Automated Indicator Sharing (AIS) Identity Anonymization Process

V1.0

Publication: December 2021
Cybersecurity and Infrastructure Security Agency

Contents

1 What is the AIS Identity Anonymization Process?

The AIS Identity Anonymization Process is a process that anonymizes the identity of organizations submitting information to the Automated Indicator Sharing (AIS) program.

2 Why is an Anonymization Needed?

Cyber threat intelligence related to attempted and successful compromises can be very valuable for organizations to proactively deploy the proper defensive measures to protect their networks. Given the often sensitive nature of this information and to encourage organizations to share cyber threat intelligence, AIS supports the anonymization of identity information for organizations wishing to protect their identity while still sharing cyber threat intelligence.

To encourage the sharing of this information, the Cybersecurity Information Sharing Act of 2015 provides requirements, liability, privacy, and other protections to organizations that share cyber threat indicators and defensive measures through AIS.[1] Additionally, as part of AIS, the Cybersecurity and Infrastructure Security Agency (CISA) uses the AIS Identity Anonymization Process to anonymize the identity of submitting organizations as appropriate, as well as support for data markings (Traffic Light Protocol for non-federal submissions and Access Control Specification for federal submissions) and labels that specify how the sharing of information should be handled.[2,3]

In AIS 1.0, anonymization meant the identity of the submitting organization was simply replaced by "DHS NCCIC". While this anonymized the submission, it made all anonymized submissions appear to be from the same organization, that is, DHS NCCIC. This prevented AIS participants from tracking which submissions came from which organizations. In AIS 2.0, each organization is given an individual, static, anonymized identity, enabling AIS participants to make better decisions about how to prioritize and utilize incoming cyber threat intelligence for their own individual organization.

3 How is Identity Information Shared?

The identity information of an organization submitting information to AIS is shared based on how they label the content in the Identity STIX Domain Object (SDO) and the **created_by_ref** property of other submitted objects.[4,5] The label should be one of the values in Table 1.

[1] https://www.cisa.gov/sites/default/files/publications/Cybersecurity%20Information%20Sharing%20Act%20of%202015.pdf

[2] https://www.first.org/tlp/

[3] https://www.cisa.gov/publication/automated-indicator-sharing-ais-documentation

[4] https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html#_wh296fiwpklp

[5] https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html#_xzbicbtscatx

Table 1: AIS Consent Values

Consent Label	Description
ais-consent-none	CISA will not disclose the identity of the submitter except as permitted in the AIS terms of use.
ais-consent-usg	CISA will only share the identity of the submitter with federal entities.
ais-consent-everyone	CISA will share the identity of the submitter with all AIS participants and with federal entities.
ais-consent-everyone-cisa-proprietary	CISA will share the identity of the submitter with all AIS participants and with federal entities. All objects in the submission that reference the Identity SDO are considered proprietary.

Once CISA receives the submission, it determines how the identity should be shared based on the consent label. If the consent label is *ais-consent-none*, the identity of the submission is immediately anonymized before any further distribution. If the consent label is *ais-consent-usg*, the original submission is sent to the AIS Federal trust group; however, the identity information is anonymized before it is shared with other trust groups. If the consent label is *ais-consent-everyone* or *ais-consent-everyone-cisa-proprietary,* the AIS Identity Anonymization Process is bypassed, and the submission is shared with AIS participants according to the specified data markings. If the consent label is not specified, or the submission contains objects that have **created_by_ref** properties that point to an Identity object not included in the submission and not known to CISA from a previous submission, anonymization defaults to *ais-consent-none*.

4 How Does the Anonymization Process Work?

As illustrated in Figure 1, when an AIS submission comes into the system through AIS Ingest, the consent label is used to determine whether anonymization is necessary (i.e., whether the label in the Identity object is *ais-consent-none* or *ais-consent-usg* or whether any **created_by_ref** properties point to an Identity object not in the submission). If anonymization is necessary, the submission is automatically processed through the AIS Identity Anonymization Process. There, the identity of the submitting organization (e.g., Foo Inc.) is automatically cross-referenced against a mapping of previously-assigned anonymized identities that is only known to CISA. If the identity is not found, a new anonymized identity is generated (e.g., LeakyRunningChair123), linked (internally for CISA) to the real identity, and added to the mapping. Once the anonymized identity is identified or generated, the submission is automatically recreated using the anonymized identity. After the submission is recreated, it is shared with AIS participants according to the specified data markings. If anonymization is not necessary (e.g., consent is *ais-consent-everyone* or *ais-consent-everyone-cisa-proprietary*), the anonymization process is bypassed and the submission is shared with AIS participants according to the specified data markings.

