AUTOMATED INDICATOR SHARING (AIS) SUBMISSION GUIDE

V.16

JANUARY 2021

Cybersecurity and Infrastructure Security Agency
Office of Cybersecurity and Communications
Capacity Building (CB) Division

Contents

1.0 Overview

The goal of the Automated Indicator Sharing (AIS) Initiative is to achieve real-time sharing of cyber threat indicators and defensive measures by enabling the Cybersecurity and Infrastructure Security Agency (CISA) to 1) receive cyber threat indicators and defensive measures submitted by AIS Participants and Federal Entities; 2) remove personally identifiable information (PII) and other sensitive information that is not directly related to a cybersecurity threat; and 3) disseminate the cyber threat indicators and defensive measures to AIS Participants and Federal Entities, as appropriate. Due to the nature of cyber threats, timely response and timely sharing is extremely important.

While human entry of cyber threat indicators and defensive measures via a web portal or email submission are available, the primary focus is the real-time exchange of machine-readable cyber threat indicators and defensive measures via a set of standard application programming interfaces, to improve the speed of response actions.

2.0 Purpose

The purpose of this document is to provide guidance for AIS Participants when submitting cyber threat indicators and defensive measures in the Structured Threat Information eXpression (STIX) format via the Trusted Automated eXchange of Indicator Information (TAXII).

3.0 Definitions

AIS Participant – a person, business, organization, non-Federal governmental body, or other non-Federal legal entity, foreign or domestic, that has accepted the Terms of Use (ToU) agreement.

Cyber Threat Indicators – information that is necessary to describe or identify:

- malicious reconnaissance, including anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat or security vulnerability;
- a method of defeating a security control or exploitation of a security vulnerability;
- a security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability;
- a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability;
- malicious cyber command and control;
- the actual or potential harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat;
- any other attribute of a cybersecurity threat, if disclosure of such attribute is not

otherwise prohibited by law; or

- any combination thereof.

Defensive Measures – an action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability.

- The term ‘‘defensive measure’’ does not include a measure that destroys, renders unusable, provides unauthorized access to, or substantially harms an information system or information stored on, processed by, or transiting such information system not owned by the private entity operating the measure; or another entity or Federal entity that is authorized to provide consent and has provided consent to that private entity for operation of such measure.
- For example, a defensive measure could be something as simple as a security device that protects or limits access to a company’s computer infrastructure or as complex as using sophisticated software tools to detect and protect against anomalous and unauthorized activities on a company’s information system. Regardless, this definition does not authorize the use of measures that are generally to be considered “offensive” in nature, such as unauthorized access of, or execution of computer code on, another entity’s information systems or taking an action that would substantially harm another entity’s information systems. Defensive measures on one entity’s network could have effects on other networks.

4.0 Guidance

4.1 AIS Participants will submit cyber threat indicators and defensive measures using the AIS STIX format. Note that deviations from this guidance at a minimum could reduce the utility of the information for others and, worst case, may result in rejection of portions or all of the indicator and defensive measures.

***NOTE:** Submission files will not exceed 5 MB.

***NOTE: For submissions IF you have a large data set you would like to share with the community (on the order of 1 Million STIX files OR 1GB of data) please contact the TAXII Administrator taxiiadmins@us-cert.gov before publishing. This will allow us to plan accordingly for operational scaling, timing and support during the data load.**

4.2 An organization submitting malicious indicators on purpose would violate both spirit of AIS and probably specifically the Producer’s responsibilities (Section 3 of the ToU).

4.3 AIS Participants shall use only the English language; plain text format when using any submission method.

4.3.1 If formats other than plain text are received, CISA analysts will review the submission, but it will not be automatically processed.

4.4 **AIS STIX Format Submissions** – AIS STIX Format and TAXII are the submission method. See section 5.0 for additional information.

4.5 Prior to submission, AIS Participants will remove all personal information that the sharer knows at the time of sharing is not directly related to a cybersecurity threat. Some personal information may still be included in the indicator submission if it is directly related to a cybersecurity threat (such as the email address of the sender of a phishing email). Note that CISA will process each submission and only PII that is directly related to a cybersecurity threat will be retained and shared by CISA.

