Published on *OASIS* (https://www.oasis-open.org)

# Call for Participation: OASIS Open Command and Control (#OpenC2) TC

Submitted by censign on Mon, 2017-04-10 21:42
**Type:**
Call for Participation

A new OASIS technical committee is being formed. The OASIS Open Command and Control (OpenC2) Technical Committee (TC) has been proposed by the members of OASIS listed in the charter below. The TC name, statement of purpose, scope, list of deliverables, audience, IPR mode and language specified in this proposal will constitute the TC's official charter. Submissions of technology for consideration by the TC, and the beginning of technical discussions, may occur no sooner than the TC's first meeting.

The eligibility requirements for becoming a participant in the TC at the first meeting are:

(a) you must be an employee or designee of an OASIS member organization or an individual member of OASIS, and

(b) you must join the Technical Committee, which members may do by using the Roster "join group" link on the TC's web page at [a].

To be considered a voting member at the first meeting:

(a) you must join the Technical Committee at least 7 days prior to the first meeting (on or before 31 May 2017), and

(b) you must attend the first meeting of the TC, at the time and date fixed below (07 June 2017).

Participants also may join the TC at a later time. OASIS and the TC welcomes all interested parties.

Non-OASIS members who wish to participate may contact us about joining OASIS [b]. In addition, the public may access the information resources maintained for each TC: a mail list archive, document repository and public comments facility, which will be linked from the TC's public home page at [c].

Please feel free to forward this announcement to any other appropriate lists. OASIS is an open standards organization; we encourage your participation.

----------?
[a] https://www.oasis-open.org/apps/org/workgroup/openc2/ [1]

[b] See http://www.oasis-open.org/join/ [2]

[c] http://www.oasis-open.org/committees/openc2/ [3]

---

?CALL FOR PARTICIPATION?
OASIS Open Command and Control (OpenC2) Technical Committee Charter

The charter for this TC is as follows.

Section 1: TC Charter

(1)(a)Name of the TC

OASIS Open Command and Control (OpenC2) Technical Committee.

(1)(b)Statement of Purpose

The fact that cyber-attacks are increasing in terms of sophistication, speed and dynamics of the attack steps is well documented. Advanced cyber actors are utilizing automation with adaptive tradecraft and these trends are likely to continue.

The traditional cyber security and response approach is through the use of monolithic systems that tightly couple the sensing, analytics, decision making and acting blocks of cyber-defense activities. Upgrading or modification of the functional blocks within the cyber-defenses is intensive, may impact the efficacy of the system as a whole and in many cases cannot be realized within cyber-relevant time. The traditional approach can lead to systems that are relatively static and are difficult to coordinate inter-domain responses to cyber-attacks.

Future defenses will require the integration of new functional blocks, coordination of responses between domains, synchronization of cyber defense mechanisms and automated actions to mitigate current and pending attacks within cyber relevant time. Key enablers for the realization of more responsive, flexible, product agnostic and interoperable cyber defense components include the standardization of interfaces and the adoption of standard protocols. This will facilitate interoperability and enable unambiguous machine to machine command and control messages.

The purpose of this technical committee is to create a standardized language for the command and control of technologies that provide or support cyber defenses.

(1)(c) Scope of Work

The technical committee will draft documents, specifications, lexicons or other artifacts to fulfill the needs of cyber security command and control in a standardized manner. The technical committee will leverage pre-existing standards to the greatest extent practical. Therefore identifying gaps pertaining to the command and control of technologies that provide or support cyber defenses is within the technical committee's scope of work.

The technical committee will base its initial efforts on artifacts generated by the OpenC2 Forum. Prior to the creation of this TC, the OpenC2 Forum was a community of cyber-security stakeholders that was facilitated by the National Security Agency. The OpenC2 Forum drafted a language description document, actuator profiles and open source prototype implementations. Since its inception, the Forum intended to transition its efforts to a recognized standards body. This TC can leverage the pre-existing artifacts produced by the OpenC2 Forum to

provide a foundation to base its development

It is recognized that command and control of technologies is necessary but insufficient for cyber-security, therefore every effort will be made to ensure that artifacts produced will be done so in the context of being implementation agnostic and striving toward an architecture that decouples the functional blocks utilized by cyber-defense.

