FIRST Standards Policy

Based on requests by the membership, FIRST may initiate development of a standard. A standard is defined as a document that is intended to ensure interoperability of a technique or tool, and is planned to see adoption and implementation by various parties. FIRST may also develop other descriptive, rather than normative, documents such as best practices, which are not required to follow the standards process.

Both FIRST members and non-members may propose the inception of a standard. A Special Interest Group (SIG) will typically shepherd the standard.

The FIRST board will evaluate proposals for a new standard based on:

- presence (or lack thereof) of a, preferably open, existing standard that meets a need addressed by the proposed standard. FIRST will avoid establishing groups that conflict with existing standards work outside of the organization;
- their applicability and value to members of FIRST.

This document describes minimum governance requirements for FIRST SIGs that aim to develop standards. SIGs may define more restrictive rules, but in any case where a SIG rule conflicts with a FIRST governance requirements, that exception must be specifically approved by the FIRST Board to be valid.

1. Governance

- Standards intended for publication and use outside of the membership must allow participation both by members and non-members of FIRST. Standards for use within the FIRST membership only may restrict membership to FIRST members only.

- Active contribution of ideas to a FIRST standard requires the signing of an Intellectual Property Rights Agreement (IPR) between FIRST and the participant. The FIRST IPR is linked in Appendix E, and must be executed by “participants” and “voting participants” prior to participation. IPRs are executed by a Legal Entity defined as an individual or organization which is legally permitted to enter into a contract, and be held accountable if it fails to meet its contractual obligations.

- Where multiple SIGs define standards in a single greater work area (e.g. threat intelligence or network security), chairs are encouraged to coordinate efforts. The FIRST board will look to all relevant groups to coordinate across their respective standards to avoid confusion and contradicting standards. FIRST will also look towards the SIGs to

have at least one chair participate as a Participant in the other SIG to ensure alignment.

- By default, FIRST grants permission for standards it develops to be implemented and/or adopted by FIRST members and non-members at no cost in perpetuity. Any exception requires an explicit approval by the FIRST board. The default license for any standard is Creative Commons CC - BY-SA (Attribution+ShareAlike). Exceptions must be approved by the FIRST Board.

- Standards SIGs are expected to use clear and uniform language. Technical (non-dictionary) language must be defined and contributed to an overarching glossary maintained by FIRST across SIGs and standards. The glossary will not be prescriptive but intended to be used by FIRST members as a best practice. Important terms must be defined internally to the standard, but the glossary should be used to limit the amount of inconsistency across multiple standards.

- FIRST standards use terminology defined in RFC 2119 as indicated in that best practice.

- FIRST will publish a list of all voting participants (defined below) that contributed to each standard, and may post a list of all Participants.

2. Participation and membership obligations

- FIRST SIGs developing a standard permit participation by three types of members:

    - **Observers:** Anyone can become a group Observer. This participation level allows access to a moderated group mailing list - used to publish proposals, vote on proposals, and more generally discuss issues pertinent to the group. Observers do not have voting rights. Although Observers can send emails to the mailing list, Chairs will reject emails with that is of such nature where it may require an IPR agreement, e.g. specific suggestions on how to solve a technical problem. Requests to become an observer should be sent to the FIRST Secretariat at first-sec@first.org. For open SIGSs, the observer will simply be added. For closed (members-only SIGs), the request will be submitted to the SIG chair.

    - **Participants:** Participants are individuals or organizations which have signed a FIRST Intellectual Property Rights agreement. Participants have unmoderated access to the group mailing list and can contribute ideas and concepts.

    - **Voting participants:** A Participant can request that they or their organization be given the right to vote on proposals. A non-member can also immediately apply to be a voting participant, or be admitted as a voting participant as part of the original SIG proposal.

