The Department of Homeland Security
The Department of Justice

Final Procedures Related to the Receipt of Cyber Threat Indicators and Defensive Measures by the Federal Government

October 2021

Table of Contents

Consistent with the Cybersecurity Information Sharing Act of 2015 (CISA 2015)[1], specifically section 1504(a)(2) and (3), this document establishes procedures relating to the receipt of cyber threat indicators and defensive measures by all federal entities under CISA 2015. It describes the processes for receiving, handling, and disseminating information that is shared with the Department of Homeland Security (DHS) pursuant to section 1503(c), including through operation of the DHS Automated Indicator Sharing (AIS) capability under section 1504(c). It also states and interprets the statutory requirements for all federal entities that receive cyber threat indicators and defensive measures under CISA 2015 to share them with other appropriate federal entities.

Federal entities engaging in activities authorized by CISA 2015 shall do so in full compliance with the Constitution and all other applicable laws of the United States, Executive Orders and other Executive Branch directives, regulations, policies and procedures, court orders, and all other legal, policy, and oversight requirements. Nothing in these procedures shall affect the conduct of authorized law enforcement or intelligence activities or modify the authority of a department or agency of the Federal Government to protect classified information and sources and methods and the national security of the United States.

1 Terms of Reference

Section 1504(c) establishes within DHS the Federal Government's capability and process[2] for the receipt of cyber threat indicators and defensive measures from non-federal entities through an automated real-time exchange, electronic mail or media, or a website interface. The following operational procedures reference several key terms. These terms have been defined by CISA 2015 and are set forth in Appendix A.

2 Receipt, Processing, and Dissemination of Cyber Threat Indicators and Defensive Measures Submitted Through Real-Time Means [Sec. 1504 (a)(3)(A)]

This section describes the sharing of cyber threat indicators and defensive measures with the Federal Government through the DHS AIS capability provided for by section 1504(c).[3] The DHS capability to receive, filter, analyze, and disseminate such information in real-time leverages Structured Threat Information eXpression (STIX) and Trusted Automated eXchange of Intelligence Information (TAXII) specifications, along with the procedures and standards

[1] CISA 2015 was enacted as Title I of the Cybersecurity Act of 2015, and is codified at 6 U.S.C. §§ 1501–1510. For ease of reference, these Procedures generally cite to the sections as codified in title 6 of the U.S. Code.

[2] That capability and process was certified as operational by the Secretary of DHS on March 17, 2016, as required by CISA 2015.

[3] Upon making a certification as provided in section 1504(c)(2)(B), the President may designate one or more other federal entities to develop and implement a capability and process pursuant to section 1504(c)(2)(B)(III). If that were to occur, the procedures in this section 2 and section 1504(a)(3)(A) would apply to that capability and process as well.

developed by the national cybersecurity centers. Any entity participating in this AIS capability must be able to communicate using these machine-to-machine specifications, as further described below. Entities wishing to share cyber threat indicators through non-real-time means should see below for other options.

2.1 Connecting to the TAXII Server

In order to participate in the AIS capability, federal entities, as well as non-federal entities participating in the program, must coordinate with DHS to ensure proper implementation, including access to the necessary technical infrastructure, establishment of network connectivity and exchange of authentication and other technical specifications, required for access to the sharing capability. For details on certifications and connectivity specifics, see the Frequently Asked Questions (FAQ).

2.2 Receipt of Cyber Threat Indicators and Defensive Measures

To make a submission via the DHS automated capability, participating Federal and non-federal entities must follow submission guidance specifications made available by DHS. Non-Federal entity submissions should conform to the AIS Profile, which can be found at https://www.cisa.gov/ais. AIS now supports nearly[4] all fully developed STIX 2.1 core objects and defined properties via TAXII 2.1 and as a result, the AIS Profile is no longer represented as a list of fields that may or may not be used. Rather, the AIS Profile is represented as a collection of requirements that must be met to ensure submissions can be shared within the AIS capability. Failure to follow these requirements will result in the rejection of portions or all the submission. In addition, DHS assesses STIX objects and properties for privacy, civil liberties, and other compliance concerns and risks such that submissions can undergo automated and/or human review to ensure compliance with CISA 2015 (see Section 2.4, below).

