--------------------------------------------------

Subject: **Call for Comment: proposed Charter for OASIS Cyber Threat Intelligence (CTI) Technical Committee**

From: **Chet Ensign <****chet.ensign@OASIS-open.org****>**

To: tc-announce@lists.OASIS-open.org, members@lists.OASIS-open.org, OASIS Charter Discuss List <OASIS-charter-discuss@lists.OASIS-open.org>

Date: Mon, 20 Apr 2015 14:09:05 -0400

OASIS Members and other interested parties:

A draft TC charter has been submitted to establish the OASIS Cyber Threat Intelligence (CTI) Technical Committee. In accordance with the OASIS TC Process Policy section 2.2: ([https://www.OASIS-open.org/policies-guidelines/tc-process#formation](https://www.oasis-open.org/policies-guidelines/tc-process#formation)) the proposed charter is hereby submitted for comment. The comment period shall remain open until 23:59 UTC on 04 May 2015.

OASIS maintains a mailing list for the purpose of submitting comments on proposed charters. Any OASIS member may post to this list by sending email to: OASIS-charter-discuss@lists.OASIS-open.org. All messages will be publicly archived at: [http://lists.OASIS-open.org/archives/OASIS-charter-discuss/](http://lists.oasis-open.org/archives/oasis-charter-discuss/). Members who wish to receive emails must join the group by selecting "join group" on the group home page: [http://www.OASIS-open.org/apps/org/workgroup/OASIS-charter-discuss/](http://www.oasis-open.org/apps/org/workgroup/oasis-charter-discuss/). Employees of organizational members do not require primary representative approval to subscribe to the OASIS-charter-discuss e-mail.

A telephone conference will be held among the Convener, the OASIS TC Administrator, and those proposers who wish to attend within four days of the close of the comment period. The announcement and call-in information will be noted on the OASIS Charter Discuss Group Calendar.

We encourage member comment and ask that you note the name of the proposed TC (CTI) in the subject line of your email message.

--- TC Charter

Section 1: TC Charter

(1)(a) TC Name

OASIS Cyber Threat Intelligence (CTI) Technical Committee

(1)(b) Statement of Purpose

Traditional approaches for cyber security that focus inward on understanding and addressing vulnerabilities, weaknesses, and configurations are necessary but insufficient in today’s dynamic cyber landscape. Effective defense against current and future threats also requires the addition of an outward focus on understanding the adversary's behavior, capability, and intent. Only through a balanced understanding of both the adversary and ourselves can we understand enough about the true nature of the threats we face to make intelligent defensive decisions.  The development of this understanding is known as cyber threat intelligence (CTI).

Cyber threat intelligence itself poses a challenge in that no single organization can have enough information to create and maintain accurate situational awareness of the threat landscape. This limitation is overcome by sharing of relevant cyber threat information among trusted partners and communities. Through information sharing, each sharing partner can achieve a more complete understanding of the threats they face and how to defeat them.

The purpose of the Cyber Threat Intelligence (CTI) Technical Committee is to define a set of information representations and protocols to address the need to model, analyze, and share cyber threat intelligence. A composable set of information sharing services will be defined to enable peer-to-peer, hub and spoke, and source subscriber threat intelligence sharing models. These services will not dictate one architecture, but strive to allow for organizations to develop standards-based sharing architectures that meet their needs. Standardized representations will be developed for campaigns, threat actors, incidents, tactics techniques and procedures (TTPs), indicators, exploit targets, observables, and courses of action.  These core components and their inter-relationships together will enable robust cyber threat analysis and intelligence sharing.

The same concepts identified above are leveraged across a variety of other applications and in this context are best characterized as cross domain interoperability requirements. Representative examples include investigating and prosecuting cybercrime; deconfliction of cybercrime investigations; cyber-related victim notification; development of integrated, all-source cyber threat intelligence including integration of information about malicious insiders; integrated risk assessment for critical infrastructure spanning physical (human and natural) and cyber-related threats; workforce skills development, tracking, training, and certification; and managing and mitigating risks from cascading failures or degradation across critical infrastructure or supply chain dependencies. The core issue is the ever present need to ensure that as the work of the CTI TC advances, it is done in a way that does not impede and instead over time improves semantic interoperability with cross domain applications.