4.5.1 CISA will conduct additional processing to ensure that PII not directly related to a cybersecurity threat has been removed prior to dissemination.

4.5.2 AIS Participants shall only submit Embedded Observables. CISA will only accept stix:Observables embedded within stix:Indicators. CISA will not accept stix:Observables defined within the main stix:Observables section of the STIX Package structure.

4.6 **Confidence Level Criteria** – Prior to submitting a cyber threat indicator or defensive measure to CISA through AIS, the submitter will use the CISA standard for assigning the Confidence level (Appendix B) as it relates directly to understanding the level of confidence placed on each cyber threat indicator or defensive measure. Each submission will have a Confidence level assigned to it, and the terminology in Appendix B provides the human-readable definitions used to assign that criteria. CISA will pass along the assigned confidence level that was submitted in all cases. Recipients of indicators can also use the Confidence level to 1) make programmatic decisions as to which indicators require immediate action, 2) which indicators to route to analyst for review, or 3) which indicators to potentially ignore. Any additional metadata or technical context that can be included with each indicator helps the receiving organization make analytical decisions.

4.7 **Traffic Light Protocol (TLP) Marking** – The TLP is a set of designations used to ensure sensitive information is shared with the correct audience. Every cyber threat indicator or defensive measure submission will include a TLP marking. Any cyber threat indicator submitted without the TLP marking would be removed during the AIS validation processes and not re-shared. AIS Participants will honor the TLP markings on received documents. Please refer to section 7.1 of this document or the TLP Matrix at https://www.us-cert.gov/tlp for more detailed information on when to employ the TLP colors (Amber, Green, and White) and how each type of TLP-designated information can be shared. **TLP Red submissions will not be accepted or processed through AIS. Any TLP Red content must be submitted to CISA manually (email or portal).**

4.8 **Malware Sample Submissions** – Do not submit malware samples with AIS. All malware samples must be submitted through the US-CERT reporting page at the following link: https://malware.us-cert.gov/MalwareSubmission/pages/submission.jsf.

5.0 STIX Submissions

5.1 For submissions to AIS, CISA is looking for TLP White or Green indicators and observables that have been seen or likely to have been seen in malicious events – examples would be the following: IP addresses; domains and URIs; email addresses; and

malware hashes.

5.1.1 With the constantly changing and increasing sophistication of cyber threats, it is becoming more likely that our adversaries may successfully breach or compromise organizational information systems. One of the best techniques to address this concern is for organizations to share threat information. This can include, for example, sharing threat events (i.e., tactics, techniques, and procedures) that organizations have experienced, and mitigations that organizations have found to be effective against certain types of threats. Below are sample AIS Submissions to help address these concerns.

- **Exploit Characterization** – Mitigation procedures, known as courses of action (COA), for defending against known Exploit Target/Vulnerability (SQL Injection) found within a system configuration of a software application (Exploit Target). Click on the below link to review the sample AIS Submission:

  https://www.us-cert.gov/sites/default/files/STIX_Namespace/coa_et_exploit_characterization.xml

- **Indicators** – Mitigations for defending against an email from a specific sender's address that appears as a reputable source (niceguy@friendlyco.com) with subject line ("Get Free Gift Cards") with an embedded link (text: "Click here for your gift card", URL: https://getowned.frienldlyco.com) which resolves to IP (10.2.3.4). Click on the below link to review the sample AIS Submission:

  https://www.us-cert.gov/sites/default/files/STIX_Namespace/coa_ind_malicious_email.xml

- **Malware Characterization** – Mitigations for a file with specific hash creates a known Mutex String and modifies the window registry keys. Click on the below link to review the sample AIS Submission:

  https://www.us-cert.gov/sites/default/files/STIX_Namespace/coa_ind_malicious_file.xml

5.2 When using the STIX format, AIS Participants shall adhere to the AIS STIX Profile (Appendix A). Submitters are encouraged to complete each field to the maximum extent before submission.