Upon receipt of cyber threat indicators or defensive measures, federal entities should adhere to all other applicable procedures, guidelines, and requirements, to the extent consistent with and in addition to the Privacy and Civil Liberties Final Guidelines: Cybersecurity and Information Sharing Act of 2015 ("Privacy and Civil Liberties Guidelines"), which can be found at https://www.cisa.gov/ais. In addition, federal entities sharing information should use the AIS Profile to standardize the submitted cyber threat indicators and defensive measures and adhere to all relevant requirements contained in the Privacy and Civil Liberties Guidelines.

The AIS Profile document, as well as the full submission guidance (which provides further guidance and recommendations for submitting information to AIS), can be found at https://www.cisa.gov/ais. Non-federal entities are encouraged to review the full submission guidance and the "Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015" for details on how to share with federal entities under CISA 2015.

[4] As described in the AIS Profile, the Incident STIX Domain Object and the Artifact STIX Cyber-observable Object are not currently supported by AIS. Support for these Objects may be added to AIS at a later time.

2.3 AIS Profile Change Control Governance

Through continued collaboration and experience, the appropriate federal entities and other information sharing participants will identify changes to the AIS Profile. DHS will chair the AIS Profile Change Control Board, the membership of which will comprise an authorized representative of the head of each appropriate Federal agency listed in section 1501(3). Requests to modify the requirements within the AIS Profile will be submitted in writing by any member of the AIS Profile Change Control Board. In addition, the AIS Profile Change Control Board will provide other federal entities and information sharing participants with opportunities to submit change requests. The following specific process will be followed by the AIS Profile Change Control Board:

- Each member can submit a written proposal to add, delete, or modify a requirement in the AIS Profile.
- DHS will forward such proposals to the AIS Profile Change Control Board.
- Upon receipt of a proposal, the AIS Profile Change Control Board members will have two weeks to consider the proposal.
- The proposal will be accepted only if no member objects.
    - If a member does not affirmatively object to a proposal within two weeks, then that member's concurrence will be presumed by the AIS Profile Change Control Board and the proposal will be accepted.
    - The AIS Profile Change Control Board will meet to discuss proposals for which an objection is provided or for which further discussion is requested.
    - The AIS Profile Change Control Board will attempt to resolve an objection or request for further discussion.
    - If the AIS Profile Change Control Board cannot resolve an objection, DHS will escalate the proposal up to and including, if necessary, each appropriate Federal agency's head for resolution with unanimous approval required.
- When considering a proposal, each member of the AIS Profile Change Control Board will ensure that requirements are added, deleted, or modified:
    - in compliance with CISA 2015's definitions of cyber threat indicators and defensive measures;
    - in compliance with CISA 2015's provisions designed to limit the receipt, retention, use, and dissemination of cyber threat indicators containing personal information of specific individuals or information that identifies specific individuals; and
    - commensurate with the overarching set of STIX objects and properties available in the latest STIX specification published by the Organization for the Advancement of Structured Information Standards (OASIS).

Note: Notwithstanding these procedures, DHS preserves its ability (1) to develop and implement emergency break fixes to the AIS Profile without having to seek approval from the AIS Profile Change Control Board; (2) to make modifications to the AIS Profile if a change to the

information technology infrastructure calls for it; and (3) to implement AIS support for the Incident STIX Domain Object and the Artifact STIX Cyber-observable Object and update the Profile accordingly.

2.4 Filtering and Analysis of Cyber Threat Indicators and Defensive Measures

Upon receipt by DHS, a series of automated actions occur. Where an automated process identifies an error, or a particular object cannot be processed by automated means, the system will not disseminate the object. When human review is required, processing and dissemination of that object will be delayed along with any objects that refer to that object within the submission. Any objects that do not refer to the held back objects will be transmitted to AIS. Following human review, the object and any objects that refer to that object will be transmitted, subject to section 2.4.2.2, below. Automated processing is designed to maximize the speed, quantity, and value of information that can be shared with the Federal Government. The following subsections identify automated actions that do not incur modifications or delays and actions that may cause modifications and delays.

2.4.1 Automated Actions That Do Not Modify or Delay Transmission of Cyber Threat Indicators or Defensive Measures

This subsection identifies automated actions that do not modify or delay transmission of cyber threat indicators or defensive measures.