Other implementation aspects such as transport, authentication, key management, cyber-threat sharing, situational awareness and other services are being addressed by other efforts. The OpenC2 Forum may specify or otherwise leverage pre-existing standards to address external dependencies, identify implementation considerations etc, however the creation of additional standards for these aspects are beyond the scope of this technical committee.

This technical committee will collaborate with other technical communities to ensure consistency and avoid duplicative efforts. In particular, this committee will work closely with the OASIS Cyber Threat Intelligence Technical Committee (CTI TC). The OpenC2 Technical Committee will focus on the Acting or Response portion of cyber defense but recognizes that there are significant interactions with the functional blocks associated with sensing, analytics and decision making.

(1)(d) Deliverables

Within 18 months of its first, meeting, this TC expects to deliver the following:

- A Language Description Document (LDD). The LDD will define a lexicon, the actions, syntax, semantics and other general aspects of the language.

- Security Considerations Document (SCD). By design, OpenC2 strives to be as agnostic of the message fabric as practical and in and of itself does not provide Information Assurance. The SCD will identify IA concerns that implementers should be aware of and are not addressed by OpenC2.

- Implementation Considerations Document (ICD). By design, OpenC2 strives to be as agnostic of the message fabric as practical and matters other than the command itself are treated as external dependencies. The ICD will identify the transport and interface concerns that must be addressed.

- JSON Abstract Encoding Notation (JAEN). JAEN will provide a schema so that commands may be validated and ensure interoperability.

- OpenC2 JSON Schema. The OpenC2 JSON schema will facilitate the encoding and validation of commands for implementations that choose to use JSON encoding.

- Other to be determined artifacts agreed upon by the TC such as interoperability specifications, implementation guidelines, OpenC2 tutorials etc.

In addition to the identified deliverables, this TC shall maintain the following:

- Actuator Profile Subcommittees. The cyber defense industry is evolving and producing new products and solutions, therefore it is not pragmatic for the LDD to encompass all aspects of the cyber defense industry. An actuator profile will document the portions of the LDD that are mandatory to implement, optional to implement as well as define any specifiers and modifiers that are specific to a particular cyber defense function.

- Library of prototype implementations, sample commands, polyglot implementation and other artifacts as they pertain to the command and control of cyber defense technologies. This library will be maintained as an Open

Repository of the TC

- Language Description Document Subcommittee. The purpose of this committee is to act as a focal point to submit comments to the language description document. The subcommittee will track comments and ensure that the comments are presented to the TC for resolution.

- Implementation Considerations Subcommittee. The purpose of this subcommittee is to identify external dependencies and provide implementation guidance.

(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 that execute tasks in order to investigate, mitigate and/or remediate cyber-attacks.

- Vendors of products that orchestrate coordinated responses by execution of a workflow.

- Organizations that architect and or integrate defenses for cyber domains.

- Academia or other stakeholders interested in the research, development and prototyping of cyber defense strategies, architectures and/or technologies.

(1)(g) Language

TC business will be conducted in English. The output documents will be written in (US) English.

Section 2: Additional Information

(2)(a) Identification Similar Work

The OpenC2 Forum was chartered in 2016 to address matters as they pertain to command and control of cyber defense technologies. The effort was appropriate for purposes of providing a forum for stakeholders to meet, propose, draft and resolve artifacts such as description documents, implementation considerations, prototype use case implementations and similar efforts however, the forum is not suitable for the creation of a recognized standard nor was it as deliberative as an OASIS Technical Committee. The proposed OASIS Technical Committee will continue and enhance the efforts of the OpenC2 Forum.

The approach taken by the OpenC2 Forum is unique in that it decouples the action, target and actuator which permits a relatively small number of defined actions to accommodate a large number of complete commands.

The Cyber-Threat Intelligence Technical Committee (CTI TC) is an OASIS Technical Committee that focuses on the modeling, analysis and sharing of cyber threat intelligence. The distinction between the proposed technical committee and the CTI TC is that the proposed TC will focus on the action in response to cyber threats which may be influenced, but not solely driven by, threat intelligence. These two efforts will complement each other in that the OpenC2 Technical Committee will be able to benefit from the threat intelligence sharing capabilities of the CTI TC. The proposed OASIS Technical Committee will liaison with the CTI TC to ensure compatibility, avoid duplication of efforts, and maintain separation of concerns.

The OpenC2 forum was unable to identify similar initiatives with the goal to standardize command and control at a similar level of abstraction, hence it is believed that this TC's work product is non-duplicative of any other standardization effort.