5.2.1 The AIS STIX Profile is a selection of the STIX fields that most directly relate to cyber threat indicators and defensive measures and has been assessed by an interagency working group to address privacy, civil liberties, and other compliance concerns and risks. The AIS STIX Profile will be updated in the future as the need changes. Any change in the AIS STIX Profile will be assessed by the AIS STIX Profile Change Control Board.

5.2.2 For fields that are not controlled vocabulary or controlled by the schema, AIS Participants shall only provide information as defined in the Guidance column

of the Appendix A. All AIS STIX fields are addressed in the Appendix A - AIS STIX Profile Fields Excel Spreadsheet. However, this section highlights additional information that pertains to the "Required", "NCCIC-Generated Only", and "Review/Potential Review" fields under the Guidance column in the Appendix A, and all other fields that require additional information.

5.3 All AIS STIX fields are addressed in the Appendix A - AIS STIX Profile Fields Excel Spreadsheet. However, this section highlights additional information that pertains to the "Required", "NCCIC-Generated Only", and "Review/Potential Review" fields under the Guidance column in the Appendix A, and all other fields that require additional information.

5.3.1 "Required" Fields under the Guidance column – These fields are required at submission. At the time of submission, cyber threat indicator or defensive measure submissions that do not contain all "required" fields in the AIS STIX Profile will be rejected. The "required" fields are highlighted in green for easy identification in the Appendix A - AIS STIX Profile Fields Excel Spreadsheet.

5.3.2 "NCCIC - Generated Only" Fields under the Guidance column – These fields are for NCCIC dissemination only. These fields will be populated by CISA. The "NCCIC-Generated Only" fields are highlighted in red for easy identification in the Appendix A - AIS STIX Profile Fields Excel Spreadsheet.

5.3.3 "Review" and "Potential Review" Fields under the Guidance column – These fields will "Always" go through a human review or require a "Potential Review" by CISA to remove personal information not directly related to the cybersecurity threat. The "Review" and "Potential Review" fields are highlighted in blue for easy identification in the Appendix A - AIS STIX Profile Fields Excel Spreadsheet.

5.3.3.1 "Potential Review" Fields under the Guidance column –The "Potential Review" fields have specific values or formatting requirements identified in the Example column. The "Under NCCIC Review" will replace any invalid value or formatting characters submitted. These fields will then be reviewed and possibly modified or sanitized via the human manual process before dissemination.

5.3.3.2 Indicators with fields marked "Under NCCIC Review" are currently undergoing a review to determine 1) if there is PII or other sensitive information not directly related to the cyber threat that should be removed or 2) if there are any invalid values or formatting characters that do not meet the requirements for that specific field. Once the indicators have undergone this manual review, an updated indicator will be published using the same indicator ID and the "Under NCCIC Review" will be removed and replaced with the modified or sanitized information.

***NOTE: Some fields may become automated or fully automated over time based on submitted values.

5.4 Review the legend tab in Appendix A for color code guidance with regard to the AIS

STIX Profile fields.

6.0 Defined Vocabulary Terms

Some AIS STIX Profile fields have been given defined vocabulary terms used for validation to ensure the information within the data fields meet a certain predetermined criterion and do not contain PII or any other sensitive information that is not directly related to a cybersecurity threat. Submit requests for additional defined vocabulary terms that should be added to the vocabulary listing to taxiiadmins@us-cert.gov.

7.0 AIS Markings

The AIS Marking is the one and only marking structure approved for AIS usage. This marking must be located as the first marking structure within the STIX_Package/STIX_Header/Handling element. The implementation schema reference can be found at the link below. The TLP marking and consent fields are controlled and defined by the bundle marking schema located at the following link:

http://www.us-cert.gov/sites/default/files/STIX_Namespace/AIS_Bundle_Marking_1.1.1_v1.0.xsd

7.1 TLP

7.1.1 TLP is a set of designations used to ensure that sensitive information is shared with the appropriate audience. It employs four colors, White, Green, Amber, and Red, to indicate recipient(s). However, TLP Red submissions will not be accepted or processed through AIS. Any TLP Red content must be submitted to CISA through manually (email or portal). All AIS Participants will follow the TLP marking schema. Please refer to Figure 1 below.

