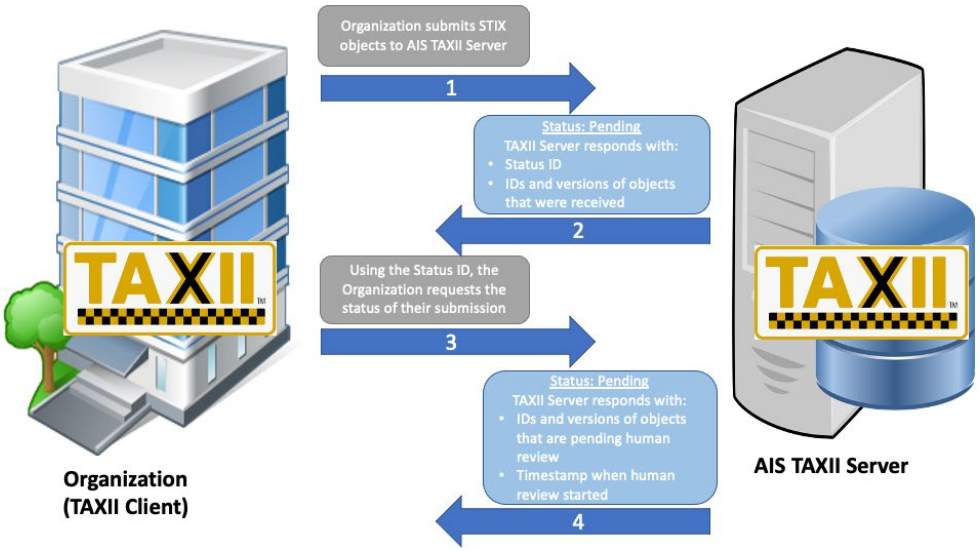

Figure 4: Status: Pending - Pending Human Review

For a more detailed understanding of the requests and responses between a TAXII client and the AIS TAXII Server, please see Pending Human Review in the Appendix -- Low-level Details.

4.2 Status: Complete

A status of complete indicates that all STIX objects in the submission have undergone validation and human review (if necessary), and have either failed or passed validation. The following sub-sections describe the interactions between a TAXII client and the AIS TAXII Server when the response status value is Complete.

4.2.1 Failure

A failed submission occurs when STIX objects that do not conform to the AIS Profile and STIX 2.1 Specification are submitted to the AIS TAXII Server or contained PII not directly related to a cyber threat that could not be redacted in a way that leaves further information to be shared. If the submitter organization wants the information contained in a failed submission to be distributed over AIS, the submission must be corrected.

As described above, when a submission is made to the AIS TAXII server, the server returns a Status: Pending response with a status identifier that can be used to make subsequent requests for the latest status information about the submission as well as the list of STIX objects (by identifier and version (i.e. modified property)) that were received.

If the status of a submission is checked after validation and any necessary human review is completed for all objects, and at least one object in the submission failed, a Status: Complete response is returned with a message indicating which STIX objects in the submission (by identifier and version (i.e. modified property)) failed validation, the reasons why, and the timestamp when processing completed. Figure 5 shows this interaction between a TAXII client and the AIS TAXII Server.

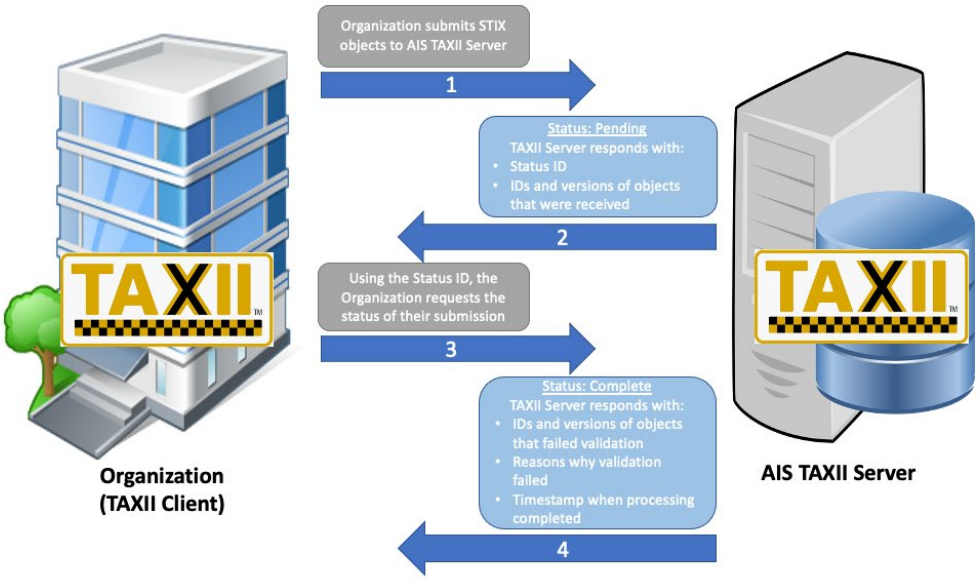

Figure 5: Status: Complete - Failure

For a more detailed understanding of the requests and responses between the TAXII client and TAXII server, please see Failure in the Appendix -- Low-level Details.