2.4.1.1 Automated validation against the AIS Profile. This confirms the submission is a valid STIX document, that the submission meets the requirements defined in the AIS Profile, e.g., individual properties and objects conform to applicable schema. If the submission is not a valid STIX document or does not meet the requirements defined in the AIS Profile, DHS will reject the objects in the submission that did not meet the requirements. Any objects that meet the requirements and do not depend on the rejected objects will be distributed through AIS.

2.4.2 Actions That May Modify or Delay Transmission of a Cyber Threat Indicator or Defensive Measure

This subsection identifies the controls pursuant to which DHS will, in limited instances, make modifications, some of which could delay the real-time sharing of one or more cyber threat indicator or defensive measure submitted by a non-Federal entity pursuant to section 1503. Consistent with section 1504(a)(3)(A), these controls will be carried out before any of the appropriate federal entities retains or uses the cyber threat indicators or defensive measures and will be uniformly applied such that each of the appropriate federal entities is subject to the same

delay, modification, or other action. As required by section 1504(a)(3)(A)(ii)(I), the heads of the appropriate federal entities unanimously agree to these controls.[5]

2.4.2.1 Automated processing for mitigation of remaining personal information risks through schema restrictions, controlled vocabulary, regular expressions (i.e., pattern matching), known good values, and autogenerated text. Any objects or properties that do not meet certain predetermined criteria or that are identified as potentially containing personal information will be referred for human review to determine whether it contains information that DHS knows to be personal information of specific individuals or information that identifies specific individuals, and, if so, whether that information is not directly related to the cybersecurity threat. When an object (or property associated with an object) is referred for human review, DHS will delay the transmission of the entire object and any objects that refer to that object, within the submission, until human review is complete. Any other objects that do not refer to the held back objects will be transmitted to AIS.

2.4.2.2 If after human review the property is determined to either (a) not contain information that DHS knows to be personal information of a specific individual(s) or information that identifies a specific individual(s), or (b) the property is determined to contain such information, but it is determined to be directly related to the cybersecurity threat, then the delayed transmission will be promptly distributed through AIS. If, after human review the property is determined to contain information that DHS knows to be personal information of a specific individual(s) or information that identifies a specific individual(s) and that information is not directly related to the cybersecurity threat, but that information is able to be removed while still preserving other information within the object, then DHS will create and distribute a new object that does not contain the personal information. If after human review, the property is determined only to contain personal information of a specific individual(s) or information that identifies a specific individual(s) that is not directly related to the cybersecurity threat (such that the information cannot be removed while still preserving other information within the property), a new object without the property will be created, to the extent possible, and issued by DHS. In both cases, if that object is referenced by any other objects within the submission, DHS will create and distribute duplicates of those objects, revised to refer to the updated object that does not contain the personal information.

[5] DHS will continuously assess the controls described below, based on the volume and content of cyber threat indicators (CTIs) received, to achieve further automation and generally to avoid the unnecessary delay of the distribution of CTIs while protecting privacy.

2.4.2.3 In the case of submissions in an AIS-supported foreign language, each property is translated into English and run through the automated processing described in 2.4.2.1. If, after this processing, the submission is referred to human review, the entry will be actioned in accordance with 2.4.2.1 and 2.4.2.2, as applicable. If as a result of this process, DHS is required to create a new object(s), the new object will be generated by removing the personal information from the English translation and translating that back into the foreign language. A new object that contains the translation of the properties from the foreign language into English (with personal information removed, as appropriate) will also be created and issued by DHS. DHS will notify the submitter that properties were changed or removed from the submission.

2.4.2.4 As described in 2.4.1.1, submissions are automatically validated against the requirements of the AIS Profile. If the submission contains objects that do not align with these requirements, DHS will remove those objects from further automated processing and delete those properties.

2.4.2.5 In some cases, DHS may append CISA opinions to Indicator objects in submissions to provide additional context.

2.4.2.6 DHS may convert markings and labels between Federal entities (e.g., Access Control Specification markings) and Non-Federal entities (e.g., Traffic Light Protocol markings and AIS Consent label), and vice-versa.