- TLP provides a simple and intuitive schema for indicating when and how sensitive information can be shared, facilitating more frequent and effective collaboration. TLP is not a “control marking” or classification scheme. TLP was not designed to handle licensing terms, handling and encryption rules, and restrictions on action or instrumentation of information. TLP labels and their definitions are not intended to have any effect on freedom of information or “sunshine” laws in any jurisdiction.
- Amber information submitted by non-Federal entities will go to government as well as other non-federal trusted partners, e.g. major CI entities, cyber threat companies, and ISACs, who work with CISA in other programs, such as CISCP. Amber information submitted by non-Federal entities will not be redistributed to other non- Federal entities outside of these criteria. However, Amber information submitted by Federal entities will be more broadly distributed, including to AIS companies. Table 1 below shows which TLP level information is made available on the AIS feed depending on the source:

Indicator Source	TLP level shared via AIS TAXII feed

Federal Entity (including US-CERT)	White, Green, Amber
Non-Federal Entity (includes AIS companies, CISCP organizations and international partners)	White, Green

Table 1: Source and TLP Levels

7.1.2 For the purpose of the AIS Initiative, the Information Sharing and Analysis Centers (ISAC) and the Information Sharing and Analysis Organizations (ISAO) receiving AIS cyber threat indicators or defensive measure marked TLP White, Green, or Amber may share that information with all their members at the same marking level. CISA recommends no proprietary information be submitted as TLP:White given the ability to post this information openly on the internet.

7.1.3 TLP markings reference the entire submission. There is no partial or field-level marking capability at this time. See Figure 1: TLP Matrix below.

Color	When should it be used?	How may it be shared?
TLP:AMBER  Limited disclosure, restricted to participants' organizations.	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**
TLP:GREEN  Limited disclosure, restricted to the community.	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.
TLP:WHITE  Disclosure is not limited.	Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Figure 1: TLP Matrix

7.2 Consent.

The Consent designations identified below are required on STIX. There are two consent choices; share identity as the source with all or identify to whom to share with.

7.2.1 AIS Submitters consent to share their identity as the source of the cyber threat indicator or defensive measure with each and every submission.

7.2.2 AIS Submitters identify to whom they choose to share their identity. There will be three choices to choose from:

7.2.2.1 Consent > None (CISA will not disclose identity, except as permitted in the AIS Terms of Use).

7.2.2.2 Consent > USG (CISA will only share your identity with Federal Entities).

7.2.2.3 Consent > Everyone (CISA will share your identity with all AIS Participants and with Federal Entities).

7.3 Source Information.

Ensure the "required" fields listed below are properly filled out.

7.3.1 Organization Name. Every submission must contain the name of the submitting organization. This will be the same organization name referenced in the AIS Terms of Use.

7.3.2 Country. Every submission must contain the country of the submitting organization. This will be same country of the organization referenced in the AIS Terms of Use. Country must be provided in ISO 3166-1 alpha-2 format.

7.3.3 Administrative Area (State, Provence, etc.). Every submission must contain the administrative area of the submitting organization. This will be same organization name used on the AIS Terms of Use. Administrative Area must be provided in ISO 3166-2 format.

7.3.4 Industry Type (Sector). Every submission must contain at least one industry type (multiple pipe "|" delimited values are allowed). Industry types are limited to the 16 critical infrastructure sectors referenced by the link below ("Other" may also be used).

https://www.dhs.gov/critical-infrastructure-sectors

7.4 CISA Proprietary Information.

Consistent with CISA and any other applicable provision of law, a cyber threat indicator or defensive measure provided by a non-Federal entity to the Federal Government under this title shall be considered the commercial, financial, and proprietary information of such non-Federal entity when so designated by the originating non-Federal entity or a third party acting in accordance with the written authorization of the originating non-Federal entity.

8.0 Personally Identifiable Information (PII)

8.1 DHS defines PII as any information that permits the identity of an individual to be directly or indirectly inferred, including any information linked or linkable to that individual, regardless of whether the individual is a U.S. Citizen, legal permanent resident, visitor to the U.S., or employee or contractor to the Department. Some PII is not sensitive, such as that found on a business card. Sensitive PII is PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Sensitive PII requires stricter handling guidelines because of the increased risk to an individual if the data are compromised.