        - The request to vote is made to the secretariat and approved by the chair of the standards SIG;
        - A prerequisite to be approved as a voting organization is to have participated in 50% of meetings in the 30 days prior to the request;
        - No organization can have more than one vote, and the person voting has to be pre-approved. Each organization can have 2 pre-approved voters.
        - The voting members have to be clearly marked on the attendance sheet prior to a vote taking place.

- In order to apply for Observer or Participant membership, an individual reaches out to the FIRST secretariat via e-mail at first-sec@first.org, noting the type of membership requested. The secretariat will liaise with the SIG chair to evaluate:
    - Whether an IPR is already on file for the individual's organization;
    - Whether the individual is eligible for the level of membership, based on the standards SIG charter.

- Each SIG developing a standard must have one chairperson, and at least one co-chair. Chairs may be either Participants or Voting Participants. The initial Chair and co-chair may be proposed by the standard initiators and is ratified by the FIRST Board. When a Chair steps down, a new Chair must be selected through a simple majority election process. Ties are addressed by re-voting. If a tie persists for more than two rounds, the tie is broken by random selection between tied candidates.

- The SIG will generally aim to achieve its outcome by building consensus amongst observers, participants and voting participants.

  The minimum requirement for voting is prior to the publication of specific deliverables. SIGs are encouraged to set regular milestones at which a deliverable is voted on. Each group can set more restrictive requirements for voting on individual decisions (e.g. conduct a vote for each change which materially changes the outcome of a technical tool described by the standard). Voting proposals can be initiated by each participant and must be submitted to the SIG mailing list, including at least the elements included in Appendix C.

  A proposal will pass when:

    - the number of yes votes exceeds the number of no votes (i.e., a simple majority);
    - at least 50% of eligible Voting Participants cast a vote (abstain votes are considered as casted votes).

- Observers, Participants or Voting Participants may leave the SIG based on simple request to first-sec@first.org. If this changes voting membership in such a way that a constituency now becomes underrepresented, the Chairs may choose to make a call for

additional SIG participants through the FIRST web site, a mail to the FIRST membership and its social media channels to identify a potential replacement.

3. Announcement of new standard development

FIRST will announce the intention to create a new standard publicly:

- Through FIRST's social media channels:
  - Twitter at https://www.twitter.com/firstdotorg
  - Facebook at https://www.facebook.com/firstdotorg
  - LinkedIn at https://www.linkedin.com/company/first_3
- Through a press release distributed by our PR partner and published on www.first.org
- Through an e-mail message to the FIRST membership
- A direct e-mail to all partners which have a Memorandum of Understanding signed with FIRST that includes awareness of new initiatives
- A direct e-mail to partners known to FIRST that are likely to have an interest in the matter

FIRST will also endeavor to identify and inform critical partners involved in the industry targeted by the standard through a direct e-mail message. As FIRST will never be aware of all possible constituents, any participant in the standard or FIRST member may request the FIRST secretariat to notify a particular constituency or can forward the notification themselves.

4. Public comment phase

Once the group has iterated through working drafts (WD), and is ready to release a public draft (PD):

- The SIG chair will submit the PD to the FIRST Board for approval, via the FIRST secretariat.
- The FIRST Board will gain an opinion from the FIRST attorney on the document prior to final release. The FIRST Board will work with standard chairs to address any issues flagged by the FIRST corporate attorney;
- The FIRST Board will review and vote on the release of the PD;
- FIRST will publish the PD for public comment on the FIRST web site, and announce the call for comments on its web site and social media channels. Comments will be submitted to a public mailing list submitted to all working group members. Comment submitters are not expected to have a signed IPR, but where a concrete, detailed, solution is provided as part of the comments, the SIG chair will invite the submitter to participate as a "participant" prior to integrating this input.
- FIRST will explicitly ask all organizations informed of the proposed standard (as defined in section 3) for comments

- A SIG chair will ensure external feedback is reviewed and addressed by the wider group, and comments are evaluated, following the process in Appendix F.
- Based on the outcome of this process, the standard may go back to internal working drafts, be released as an updated PD, or move towards publication, based on a vote by the SIG.