The recommendation is that OASIS in general, and the CTI TC specifically, leverage OASIS’ active role with the Standards Coordination Council (SCC), chartered under the White House’s Information Sharing and Access Policy Committee, to explore opportunities to further semantic interoperability with cross domain applications being advanced by stakeholders outside the core CTI TC community. The SCC is an advisory group composed of industry consortium and standards development organizations, including but not limited to the Object Management Group, IJIS, Association for Enterprise Integration, and American Council for Technology – Industry Advisory Council, OASIS, the Global Justice Information Sharing Initiative, the National Information Exchange Model Program Office, FBI’s Criminal Justice Information Systems Advisory Policy Board, NIST’s Identity Ecosystem Steering Group, and many others. The SCC member organizations represent different communities of interest from multiple mission partners and the broader standards landscape.

The TC will base its efforts on the Structured Threat Information \_expression\_ (STIX) and Trusted Automated Exchange of Indicator Information (TAXII) specifications developed and contributed to the TC by U.S. Department of Homeland Security (DHS). Prior to creation of the CTI TC, the STIX and TAXII initiatives have been led by DHS through development based on open community collaboration. STIX and TAXII, as well as STIX?s dependent specification of Cyber Observable \_expression\_ (CybOX), have already achieved significant international adoption among threat intelligence vendors, end-user organizations, and cyber threat information sharing communities. By building upon the success of these existing specifications, the CTI TC can offer immediate value as well as provide a solid foundation on which to base future development.

(1)(c) Scope

In order to leverage existing value of STIX/TAXII/CybOX in the CTI community while working towards future capabilities and advancements, the OASIS CTI TC work will be divided into two phases: in phase one, existing input specifications contributed by the United States Department of Homeland Security (DHS) will be formally codified as OASIS specifications. In the second phase, continued development of STIX, TAXII, and CybOX will begin based on the needs identified by the CTI TC Members.

Phase One Scope:

\* Specifications identified in Section (2)(h) (STIX 1.2, TAXII 1.1, and CybOX 2.1) will be contributed to the OASIS CTI TC by DHS

\* The TC will use these contributions as the basis for corresponding OASIS Standards Track Work Products. A key objective of the TC will be to limit changes to the input specifications in order to minimize impacts on existing implementations

\* The OASIS CTI TC will develop the specifications under the OASIS TC Process with the goal of submitting them at the appropriate time to the membership of the organization for consideration as OASIS Standards

Other contributions will be accepted for consideration without any prejudice or restrictions and evaluated based on technical merit insofar as they conform to this charter.

Phase Two Scope:

Phase two will take the specifications defined in phase one and evolve them under the direction of the OASIS CTI TC. Further work related to information representations for codifying, analyzing, or sharing of cyber threat intelligence that was not included in the input specifications is also in scope.

In addition to Standards Track Work Products, the OASIS CTI TC work products in both phase one and phase two may include supporting documentation, open source tooling, and any other materials deemed necessary to encourage the adoption of the TC?s specifications.

We recommend explicitly loosening the narrow scope identified in Phase One, whereby the initial focus seems to be on ratifying existing efforts, and explicitly embracing the opportunity and need to resolve cross domain semantic interoperability based on validated public and private sector requirements, existing installed base, and industry (vendor) support (in Phase Two).

(1)(d) Deliverables

The OASIS CTI TC will establish three Subcommittees to develop and refine the specifications and supporting materials of the TC:

\* The STIX Subcommittee

\* The TAXII Subcommittee

\* The CybOX Subcommittee

In phase one, each Subcommittee will submit initial draft deliverables to the OASIS CTI TC for approval based on making minimal changes to the input specification as necessary conform to OASIS publication formats and support OASIS CTI TC design requirements:

\* The STIX Subcommittee will submit STIX 1.2.1

\* The TAXII Subcommittee will submit TAXII 1.1.1

\* The CybOX Subcommittee will submit CybOX 2.1.1

In phase two, the OASIS CTI TC will make substantive additions and other changes to the specifications to correct errors and evolve capabilities based on requirements and capabilities identified by OASIS TC members. Deliverables will include updated versions of the specifications (STIX, TAXII, CybOX, and possibly others) as deemed appropriate by the Subcommittees and by the OASIS CTI TC as a whole.

In addition to the specification deliverables, the OASIS CTI TC may deliver supporting documentation and open source tooling on an ongoing basis in support of the CTI TC?s published standards.