8.2 Examples of PII that should not typically be in a submission include: Social Security number (SSN), driver's license or state identification number, passport number, Alien Registration Number (A-Number), or financial account number. Other data elements such as citizenship or immigration status, medical information, ethnic, religious, sexual orientation, or lifestyle information, and account passwords, in conjunction with the identity of an individual (directly or indirectly inferred), are also sensitive PII. In addition, the context of the PII may determine its sensitivity, such as a list of employees with poor performance ratings.

8.2.1 PII will not be submitted unless it is information that is directly related to the cybersecurity threat. AIS Participants will remove all PII that is not directly related to a cybersecurity threat prior to submission of a cyber threat indicator or defensive measure.

8.2.2 CISA will ensure all indicators it shares within the Federal Government or with AIS Participants are mitigated with regard to privacy, civil liberties, and other compliance concerns as otherwise required by law.

9.0 Protected Critical Infrastructure Information (PCII)

Critical Infrastructure Information (CII), which becomes PCII upon completion of the submission and validation process, is defined in the CII Act as: Information not customarily in the public domain and related to the security of critical infrastructure or protected systems –

(A) actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct (including the misuse of or unauthorized access to all types of communications and data transmission systems) that violates federal, state, or local law, harms interstate commerce of the United States, or threatens public health or safety;

(B) the ability of any critical infrastructure or protected system to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection, or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation thereto, risk management planning, or risk audit; or

(C) any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, reconstruction, insurance, or continuity, to the extent it is related to such interference, compromise, or incapacitation.

At this time, AIS Participants should not submit or share PCII through AIS as adequate marking and information protections schemes are not currently implemented; however, future AIS updates may allow for this capability.

If an AIS Participant, which also participates in the CISA Cyber Information Sharing and Collaboration Program (CISCP), has PCII or classified information to share, it may submit that information under the CISCP program. Such sharing is outside of the AIS Program. Please visit the US-CERT webpage for additional CISCP information at:

https://www.us-cert.gov/sites/default/files/c3vp/CISCP_20140523.pdf

10.0 Versioning

In the event cyber threat indicators or defensive measures are disclosed by mistake, such as in error, or with an incorrect TLP marking, CISA should be notified immediately at toll free 1-888-282-0870 or cisacentral@cisa.gov. All reasonable steps to mitigate, including sending a versioning update, will take place as soon as practicable, as stated in the Terms

of Use.

In the event personal information, which pertains to a U.S. person, has been shared by any government agency in violation of CISA, the NCCIC should be notified immediately at toll free 1-888-282-0870 or cisacentral@cisa.gov. All reasonable steps to mitigate, including sending a versioning update, will take place as soon as practicable. Agencies should notify the affected person in a timely manner in accordance with their breach/incident response plan. For more information on how DHS identifies and reports privacy incidents, please reference the DHS Privacy Incident Handling Guidance.[1]

11.0 Outreach Program

CISA will sponsor, at a minimum, quarterly meetings/webinars to promote cybersecurity best practices that are developed based on ongoing analyses of cyber threat indicators, defensive measures, and any additional information relating to cybersecurity threats. Requests for engagements and/or webinars on AIS or Cyber threat indicators can be sent to cyberservices@cisa.dhs.gov

12.0 CISA Contact and Administration Information

If you have any questions concerning the submission or dissemination of cyber threat indicators or defensive measures please send your questions using one of the following methods; email cisacentral@cisa.gov or toll free 1-888-282-0870.

Changes to the Submission Guidance may be made without notice; however, AIS Participants will receive updated copies as they are published.

For additional AIS information please visit the AIS web page at Automated Indicator Sharing: https://www.cisa.gov/automated-indicator-sharing-ais. Any additional inquiries on AIS program can be sent to cyberservices@cisa.dhs.gov.

[1] The DHS Privacy Incident Handling Guidance can be found at http://www.dhs.gov/sites/default/files/publications/privacy-incidence-handling-guide.pdf

Appendix A - AIS STIX Profile Fields

To access the AIS STIX Profile Fields click on the following link:

https://www.us-cert.gov/sites/default/files/ais_files/AIS_Submission_Guidance_Appendix_A.pdf.