5. Publication of the standard

Once the SIG has addressed external comments, they will update the standard if necessary and present it to the FIRST Board for final publication.

- The group will submit the final work product to the FIRST Board for approval.
- The FIRST Board will gain an opinion from the FIRST attorney on the document prior to final release. The FIRST Board will work with the standard chairs to address any issues flagged by the FIRST corporate attorney;
- The FIRST Board will review and vote on the final release of the standard;
- FIRST will publish the standard on the FIRST web site, and announce the final release through its web site, a press release by our PR partner and its social media channels;
- FIRST will, where possible, create opportunities for standard chairs to engage with the media to promote the standard;
- The FIRST Board will evaluate opportunities for contributing the FIRST standard to external standards bodies it collaborates with, such as ISO, ITU, OASIS and IETF.
- Final standards must be marked with an @first.org e-mail address for comments. This address will typically go to the standards group, but may be replaced with the FIRST secretariat over time, if the maintaining group is no longer active.

6. Development speed

- Proposed standards pass through two major phases: working drafts, which are published at least internally, and public drafts, published for public comment. During its development multiple working drafts and public drafts could be produced.

Working drafts follow the following process:

  - T+0 a WD is produced and published for comments
  - T+1 is the deadline for comments,
  - T+2 a tentative WD+1 is produced and distributed for review
  - T+3 the tentative WD+1 is discussed within a group and changes are finalized
  - T+4 the final WD+1 is released as the first PD.

- The external comment period for a public draft is always at least one month. When the public draft comment period starts, the Chair sends a reminder of the disclosure obligations under the Common Patent Policy and the Specifications for Implementation of the Common Patent Policy along with a copy of the form set forth in Exhibit A.

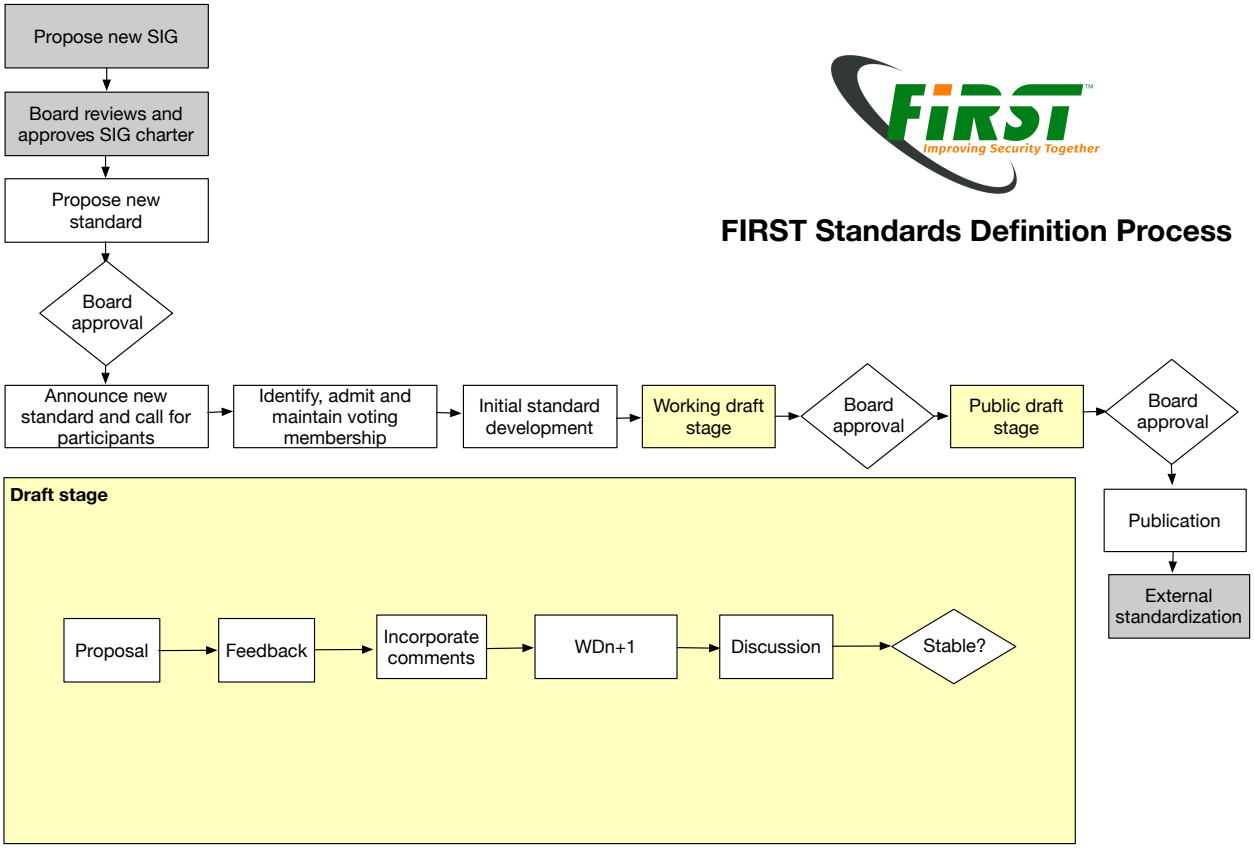
- During a standard's lifetime, it may be in one of the following states: "Draft", "In force" and "Obsolete". The status must be clearly marked on any document which contains the complete standard text. Draft can be "Working Draft (WD)" or "Public Draft (PD)". When a standard is made "Obsolete" it is no longer in force and it must not be used in new products/processes/services. An obsolete standard can be superseded by a newer or different standard. In that case it will be marked as "Obsolete, Replaced by: ....".