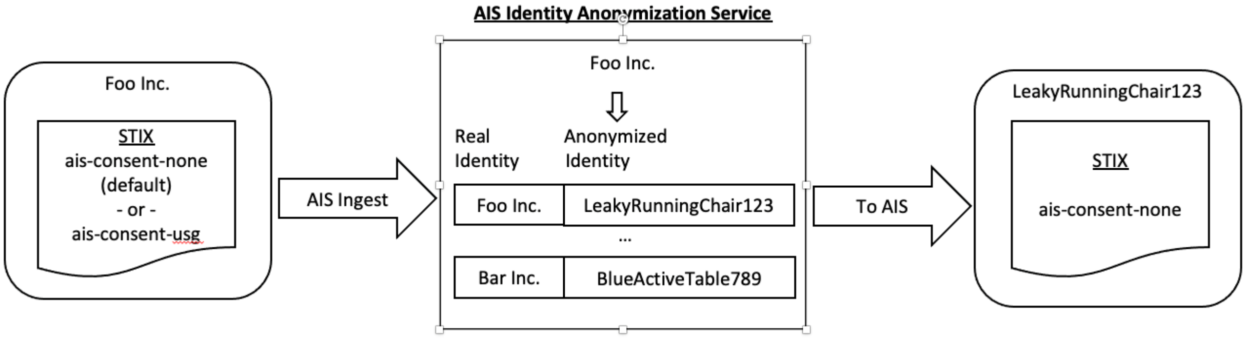

Figure 1: STIX Submission Processed by the AIS Anonymization Process

5 Examples of Anonymized Identities

When submitting STIX content, an organization may leverage multiple identities depending on whether or not they want to associate their identity with the cyber threat intelligence. The following examples show the different ways an organization may submit their identity information and the resulting identity that gets shared with AIS participants.

5.1 AIS Consent: ais-consent-none

In this situation, the organization decides that they do not wish to share their identity information with any AIS participants. To indicate this, the organization creates an Identity object such as that shown in Figure 2.

```
{
  "id": "identity--e377227a-3380-47c6-b28f-00449999d38c",
  "created_by_ref": "identity--e377227a-3380-47c6-b28f-00449999d38c",
  "identity_class": "organization",
  "created": "2021-04-03T00:00:00.000Z",
  "modified": "2021-04-03T00:00:00.000Z",
  "name": "Foo Inc.",
  "labels": ["ais-consent-none"],
  "object_marking_refs": [
    "marking-definition--613f2e26-407d-48c7-9eca-b8e91df99dc9"
  ],
  "sectors": [
    "technology"
  ],
  "spec_version": "2.1",
  "type": "identity"
}
```

Figure 2: STIX Identity Object (ais-consent-none)

When the organization submits this Identity object, along with other objects referencing this object in the **created_by_ref** property, the AIS Identity Anonymization Process automatically processes this submission, identifies the *ais-consent-none* label and determines the Identity object associated with the submission needs to be anonymized. The process looks up the anonymized identity of the submitter (generating one if not available) and creates a new Identity object using the anonymized identity. The new Identity object, created by CISA (identity--b3bca3c2-1f3d-4b54-b44f-dac42c3a8f01), looks as shown in Figure 3.

```
{
  "id": "identity--afa5740f-0680-41ce-af45-c61e45218129",
  "created_by_ref": "identity--b3bca3c2-1f3d-4b54-b44f-dac42c3a8f01",
  "identity_class": "organization",
  "created": "2021-04-03T00:05:00.000Z",
  "modified": "2021-04-03T00:05:00.000Z",
  "name": "LeakyRunningChair123",
  "labels": ["ais-consent-none"],
  "object_marking_refs": [
    "marking-definition--613f2e26-407d-48c7-9eca-b8e91df99dc9"
  ],
  "sectors": [
    "technology"
  ],
  "spec_version": "2.1",
  "type": "identity"
}
```

Figure 3: STIX Identity Object (ais-consent-none, anonymized)

Each object in the submission that references the STIX identity object with the *ais-consent-none* label is recreated with a new identifier and **created_by_ref** property that points to the new Identity object. The recreated submission is then shared with all federal and non-federal organizations according to the specified data markings.