We recommend adding focus on providing guidance for integration/interoperability with other specifications already in existence and implemented within the mission communities. This could also include addressing requirements for exchange mechanisms other than XML Schema based, such as JSON. Current in-process activities include--
(1) A UML based Conceptual Model for Cross Domain Threat/Risk Information Sharing
(2) UML Profile for NIEM 3.0

(3) Planned Inclusion of the CWE ([Common Weakness Enumeration](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CB4QFjAA&url=https%3A%2F%2Fcwe.mitre.org%2F&ei=QalHVZ71DpLFogTx94HIDg&usg=AFQjCNHyDo5uRsdGZbhj0dnW1x-3taBQrg&sig2=pZDrOZg-AkGlEaMHV38FgQ&bvm=bv.92291466,d.aWw)) in models

There have been significant advances in model driven architecture approaches that have been proven in other initiatives like NIEM UML that uses a UML-based model to capture mission information sharing requirements and generate technology specific representations. This approach allows for semantic interoperability at the model level while providing syntactic interoperability for the exchanges on the wire. We believe this approach has merit as the basis for enabling cross domain sematic interoperability, and we recommend consideration of the same as a potential option to further support for identified options.

(1)(e) IPR Mode

This TC will operate under the Non-Assertion IPR mode as defined in Section 10.3 of the OASIS IPR Policy document.

(1)(f) Audience

The anticipated audience for this work includes:

\* Vendors of products and services that produce, consume, or process cyber threat intelligence, in particular that which is expressed via STIX/CybOX and shared via TAXII

\* Organizations that produce or consume cyber threat intelligence, in particular that which is expressed via STIX or CybOX and shared via TAXII

\* Organizations that purchase or may purchase products that support STIX, TAXII, or CybOX

\* Information Sharing and Analysis Organizations (ISAOs), including Information Sharing and Analysis Centers (ISACs)

We commented in the preamble on the potential for improved coordination with other international and government standards organizations, especially as it pertains to cross domain applications and furthering semantic interoperability. We recommend explicitly referencing standards coordination, either through the SCC or some other mechanism, to improve the ability for others outside the CTI TC but with a vested interest in cross domain semantic interoperability that cross into or are adjacent to the CTI TC scope to be better positioned to engage.

The Federal government has had a major role in this effort to date as well as with continued funding and support. DHS shifting this effort to an open international standards organization is a major and laudable step forward. DHS and other public sector entities will continue to engage on this and the many other related initiatives mentioned in this charter. In keeping with the U.S. Government’s Open Government Policy and its emphasis on transparency, participation, and collaboration; we recommend greater transparency in terms of identifying government coordination processes, procedures, and forums that will influence government participation in the CTI TC. At the level of the CTI Charter, this could be done by embracing Open Government principles with the specifics to be developed and promulgated in the course of the work.

(1)(g) Language

TC business will be conducted in English.  The output documents will be written in (US) English. Translations to other languages may be made based on interest and ability.

We believe that other countries and businesses that operate in multiple countries face similar challenges and have similar needs for information sharing. In addition, international sharing has the potential to strengthen the collective defense of all parties who participate. We recommend adding recognition of this need and the intent to address it in a future phase at the appropriate place in this charter. We note that the model driven approaches identified above provide an established, recognized, and proven pathway to support internationalization.

Section 2: Additional Information

(2)(a) Identification of Similar Work

Similar efforts include:

\* IODEF/RID/RID-T (RFC 5070, RFC 6545, RFC 6546): IODEF, RID, and RID-T are IETF specifications (<https://tools.ietf.org/wg/mile/>) to describe and share incident information. They have a much narrower scope than STIX/TAXII and therefore are often not adequate to most potential users of STIX/TAXII.

\* OpenIOC ([http://www.openioc.org](http://www.openioc.org/)): OpenIOC is a specification developed by FireEye (a commercial company) to describe Indicators of Compromise and made available for public use. OpenIOC addresses a narrow use case (observable patterns for Indicators of Compromise) and represents a partial solution to part of the overall cyber threat information problem, but does not fully address the needs of a holistic cyber threat intelligence information model. Additionally, though OpenIOC is developed as a public specification by FireEye it is not a consensus standard in an international standards body.