4.2.2 Success

A successful submission occurs when valid STIX objects are submitted to the AIS TAXII Server and they complete validation and human review if necessary. As described above, when a submission is made to the AIS TAXII server, the server returns a Status: Pending response with a status identifier that can be used to make subsequent requests for the latest status information about the submission as well as the list of STIX objects (by identifier and version (i.e. modified property)) that were received.

If the status of a submission is checked after successful validation and any necessary human review is completed (and either the submission did not contain PII not directly related to a cyber threat or a duplicate object was made with such PII removed), a Status: Complete response is returned with a message indicating which STIX objects (by identifier and version (i.e. modified property)) passed validation, which AIS feeds the STIX objects were routed to (e.g., public, federal, etc.), what modifications were made to the submission (e.g., new STIX objects created due to anonymization or PII removal), and the timestamp when processing completed. Figure 6 shows this interaction between a TAXII client and the AIS TAXII Server.

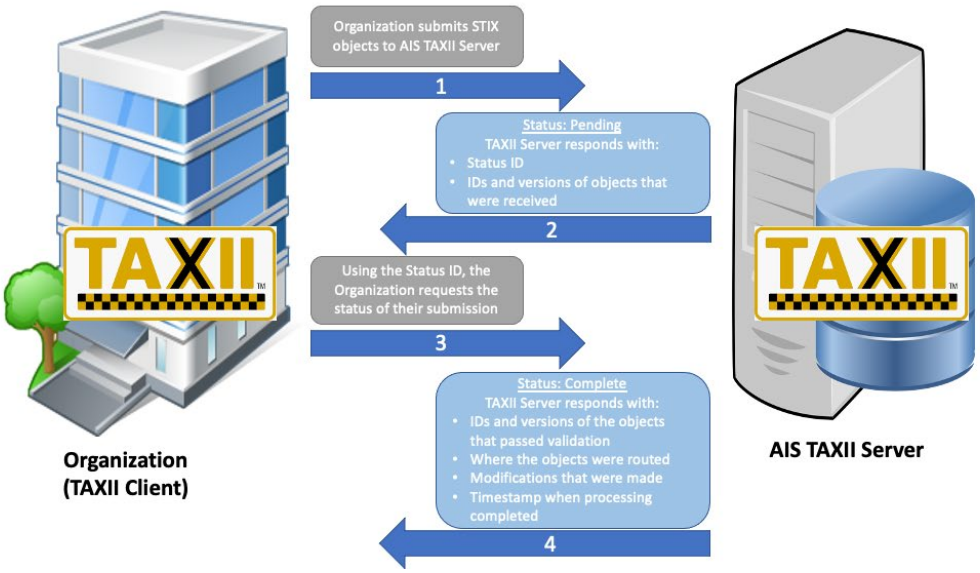

Figure 6: Status: Complete - Success

For a more detailed understanding of the requests and responses between the TAXII client and TAXII server, please see Success in the Appendix -- Low-level Details.

5 Appendix – Low-level Details

The following sub-sections provide the low-level details of what the requests and responses between a TAXII client and the AIS TAXII Server look like. Note that these examples all assume that a submission contains only the object indicated, and does not contain other objects.

5.1 Pending Validation

The following example contains a submitted object that returns a Status: Pending response when the object is in the pending validation stage of the processing workflow:

5.1.1 Submitted Object

The following Indicator object with PII is submitted by the organization to the AIS TAXII Server.


```
{
   "type": "indicator",
   "id": "indicator--e8bae515-20e9-4a39-970e-bddd08003f02",
   "created": "2017-11-02T12:30:58.000Z",
   "modified": "2017-11-02T12:30:58.000Z",
    "description": "This indicator was identified by Jane Doe (jdoe@company.com).",
   "pattern": "[url:value = 'http://x4z9arb.cn/4712']",
   "pattern_type": "stix",
   "spec_version": "2.1",
   "revoked": false,
   "valid_from": "2017-11-03T12:30:59.000Z",
   "valid_until": "2018-11-03T12:30:59.000Z"
}
```


Figure 7: Indicator Object with PII Submitted to AIS

5.1.2 Returned Status Response

In response to the submission, the following would be returned by the AIS TAXII Server to the submitter organization's TAXII client.


```
{
   "id": "47c50d3d-3ede-4212-978f-5eb971d44f8c",
   "status": "pending",
   "request_timestamp": "2021-09-21T17:10:16.214314Z",
   "total_count": 1,
   "success_count": 0,
   "failure_count": 0,
   "pending_count": 1,
   "pendings":
      [{
         "id": "indicator--e8bae515-20e9-4a39-970e-bddd08003f02",
         "version": "2017-11-02T12:30:59Z"
      }]
}
```


Figure 8: Status Response Returned by the AIS TAXII Server

5.1.3 Get Status Request

Upon the submitter organization issuing a status request with their TAXII client to the AIS TAXII Server using the GET request below, the AIS TAXII Server would provide the response that follows when the object is pending validation.