2.4.2.7 In cases where the submitter has not consented to transmission of its identity to other federal entities, automated preprocessing will replace the information identifying the submitter with the anonymized version of the information. Submitters are required to indicate whether they consent to transmission of their identity to other federal entities. If submitters consent to transmission of their identity to other federal entities, DHS will transmit their identity. If submitters do not initially consent to transmission of their identity to other federal entities, but another federal entity wishes to contact the submitter, DHS will transmit that request and ask whether the submitter consents to sharing its identity with that Federal entity.

2.5 Dissemination of Cyber Threat Indicators and Defensive Measures

Once automated processing has been performed on a submission made to DHS by a non-Federal entity, a sanitized cyber threat indicator or defensive measure will be made available to the appropriate federal entities. If human review of one or more objects or properties is required, then the cyber threat indicator or defensive measure along with any other cyber threat indicators or defensive measures that refer to those objects or properties will not be immediately sent to the appropriate federal entities. Once human review is completed, the cyber threat indicator or defensive measures and any other cyber threat indicators or defensive measures that refer to them will either be sent to the appropriate federal entities or, if modifications are necessary, DHS will create and distribute new objects (as described in 2.4.2.2) to the appropriate federal entities.

3 Receipt, Processing, and Dissemination of Cyber Threat Indicators Submitted Through Non-Automated Means [Sec. 1504 (a)(3)(B)]

This section outlines the overall process by which cyber threat indicators and defensive measures that are shared with the Federal Government by any non-Federal entity pursuant to section 1503 through non-real-time mechanisms are shared with all of the appropriate federal entities.

3.1 General Guidance

3.1.1 Timeliness

Upon receipt of a cyber threat indicator or defensive measure from a non-Federal entity in a manner other than the real-time process described in section 1504(c), a recipient Federal entity shall share such cyber threat indicator or defensive measure with each appropriate Federal entity as quickly as operationally practicable, consistent with applicable law and the mission of those entities, and with other Federal entities, as appropriate. In no event should a recipient Federal entity introduce an unnecessary delay, interference, or any other action that could impede receipt by all appropriate Federal entities. Modifications, delays or other actions undertaken to remove personal information of specific individuals or information that identifies specific individuals that is not directly related to the cybersecurity threat are permissible.

3.2 DHS Procedures

3.2.1 Web Form Submissions (http://us-cert.cisa.gov/forms/share-indicators)

DHS can receive web submissions of cyber threat indicators and defensive measures from Federal and non-federal entities, although the automated exchange using STIX and TAXII specifications, and described in greater detail in Section 2, is strongly preferred since it encompasses a real time, machine-to-machine exchange that supports a higher volume of cyber threat indicators and defensive measures. The web submission includes validation that all required fields are present. Upon submission, the web form submission will be forwarded to DHS cyber threat analysts to determine if there is valid cyber threat indicator or defensive measure, and after review (including a review to determine whether the cyber threat indicator or defensive measure contains any information that DHS knows to be personal information of specific individuals or information that identifies specific individuals that is not directly related to the cybersecurity threat), may be entered into the main DHS cyber threat repository. Once there, it will be delivered to the DHS TAXII server for dissemination to the appropriate federal entities. DHS will make available a publicly accessible web form for submission of cyber threat indicators and defensive measures to DHS.

3.2.2 Email Submissions (central@cisa.dhs.gov)

DHS can receive email submissions of cyber threat indicators and defensive measures from Federal and non-federal entities to central@cisa.dhs.gov. The ingestion of submissions to this email address includes validation that all required fields are present. Due to the additional review and separate processing workflow, email submissions are not the preferred method of

submission and may result in processing delays due to the unstructured nature of email. Submissions to this email address will be forwarded to DHS cyber threat analysts to determine if there is a valid cyber threat indicator or defensive measure, and after review (including a review to determine whether the cyber threat indicator or defensive measure contains any information that DHS knows to be personal information of a specific individual(s) or information that identifies a specific individual(s) that is not directly related to the cybersecurity threat), may be entered into the main DHS cyber threat repository. Once there, it will be delivered to the DHS TAXII server for dissemination to the appropriate federal entities.