\* VERIS ([http://veriscommunity.net](http://veriscommunity.net/)): The VERIS Framework is a set of metrics designed to provide a common language for describing security incidents. VERIS addresses a narrow use case and represents a partial solution to part of the overall cyber threat information problem but does not fully address the needs of a holistic cyber threat intelligence information model. Additionally, though VERIS is a published format available on GitHub, it is developed at the sole discretion of the VERIS community rather than as a consensus standard in an international standards body.

\* OMG Threat Modeling Working Group (<http://www.omg.org/hot-topics/threat-modeling.htm>): The Object Management Group (OMG) has issued a proposal for a combined risk-threat information model that incorporates STIX (among other things). That model is expected to cover a broader scope (cyber and physical, threat and risk) in order to coordinate across these domains but does not seek to re-define a model within the domain to the low level that STIX and CybOX do.

Is the identification of other standards limited to inclusion in this charter?  Or is there a desire to evaluate these as potential candidates for integration/interoperability?  How will these communities be invited to participate in this effort if the intent is to not make changes to the current input specifications?  How will this initiative integrate enterprise standard frameworks like NIEM that is actively used by mission specific entities across the Justice, Law Enforcement, Defense, Homeland Security, Human Services and domains? The Homeland Security/Emergency Management community is already working within OASIS (Common Alerting Protocol) developing their disaster management standards. What are the plans for reconciling with these communities?

We note that under the SCC umbrella OASIS is leading an effort to inventory cybersecurity information sharing and related standards and associated initiatives. This is a robust effort spanning SCC members and is documented on the SCC web site, [www.standardscoordination.org](http://www.standardscoordination.org). The point of this effort is to identify activities with a consistent taxonomy, and to provide under the SCC a neutral forum within which to support improved coordination and collaboration. We recommend the CTI TC participate in this process, in particular in Phase Two of your work.

(2)(b) First TC Meeting

The first TC meeting will be held on 18 June 2015 at 17:00 UTC / 1:00 PM EDT / 10:00 AM PDT via teleconference. The teleconference infrastructure will be Microsoft Lync hosted by The MITRE Corporation.

(2)(c) Ongoing Meeting Schedule

The full OASIS CTI TC plans to meet monthly via a teleconference hosted via MITRE Lync. Subcommittees will set their own meeting schedules, initially meeting bi-weekly by teleconference hosted via MITRE Lync.

(2)(d) TC Proposers

\* Richard Struse, Department of Homeland Security, Richard.Struse@hq.dhs.gov

\* Sean Barnum, The MITRE Corporation, sbarnum@mitre.org

\* Mark Davidson, The MITRE Corporation, mdavidson@mitre.org

\* John Wunder, The MITRE Corporation, jwunder@mitre.org

\* Aharon Chernin, Soltra, achernin@soltra.com

\* Mona Magathan, US Bancorp, mona.magathan@usbank.com

\* Bret Jordan, Blue Coat Systems Inc, bret.jordan@bluecoat.com

\* Alexander Foley, Bank of America, alexander.foley@bankofamerica.com

\* Tony Rutkowski, Yaana Technologies, LLC, tony@yaanatech.com

\* Joel J. Fleck, Hewlett-Packard, joel.fleck@hp.com

\* Richard Freeman, Symantec Corporation, richard\_freeman@symantec.com

\* Rob Walters, Symantec Corporation, Rob\_Walters@symantec.com

\* Paul McKitrick, Microsoft, pmckit@microsoft.com

\* Pam Smith, Johns Hopkins University Applied Physics Laboratory (JHU/APL), pam.smith@jhuapl.edu

Can others be added to this list of proposers? We recommend adding the SCC as a member to enable broader involvement from other organizations. Assuming no irreducible conflicts arise from collaborative adjudication of our comments, PM-ISE is interested in being a constructive and supportive member of the CTI TC and being represented in the CTI TC Charter.

(2)(e) Primary Representatives' Support

\* I, Richard Struse, Richard.Struse@hq.dhs.gov, as the US Department of Homeland Security Office of Cybersecurity and Communications Primary Representative to OASIS, I confirm our support for the proposed OASIS Cyber Threat Intelligence (CTI) Technical Committee charter and endorse our participation as a TC Proposer.

\* I, Raj Rajagopal, rajagop@mitre.org, as Primary Representative for MITRE approve the CTI TC Charter, and endorse our participation as a TC Proposer.