GET https://ais2.cisa.dhs.gov/public/status/47c50d3d-3ede-4212-978f-5eb971d44f8c


```
{
  "id": "47c50d3d-3ede-4212-978f-5eb971d44f8c",
  "status": "pending",
  "request_timestamp": "2021-09-17T17:03:19.715326Z",
  "total_count": 1,
  "success_count": 0,
  "failure_count": 0,
  "pending_count": 1,
  "pendings":
    [{
      "id": "indicator--e8bae515-20e9-4a39-970e-bddd08003f02",
      "version": "2017-11-02T12:30:59Z",
      "message": "Pending validation 2021-09-17T17:03:19.986526Z"
     }]
}
```


Figure 9: Status Response Indicating an Object is Pending Validation

5.2 Pending Human Review

The following example builds off the example above when, after validation, the object is flagged for human review due to potential PII.

5.2.1 Get Status Request

Upon the submitter organization issuing a status request with their TAXII client to the AIS TAXII Server using the GET request below, the AIS TAXII Server would provide the response that follows while the submission was still pending human review.

GET https://ais2.cisa.dhs.gov /public/status/47c50d3d-3ede-4212-978f-5eb971d44f8c


```
{
  "id": "47c50d3d-3ede-4212-978f-5eb971d44f8c",
  "status": "pending",
  "request_timestamp": "2021-09-21T17:10:18.214314Z",
  "total_count": 1,
  "success_count": 0,
  "failure_count": 0,
  "pending_count": 1,
  "pendings":
    [{
```

```
      "id": "indicator--e8bae515-20e9-4a39-970e-bddd08003f02",
      "version": "2017-11-02T12:30:58Z",
      "message": "Pending human review 2021-09-21T17:11:02.291231Z"
    }]
}
```

Figure 10: Status Response Indicating an Object Pending Human Review

5.3 Failure

The following example contains a submission that includes invalid STIX content which returns a Status:Complete response when the object is in the failed validation stage of the processing workflow:

5.3.1 Submitted Object

The following Indicator object, containing malformed timestamps, is submitted by the organization to the AIS TAXII Server.

```
{
  "type": "indicator",
  "id": "indicator--6982d19f-4b9a-4e51-98b7-3ffaa7d5bf21",
  "created": "2017-11-02T12:30:58Z",
  "modified": "2017-11-02T12:30:58Z",
  "pattern": "[url:value = 'http://x4z9arb.cn/4712']",
  "pattern_type": "stix",
  "spec_version": "2.1",
  "revoked": false,
  "valid_from": "2017-11-03T12:30:59.000Z",
  "valid_until": "2018-11-03T12:30:59.000Z"
}
```

Figure 11: Invalid Indicator Object Submitted to AIS

5.3.2 Returned Status Response

In response to the submission, the following would be returned by the AIS TAXII Server to the submitter organization's TAXII client.

```
{
  "id": "1095fd43-8e11-4228-a071-3f8622db4140",
  "status": "pending",
  "request_timestamp": "2021-09-17T17:02:59.904994Z",
  "total_count": 1,
  "success_count": 0,
  "failure_count": 0,
  "pending_count": 1,
  "pendings":
    [{
      "id": "indicator--6982d19f-4b9a-4e51-98b7-3ffaa7d5bf21",
      "version": "2017-11-02T12:30:59Z"
    }]
}
```

Figure 12: Status Response Returned by the AIS TAXII Server

5.3.3 Get Status Request

Upon the submitter organization issuing a status request with their TAXII client to the AIS TAXII Server using the GET request below, the AIS TAXII Server would provide the response that follows after validation failed.