3.2.3 Other Methods

DHS can receive submissions of cyber threat indicators and defensive measures through other programs that leverage machine-to-machine sharing, web forms, or emails (or may integrate these other programs as part of AIS). Where such submissions require additional review and separate processing workflow (such as the need to convert submissions into formats consistent with AIS), such submissions are not the preferred method of submission and may result in processing delays. Such submissions may be forwarded to DHS cyber threat analysts to determine if there is a valid cyber threat indicator or defensive measure, and after review (including a review to determine whether the cyber threat indicator or defensive measure contains any information that DHS knows to be personal information of specific individuals or information that identifies specific individuals that is not directly related to the cybersecurity threat), may be entered into the main DHS cyber threat repository. If entered there, it will be delivered to the DHS TAXII server for dissemination to the appropriate federal entities. For certain commonly used other submission methods, DHS may, at its discretion, develop automated processes to automatically convert submissions of cyber threat indicators or defensive measures for processing by AIS (or otherwise integrate these programs as part of AIS), at which point such submissions will proceed through AIS as described in section 2.4.

3.2.4 Vulnerability Disclosure Programs

DHS will not unilaterally share cyber threat indicators that are exclusively security vulnerabilities related to particular U.S. Government agency systems that are shared with DHS pursuant to that agency's vulnerability disclosure program.

4 Audit Capabilities and Unsanctioned Use [Sec. 1504(a)(3)(C)]

This section outlines the provisions and requirements for auditing and accountability to usage requirements.

4.1 Auditing Capabilities

The appropriate federal entities shall maintain data, at the appropriate level of classification, regarding:

- The number of cyber threat indicators or defensive measures for which personal information of specific individuals or information that identifies specific individuals, that is not directly related to a cybersecurity threat, was removed;
- The number of notices issued with respect to a failure to remove personal information of specific individuals or information that identifies specific individuals, that is not directly related to a cybersecurity threat;
- The extent to which cyber threat indicators or defensive measures were properly classified;
- The number of cyber threat indicators or defensive measures received through the DHS AIS capability and process established pursuant to section 1504(c); and
- A list of the federal entities with which cyber threat indicators or defensive measures have been shared pursuant to CISA 2015.

The appropriate federal entities may choose to individually maintain additional data for auditing purposes based on those entities' individual requirements. Furthermore, the appropriate federal entities may evolve their audit data based on experience sharing under CISA 2015.

4.2 Sanctions

Failure by an individual to abide by the usage requirements set forth in these guidelines will result in sanctions applied to that individual in accordance with their department or agency's relevant policy on Inappropriate Use of Government Computers and Systems. Penalties commonly found in such policies, depending on the severity of misuse, include: remedial training; loss of access to information; loss of a security clearance; and termination of employment.

5 Appendix A: Glossary

Please note that, with the exception Structured Threat Information Expression (STIX) and Trusted Automated Exchange of Intelligence Information (TAXII), all defined terms are from 6 U.S.C. § 1501.

AGENCY—The term ''agency'' has the meaning given the term in section 3502 of title 44, United States Code.

APPROPRIATE FEDERAL ENTITIES—The term ''appropriate federal entities'' means the following:

(A) The Department of Commerce.
(B) The Department of Defense.
(C) The Department of Energy.
(D) The Department of Homeland Security.
(E) The Department of Justice.
(F) The Department of the Treasury.

(G) The Office of the Director of National Intelligence.

CYBERSECURITY THREAT—

(A) IN GENERAL—Except as provided in subparagraph (B) of this definition, the term ‘‘cybersecurity threat’’ means an action, not protected by the First Amendment to the Constitution of the United States, on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system.

(B) EXCLUSION—The term ‘‘cybersecurity threat’’ does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement.

CYBER THREAT INDICATOR—The term ‘‘cyber threat indicator’’ means information that is necessary to describe or identify—

(A) 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;

(B) a method of defeating a security control or exploitation of a security vulnerability;

(C) a security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability;

(D) 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;

(E) malicious cyber command and control;

(F) the actual or potential harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat;

(G) any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law; or

(H) any combination thereof.

DEFENSIVE MEASURE—

(A) IN GENERAL—Except as provided in subparagraph (B) of this definition, the term ‘‘defensive measure’’ means 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.

