STIX/TAXII Standards Transition – Frequently Asked Questions

1. **What are STIX and TAXII and why were they developed?**
   The Structured Threat Information Expression (STIX) is a language for describing cyber threat information in a standardized and structured manner. STIX characterizes an extensive set of cyber threat information, to include indicators of adversary activity (e.g., IP addresses and file hashes) as well as additional contextual information regarding threats (e.g., adversary Tactics, Techniques and Procedures [TTPs]; exploitation targets; Campaigns; and Courses of Action [COA]) that together more completely characterize the cyber adversary's motivations, capabilities, and activities, and thus, how to best defend against them. It is intended to support both more effective analysis and exchange of cyber threat information.

   STIX evolved out of a series of discussions on email distribution lists and face-to-face meetings among cyber threat intelligence, incident response and operations practitioners seeking to develop a consistent way to automate and share indicators of adversary activity. The initial focus was on indicators, but further discussion identified structured threat needs beyond indicators, and STIX was broadened to include related threat and mitigation information.

   Trusted Automated Exchange of Indicator Information (TAXII) standardizes the trusted, automated exchange of cyber threat information. TAXII defines a set of services and message exchanges that, when implemented, enable sharing of actionable cyber threat information across organization and product/service boundaries for the detection, prevention, and mitigation of cyber threats. TAXII is not a specific information sharing initiative, and it does not 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, while leveraging existing relationships and systems.

   The U.S. Department of Homeland Security (DHS) initiated TAXII to simplify and speed the secure exchange of cyber threat information. TAXII eliminates the need for custom sharing solutions with each sharing partner, and widespread automated exchange of cyber threat information is now possible. DHS solicited community input and engaged MITRE to write the TAXII specifications.

2. **Why is DHS transitioning STIX and TAXII to an international standards development organization? What are the benefits?**
   STIX and TAXII have reached a level of maturity where they will benefit from a more formal collaboration guided by a recognized standards development process that ensures transparency, participation, stability, reciprocity, and ease of access both during the development and long after the project is complete. OASIS provides all of this, and is an ANSI accredited developer of American National Standards as well as an authorized PAS Submitter to ISO. Having these certifications available to STIX and TAXII means they will be implementable by the broadest possible stakeholder community.

3. **Why is the transition being announced now?**
   From the inception of STIX and TAXII in 2012, DHS has maintained that the specifications would be transitioned to an internationally recognized voluntary consensus standards development organization once they reached an appropriate level of maturity. That day has come and the transition to OASIS represents an exciting next step in the continued advancement of STIX and TAXII.

4. **What is OASIS?**
   OASIS is a nonprofit consortium that drives the development, convergence and adoption of open standards for the global information society. OASIS standards are widely used in security, Internet of Things, cloud computing, content technologies, emergency management, energy, and other areas. The OASIS technical agenda is set by the members themselves, using a lightweight process expressly designed to promote industry consensus and unite disparate efforts. Completed work is ratified by open ballot.

5. **Why was OASIS selected?**
   OASIS has an excellent track record in successfully transitioning accepted technical specifications to voluntary consensus standards and in recognizing and building on that existing work. For example, Advanced Message Queuing Protocol (AMQP), Message Queuing Telemetry Transport (MQTT), and Open Data Protocol (OData) have been successfully transitioned from outside organizations to become OASIS standards.

   In addition, the global membership of OASIS mirrors the diversity of the STIX/TAXII community and includes a wide variety of government entities, technology vendors, academic institutions, and end-user organizations that have been so critical to the success of the specifications. The selection of OASIS guarantees that the STIX/TAXII family of specifications will always be freely available to anyone around the world.

6. **Who will be able to access the STIX/TAXII specifications? Do I have to join OASIS in order to access STIX and TAXII?**
   All OASIS specifications are available for download and use by anyone without cost. You do not have to be an OASIS member to access any OASIS specification.

7. **How can I participate in the evolution of STIX/TAXII once this transition is complete?**
   There are three different levels at which organizations and individuals may participate in the evolution of STIX/TAXII as managed by OASIS: *Consuming*, *Tracking* and *Developing*.

   For Consuming, an organization or individual may wish to participate through accessing and utilizing current or future versions STIX/TAXII OASIS standard specifications. As stated in the answer to Question 6 above, all OASIS specifications are available for download and use by

anyone without cost.

For Tracking, an organization or individual may wish to stay abreast of ongoing evolution of the STIX/TAXII OASIS standard specifications but not actively participate in their development. Anyone is able to track the STIX/TAXII work online and provide public comments to the Technical Committee. All OASIS work is publicly archived.

For Developing, an organization or individual may wish to play an active and official role in the ongoing evolution and development of the STIX/TAXII OASIS standard specifications. This level of participation requires membership in OASIS and offers an official voice and vote in development discussions and decisions. If you are not already a member of OASIS, you may join either through your employer or as an individual. If your employer is a member of OASIS, you may participate in the STIX/TAXII working group – which will be called the OASIS Cyber Threat Intelligence (CTI) Technical Committee (TC) – under your employer's corporate membership at no additional cost. See OASIS Participation Instructions.

Please note that the OASIS CTI TC does not currently exist in the "All Groups" list on the OASIS website. A subsequent announcement will be made when the group is available to join.

8. Is there a fee to join OASIS? Will I have to travel to attend meetings?

The work of OASIS is funded by membership dues. The consortium offers a range of membership options with discounted dues for academics, associations, local government agencies, and individuals.