\* I, Aharon Chernin, achernin@soltra.com, as Primary Representative for Soltra approve the CTI TC Charter, and endorse all our proposers listed in (2)(d).

\* As the US Bancorp's Primary Representative at OASIS, I, Mona Magathan, mona.magathan@usbank.com, confirm our support for the proposed OASIS Cyber Threat Intelligence (CTI) Technical Committee charter and endorse our participation as a TC Proposer.

\* I, Bret Jordan, bret.jordan@bluecoat.com, as the Blue Coat Systems Primary Representative at OASIS, confirm our support for the proposed OASIS Cyber Threat Intelligence (CTI) Technical Committee charter and endorse our participation as a TC Proposer.

\* I Abbie Barbir, abbie.barbir@bankofamerica.com, Bank of America primary rep approve adding Alexander Foley as a co-proposer of the OASIS Cyber Threat Intelligence (CTI) Technical Committee.

\* I, Anthony M. Rutkowski, tony@yaanatech.com, as Primary Representative for Yaana Technologies, LLC, approve the OASIS Cyber Threat Intelligence (CTI) Technical Committee Charter, support this proposal of formation together with the other proposers and are committed to the Charter and projected meeting schedule.

\* As principal representative of Hewlett-Packard at OASIS, I, Joel J. Fleck, joel.fleck@hp.com, am pleased to endorse the creation of a new OASIS Technical Committee on Cyber Threat Intelligence to support, maintain and advance the work on the specifications for the STIX/TAXII protocols.

\* I, Richard Freeman, richard\_freeman@symantec.com, as Primary Representative for Symantec Corporation approve the CTI TC Charter, and endorse all our proposers listed in (2)(d). (2)(d) currently consists of myself and Rob Walters Rob\_Walters@symantec.com.

\* I, Ram Jeyaraman, Ram.Jeyaraman@microsoft.com, as Primary Representative for Microsoft Corporation approve the OASIS Cyber Threat Intelligence Technical Committee Charter, and endorse our Proposer, Paul McKitrick, as listed in section (2)(d).

\* I, Tom Smith, tom.smith@jhuapl.edu, as Primary Representative for Johns Hopkins University Applied Physics Laboratory, approve the OASIS Cyber Threat Intelligence Technical Committee Charter, and endorse our proposer, Pam Smith, as listed in (2)(d).

(2)(f) TC Convener

The TC Convener is Richard Struse of the U.S. Department of Homeland Security, Richard.Struse@hq.dhs.gov.

(2)(g) OASIS Member Section

N/A

(2)(h) Anticipated Contributions

The U.S. Department of Homeland Security will contribute the following materials, delivered by the Homeland Security Systems Engineering and Development Institute (operated by The MITRE Corporation):

\* STIX 1.2

  - The specification itself, including specification documents, UML, and schemas: <http://stix.mitre.org/language/version1.2/>

  - Supporting non-normative documentation: [http://stixproject.github.io](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](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](http://cyboxproject.github.io/)

  -  Open source tools and utilities: <http://github.com/CybOXProject/>

(2)(i) FAQ Document

[https://stixproject.github.io/OASIS-faq.pdf](https://stixproject.github.io/oasis-faq.pdf)

(2)(j) Work Product Titles and Acronyms

The OASIS CTI TC will produce material related to the following work products:

\* Structured Threat Information \_expression\_ (STIX)

\* Trusted Automated Exchange of Indicator Information (TAXII)

\* Cyber Observable \_expression\_ (CybOX)

--

/chet   [§]
----------------
Chet Ensign
Director of Standards Development and TC Administration
OASIS: Advancing open standards for the information society
[http://www.OASIS-open.org](http://www.oasis-open.org/)

Primary: +1 973-996-2298
Mobile: +1 201-341-1393

Check your work using the Support Request Submission Checklist at [http://www.OASIS-open.org/committees/download.php/47248/tc-admin-submission-checklist.html](http://www.oasis-open.org/committees/download.php/47248/tc-admin-submission-checklist.html)

TC Administration information and support is available at [http://www.OASIS-open.org/resources/tcadmin](http://www.oasis-open.org/resources/tcadmin)

Follow OASIS on:
LinkedIn:    <http://linkd.in/OASISopen>
Twitter:        <http://twitter.com/OASISopen>
Facebook:  [http://facebook.com/OASIS.open](http://facebook.com/oasis.open)