5.2 AIS Consent: ais-consent-usg

In some cases, an organization is willing to share their identity information with the federal government but not with non-federal organizations. To do this, the organization uses the *ais-consent-usg* label and creates an Identity object such as that shown in Figure 4, accompanied with and referenced in the **created_by_ref** of the relevant Objects in their submission.

```
{
  "id": "identity--030f478f-7274-4cae-b159-d1b2f51c4026",
  "created_by_ref": "identity--030f478f-7274-4cae-b159-d1b2f51c4026",
  "identity_class": "organization",
  "created": "2021-04-03T00:00:00.000Z",
  "modified": "2021-04-03T00:00:00.000Z",
  "name": "Foo Inc.",
  "labels": ["ais-consent-usg"],
  "object_marking_refs": [
    "marking-definition--613f2e26-407d-48c7-9eca-b8e91df99dc9"
  ],
  "sectors": [
    "technology"
  ],
  "spec_version": "2.1",
  "type": "identity"
}
```

Figure 4: STIX Identity Object (ais-consent-usg)

The AIS Identity Anonymization Process automatically processes this submission, identifies the *ais-consent-usg* label, and determines the Identity object associated with the submission needs to be anonymized when shared with non-federal organizations. The process looks up the anonymized identity of the submitter (generating one if not available) and creates a new Identity object using the anonymized identity. The new Identity object, created by CISA (identity--b3bca3c2-1f3d-4b54-b44f-dac42c3a8f01), looks as shown in Figure 5.

```
{
  "id": "identity--7f3be179-13c4-4afb-8079-af093224214b",
  "created_by_ref": "identity--b3bca3c2-1f3d-4b54-b44f-dac42c3a8f01",
  "identity_class": "organization",
  "created": "2021-04-03T00:07:00.000Z",
  "modified": "2021-04-03T00:07:00.000Z",
  "name": "LeakyRunningChair123",
  "labels": ["ais-consent-usg"],
  "object_marking_refs": [
    "marking-definition--613f2e26-407d-48c7-9eca-b8e91df99dc9"
  ],
  "sectors": [
    "technology"
  ],
  "spec_version": "2.1",
  "type": "identity"
}
```

Figure 5: STIX Identity Object (ais-consent-usg, anonymized)

In this scenario, two sets of content are shared. First, the original submission, with the non-anonymized Identity object and other objects referencing that Identity object in the **created_by_ref** property, is sent without anonymizing the identity to federal organizations since the submitting organization indicated it is willing to share its identity with them. However, given the submitting organization is not willing to share its identity with non-federal organizations, each object in the submission is recreated with a new identifier and **created_by_ref** property that points to the anonymized Identity object. The recreated submission is then shared with all non-federal organizations according to the specified data markings.

5.3 AIS Consent: ais-consent-everyone

When the submitting organization is willing to share its identity information with all federal and non-federal organizations participating in AIS, it uses the *ais-consent-everyone* label. The Identity object looks as shown in Figure 6.

```
{
  "id": "identity--f1dc8ce2-05c9-42a5-ae7f-8fba09c81a2d",
  "created_by_ref": "identity--f1dc8ce2-05c9-42a5-ae7f-8fba09c81a2d",
  "identity_class": "organization",
  "created": "2021-04-03T00:00:00.000Z",
  "modified": "2021-04-03T00:00:00.000Z",
  "name": "Foo Inc.",
  "labels": ["ais-consent-everyone"],
  "object_marking_refs": [
    "marking-definition--613f2e26-407d-48c7-9eca-b8e91df99dc9"
  ],
  "sectors": [
    "technology"
  ],
  "spec_version": "2.1",
  "type": "identity"
}
```

Figure 6: STIX Identity Object (ais-consent-everyone)

Since the *ais-consent-everyone* label is used, the AIS Anonymization Process is bypassed and the submission and identity information are shared with other AIS participants without anonymizing the identity and according to the specified data markings.

5.4 AIS Consent: ais-consent-everyone-cisa-proprietary

Sometimes the information an organization shares within a submission is proprietary. To indicate this and receive the protections for information designated as proprietary afforded by Cybersecurity Information Sharing Act of 2015, the organization creates an Identity object that uses the *ais-consent-everyone-cisa-proprietary* label. Each object containing proprietary information must reference this Identity object via the **created_by_ref** property to receive protections. The Identity object looks as shown in Figure 7.

```
{
  "id": "identity--0c369ac1-786b-4f07-9648-c66109c9d0c2",
  "created_by_ref": "identity--0c369ac1-786b-4f07-9648-c66109c9d0c2",
  "identity_class": "organization",
  "created": "2021-04-03T00:00:00.000Z",
  "modified": "2021-04-03T00:00:00.000Z",
  "name": "Foo Inc.",
  "labels": ["ais-consent-everyone-cisa-proprietary"],
  "object_marking_refs": [
    "marking-definition--613f2e26-407d-48c7-9eca-b8e91df99dc9"
  ],
  "sectors": [
    "technology"
  ],
  "spec_version": "2.1",
  "type": "identity"
}
```

Figure 7: STIX Identity Object (ais-consent-everyone-cisa-proprietary)

Since the *ais-consent-everyone-cisa-proprietary* label is used, the AIS Identity Anonymization Process is bypassed and the submission and identity information are shared with other AIS participants without anonymizing the identity and according to the specified data markings, including the label indicating that the information is proprietary.