GET https://ais2.cisa.dhs.gov /public/status/1095fd43-8e11-4228-a071-3f8622db4140


```
{
  "id": "1095fd43-8e11-4228-a071-3f8622db4140",
  "status": "complete",
  "request_timestamp": "2021-09-17T17:03:59.904994Z",
  "total_count": 1,
  "success_count": 0,
  "failure_count": 1,
  "failures":
    [{
      "id": "indicator--6982d19f-4b9a-4e51-98b7-3ffaa7d5bf21",
      "version": "2017-11-02T12:30:59Z",
      "message": "STIX validation failure:  created: '2017-11-02T12:30:59Z' does not match
                  the timestamp format YYYY-MM-DDTHH:mm:ss.sssZ (must be precise to
                  the millisecond); modified: '2017-11-02T12:30:59Z' does not match the
                  timestamp format YYYY-MM-DDTHH:mm:ss.sssZ (must be precise to the
                  millisecond). Processing completed at: 2021-09-17T17:04:00.988085Z. Please
                  review the AIS submission guidance for recommendations and requirements
                  for submissions. If you have any questions about this submission, contact us
                  at cyberservices@cisa.gov."
    }],
  "pending_count": 0
}
```


Figure 13: Status Response Indicating an Object Failed Validation

5.4 Success

The following example contains a submission that is valid STIX content which returns a Status: Complete response when the object is in the passed validation stage of the processing workflow:

5.4.1 Submitted Object

The following Indicator object is submitted by the organization to the AIS TAXII Server.


```
{
  "type": "indicator",
  "id": "indicator--5c742b26-fa3c-406f-b432-333066e0fc89",
  "created": "2017-11-02T12:30:58.000Z",
  "modified": "2017-11-02T12:30:58.000Z",
  "pattern": "[url:value = 'http://x4z9arb.cn/4712'] ",
```

```
  "pattern_type": "stix",
  "spec_version": "2.1",
  "revoked": false,
  "valid_from": "2017-11-03T12:30:59.000Z",
   "valid_until": "2018-11-03T12:30:59.000Z",
  "object_marking_refs": ["marking-definition--34098fce-860f-48ae-8e50-ebd3cc5e41da"]
}
```

Figure 14: Valid Indicator Object Submitted to AIS

5.4.2 Returned Status Response

In response to the submission, the following would be returned by the AIS TAXII Server to the submitter organization's TAXII client.

```
{
  "id": "d1c6219f-b4d0-4c7e-b1ef-e3febffd90f5",
  "status": "pending",
  "request_timestamp": "2021-09-17T17:03:19.715326Z",
  "total_count": 1,
  "success_count": 0,
  "failure_count": 0,
  "pending_count": 1,
  "pendings":
    [{
      "id": "indicator--5c742b26-fa3c-406f-b432-333066e0fc89",
      "version": "2017-11-02T12:30:59Z"
    }]
}
```

Figure 15: Valid Indicator Object Submitted to AIS

5.4.3 Get Status Request (Success)

Upon the submitter organization issuing a status request with their TAXII client to the AIS TAXII Server using the GET request below, the AIS TAXII server would provide the response that follows after the STIX object has passed validation and a determination was made that human review was not required. Because the single submission is sent over AIS in two forms (in the public feed and in the federal feed with ACS markings), the status for the single object submission indicates that two objects were successfully transmitted.

GET https://ais2.cisa.dhs.gov /public/status/d1c6219f-b4d0-4c7e-b1ef-e3febffd90f5

```
{
  "id": "d1c6219f-b4d0-4c7e-b1ef-e3febffd90f5",
  "status": "complete",
  "request_timestamp": "2021-09-17T17:03:19.715326Z",
  "total_count": 2,
  "success_count": 2,
```

```
  "successes":
    [{
      "id": "indicator—5c742b26-fa3c-406f-b432-333066e0fc89",
      "version": "2017-11-02T12:30:59Z",
      "message": "Added to public collection a6313101-fa6c-4276-bb96-7e826f0b248a. Added to
                 federal collection 13109a4c-ab86-49df-a7e1-c212ae7b4816.
                 Processing completed at: 2021-09-17T17:03:21.722128Z. Modifications: [
                 ACS marking (id = marking-definition--
                 55b0a4bc-7136-47f6-b3b0-538f405d802e) created and associated with object.]
                 If you have any questions regarding modification or anonymization of your
                 submission, contact us at cyberservices@cisa.gov."
    },
    {
      "id": "marking-definition—55b0a4bc-7136-47f6-b3b0-538f405d802e",
      "version": "2021-09-17T17:00:03.639296Z",
      "message": "Added to federal collection 13109a4c-ab86-49df-a7e1-c212ae7b4816.
                  Processing completed at: 2021-09-17T17:03:21.617671Z. If you have any
                 questions regarding modification or anonymization of your submission,
                 contact us at cyberservices@cisa.gov."
    }],
  "failure_count": 0,
  "pending_count": 0
}
```


Figure 16: Status Response Indicating an Object Passed Validation

6 Appendix – Acronyms

Acronyms are provided below.

Acronym	Definition
AIS	Automated Indicator Sharing
CISA	Cybersecurity and Infrastructure Security Agency
CTI	Cyber Threat Indicator
CTIS	Cyber Threat Information Sharing
DM	Defensive Measure
STIX	Structured Threat Information Expression
TAXII	Trusted Automated Exchange of Intelligence Information