- Standards releases are versioned. Large versions, such as v1, v2, v3 indicate a thorough, all-up review of the standard. Minor versions, v1.1, v1.2 indicate only portions of the standard were revised.

- Standard groups can choose the format they prefer for editing language of the standard. Tools that allow versioning controls are recommended, such as Word or LaTex, or the use of a versioning repository such as GitHub. A master, readable copy of the standard must be created in ASCII which is stored on the FIRST web site.

- FIRST does not prescribe a standard format for standards, but recommends including an About and Background section explaining the relevance of the standard, and including sample code in appendixes or associated documents. The following mandatory metadata should be included: (1) date of release, (2) status of the standard, (3) version number, (4) contact e-mail address @first.org, (5) license.

Appendix A: Standards definition flow diagram



Appendix B: Required information to propose chartering a standard

The following minimum information is due to the FIRST secretariat to propose the development of a standard. The typical process would be for a group to be proposed on the topic, and this SIG to contain the standard as a work item.

When an existing group plans to develop a new standard, only the items marked with a (*) items are due. A Planning Checklist will be made available:

- Proposed **working group name**
- **Submitter** of the working group
- **Date** of proposal
- **Mission statement**
- Description of the **intended outcome standard**(*)

- Description of **who is expected to adopt the standard**(*)
- **Proposal on the constituency of the SIG** (e.g. industry sectors)
- **Goals and deliverables for the first year**(*)
- **Initial Chairpersons**
- **Interested observers and participants**
- **Budget** request (e.g. if contractors are required for statistical analysis or software development, the expected cost should be noted);
- **Meeting confidentiality:** The SIG can decided whether information on the mailing list is to be considered TLP RED, TLP AMBER, or whether the mailing list should be open (with only active participants having write access). FIRST recommends transparency, but recognizes some topics may require closed discussion.
- **Infrastructure** needs (mailing list, wiki page, phone bridge, video bridge)
- Other **comments**.