(B) EXCLUSION—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—

(i) the private entity operating the measure; or

(ii) another entity or Federal entity that is authorized to provide consent and has provided consent to that private entity for operation of such measure.

FEDERAL ENTITY—The term ‘‘federal entity’’ means a department or agency of the United States or any component of such department or agency.

INFORMATION SYSTEM—The term ‘‘information system’’—

(A) has the meaning given the term in section 3502 of title 44, United States Code; and

(B) includes industrial control systems, such as supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers.

LOCAL GOVERNMENT—The term ‘‘local government’’ means any borough, city, county, parish, town, township, village, or other political subdivision of a State.

MALICIOUS CYBER COMMAND AND CONTROL—The term ‘‘malicious cyber command and control’’ means a method for unauthorized remote identification of, access to, or use of, an information system or information that is stored on, processed by, or transiting an information system.

MALICIOUS RECONNAISSANCE—The term ‘‘malicious reconnaissance’’ means a method for actively probing or passively monitoring an information system for the purpose of discerning security vulnerabilities of the information system, if such method is associated with a known or suspected cybersecurity threat.

MONITOR—The term ‘‘monitor’’ means to acquire, identify, or scan, or to possess, information that is stored on, processed by, or transiting an information system.

NON-FEDERAL ENTITY—

(A) IN GENERAL—Except as otherwise provided in this definition, the term ‘‘nonfederal entity’’ means any private entity, non-Federal government agency or department, or State, tribal, or local government (including a political subdivision, department, or component thereof).

(B) INCLUSIONS—The term ‘‘non-federal entity’’ includes a government agency or department of the District of Columbia, the Commonwealth of Puerto Rico, the

United States Virgin Islands, Guam, American Samoa, the Northern Mariana Islands, and any other territory or possession of the United States.

(C) EXCLUSION—The term ‘‘non-federal entity’’ does not include a foreign power as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

PRIVATE ENTITY—

(A) IN GENERAL—Except as otherwise provided in this paragraph, the term ‘‘private entity’’ means any person or private group, organization, proprietorship, partnership, trust, cooperative, corporation, or other commercial or nonprofit entity, including an officer, employee, or agent thereof.

(B) INCLUSION—The term ‘‘private entity’’ includes a State, tribal, or local government performing utility services, such as electric, natural gas, or water services.

(C) EXCLUSION—The term ‘‘private entity’’ does not include a foreign power as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

SECURITY CONTROL—The term ‘‘security control’’ means the management, operational, and technical controls used to protect against an unauthorized effort to adversely affect the confidentiality, integrity, and availability of an information system or its information.

SECURITY VULNERABILITY—The term ‘‘security vulnerability’’ means any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control.

STRUCTURED THREAT INFORMATION EXPRESSION (STIX)—“STIX” is a language for describing cyber threat information in a standard manner for the reading convenience of machines, not humans. STIX provides a common mechanism for addressing structured cyber threat information across and among this full range of use cases improving consistency, efficiency, interoperability, and overall situational awareness. In addition, STIX provides a unifying architecture tying together a diverse set of cyber threat information including:

- Cyber observables
- Indicators
- Adversary tactics, techniques, and procedures (including attack patterns, malware, kill chains, tools, infrastructure, etc.)
- Courses of action (e.g., incident response or vulnerability/weakness remedies or mitigations)
- Campaigns
- Threat actors

For more information on STIX, see https://oasis-open.github.io/cti-documentation/ .

TRUSTED AUTOMATED EXCHANGE OF INTELLIGENCE INFORMATION (TAXII)—
"TAXII" is a standard for exchanging structured cyber threat information in a trusted manner. TAXII defines services, protocols and messages to exchange cyber threat information for the detection, prevention, and mitigation of cyber threats. TAXII is not an information-sharing initiative or application and does not attempt to define trust agreements, governance, or nontechnical aspects of cyber threat information sharing. Instead, TAXII empowers organizations to achieve improved situational awareness about emerging threats, and enables organizations to easily share the information they choose with the partners they choose all while using a single, common set of tools. For more information on TAXII, see https://oasis-open.github.io/cti-documentation/.

TRIBAL—The term ''tribal'' has the meaning given the term ''Indian tribe'' in section 4 of the Indian Self-Determination and Education Assistance Act (25 U.S.C. 450b).