(2)(b) First TC Meeting

The first meeting of the TC will be held June 7, 2017 at 13:00 EDT at the offices of General Dynamics, 430 National Business Parkway, 2nd Floor, Annapolis Junction, MD., on behalf of the National Security Agency.

The kickoff will be a face to face meeting and electronic means will be provided to accommodate those who cannot attend in person.

(2)(c) Ongoing Meeting Schedule

For the 12 month period following the first meeting, the National Security Agency will host monthly teleconferences and webex meetings for the purpose of executing the business of the OpenC2 Technical Committee.

(2)(d) TC Proposers

The following OASIS members have identified themselves as being supportive of the proposal, are committed to the charter, and support the proposed schedule.

1. Brule, Joseph, National Security Agency, jmbrule@nsa.gov [4]
2. Darley, Trey, Kingfisher Operations, sprl, trey@kingfisherops.com [5]
3. Ginn, Jane, Cyber Threat Intelligence Network, Inc, jg@ctin.us [6]
4. Gonzalez, Juan, DHS Office of Cybersecurity and Communications (CS&C), juan.m.gonzalez@hq.dhs.gov [7]
5. Hagen, Stefan, Individual Member, stefan@hagen.link [8]
6. Jordan, Bret, Symantec, Bret_Jordan@symantec.com [9]
7. Landfield, Kent, Intel, kent.b.landfield@intel.com [10]
8. Patrick, Paul, FireEye, Paul.Patrick@FireEye.com [11]
9. Satish, Sourabh, Phantom Cyber, sourabh@phantom.us [12]
10. Sparrell, Duncan, sFractal Consulting, duncan@sfractal.com [13]
11. Storms, Andrew, New Context Services Inc, storms@newcontext.com [14]
12. Thomson, Allan, LookingGlass Cyber, athomson@lookingglasscyber.com [15]
13. Verma, Jyoti, Cisco, jyoverma@cisco.com [16]
14. De Beer, Dean, Cisco, dedebeer@cisco.com [17]
15. Yu, Sounil, Bank of America, sounil.yu@bankofamerica.com [18]
16. Al-Shaer, Ehab, University of North Carolina Charlotte, ealshaer@uncc.edu [19]

(2)(e) Primary Representatives? Support

The following primary representatives have stated their support of the OpenC2 TC:

- I, Bret Jordan, bret_jordan@symantec.com [20], as Symantec Corporation's Primary Representative to OASIS, confirm our support for the OASIS OpenC2 Technical Committee (OpenC2 TC) charter and the participation.

- I, Duncan Sparrell (duncan@sfractal.com [13]) as sFractal Consulting?s Primary Representative to OASIS, confirm our support for the OASIS OpenC2 Technical Committee (OpenC2 TC) charter and my participation.

- I, Allan Thomson, athomson@lookingglasscyber.com [15], as LookingGlass Cyber Solutions? Primary Representative to OASIS, confirm our support for the OASIS OpenC2 Technical Committee (OpenC2 TC) charter and my participation.

- I, Narendra Vad (nvad@cisco.com [21]) as a Primary representative from Cisco to OASIS confirm our support to OASIS Open C2 Technical committee (Open C2 TC) charter and participation of our co proposers from Cisco.

- I, Trey Darley (trey@kingfisherops.com [5]), as Kingfisher Operations? Primary Representative to OASIS, confirm our support for the OASIS OpenC2 Technical Committee (OpenC2 TC) charter and my participation.

- I, Sourabh Satish (sourabh@phantom.us [12]), as Phantom Cyber?s Primary Representative to OASIS, confirm our support for the OASIS OpenC2 Technical Committee (OpenC2 TC) charter and my participation.

- I, Kent Landfield (kent.b.landfield@intel.com [10]), as Intel Corporation?s Primary Representative to OASIS, confirm our support for the OASIS OpenC2 Technical Committee (OpenC2 TC) charter and my participation.

- I, Paul Patrick (Paul.Patrick@FireEye.com [11]), as FireEye?s Primary Representative to OASIS, confirm our support for the OASIS OpenC2 Technical Committee (OpenC2 TC) charter and my participation.

- I, Gunnar Peterson (gunnar.peterson@baml.com [22]), as Bank of America?s Primary Representative to OASIS, confirm our support for the OASIS OpenC2 Technical Committee (OpenC2 TC) charter and the participation of our co-proposer from Bank of America.