Appendix C: Minimum information required for a vote

This list contains all information that is expected to be provided by the standard chairs when a vote on a milestone is to be made. Depending on the group's proposed governance model, a milestone could be accepting a specific technical contribution, or the finalization of a document for publication.

- **Subject** - starts with the text "[Voting]" (including the brackets), a short title of the proposal, and a version number (to differentiate future modified versions of the proposal).
- Paragraph **summarizing the proposal**.
- The **date and time (with time zone), when the last vote will be accepted**.
- A statement that votes No must be accompanied by an **explanation of why the voter is against**.
- The **full proposal**, either in the body of the email or as an attachment.
- Optionally, any **supporting documentation**.

Appendix D: Example definition of constituency

While not a requirement, SIGs may choose to define their constituency up front, and maintain a balanced constituency throughout the development of the standard. An example is the below constituency used by the CVSS Standards SIG. This is an example only, and standards groups may be more open, or more flexible:

  - *Banking*
  - *Health Care*

- *Government*
- *Academic*
- *Manufacturing and Retail*
- *Technology / Hardware*
- *Technology / Software*
- *Technology / Networking*
- *Telecommunications*
- *CIRTs*
- *Energy*
- *Transportation*

Each organization requesting voting rights is categorized as being in one of the following constituencies, based on its primary business or purpose. Requests are only accepted if the organization's constituency will represent 25% or less of the total organizations with voting rights if the organization is added. When a constituency is full, new Participants wishing to become Voting Participants must wait until other constituencies grow, allowing for additional room, or an existing constituency member loses or relinquishes their voting rights.

Appendix E: Intellectual Property Rights agreement

In order for FIRST to be successful in developing content which can be used by our community in an unfettered way, we must protect the intellectual property rights on our deliverables. This means that our output must not contain information over which third parties may hold a license, and deliverables we develop should be owned by FIRST. The FIRST Uniform IPR policy ensures an organization does not have the ability to introduce patented content without notification by ensuring organizations are asked to declare any patented content they are introducing.

The FIRST Intellectual Property Rights (IPR) agreement can be found at https://www.first.org/about/policies/uniform-ipr. A single IPR must be signed per SIG that an organization participates in.

Appendix F: Providing comments

Comments must be as precise as possible. A comment must contain the following elements:

1. To what document comments pertain to – this must include the name and the exact version of a document, e.g. "CVSS WD2", "TLP v1.1, WD3".
2. Comment ID – the ID consists of submitter's initials or a designator (a person or an organization) and the comment number.

3. Reference – to what portion of the document the comment refers to. The reference must be unambiguous and given in a hierarchical manner. Examples of a good referee is "Section 2, bullet 1, second paragraph". Using page number (e.g. "page 3, fourth paragraph, line 3") is permitted but discouraged as page numbers will change as the text is added or removed.
4. Comment type – the comment can be technical or editorial. Technical comments pertain to the matter while editorial to the writing style, syntax, grammar and anything else (e.g. moving paragraph).
5. Current text – reference to the content on which the comment refers. For example "a software must use" or "second sentence".
6. Comment – proposed action. This must be as precise as possible. For example: "delete sentence", "replace the text with 'the new exact wording'", "move paragraph to section 4, bullet 3"

All comments from a single person or an organization must be submitted in a single file. The file with comments can be submitted only once. Comments must have consecutive numbers.

The editor must resolve all comments that are submitted on time. The editor can use discretion to address late comments and/or accept new comments during the discussion. Possible resolutions are: "Accepted", "Accepted in principle", "Not accepted". Their meanings are as follows:

- Accepted – the comment is accepted as is
- Accepted in principle – the comment is accepted but with some modifications
- Not accepted – the comment is not accepted

Once a comment is resolved participants do have right to raise it again (e.g. re-submit a comment that was not accepted) but it is up to editor's discretion to choose not to address it.

A file with all comments and their resolution must be distributed to the whole SIG as a reference as soon as the process is finished.