Membership dues are the major source of OASIS funding; they make it possible for the consortium to provide high quality standards without charge and to assure that all OASIS deliverables are publicly accessible in perpetuity. Dues are used to provide technical infrastructure for standards development, review, and publication. Dues are used to promote adoption of the standards through staff-led outreach, press and analyst relations, conference presentations, seminars, workshops, training, and support materials. Dues also fund liaison activities that encourage endorsements from peer organizations and trade associations and make it possible for OASIS standards to be approved by de jure standards bodies and governments around the world.

Members are never required to travel to participate in standards development. The majority of OASIS TC work is conducted via email and by teleconference meetings. The frequency and scheduling of meetings is determined by the TC members. Should the OASIS CTI TC members choose to hold a face-to-face meeting, teleconference facilities will be provided to enable members to participate remotely.

STIX/TAXII Standards Transition – Frequently Asked Questions

9. What exactly is being transitioned to OASIS?

The full body of work specifying, explaining and supporting the STIX/TAXII family of specifications under the current DHS-sponsored and MITRE coordinated efforts will be transitioned to OASIS, including:

- STIX 1.2
  - The specification itself, including specification documents, UML, and XML schemas: http://stix.mitre.org/language/version1.2/
  - Supporting non-normative documentation: http://stixproject.github.io
  - Sample documents: http://stix.mitre.org/language/version1.2/samples.html
  - Profiles and Profile Documentation: http://stix.mitre.org/language/profiles.html
  - Open source tools and utilities: http://github.com/STIXProject/
- TAXII 1.1
  - The specification itself, including specification documents and schemas: http://taxii.mitre.org/specifications/version1.1/
  - Supporting non-normative documentation: http://taxiiproject.github.io
  - Open source tools and utilities: http://github.com/TAXIIProject/
- CybOX 2.1
  - The specification itself, including specification documents, UML, and schemas: http://cybox.mitre.org/language/version2.1/
  - Supporting non-normative documentation: http://cyboxproject.github.io
  - Open source tools and utilities: http://github.com/CybOXProject/

10. What will the process for transition to OASIS look like?

The first step in the transition will be the drafting and agreement on a Charter for a new OASIS Technical Committee (TC) for Cyber Threat Intelligence (CTI). Once the TC is stood up, its membership will review the STIX/TAXII input technical specifications, identify and address specific OASIS technical considerations (namespace requirements, specification layout, etc.) then develop and publish initial versions of the STIX/TAXII OASIS standard specifications. These initial versions will codify the existing STIX/TAXII specifications with only very minor changes as required to conform to OASIS standards policy.

The TC will then develop, publish and implement a roadmap for continuing evolution of the specifications as is determined appropriate by its members according to OASIS policies and procedures.

11. What is the timeline for transition?

The launch of the CTI TC is planned for Friday, April 17th, 2015. The Charter will be circulated for a two week comment period after which the final Charter will be released in a formal Call for Participation on or about Friday, May 15th, 2015. The Charter will include the date, time and

location of the first meeting. Members will be able to go to the Technical Committee's web site and join the effort as soon as the call is issued.

At the first meeting of the TC, the first order of business will be to elect one or two Chairs of the TC and pass the necessary motions to establish the Subcommittees for STIX, TAXII, and CybOX. Once this is done, the latest STIX, TAXII and CybOX specifications will be formally contributed to OASIS and the TC and the transition will be complete.

12. **Will the STIX and TAXII specifications change significantly as a result of the transition to OASIS? Will my existing investments in STIX and TAXII be preserved?**
    The direction of STIX and TAXII will now be managed under a formal governance process but decisions within that process will still be fully in the hands of a robust global community committed to its success. Your existing investments in STIX and TAXII will be preserved.
    For the initial versions of the STIX/TAXII OASIS standard specifications, it is expected that namespaces will need to be changed from the current MITRE-based domains to appropriate OASIS-based namespaces. This one-time change should be relatively low-impact but will likely affect current implementations.

13. **What will DHS's role be with respect to STIX and TAXII after transition?**
    DHS and the US Government as a whole have made significant investments in STIX and TAXII and will continue to encourage the adoption and implementation of these critical enablers. DHS employees will join the OASIS CTI TC as active participants helping shape the standards as they evolve.

14. **Will MITRE, which operates the Homeland Security System Engineering and Design Institute (HSSEDI) on behalf of DHS, continue to be active in the development of STIX and TAXII?**
    MITRE employees will join the OASIS CTI TC as active participants helping shape the standards as they evolve. DHS will continue to fund HSSEDI, operated by MITRE, to actively develop these specifications, supporting documentation, and open source projects under the governance of the OASIS CTI TC in collaboration with the other TC participants.

15. **Will there continue to be supporting documentation, tools and application programming interfaces for STIX and TAXII?**
    Yes. Supporting resources now made available in the STIX, TAXII, and CybOX GitHub repositories will continue to be publicly available under a BSD three-clause license from OASIS. These products are considered Non-Standards Track Work Products and will be maintained as they are now on GitHub. DHS will continue to fund the development of these resources in collaboration with the OASIS CTI TC.

16. **Who will own the copyrights and trademarks associated with STIX and TAXII after transition to OASIS?**

    Ownership of the STIX and TAXII names and marks will be transferred to OASIS. As is the case today, the public is welcome to reference the STIX and TAXII names and marks provided they are not used in a way that causes confusion about source or authenticity, such as any incorporation into a product, service or organization name.

17. **What Intellectual Property Rights (IPR) policies will be in effect after transition to OASIS?**
    The OASIS CTI TC will operate under the Non-Assertion mode as defined in the OASIS IPR Policy. All TC members agree not to enforce any patent or other IP rights they may have concerning the work of the TC.