- I, Daniel Riedel (daniel@newcontext.com [23]), as New Context Services, Inc's Primary Representative to OASIS, confirm our support for the OASIS OpenC2 Technical Committee (OpenC2 TC) charter and the participation of our proposer listed above.

- I, Jane Ginn (jg@ctin.us [6]), as Cyber Threat Intelligence Network, Inc's Primary Representative to OASIS, confirm our support for the OASIS OpenC2 Technical Committee (OpenC2 TC) charter and the participation of our proposer listed above.

- I, Juan Gonzalez (juan.m.gonzalez@hq.dhs.gov [7]), as the DHS Office of Cybersecurity and Communications (CS&C) Primary Representative to OASIS, confirm support for the OASIS Open C2 Technical Committee (Open C2 TC) charter and my participation.

- I, Vincent Boyle, vmboyle@nsa.gov [24], as the National Security Agency's Primary Representative to OASIS, confirm our support for the OASIS OpenC2 Technical Committee (OpenC2 TC) charter and the participation of our proposer as listed above.

- I, Dr. Ehab Al-Shaer, ealshaer@uncc.edu [19], as the University of North Carolina Charlotte's Primary

Representative to OASIS, confirm our support for the OASIS OpenC2 Technical Committee (OpenC2 TC) charter and the participation of our proposer as listed above.

(2)(f) TC Convener

The convener of the TC will be Mr. Joseph Brule (jmbrule@nsa.gov [4]) of the National Security Agency.

(2)(h) Anticipated Contributions (now in draft)

The OpenC2 TC anticipates the following contributions from the OpenC2 Forum:

- Draft Language Description Document; Defines the actions, syntax and other semantics associated with the OpenC2 language (http://openc2.org/docs/language-description-document_v1.0.0-rc.3.pdf [25] )

- Draft Firewall Profile; defines the actions, targets, actuator namespace, specifiers and modifiers that are Minimum to Implement and Optional to Implement in the context of firewall functionality. ( https://drive.google.com/drive/folders/0B-FunCZrr-vteU9DTVdkVUxocWs [26])

- JSON Abstract Encoding Notation: Specifies the data model that is minimum to implement for OpenC2. ( https://github.com/OpenC2-org/jaen [27])

- Codebase to generate and validate OpenC2 commands (https://github.com/OpenC2-org/jaen [27])

- A repository of open source prototype implementations. (https://github.com/OpenC2-org/openc2-org/wiki/Prototype-Use-Case-Impleme... [28])

**Associated TC:**
Open Command and Control (OpenC2)
**Deadline:**
Mon, 2017-04-10 - Wed, 2017-06-07

---

**Links:**
[1] https://www.oasis-open.org/apps/org/workgroup/openc2/
[2] http://www.oasis-open.org/join/
[3] http://www.oasis-open.org/committees/openc2/
[4] mailto:jmbrule@nsa.gov
[5] mailto:trey@kingfisherops.com
[6] mailto:jg@ctin.us
[7] mailto:juan.m.gonzalez@hq.dhs.gov
[8] mailto:stefan@hagen.link
[9] mailto:Bret_Jordan@symantec.com
[10] mailto:kent.b.landfield@intel.com
[11] mailto:Paul.Patrick@FireEye.com
[12] mailto:sourabh@phantom.us
[13] mailto:duncan@sfractal.com
[14] mailto:storms@newcontext.com
[15] mailto:athomson@lookingglasscyber.com
[16] mailto:jyoverma@cisco.com
[17] mailto:dedebeer@cisco.com
[18] mailto:sounil.yu@bankofamerica.com

[19] mailto:ealshaer@uncc.edu
[20] mailto:bret_jordan@symantec.com
[21] mailto:nvad@cisco.com
[22] mailto:gunnar.peterson@baml.com
[23] mailto:daniel@newcontext.com
[24] mailto:vmboyle@nsa.gov
[25] http://openc2.org/docs/language-description-document_v1.0.0-rc.3.pdf
[26] https://drive.google.com/drive/folders/0B-FunCZrr-vteU9DTVdkVUxocWs
[27] https://github.com/OpenC2-org/jaen
[28] https://github.com/OpenC2-org/openc2-org/wiki/Prototype-Use-Case-Implementations