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

June 15, 2016

Table of Contents

Consistent with section 105(a)(2) and (3) of the Cybersecurity Information Sharing Act of 2015 (CISA), this document establishes procedures relating to the receipt of cyber threat indicators and defensive measures by all federal entities under CISA. It describes the processes for receiving, handling, and disseminating information that is shared with DHS pursuant to section 104(c) of CISA, including through operation of the DHS Automated Indicator Sharing capability under section 105(c) of CISA. It also states and interprets the statutory requirements for all federal entities that receive cyber threat indicators and defensive measures under CISA to share them with other appropriate federal entities.

Federal entities engaging in activities authorized by CISA 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 105(c) of CISA establishes within the Department of Homeland Security the Federal Government's capability and process[1] 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 the CISA and are set forth in Appendix A.

2. Receipt, Processing, and Dissemination of Cyber Threat Indicators Submitted Through Real-Time Means [Sec. 105 (a)(3)(A)]

This section describes the sharing of cyber threat indicators and defensive measures with the Federal Government through the DHS Automated Indicator Sharing (AIS) capability provided for by section 105(c) of CISA.[2] 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 Indicator Information (TAXII) specifications, along with the procedures and standards 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.

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

[2] Upon making a certification as provided in section 105(c)(2)(B) of the CISA, the President may designate one or more other federal entities to develop and implement a capability and process pursuant to 105(c)(2)(B)(III) of CISA. If that were to occur, the procedures in this section 2 and section 105(a)(3)(A) of CISA would apply to that capability and process as well.

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) located at the Enhanced Shared Situational Awareness site on Office of Management and Budget's MAX.gov, which is accessible at https://www.us-cert.gov/essa.

2.2. Receipt of 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. Federal entities should use a profile to standardize the indicator information and adhere to all relevant requirements contained in the Privacy and Civil Liberties Guidelines, which can be found at https://www.us-cert.gov/ais. Non-Federal entity submissions should conform to the AIS Profile, which can also be found at https://www.us-cert.gov/ais. The AIS Profile is intended to ensure that submissions include input fields most directly related to cyber threat indicators and defensive measures, as assessed by DHS in consultation with other federal entities. This assessment included a review of STIX fields for privacy, civil liberties, and other compliance concerns and risks. The STIX format includes several thousand fields, whereas the AIS Profile is a subset of those fields that are determined to directly relate to a cybersecurity threat and that otherwise protects privacy and civil liberties as required by CISA. Different indicator types may require the submission of a specific subsection of the fields in the AIS Profile.

Upon receipt of cyber threat indicators or defensive measures, federal entities should still follow all other applicable procedures, guidelines, and requirements, to the extent consistent with and in addition to the Privacy and Civil Liberties Guidelines produced under section 105(b) of CISA, to ensure appropriate handling of cyber threat indicators and defensive measures. In addition, federal entities should use the AIS Profile to standardize the indicator information and adhere to all relevant requirements contained in the Privacy and Civil Liberties Guidelines. As discussed in the Privacy and Civil Liberties Guidelines, using the

AIS Profile in this manner further minimizes privacy, civil liberties, and other compliance risks and discourages the submission of personal information of specific individuals or information that identifies specific individuals. In addition, the AIS Profile also reduces the risk of submission of content of communications that is not necessary to describe or identify a cybersecurity threat.

The full submission guidance document and AIS Profile can be found at https://www.us-cert.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.

2.3. AIS Profile Change Control Governance

Through continued collaboration and experience, the appropriate federal entities and other information sharing participants will identify STIX fields to be added and removed from 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 102(3). Requests to modify the STIX schema used 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 or delete a field.
- 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 fields are added or deleted:
    - in compliance with CISA's definitions of cyber threat indicators and defensive measures;
    - in compliance with CISA'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 fields available in the latest STIX schema available within the STIX community of users.

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

2.4. Filtering and Analysis of Indicators and Defensive Measures

Upon receipt by DHS, a series of automated actions occur. Where an automated process identifies an error or a particular field that cannot be processed by automated means, the system will flag the field for human review. When human review of a field is required, processing and dissemination of that field will necessarily be delayed, but the rest of the cyber threat indicator or defensive measure will be transmitted, with a second version following the human review. 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 STIX schema. This confirms the submission is a valid STIX document and that it contains the minimum set

of required AIS Profile STIX fields. If the submission is not a valid STIX document or does not contain the minimum AIS Profile fields, DHS will notify the submitter that the STIX document was invalid or rejected and delete the record.