Appendix B – Confidence Level Criteria

B-1 **Purpose.** The purpose of this Appendix is to provide guidance for assigning confidence levels to AIS cyber threat indicators and defensive measures.

B.2 **Reference.** Defense Intelligence Agency, Confidence Level Definitions, 08/06/2010.

B-3 **Definition.** Confidence Level – For an indicator or defensive measure, it is the criteria, assigned by the analyst, which succinctly expresses the sureness of the indicator or defensive measure.

Confidence levels are assigned to a cyber threat indicator or defensive measure based on:

- The context of the event
- The validity of the source, and
- The knowledge of the threat.

B.4 **Confidence Level Criteria.** Prior to submitting a cyber threat indicator or defensive measure to CISA through AIS, the submitter will use the following CISA standard for assigning the confidence level criteria as it relates directly to understanding the level of threat placed on each cyber threat indicator or defensive measure.

- HIGH – This confidence is based on judgements of high-quality information from multiple sources or from a single, highly reliable source. This makes it possible to render a solid decision on the information.
- MEDIUM – The information is credibly sourced and plausible, but can be interpreted in various ways, or is not sufficient quality or collaborated sufficiently to warrant a higher level of confidence.
- LOW/UNKNOWN – The information's credibility and/or plausibility is questionable, the information is too fragmented or poorly collaborated to make solid analytical inferences, or that CISA has significant concerns or problems with the sources.

Appendix C – AIS Submission Guidance Change Log

Version	Date	Change
1.0	11/6/15	Initial version
2.0	2/11/16	Internal version incorporating CISA requirements
3.0	2/16/16	Released version with CISA changes
4.0	4/26/16	Added table for TLP level information/AIS feed
5.0	5/18/16	Updated link to TLP / Consent schema
6.0	7/20/16	Added link to AIS STIX Profile Fields in Appendix A; added "STIX" to the title of the Appendix A; removed "See Attachment" in the header; and added 12.3
7.0	8/9/16	Updated the TLP URL
8.0	9/6/16	Added 4.1.1: Submission files will not exceed 5 MB
9.0	10/17/16	Added: 7.3 Source Information, which changed CISA Proprietary Information to 7.4 Updated: 4.5 – TLP Red submission statement; 7.0 AIS Markings; 7.1.1 TLP; 7.2 Consent statement; 7.2.1 AIS Submitters consent; 7.2.2.1; 7.2.2.2; 7.2.2.3; and Figure 1 with current information: the TLP Red was deleted; AIS STIX Profile line 323; Example and Guidance columns;

		Deleted: section number 6.1 only - no changes were made to the paragraph; 7.2.3 Consent, but added the information under 7.2; 7.2.4 For Email submissions;
10.0	10/21/16	Added: Under the CIQ Identity 3.0 - Organisation Info Inline Type – Guidance Column - Inserted a "," after Reactors in the Nuclear Reactors, Materials, and Waste Sector
11.0	01/24/17	Added: 5.2.3.1 "Potential Review" Fields under the Guidance column – The "Potential Review" fields have specific values or formatting requirements identified in the "Example" column. The "Under NCCIC Review" will replace any invalid value or formatting characters submitted. These fields will then be reviewed and possibly modified or sanitized via the human manual process before dissemination.
12.0	03/28/17	Added: 4.5 - Confidence Level Criteria; 5.1 – For submissions to AIS, CISA is looking for TLP White or Green; 5.1.1 - With the constantly changing and increasing sophistication of cyber threats; 5.3.3.2 - Indicators with fields marked "Under NCCIC Review"; Appendix B – Confidence Level Criteria Changed: AIS Submission Guidance Change Log is now Appendix C

13.0	02/12/18	Added Cover Page; Table of Contents; corrected formatting
14.0	3/27/18	Added 4.2 and renumbered Section 4.
15.0	10/2/18	Added “Note” to Section 1 concerning data submissions of 1GB and/or 1 Million STIX files.
16.0	01/25/21	Added new CISA template. Updated CISA email addresses and program URLs. Updated and finalized for public release.