5.5 Object With No created_by_ref Property

The STIX specification supports the concept of an anonymous creator where the **created_by_ref** property is omitted from objects in the submission.[6] To leverage this concept, the organization creates an Indicator object without a **created_by_ref** property. For example, see Figure 8.

```
{
  "id": "indicator--fc0033d3-72d3-4f47-b919-aee66b00a31f",
  "created": "2021-04-03T00:00:00.000Z",
  "modified": "2021-04-03T00:00:00.000Z",
  "name": "Malicious Indicator",
  "description": "This indicator represents a known bad URL.",
  "object_marking_refs": [
    "marking-definition--f88d31f6-486f-44da-b317-01333bde0b82"
  ],
  "indicator_types": ["malicious-activity"],
  "pattern": "[url:value = 'http://bad.url.com/Az123/']",
  "pattern_type": "stix",
  "valid_from": "2021-04-03T00:00:00.000Z",
  "spec_version": "2.1",
  "type": "indicator"
}
```

Figure 8: STIX Indicator Object (anonymous creator)

[6] https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html#_xzbicbtscatx

In this situation, since the creator is already anonymized, the AIS Identity Anonymization Process is bypassed and the submission is shared with other AIS participants without anonymizing the identity and according to the specified data markings. While submissions without **created_by_ref** properties will be accepted, it is a best practice to include **created_by_ref** properties where supported by STIX, pointing to a producer Identity object that is anonymized if needed.

All STIX Cyber-observable Objects (SCOs) are by definition shared anonymously because they do not support the **created_by_ref** property.[7] Furthermore, if a **created_by_ref** property is included on an SCO using custom properties or extensions, it will not be recognized by AIS, as custom properties and STIX Extensions are not supported in AIS.

5.6 Identity Object Referenced by created_by_ref Property Isn't Available

The organization creates and submits an Indicator object that points to an Identity object that is not included in the submission and is not known to CISA (e.g., it was also not included in a previous submission to AIS by the submitter). For example, see Figure 9.

```
{
  "id": "indicator--6ce7dfad-91de-489a-8881-6f3e1c8d0958",
  "created_by_ref": "identity--1d503d17-94d6-42d9-b58a-d41b6b4a30c2",
  "created": "2021-04-03T00:00:00.000Z",
  "modified": "2021-04-03T00:00:00.000Z",
  "name": "Malicious Indicator",
  "description": "This indicator represents a known bad URL.",
  "object_marking_refs": [
    "marking-definition--f88d31f6-486f-44da-b317-01333bde0b82"
  ],
  "indicator_types": ["malicious-activity"],
  "pattern": "[url:value = 'http://another.bad.url.com/A1b2c3d/']",
  "pattern_type": "stix",
  "valid_from": "2021-04-03T00:00:00.000Z",
  "spec_version": "2.1",
  "type": "indicator"
}
```

Figure 9: STIX Indicator Object (creator unknown)

In this scenario, since the anonymization preference of the organization is unknown, the AIS Identity Anonymization Process treats this submission as if it were *ais-consent-none*. As a result, a placeholder STIX identifier (in this example, identity--a15d89df-9b8d-410f-96fd-8291ed1759ac) is created by CISA and the submission is recreated with the **created_by_ref** property containing the new placeholder identifier. For example, see Figure 10.

[7] https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html#_mlbmudhl16lr

```
{
  "id": "indicator--cc451572-16dd-4254-b0d8-ea7e3aae33f6",
  "created_by_ref": "identity--a15d89df-9b8d-410f-96fd-8291ed1759ac",
  "created": "2021-04-03T00:08:00.000Z",
  "modified": "2021-04-03T00:08:00.000Z",
  "name": "Malicious Indicator",
  "description": "This indicator represents a known bad URL.",
  "object_marking_refs": [
    "marking-definition--f88d31f6-486f-44da-b317-01333bde0b82"
  ],
  "indicator_types": ["malicious-activity"],
  "pattern": "[url:value = 'http://another.bad.url.com/A1b2c3d/']",
  "pattern_type": "stix",
  "valid_from": "2021-04-03T00:00:00.000Z",
  "spec_version": "2.1",
  "type": "indicator"
}
```

Figure 10: STIX Indicator Object (creator anonymized)

The submission is then shared with federal and non-federal organizations according to the specified data markings. If AIS receives the Identity object corresponding to the original **created_by_ref** at a later time (and that Identity object does not use the *ais-consent-everyone* or *ais-consent-everyone-cisa-proprietary* label), it will be used to create and share an anonymized Identity object using the previously created placeholder STIX identifier. While submissions without the producer Identity object will be accepted, it is a best practice to include the producer Identity object.

6 Appendix A – 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