2.4.1.2. If the submission contains fields that are not in the AIS Profile (i.e., AIS-prohibited fields, which are not part of a cyber threat indicator or defensive measure), then DHS will remove those fields from further automated processing and delete those fields. In addition, if the submission contains values that do not match the AIS Profile controlled values, then DHS will remove those fields from further automated processing and delete those fields.

2.4.1.3. In cases where the submitter has not consented to transmission of its identity to other federal entities, automated preprocessing will remove information identifying the submitter 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. Regardless of whether the submitter consents to transmit its identity to other entities, submitters are required to identify the sector to which they belong as well as their approximate geolocation i.e. country and state/region). These data fields, as provided by the submitter, will be transmitted to other federal entities in all instances.

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

This subsection identifies the controls pursuant to which DHS will, in limited instances, make modifications that could delay the real-time sharing of one or more fields within a cyber threat indicator or defensive measure submitted by a non-Federal entity pursuant to section 104 of CISA. Consistent with section 105(a)(3)(A) of CISA, 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

105(a)(3)(A)(ii)(I) of CISA, the heads of the appropriate federal entities unanimously agree to these controls.[3]

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 auto-generated text. Any fields that do not meet certain predetermined criteria defined through the AIS Profile and in the submission guidance will be referred for human review to ensure the field does not contain personal information of specific individuals or information that identifies specific individuals not directly related to the cybersecurity threat. When a field within a cyber threat indicator or defensive measure is referred for human review, DHS will still transmit the fields that do not require human review to the appropriate federal entities without delay.

2.4.2.2. Human review of a small number of fields where the risk of personal information of specific individuals or information that identifies specific individuals that cannot be mitigated via automated means. If after human review: the field is determined to not contain personal information of specific individuals or information that identifies specific individuals; the field is determined to contain such information, but it is determined to be directly related to the cybersecurity threat; or the field is determined to contain personal information of specific individuals or information that identifies specific individuals that is not directly related to the cybersecurity threat, however the personal information is able to be removed while still preserving other information within the field that is directly related to the cyber threat; then an updated cyber threat indicator or defensive measure will be issued using the versioning feature within STIX. If after human review, the field is determined only to contain personal information of specific individuals or information that identifies specific individuals that is not directly related to the cybersecurity threat, the field will be deleted.

2.4.2.3. Indicator validation to remove nuisance indicators and enrichment of indicators using other information available to DHS.

Further details on the automated processing can be found in the System Description Document, located at https://www.us-cert.gov/ais.

[3] 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.

2.5. Dissemination of 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 fields is required, then the cyber threat indicator or defensive measure will be sent to the appropriate federal entities without those fields. Once human review is completed, updated indicators or defensive measures will be made available to the appropriate federal entities using the versioning feature within STIX.

3. Receipt, Processing, and Dissemination of Cyber Threat Indicators Submitted Through Non-Automated Means [Sec. 105 (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 104 of CISA 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 105(c) of CISA, 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

DHS can receive web submissions of cyber threat indicator and defensive measure information 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 information, and after review (including a review to determine whether the cyber threat indicator or defensive measure contains any 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

DHS can receive email submissions of cyber threat indicators and defensive measure information from Federal and non-federal entities. The email ingestion 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. Email submissions will be forwarded to DHS cyber threat analysts to determine if there is valid cyber threat indicator or defensive measure information, and after review (including a review to determine whether the cyber threat indicator or defensive measure contains any 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.

4. Audit Capabilities and Unsanctioned Use [Sec. 105 (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 105(c) of CISA; and
- A list of the federal entities with which cyber threat indicators or defensive measures have been shared pursuant to CISA.

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.

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.

Appendix A: Glossary

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

ANTITRUST LAWS—The term ‘‘antitrust laws’’—(A) has the meaning given the term in the first section of the Clayton Act (15 U.S.C. 12); (B) includes section 5 of the Federal Trade Commission Act (15 U.S.C. 45) to the extent that section 5 of that Act applies to unfair methods of competition; and (C) includes any State antitrust law, but only to the extent that such law is consistent with the law referred to in subparagraph (A) of this definition or the law referred to in subparagraph (B) of this definition.

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 PURPOSE—The term ‘‘cybersecurity purpose’’ means the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability.

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 ‘‘non-federal 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
- Incidents
- Adversary tactics, techniques, and procedures (including attack patterns, malware, exploits, kill chains, tools, infrastructure, victim targeting, etc.)
- Exploit targets (e.g., vulnerabilities, weaknesses or configurations)
- Courses of action (e.g., incident response or vulnerability/weakness remedies or mitigations)
- Cyber attack campaigns
- Cyber threat actors

TRUSTED AUTOMATED EXCHANGE OF INDICATOR 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 non-technical 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 STIX and TAXII, see https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity.

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).